UTS UNIVERSITY OF TECHNOLOGY SYDNEY

Design and Implementation of a Secure and Efficient E-Governance Model Using Blockchain for a Developed Country

By **Haitham Assiri**

Thesis submitted in fulfilment of the requirements for the degree of

Doctor of Philosophy
in
Information Systems

Under the supervision of
Dr. Priyadarsi Nanda

University of Technology Sydney
Faculty of Electrical and Data Engineering

July 2022

Certificate of Original Authorship

I, *Haitham Assiri*, declare that this thesis is submitted in fulfilment of the requirements for the award of *Doctor of Philosophy in Information Systems* in the *School of Electrical and Data Engineering, Faculty of Engineering and Technology* at the *University of Technology Sydney, Australia*.

This thesis is wholly my own work unless otherwise referenced or acknowledged. In addition, I certify that all of the information source and literature used are indicated in the thesis.

This document has not been submitted for qualifications at any other academic institution.

This research is supported by the Australian Government Research Training Program.

Signature: Production Note:
Signature removed prior to publication.

Date: 18-07-2022

Table of Contents

Abstract

We are witnessing the world steadily heading towards the fourth industrial revolution. With the advent of e-government systems, public service dispersion is being scaled up all around the world. Any e-government system that is vulnerable to cyberattacks, poses serious security challenges and raises concerns about confidentiality and data integrity, in turn resulting in public distrust. This research focuses on the Saudi Arabian e-government portal YESSER as a case study to determine its degree of vulnerability by exposing it to three network penetration testing tools, namely Zap, Rapid7 and Nessus and examine the possibility of strengthening the Saudi e-government system through a rigorous examination of the existing literature to address the security of future e-government frameworks. Blockchain is a distributed ledger, and it is described as a continuously increasing set of publicly available records that are encrypted to provide security against tampering and alteration. This work proposes an effective Blockchain e-government framework to secure the Saudi Arabian e-government portal (YESSER).

Acknowledgements

First, I would like to thank GOD the Almighty, for helping me to complete this thesis. This work would not have been possible to achieve without the support and help of GOD. I am extending my sincere thanks to GOD.

The most meaningful thing that I can say about Dr. Priyadarsi Nanda is how much I appreciate him. I am deeply grateful for the excellent advice, care and patience he has provided me with as part of helping me to carry out this research to the fullest extent possible and in the best way. He always helped me even when I was overseas due to COVID-19. Dr. Priyadarsi Nanda supported me through the difficult times I faced during my research. I am grateful to him for everything.

I am incredibly thankful to my loving and supportive parents, Nasser and Sharifah, my lovely wife, Abrar, as well as my beautiful kids, Nasser and Mahdi, and my fantastic brother Abdullah for their sacrifices, prayers, encouragement and endless love.

Moreover, I am grateful to Jazan University for giving me the scholarship needed to complete my PhD.

Finally, I would like to thank the University of Technology Sydney, especially the School of Electrical and Data Engineering and its staff, and students for positively affecting my studies and providing a suitable environment that enabled me to do this research.

List of Figures

List of Tables

List of Publications

1. Risk and Vulnerability Assessment of e-Government Framework using Blockchain. (Accepted and Published at "36th IBIMA Conference, Web of Science ISBN 978-0-9998551-57")
2. A Novel e-Government Framework Using Blockchain. (Accepted and Published "Journal of Information Assurance & Cyber security, Vol. 2021 (2021), Article ID 164568, DOI: 10.5171/2021.164568")
3. Blockchain in Saudi e-Government: A Systematic Literature Review. (Accepted and Published " *International Journal of Electrical and Computer Engineering* 16, no. 1 (2022): 11-19.")
4. A Novel Design of e-Government System Using Blockchain. (Submitted to "Journal of Computer Security, Vol. 30,6 May 2022, ISSN print 0926-227X, ISSN online 1875-8924")

Chapter 1: Introduction

1.1 Overview

E-governance utilises the best of (evolved and advanced) Information and Communication Technology (ICT) to provide various services that are promoted and implemented by the government to serve fellow citizens. The pertinent implementation of ICT enables the government to provide better, faster, timely and efficient services (West, 2004). It is a fact that the technology is rapidly growing, and it has become a necessity for the government to efficiently use the advanced technology to implement uninterrupted and efficient policies for its citizens at the local, regional, and national levels (Marchionini et al., 2003). The twentieth century is currently endorsed to become the century of ICT which acts like a bridge between citizens and the government. The explicit implementation of ICT empowers citizens to take part in the government's policymaking and it also ensures the translucent usage of funds (Sigdel, 2007). With the introduction of network-based technology during the 1990s, governments had the convenience of taking advantage of e-commerce to accomplish their manifesto through e-government (Kalakota and Whinston, 1997). The appropriate implementation of ICT will scale down the cost of operations and enable citizens to experience a transparent and answerable government (Harris, 2000). Subsequently, mobile phones have made the citizens expect the government's policy and service information to be provided through websites or secured apps.

Governance means *to administer, to control, to govern, to lead* and *to work* with the authority to implement policies and programs for citizens. After the introduction and considerable implementation of ICT, the manual government has become e-government and manual governance has become e-governance. ICT caters to the needs of the people and offers a platform that leads to easy and un-interrupted interactions with each other. E-government is defined as the web-based services provided by the government using e-commerce mechanisms. During the late 90s and early 21st century, almost every developing and developed country has realised the need of advancing towards an electronic system of government from a manual system of government. The World Bank (2004a, b) defines e-government as the implementation of ICT to renew the relationships between the government, businesses and citizens. The communication between entities is in the form of the receipt of information, the filing of documents, making payments for the utilisation of services, the acknowledgement of payments, and various other activities through WWW (Sharma, 2006).

Dawes (2008) defined e-governance as a progressive association between ICT and the government to fill the gap between citizens and the government to achieve steady, safe, and secured public services, administration

and democratic processes. E-governance is defined by UNESCO as the appropriate use of ICT to offer better information and services, to engage citizens in decision-making and to administer a government with accountability, transparency, efficiency and effectiveness (Bannister and Connoiiy, 2012). Furthermore, an e-government that publicises according to electronic democracy allows citizen participation and encourages public discussions in an online fashion with the intent of efficient and on-time online public service delivery is known as e-governance (Marc and Aroon, 2009).

The United Nations defined e-government as the utilisation of the internet and www. for exhibiting government information and services to its citizens. Officials working on e-government from developed countries describe it as the management of ICT to encourage better, easy access, adequate, and effective government, to expedite public services, to grant easy access to information and to make the government answerable to the public. Despite the varied definitions of e-government, there is a mutual theme and that is ICT. E-government empowers the public to enquire and obtain services from the local, state or national level governments around the clock. E-government is intended to be digitally sound, knowledge-driven, thoroughly guided by innovation and mutually dependent on technology (Roy, 2003).

The UN e-government survey reports that all 193 countries in the UN have implemented e-governance to varying degrees ranging from a very low level to a very high level. The UN considered the E-Government Development Index (EGDI) to rank the countries that are successfully implementing e-governance for administration activities.

In the latest edition of the methodology of e-governance, there are three components of EGDI:

(i) Online Services Index (OSI) referring to the range of services.

(ii) Human Capital Index (HCI) indicating the skills available in the e-government.

(iii) Technological Infrastructure Index (TII) denoting the technological components used in the e-government systems.

The year 2020 witnessed a couple of decades of standardising the e-government development of the Member States of the UN. Subsequently, the survey presented by the UN every year has grown into an indispensable mechanism for political analysts and the public authorities to measure the OSI, HCI and TII offered by e-governments and to rank them accordingly. During the year 2020, we witnessed a completely different world after the announcement of the initiation of a decade-long implementation strategy for sustainability to support the achievement of Sustainable Development Goals (SDGs). A primary goal of the SDGs is to end poverty

and develop economic growth, social protection, health (including pandemic response), education, electricity, water, sanitation, transportation and infrastructure as well as providing access to the internet. E-governments are expected to help achieve this by offering continuous, comprehensive and unbiased public services to people without leaving anyone behind specifically through innovations, efficiency and solutions. Table 1 below presents the leading countries successfully implementing e-government in 2020 (UN Survey of the year, 2020). Saudi Arabia is one of the contributing Member States and Organisations that provides the UN E-Government Development Group with inputs towards better policies, programs and operations.

Table 1: A survey on leading countries having e-government initiatives [260]

Country	**Region**	**OSI value**	**HCI value**	**TII value**	**Rating Class**	**EGDI value (2020)**	**EGDI value (2018)**
Denmark	Europe	0.9706	0.9588	0.9979	VH	0.9758	0.915
Republic of Korea	Asia	1	0.8997	0.9684	VH	0.956	0.901
Estonia	Europe	0.9941	0.9266	0.9212	VH	0.9473	0.8486
Finland	Europe	0.9706	0.9549	0.9101	VH	0.9452	0.8815
Australia	Oceania	0.9471	1	0.8825	VH	0.9432	0.9053
Sweden	Europe	0.9	0.9471	0.9625	VH	0.9365	0.8882
UK	Europe	0.9588	0.9292	0.9195	VH	0.9358	0.8999
New Zealand	Oceania	0.9294	0.9516	0.9207	VH	0.9339	0.8806
USA	Americas	0.9471	0.9239	0.9182	VH	0.9297	0.8769
Netherlands	Europe	0.9059	0.9349	0.9276	VH	0.9228	0.8757
Singapore	Asia	0.9647	0.8904	0.8899	VH	0.915	0.8812
Iceland	Europe	0.7941	0.9525	0.9838	VH	0.9101	0.8316
Norway	Europe	0.8765	0.9392	0.9034	VH	0.9064	0.8557

Country	Region	OSI value	HCI value	TII value	Rating Class	EGDI value (2020)	EGDI value (2018)
Japan	Asia	0.9059	0.8684	0.9223	VH	0.8989	0.8783

It can be observed that National Income Level and EGDI are directly proportional to each other. In the survey of 2020, 18 countries are ranked in the "very high EGDI group" for the first time, namely Argentina, Chile, Brazil and Costa Rica from the Americas (four countries), Saudi Arabia, China, Kuwait, Malaysia, Oman, Turkey and Thailand from Asia (seven countries), and the Czech Republic, Bulgaria, Slovakia, Latvia, Croatia, Hungary and Romania from Europe (seven countries). In fact, 14 of these countries reached the V1 rating class but Argentina, Chile, the Czech Republic, and Saudi Arabia jumped right up to the V2 rating class which has the lowest rating standard (**L**ow, **M**iddle, **H**igh and **V**ery High).

Blockchain technology is a fully functional distributed database that allows the nodes on the network to access data. Blockchain technology is known for providing the secure and decentralised digital storage of data. Furthermore, Blockchain technology guarantees the fidelity and security of data without involving a third party. Consent from the majority of participants is first obtained to record any transaction (permanently) in the database. The structure of the database consists of blocks that contain information from multiple sources. These blocks have a defined storage capacity; once the block is occupied completely, it is closed and linked to the previous block. Hence, a chain of blocks is formed via a type of cryptography that is known as Blockchain. Unlike traditional databases where the data is stored in data tables, Blockchain stores data in blocks that are segregated from one another. Blockchain can be implemented to store any kind of information but generally data that is related to the ledger of transactions is stored in said blocks. The prima facie objective of creating distributed blocks is to allow every participant to perceive any transaction on a public ledger platform. The structure and workings of Blockchain technology has invited the interest of the e-government administration to invest and develop a scalable, distributed and decentralised e-government system.

The primary objective of the Blockchain is to collect, store and distribute the electronic information in blocks that is not tweakable. Therefore, Blockchain technology is expected to provide the infrastructure for stringent ledgers i.e., information which cannot be corrected, modified, transformed, updated or deleted (Olnes and Jansen, 2017; Wust, 2018; Carter and Ubacht, 2018). Hence, Blockchain technology is also called Distributed Ledger Technology (DLT). Blockchain technology is also secure and trusted as the blocks always go at the end of the Blockchain in a linear and chronological manner. Once the block is stored, it cannot be altered or deleted, and every block has its own hash and previous time stamp.

The blocks enable users over the network to get the information available on any block from the millions of blocks that represent citizens, businesses and government authorities. Blockchain technology has led to governments all over the world switching to a more advanced and secure infrastructure instead of traditional and conventional means of governance in public services (Yildiz, 2007; Batubara et al., 2018). Every innovation and development in Telecommunication and Information Technology invites the interest of e-governments to adapt to the new technological advancements to offer automatic services to its citizens in the easiest and most secure manner possible (Fountain, 2009; Baqir and Iyer, 2010; Ramli, 2017). The information acquired and saved in the blocks is shared among the users who access the Blockchain at the same time. The decentralised database structure, single block access at a time and uneditable stored blocks make it one of the best picks for a transparent and secured infrastructure responsible for dealing with e-government systems. It can also be observed that the confidence of the users is enhanced when using Blockchain technology in e-governance.

The relevant network, which was first announced as Bitcoin, is a peer-to-peer network that provides transparency through transaction consensus. Blockchains' immutability and consensus role minimise the need for central authorities, making it an ideal solution for dispersed environments. Because data is today's asset, the use of Blockchain in data-driven architecture can bring about decentralisation, anonymity and the other benefits of audibility and persistence. The most frequently encountered terminologies used in Blockchain technology are explained below. Node and Block: In a peer-to-peer network, a node is a computer that represents the landlord of transactions carried out by a certain user. A block is a page that cannot be changed. The Blockchain is a distributed ledger when you get there. Following this, the transaction is approved, and the corresponding block is added to the Blockchain.

Node and Block: The node is the workstation that represents the transaction by a user and the block is an entity that is not editable.

Consensus: Transaction processing and validation is done during the consensus step. Most employed consensus algorithms include Practical Byzantine Fault Tolerance, proof-of-stake and proof-of-work.

Scalability: The range of access to the solutions is scalability. Ethereum and Bitcoin are examples of the scalability of any block.

Smart Contract: Third generation Blockchain Technology has proven to be emerging as part of the increased acceptance of Blockchain in various application areas. Arbitrary rules are defined prior to the smart contracts that need to be followed.

Cybersecurity has become a vital and essential symbol which countries around the globe have decided to encourage professionals to understand. Technology has evolved so much that it has become an uninterrupted part of daily life. Technological advancements come with issues that are social, economic and political. Soon after the invention of mobile devices for communication, it became challenging for the information technology community to safeguard each and every component of the system including desktops, laptops, smart TVs, tablets, smartphones etc. to make the whole system secure. This is because cybercriminals are always looking for weaknesses in the system. The Global Cybersecurity Index (GCI) is the most reliable indicator that determines the pledge made by countries to cybersecurity at a global level to educate others on the importance of and issues relating to cybersecurity issues. The cybersecurity of any country is assessed based on its legal, technical, organisational, capacity and cooperation measures. The accumulation of these measures results in the overall score. As reported by the International Telecommunication Union (ITU), the International Cybersecurity Index (GCI) of Singapore and the USA is realised to be outperforming with the highest possible cybersecurity in their systems whereas when it comes to the highest FCGI ratings, Australia stands in 7th position for GCI indexing.

1.2 Outline of the Research Problem

Over the past few years, Saudi Arabia has increasingly implemented advanced ICT infrastructure to deliver e-government services to its citizens, achieving a remarkable score in the UN Survey 2020's e-Government Development Index (EGDI). In spite of achieving better EGDI scores by 2020 (unlike other developed countries), Saudi Arabia's electronic government systems do not offer sufficient security. Due to this, Saudi Arabia's e-government system has not been able to influence citizens to make use of the e-government services. Instead, they prefer interacting with their government representatives in person. To offer better services to the public and to win their trust, cybersecurity is one of the biggest concerns related to the Saudi government's e-government system.

A security breach of one of the Saudi Arabia’s e-government sites is a highly sensitive aspect and could result in serious consequences. Cyberterrorism is understood to be a highly critical security threat to the e-government systems and its aftermath has an effect in both political settings and the environment around it. Preserving the security of the systems thus has become crucial for the Saudi Arabian government. The introduction of an e-government system by almost 200 countries over the globe has brought in a sense of competition for the countries to perform better on a global scale (Srivastava and Tao, 2008).

Admitting to the fact that Saudi Arabia is a high-income country, other indicators pertaining to its competitiveness are far below when they are compared to other developed countries. Hence, Saudi Arabia needs an adequate and efficient e-government system to upgrade to higher levels of competitiveness. Furthermore, Saudi Arabia needs to popularise their services and encourage the public to utilise its e-government services to its full potential to achieve the economic advantage established in the Vision 2030 document of Saudi Arabia (Vision 2030 of Saudi Arabia, 2016). It is evident that the turnover of potential users is reduced due to its limited cybersecurity which in turn affects attaining the full potential of the services available. It is observed that cybersecurity issues influence a country's performance and that traditional security procedures lack the efficiency necessary to overcome cybersecurity issues (Khan et al., 2021).

In today's high-tech and advanced technological age, Blockchain technology has become almost everyone's choice through which to exercise swift, agile, transparent and protected transactions. The security and credibility of online transactions using Blockchain technology has become the primary and vital concern of the authorities. If online transactions are carried out without appropriate security channels, there is a high chance of an illegal data breach and data being stolen (Karame, 2016).

As Blockchain technology is in its younger stages of development, organisations hesitate to implement such a developing technology (Garg et al., 2020). Furthermore, organisations are not very familiar with the implementation and advantages of the latest revolutionary Blockchain technology. Blockchain technology must exert an effort to overcome the security issues growing around the globe. Currently, Blockchain technology is typically employed for safe and secure financial transactions by financial institutions.

It is reported in the literature that Blockchain technology offers better security services compared to the traditional approaches that are in place. Khan et al. (2021) concluded that the implementation of Blockchain technology improves the protection of e-government systems. Hence, it is recommended to analyse the best possible practises of Blockchain technology and to implement them in the e-government systems of Saudi Arabia. Such approach will prompt researchers to investigate future cyberattacks and to let the government take adequate precautionary steps based on the findings to safeguard the public and its services as part of its e-government setup. Hence, in our research, we propose a secure and efficient e-government scheme for the Saudi Arabia government to let the government take adequate precautionary steps and safeguard the public and its services as part of its e-government setup.

1.3 Research Questions

Based on the above mentioned, this thesis is going to address following two important questions:

Q1. What is the degree of vulnerability associated with Saudi Arabia's e-governance services to cyberthreats?

Q2. To what extent can Blockchain technology contribute to the security of Saudi's e-governance services?

1.4 Research Aims and Objectives

The Yesser program was initiated in Saudi Arabia with the idea of providing secured services to the public in the easiest way and with the least effort. Furthermore, some of the most developed countries like the USA, Australia and the UK have been observed to be exploring the benefits of implementing Blockchain technology and succeeded in offering a secured public service. Accordingly, the aim of the current research is to analyse, design and propose a protected and efficient e-government scheme using Blockchain technology for Saudi Arabia. This thesis also studies the efficacy of Blockchain technology (adoption and implementation) in other developed countries. The proposed implementation of Blockchain technology will enable Saudi Arabia to provide secured and efficient public services in accordance with the safety and security of information resulting in better and quicker services under the Yesser initiative of the country.

The aim of this research is to design a secure and efficient e-governance scheme for Saudi Arabia. This scheme will enhance the e-governance security of information. Therefore, using Blockchain to secure the e-government program (Yesser) services to prevent the security threats that are facing the e-governance services will make them more secure. The main objectives of this thesis are summarized as follows:

Objective 1 – To determine the degree of vulnerability of e-government services and develop a model to support better privacy, trust, confidentiality, and security.

Objective 2 – To propose a secure e-government framework integrating Blockchain Technology.

Objective 3 – To compare the performance of the proposed e-government framework with or without the blockchain technology.

1.5 Research Approach

The research carried out in this thesis is based on both the theoretical and empirical analysis of Blockchain technology. During the theoretical foundation of this thesis, Blockchain technology is explored meticulously and in depth including its implementation and shortfalls. Later, a comparative analysis is carried out to understand its implications in developed countries who also employ Blockchain technology. Furthermore, a detailed analysis has been carried out to understand how Saudi Arabia is making use of this technology to provide safe and secured public services under the e-government setup. Furthermore, in this research thesis, we also propose the procedures to be adopted by Saudi Arabia to use the Blockchain technology to help them to provide effective and efficient services to the public using the latest technologies.

1.5.1 Research Tasks

To accomplish the research objectives presented in the previous section, we have divided the research into four tasks as follows.

Task 1: To determine the degree of effectiveness of the existing security measures of Saudi's e-governance services.

It is the outcome yielded after an appropriate study of the literature (survey and review articles). The present status and position of the countries offering e-government services was obtained from the UN Survey 2020 (countries ranked based on their E-Government Development Index (EDGI) scores). EDGI considers OSI, HCI and TII to be major concerns when evaluating a country's EGDI score. The data related to Saudi Arabia and developed countries (for a comparative analysis) was obtained from the official UN survey 2020 document. Earlier similar studies have also been carried out and reported (Mukhoryanova et al., 2016). Later, an extensive literature review of the available white papers and reported research (research articles) was carried out using search terms like "e-government", "vulnerability of e-governance sites", "Saudi Arabia", "e-governance implementation by Saudi Arabia", "cyberthreats in e-governance", "trust in e-governance", "reliability of e-governance", and "security of e-governance" etc. Since the inception of the e-government mode of governance by countries all over the globe, a considerable amount of research has been produced and reported.

Task 2: To find out the suitability of Blockchain as a solution to cyberthreats and to achieve security in Saudi Arabia's e-governance services.

To accomplish this task, a literature review of Blockchain technology employed specifically in Saudi Arabia was done. The search terms used to reach the research articles specifically pertaining to Saudi Arabia were “Blockchain technology in Saudi Arabia", “application of Blockchain technology in e-government”, “application of Blockchain technology by Saudi Arabia", “privacy and protection by Blockchain technology”, “how Blockchain enhances the security of online transaction”, and “how Blockchain deals with cyber threats", etc. After the reports on the successful implementation of Blockchain technology emerged from developed countries, Saudi Arabia decided to invest in the same advanced technology infrastructure to provide safe and secured online public services.

Task 3: To develop a model to address the e-governance security issues using Blockchain Technology - design and validation through implementation.

To attain the expected results of this task, an intensive comparative analysis was undertaken for the procedures and approaches that address the security of Blockchain technology of various countries, especially Saudi Arabia. Subsequently, a novel, secure and efficient Blockchain integrated model-based e-government structure has been proposed for Saudi Arabia.

The proposed architecture was then evaluated using the procedures mentioned below.

a. The implementation of the proposed system is carried out. The proposed system was studied thoroughly and compared with the proposed e-government system using Blockchain technology to realise the issues and challenges of security.

b. Validation concerning the security aspects of the proposed integrated Blockchain model for e-governance was carried out. A detailed study was carried out to analyse the data’s safety and security by breaching the security, thus indicating whether the Blockchain technology can provide improved security.

c. The model proposed and presented here in this research thesis is known to be optimal and always has room for further development (extension and future work).

1.6 Implications of the Research

The current research carried out in this thesis is designed to implement Blockchain technology and achieve a safer and more secured public services for e-governments. Saudi Arabia’s Vision 2030 includes the best possible use of modern technology to provide e-government services to several users in the most

secure fashion. It was observed from the survey report of the UN for the years 2018 and 2020 that, Saudi Arabia is keen to offer services to everyone possible using the latest technology. Saudi Arabia has achieved a competitive TII score of 0.8442 (0.5339 score in the year 2018) compared to other developed countries (Table 2).

Table 2: Comparison between countries for the 2018 and 2020 scores

	TII scores		**HCI scores**		**OSI scores**	
	2020	**2018**	**2020**	**2018**	**2020**	**2018**
Saudi Arabia	0.8442	0.5339	0.8648	0.8101	0.6882	0.7917
USA	0.9182	0.7564	0.9239	0.8883	0.9471	0.9861
UK	0.9195	0.8004	0.9292	0.92	0.9588	0.9792
Australia	0.8825	0.7436	1	1	0.9471	0.9722

The successful implementation of technology comes at the cost of security and the integrity of the transactions carried out in online mode. Hence, the proposed Blockchain integrated e-government model in this research thesis will help Saudi Arabia to offer more secured services to its consumers.

1.7 Thesis Structure

The research thesis presented here is composed of seven chapters. The first chapter introduces the subject and provides a brief overview of the research topic followed by the research outline, research questions, research aims and objectives, research approach and implications of the study. Chapter 2 presents a detailed and extensive literature review report pertaining to e-government, Blockchain technology, the UN survey and the issues and challenges of Blockchain technology implementation, especially by Saudi Arabia. Chapter 3 showcases the research methodology employed in this research. Chapter 4 presents a detailed study of the risks and vulnerability assessment of the e-governance framework. Chapter 5 analyses the literature on Blockchain technology in relation to the Saudi Arabian governance. Later, the detailed structure of the proposed Blockchain integrated e-governance model for Saudi Arabia is presented in Chapter 6. Chapter 7 presents the conclusions drawn from the

empirical analysis and recommendations for the future extension of the research followed by references at the end.

Chapter 2: Literature Review

2.1 Introduction

Most governments worldwide have successfully employed, and some are planning to employ e-governance to offer public services efficiently to their citizens. E-governance aims to simplify the governmental bureaucratic processes for all including the government, citizens, businesses and others. (Business Jargons, 2019). The prima facie of e-governance is to bring about SMART governance i.e., Simple, Moral, Accountable, Responsive and Transparent (GK Today, 2016). Here are some of the benefits/advantages listed that are attributed to e-governance.

1. Reduced corruption as the corrupt officials cannot influence online transactions to their advantage.
2. Transparency: All service activities are accessible by all users.
3. Convenience and ease of use: Avoiding lengthy visits and waiting in queues at the relevant offices.
4. Efficiency: it triggers more economic activities which is conducive to the better growth of the GDP.
5. Direct participation of the constituents in the service transactions is made possible.
6. Cost effective: There is a significant reduction in overall cost when the system functions smoothly.
7. Online services: The reach of the service is always expanded to consumers regarding the specific services according to their needs.

It should be noted that to implement e-governance successfully, the government needs adequate preparation which includes computerisation, networking, online presence and online interconnectivity (GK Today, 2016). The UN Summit in 2015 adopted an ambitious target for the Sustainable Development Goals (SDG) to reach by 2030 (UN P.A., 2016). Goal 16 of 17 is to encourage an inclusive environment for viable development and to offer easy entry to all levels of e-government system inclusively, whereas Goal 17 of 17 is to enhance the implementation and modernise global partnership for SDG. Furthermore, the 2030 Agenda highlights the high potential of ICT and global connectivity to accelerate the development of human ability and developing knowledge societies along with scientific and technological innovation across sectors like medicine and energy.

Singapore's eCitizen Portal, the South African government, Visakhapatnam Municipal Corporation Website and the Pakistan Government's Forms Website are some good examples of e-governance that are given in eGov4dev (2008). The evaluation criteria considered are listed below.

1. Quantity and quality of the information.
2. Information visualisation.
3. Online interactions.
4. Availability of public services (partial or full).
5. Accessibility for disabled and other visitors using alternative technologies.
6. Ease of use.

An extensive and comprehensive review was carried out of the e-governance frameworks that are currently being used in Saudi Arabia compared to the USA and the UK. The USA and the UK are developed and have employed e-governance from the inception of the idea. During the current research study, we investigated the advantages of the e-governance frameworks in the USA and the UK and proposed a more efficient, safe and secured e-government system for Saudi Arabia using Blockchain technology.

2.2 What is E-Governance?

The appropriate implementation of ICT for e-governance is necessary for smooth communication between the administration and its citizens to offer and allow them to use the public services, respectively (Dawes, 2008; Riad et al., 2011; Bannister and Connoiiy, 2012). Employing ICT for e-governance, which includes supervising resources and administering policies, results in a citizen-directed system (Palvia and Sharma, 2007). UNESCO defined e-governance as the national level implementation of ICT with the objective of enhancing the displaying of information and the delivery of public services.

E-governance provides unflinching access to government services and information round the clock every day to users. Governments need to restructure their operations to improve their service delivery to the point where it is efficient, safe and secured. Furthermore, public participation in decision-making helps the government to achieve the implementation of its services to a higher degree. This is exactly what this study seeks to do and the process of doing so clearly involves understanding the state of the existing e-government frameworks in use by different countries around the world. Data protection becomes vital and challenging when public services are provided online, especially at times when a considerable rise has been recorded in cybercrime and online security threats. Hence, it becomes necessary to develop both

systems and models that provide and improve the security of e-government. In the present research study, we explored the state of the e-government security framework of developed countries (the USA and the UK in this study). Speed, services at a low cost, transparency and accountability are the advantages whereas huge infrastructure investments, a loss of interpersonal communication, illiteracy and cybercrime are the challenges faced by e-governance (Topprcom, 2019).

2.3 The Importance of E-Governance

The whole system of e-governance is aimed at transforming and improving government services in terms of a cost reduction, providing efficient and effective public administration and improving the service delivery with increased transparency on behalf of the government (Satyabrata and Subhendu, 2016). In e-governance, information is made accessible on the internet which includes reports related to government debates, budgets and financial rationales for key government decisions. Therefore, higher levels of transparency are achieved and the reverification of data through official sources becomes easy before publishing the facts.

To enhance the efficiency of the public administration system of e-government, systems such as human resources management systems, integrated financial management information systems and computerised treasuries can be employed to help control expenditure, to intelligently audit data and to publish financial data. To achieve the goals of e-governance, public administration should use ICT to equip themselves to deliver better services to society. Using ICT in public services requires a large amount of management and technological expertise for it to be successfully implemented. This requirement leads to advanced learning courses for students in universities, schools and institutes so then they can be industry-ready whenever necessary.

The context and essential details of e-governance in selected countries are briefly described in the next section. The countries chosen (developed, developing and underdeveloped) are purely random and no specific rule, reason or preference is given to any country. This is to help understand and provide generalised information about e-governance worldwide.

2.4 Key Elements of E-Governance

E-governance is about creating a smart collaboration between the public administration and its citizens to provide and receive services respectively. The public authorities are expected to offer information and services online in an efficient, safe and secured way.

1. Encourage the use of smart devices with the invention of the internet and mobile phone technology, traditional governance has been transformed into e-governance. Governments and the local authorities are trying to improve their online service delivery through departmental websites. Citizens are allowed to use the internet services (desktop or mobile) to receive public services and interact with the authorities.
2. Protection from cybercrime: Skilled hackers have raised the level of concern over cybercrime and have become a very common threat to online service providers. To achieve security, confidentiality and integrity of the data, one needs to induce multi-factor authentication to restrict unauthorised access.
3. Democracy restoration: The proper implementation of an e-governance system improves the quality of the services and participation of its citizens. An online, secured, and easy voting system encourages the citizens to demonstrate their right to vote (preserving their privacy) to opt for a better governing body.

Society with financial and social inclusion: It becomes mandatory to provide digital identity to its citizens for them to be able to receive financial services from banks and other financial institutes. The United Nations and World Bank groups are putting an effort in to propose and implement strategies to reach every citizen to help them receive financial products easily.

2.5 A Preview of Existing E-Governance Frameworks in Different Countries

2.5.1 China

The development of e-governance in China can be traced to the year of the adoption of computers by the government in the 1970s. After an initial push for reforms in 1978, a further push was made in 1991. In the first stages of development, China adopted the e-governance systems of the West. Over 30 years of its use helped the country to learn by experience and it then adapted the Western system to its own interests. Government initiatives in IT, heavily funded research projects as links, the large-scale promotion of IT adoption in the society and the national economy were the most important success factors of e-governance in China.

Over two decades, China has implemented and improved upon its e-government services since 2001. Making the best use of mobile communication for e-governance through the mass involvement of citizens has resulted in better and effective public service delivery (Jun and Hui, 2010). Therefore, the Chinese e-government was created largely to fast-track the government's resolve of using ICT to improve its

administrative effectiveness and efficiency to promote the Chinese economic development. Despite copying some aspects of Western e-governance, China has a different structure and content priority (Zhang, 2006). It is reported in the literature that the e-government of China has played a vital role in promoting administrative institutions and providing public services.

The Chinese e-government setup has also been criticized for focusing only on the technological aspects and not the social aspects (Guanghua, 2009). An evaluation report of e-governance in 31 provinces in China using Data Envelopment Analysis (DEA) showed that most of them are inefficient and badly operated (Wu, 2015). Wu and Bauer (2010) reported that information delivery and basic interactional and communicative features dominated, and that many advanced transactional and participatory services were offered. China was ranked 57th in the UN's E-governance Readiness Index report of 2005 where the USA topped the list. Later in 2011, considering both qualitative and quantitative components, a field-based measurement was proposed to evaluate the readiness of the Chinese local government.

The first stage of the pilot phase consisted mainly of data processing during the period 1973-1983. In the second phase in 1983-1993, the vertical development of information management was done. In the third phase of 1993-2000, transaction processing was done to implement important transaction systems. The promotion of comprehensive e-governance happened through the e-governance guiding national information policy in the fourth phase of 2000-2006. The fifth and current phase started in 2006 and was focused on the deep application of e-governance (Du et al., 2018).

A conceptual model of the mechanisms proposed according to which China's e-government was able to encourage reforms through aligning policies, technologies, management systems and data designing to cross the technical capacity barrier, lessen staff resistance and a lack of cross-boundary collaborations (Chen et al., 2017). The interaction of policies and e-governance led to issues like corruption and public engagement. Viewing the e-government as a part of e-development, the historical performance of China's e-governance was rated by Loo and Wang (2017) as being formative in 1998, under development from 1999 to 2002 and mature from 2003 to 2014, and to the end of the analysis period. The solo ICT paradox, SDM and super SDM methods were employed and found out that e-governance may reduce productivity with wide discrepancies across the various regions in China, negatively impacting the central and western regions (Chen and Xie, 2015). A comprehensive report of the countries employing smart e-governance including China has been presented (Paskaleva, 2009; Lin, 2018). A pilot project was successfully implemented for increasing the access of citizens to the government services in Yichang, China (Mingus and Zhu, 2018).

2.5.2 New Zealand

The e-government framework in New Zealand has two trends: the integration of business and people through access to portals, call centres, mail, TV etc., providing the foundation for all layers like the services layer, policies and standards layers, as well as the data and information layer of e-governance. Recently, a detailed description of the digital transformation of the governance system in New Zealand was provided by the New Zealand Government (2019).

The effectiveness of using ICT by public officials has been studied thoroughly and it has been reported that the implementation of e-governance by the New Zealand government has improved their services exponentially (O'Neill, 2009). In the process of the improvement and expansion of their services, various policy and service delivery issues were addressed. Individual departments started offering services online in 1990 and it can be observed that the effective initialisation of ICT in e-governance benefits the public at large. The New Zealand government took on a national level initiative in the year 1995 to inculcate e-governance across various departments where cross-government collaborations were ensured. ICT in the government has improved the participation opportunities as well (Millar, 2004). It was recognised that technology was only an instrument for improving the public sector services and not an end by itself. New Zealand has a compact single tier government and established solid e-government standards during the early 2000s. People are internet savvy and adopt new technologies quickly and make the government collaborate to provide better services. The public services need to be demand-based rather than supply-based. Effective models of governance and funding for shared structures need to be developed for this purpose. A detailed paper covering all aspects of developing an e-governance system with a framework was published by Okot-Uma (2004). The e-governance framework proposed by the author has been reproduced in Figure 1 below. The process of developing and implementing e-governance starts with assessing the requirements of the various stakeholders. To achieve the best of the results according to the baseline assessment, the preparation of a blueprint for e-governance and implementation as per the blueprint follows one after another. What is not shown in the diagram is the regular review and follow-up for any improvements that will become inevitable due to the rapid changes in technology.

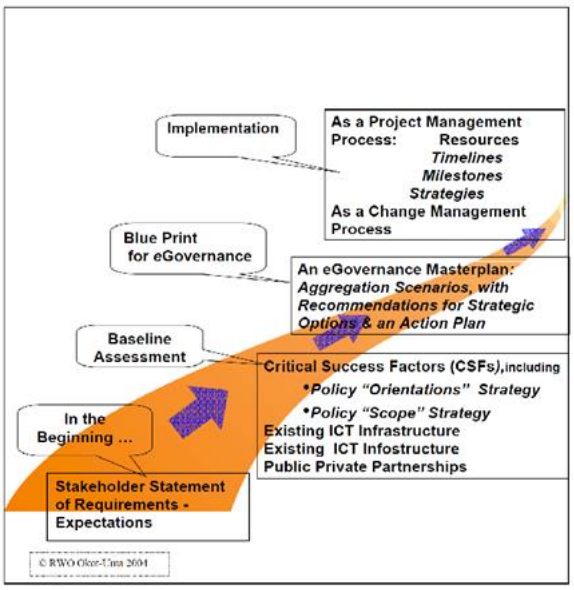

Figure 1: An e-governance framework (Okot-Uma, 2004)

Oakley in the year 2002 proposed and discussed three e-governance models viz., the economy, community and planned economy (Oakley, 2002). The idea of these models was to treat e-government as an e-business establishment which accords the highest priority to any public services and is demand-driven round the clock. Furthermore, it attracts technology and infrastructure investment which helps in terms of economic development. The market requirement leads to a digital divide.

2.5.3 Australia

The government of Australia developed its own e-government framework known as the interoperability framework. It emphasises and implements standards and policies like privacy, security, web service integration, data exchange and authentication. This framework uses many portals to store and retrieve data. These include customer portals, government entry points and subject portals. The UN Global e-governance readiness index for 2005 places Australia in 6th rank (Palvia and Sharma, 2007).

The e-government of Australia in 2002 was focused on information only with an uneven spread in most cases which was true mainly for rural and remote areas. It can be observed that the e-government used to have separate portals for every department instead of constraining similar services together in a single portal without further improvement.

There was a tendency to create separate websites for each government department instead of having a single portal for multiple services of the same department. There was no sign of progressing towards a joined-up government as the final target. It was also observed that the local government websites were

oriented towards information only because they only fulfilled the requirement of providing information from the government to its citizens (Teicher and Dow, 2002; Fan, 2011). Furthermore, the sites of e-government services made by the local governments were less sophisticated than what was required to go beyond the information level.

Only very few local governments used e-governance to the point of its interactions with its citizens being for the purpose of making online payments and downloading forms. Despite the implementation of a participative model of e-governance which has been accepted in principle, most local governments were still at managerial model stage only. A limited form of consultative model also exists in some cases where the feedback mechanisms for citizens on selective issues exist (O'Toole, 2007). A lack of a unified way for the e-government to join together all government services and the failure to provide direct G2C transactions has lowered the performance ranking of Australia compared to its peers (Ott et al., 2018). A decentralised architecture consisting of a digital identity system, secure data exchanges among the different IT systems of the government and the use of a digital signature are critically absent.

From a longitudinal evaluation study, substantial but variable e-government services among the Greater Western Sydney councils seems necessary (Fan, 2018). The introduction of high-speed broadband in Australia has facilitated some federally funded and locally driven e-governance initiatives (Alizadeh and Shearer, 2015). However, there are a lot of uncertainties about its future progress and the negative impact on strategic planning as part of capitalising on digitally driven opportunities.

2.5.4 India

The e-government framework established in India enables integrated services and middleware to bring businesses and citizens together. This is referred to as the e-India portals. Despite investing huge funds and a lot of time, it can be observed that India has not achieved its expected results for e-governance (Kumar et al., 2014). Researchers have also recommended that the Indian government to learn from developed countries like Australia, Singapore and Korea to implement e-governance successfully. Gillmore and D'Sourza (2006) reported that the public service offering in India is encouraged in the local language. Higher levels of illiteracy, lower per capita income and limited financial resources are reasoned to be the primary challenge faced by India when trying to score higher for e-governance (Dwivedi and Sahu, 2008; Prakash and Singh, 2016). It is also reported that the implementation of poverty alleviation programs by the government across India can encourage and motivate the poor to access the information and public services (Pathak et al., 2016).

2.5.5 Pakistan

Pakistan is in the beginning stage of implementing e-governance as depicted in Figure 2 below (Ghayur, 2006). The external environment of the service delivery is shown on the left side whereas the government, its departments, policies, technology management, interactions etc. are shown on the right side. Ghayur also listed the seven basic principles of the e-government framework (easy access for all including the physically challenged, automated and reengineered systems, one-stop services for all requirements, service determined by the customer needs and not those of the provider, the protection of privacy and security) implemented successfully in the USA which can be followed by Pakistan's public administration to achieve better e-governance. It can be observed that in early 2000, Pakistan was ranked the lowest in a survey carried out by the World Markets Research Centre and Brown University which alerted the Pakistan government to the need to employ and invest in its e-government infrastructure and to promote the same quality at every level.

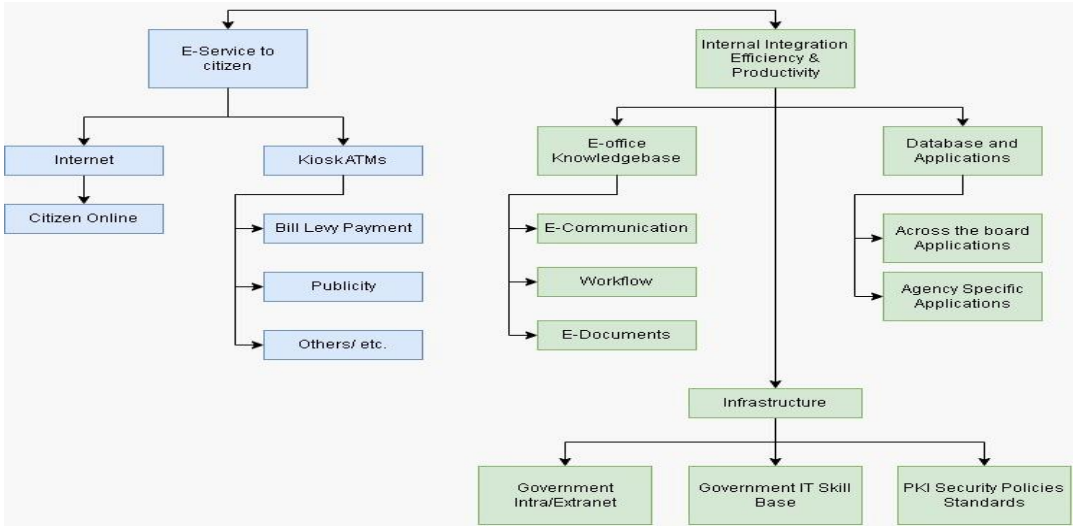

Figure 2: E-governance framework for Pakistan (Ghayur, 2006)

Even after a decade following the inception of the e-governance strategy, Pakistan's ranking in terms of its e-governance establishment is observed to be very low in the UN E-Government Development Index (EGDI) survey in the year 2014 (Shaikh et al., 2016). They have identified the barriers and challenges to do with improving the global ranking of Pakistan for e-governance and offer public services online as presented in Figure 3.

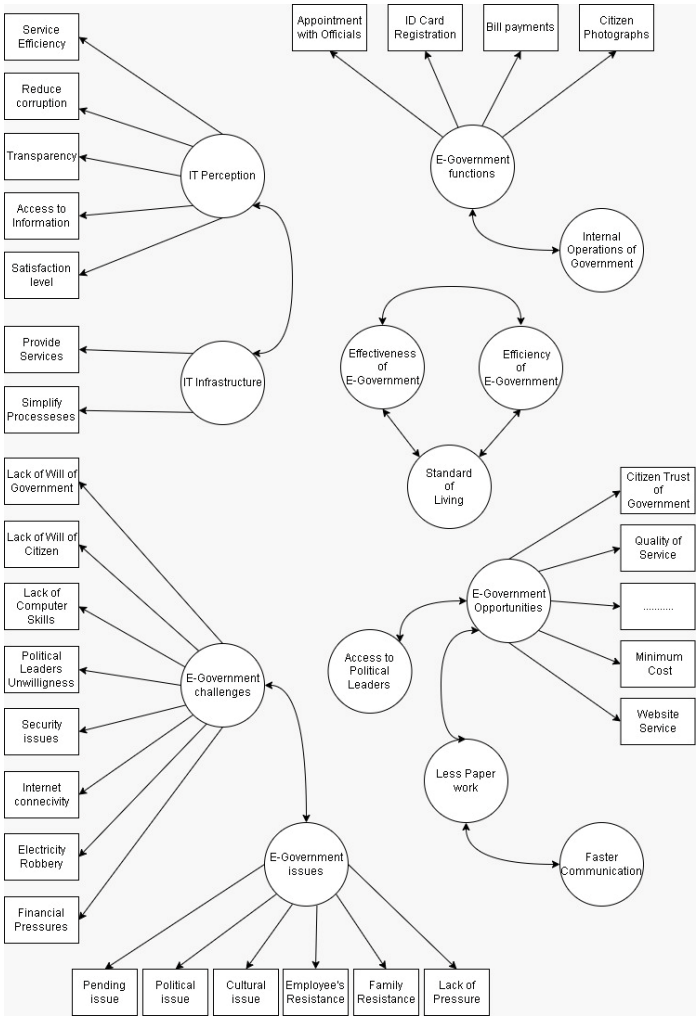

Figure 3: Factors of e-governance in Pakistan (Shaikh et al., 2016)

2.5.6 Sri Lanka

Sri Lanka implements a three tier (data, network and application) architecture framework for its e-governance. The application architecture encompasses the government's internal solutions like e-human resource management, e-pensions, e-tax filing and e-pension solutions (Riad et al., 2011). The poor interpersonal and full-fledged use of computers by people, politicians, and bureaucrats is one of the major challenges faced. Furthermore, the infrastructure and implementation capacity of the government is inadequate for e-governance, as well as there being an unstable political scenario, the breakdown of the ICT architecture, and the inadequacy of the legal structure also restricting the efficient implementation and utilisation of e-governance (Irfan, 2017). Awareness programs, skills training, the strengthening of mobile technology, websites in the three major languages, user-friendly and congenial policy atmosphere, facilitating feedback from stakeholders and encouraging public-private partnerships are some of the possible steps that can be used to address these challenges.

2.5.7 USA

The USA has one of the most sophisticated and utilised national e-government infrastructures in the world. The detailed history of e-governance in the USA was presented by Pardo and Styrin in the year 2010. The implementation of the e-government framework in the USA goes back to the beginning of 1993 when Clinton-Gore implemented his administration through re-engineering information technology. The aim was to make the governance more customer-oriented and responsive to different social needs. Information systems were used by the federal government to improve its efficiency, accountability and performance in the domain of public service delivery. Many national and international information systems, databases, law enforcement networks and online tax filing facilities were created to reach the masses easily and efficiently. The integration and interoperability of multiple departments of public administration to achieve efficiency, accuracy and performance were the primary focus of the Bush administration. The USA has successfully implemented an e-government framework aimed at the fair delivery of services to all citizens irrespective of ethnicity (Forman, 2002). Since its inception, various new attempts have been adopted that have been aimed at simplifying and integrating the agency processes and information flows, streamlining the acquisition of information and reusing it to offer one-stop public services. Later, the Obama regime continued to use web 2.0 and other ICT developments to achieve improved efficiency and a better level of integrity to be a government ran according to accountability.

The USA is ranked between 2nd and 4th in the UN e-governance readiness index according to different rating agencies. The USA follows three major strategies for successfully implementing e-government: (i) It is citizen-centric not bureaucracy-centric. (ii) It is market-based in that it is continuously promoting innovation. (iii) It is progressive and results oriented. In other words, the e-governance in the USA is market-based which is continuously adopting innovations with the primary objective of efficiently serving the American citizens' requirements at large (Chen et al., 2006).

The survey results showed that the USA's municipal websites have rich information on diverse topics of public interest but not the more standard services (Scott, 2006). Cities seemed to be reluctant to post the deliberations and actions made by their public administration boards. The UN rankings for the e-governance readiness index of the USA has seen a progressive slide from the top spot in the year 1993 to the 11th spot in the year 2017 (Leonard, 2018). One of the major reasons for such a slide is possibly the huge investments made by other neighbouring countries for the successful implementation of e-governance. A comparative survey between state and federal government websites was carried out in the years 2000, 2007 and 2008 to evaluate the changes in online content. Improvements over the years were

observed with respect of the extent of fully executable services online, the mobile accessibility of some sites, privacy and security policies, foreign language translations, ease of understanding the content, user fees on limited sites and accessibility for the disabled. This e-governance can be used for government-citizen access both ways and this was highlighted as a beneficial aspect of e-governance in the USA and China (Seifert and Chung, 2009). Considering the fame and position of the USA in terms of e-governance scores, the amount of research reported which is directly dealing with e-governance is substantially less. Interoperability determines the capabilities of these models in terms of discovering and sharing data and services across different and disconnected systems and vendors (Pankowska, 2008).

2.5.8 The UK

The history and strategies implemented in the UK to establish an efficient and working model of e-government has been published (Hudson, 2001). The UK e-government (online public services) was launched in September 2000 by the prime minister at the time, Tony Blair. The aim of the inception of e-government services was to provide access to government services online to all those who wanted it. The state and federal role was defined as complementary to the market, responding to the expectations of UK citizens as consumers. It requires skill, confidence, and access to the internet to achieve the e-government aims and objectives. By the end of 2001, about 33% of government services were made available online to request. Later, efforts were made to make the system citizen-driven (target users should determine the content). The current attempt is to improve the public services to minimise the delay in finding and reaching out to specific departments to do with the public request. The various types of services provided by the UK Government Digital Services (GDS), as its e-government program were presented and explained in a corporate report (Govt.UK, 2019).

An architectural model of e-government consisting of access, services, e-business and interoperability for the UK has been presented in a cabinet office report and the same is presented in Figure 4 (Cabinet Office, 2000).

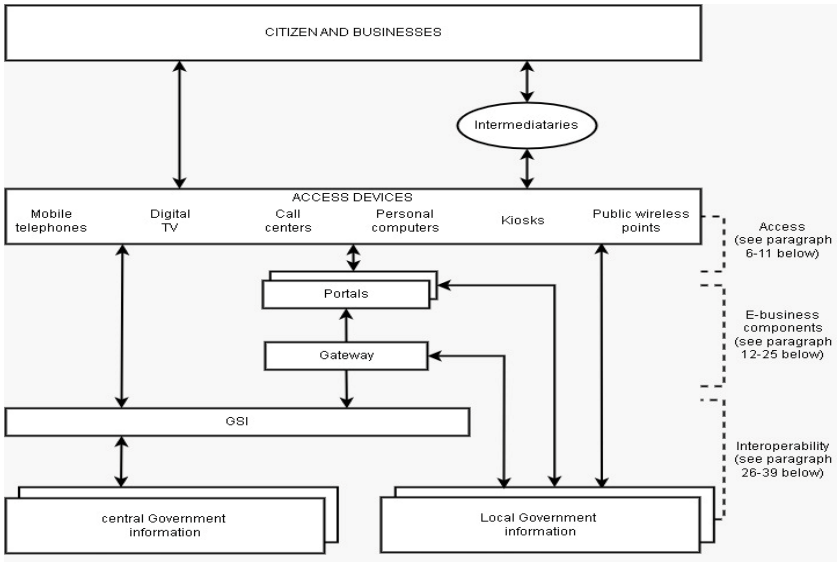

Figure 4: An architectural model of the e-governance framework of the UK (Cabinet Office, 2000)

A parliamentary note issued on 27 May 2009 described the aims, the progress observed during 2004-2007, the abandonment of the 100% target by 2005, the strategy for 2005-2011 and some of the recent issues regarding the better use of public data, privacy concerns, data loss, free data, government ICT problems and greening the government ICT for efficiency, sustainability and improved responsibility (Bennett, 2009). The public were largely satisfied with the system quality and information of the UK's e-government framework and it trusted the sites but expressed a negative attitude towards the cost as presented in a survey by Weerakkodi et al. (2016). This is an indication of the framework being good for its intended purpose. E-government is defined as, "Internet applications for public administration processes and decision making on local, regional, national as well as cross-national level" (Pankowska, 2008). This definition signifies the importance of vertical and horizontal interoperability at various levels to ensure smooth information and document flows.

The UK has the e-Government Interoperability Framework (e-GIF) through which to determine the policy and specifications of the technology used by the UK government to achieve interoperability. It contains a framework for the policy, management, implementation and compliance aspects. There is an e-registry consisting of metadata standardisation and a categorisation list. The key policy decisions cover many aspects including adherence to e-GIF in the entire public sector.

2.5.9 Saudi Arabia

The Kingdom of Saudi Arabia has taken initiatives to implement an e-government system consisting of its public service providers since the beginning of the 21st century. The huge investment in acquiring and deploying ICT had a focus on preparing the country for e-governance in terms of e-readiness, e-society and e-training. As an e-government program to achieve continuous growth and development of the economy, the Yesser project was created in the year 2003. The e-government readiness index of the different rating agencies ranked Saudi Arabia from 58 to 98 during the span of 2005 to 2010. The Yesser 2003 framework of e-government system is determined to enhance how things operate to achieve an effortless, timely and cost-effective information exchange among various government institutions for successful e-government applications. The technical policy was selected based on interoperability, market support, scalability, openness and international standards (Pankowska, 2008).

The Saudi Arabian government implemented Yesser 2003 to speed up its service operations in the public sector throughout the nation. Yesser 2003 project's action plan is to promote teamwork and innovation, to build an e-government workforce that is sustainable, to improve collaborations between the public and the government and to improve the government's efficiency when providing public service at a larger scale easily. The Yesser 2003 project offered efficient public services and created initiatives like a government secure network, national contact centre, government portal and digital certification. The motivations behind the introduction of e-governance in the country were down to economic, political, social, and cultural, geographic, technological, demographic, and managerial reasons, as well as the expectations of its citizens and regional comparisons (Abdullah et al., 2006; Basahel and Yamin, 2017). A diagram of the Yesser 2003 project is presented in Figure 5. Initiatives like the e-payment gateway, Sadad, smart cards and the portal for all 20 services of the Ministry of Interior are examples of successful e-governance applications.

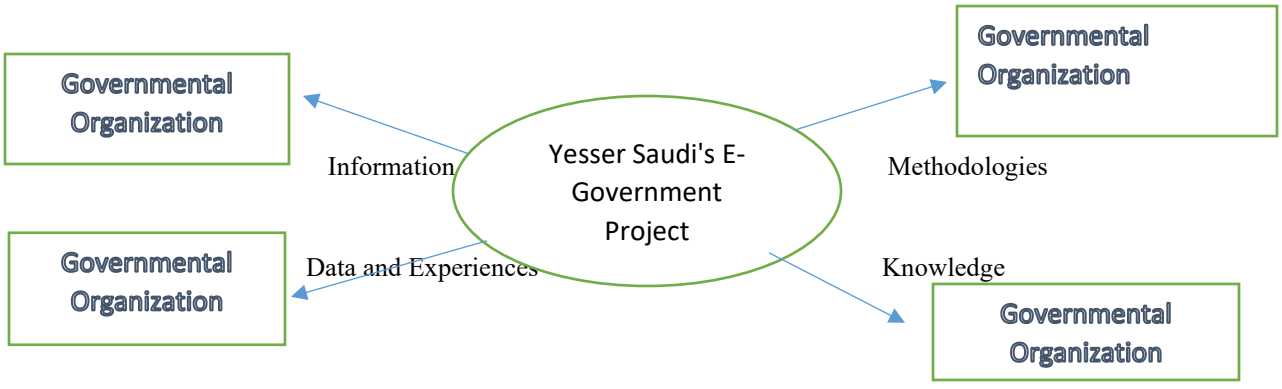

Figure 5: The Yesser 2003 project for e-governance in Saudi Arabia (Abdullah et al., 2006)

Factors like the resistance to the change to electronic systems, culture (e-government allows women to interact), inadequacies of policy and regulatory aspects, trained personnel, promotion programs to inform their partnerships and collaborations, strategic planning, funding problems, inadequate leadership management support, infrastructure related to ICT and privacy, security and trust issues related to e-services were listed as the barriers and challenges of e-governance which exist in varying degrees in Saudi Arabia according to the survey results (El-sofany et al., 2012).

An extensive analytical study of Saudi Arabia's e-government framework has been reported by Al-Nuaim (2011). The four main e-governance frameworks proposed for the successful implementation of e-governance are employed widely.

- United Nations (2002) and its subsequent updates (UN, 2018) (worldwide)
- Accenture (2000) (developed countries)
- Brown University (2001) (worldwide)
- Capgemini Europe (2002) (European countries)

The objectives of the Yesser 2003 project of Saudi Arabia include creating 150 top-priority services available to everyone round the clock 24/7 with at least a 75% and 80% usage and satisfaction rating by the end of 2010. The structure of the Yesser 2003 project is to (i) have the vision and objectives defined, (ii) create a user-centric service component, (iii) create a national major cross-departmental application network and (iv) create an infrastructure and organisational governance system to meet the public service needs. A quantitative stage-wise evaluation framework was proposed and employed to evaluate the e-government system in Saudi Arabia. Variations among the different ministries regarding the stages they surpassed and the current stage they were at were studied. However, it can be observed that no ministry had got to the third stage of the two-way interactions, meaning that only a one-way interaction was possible on the best e-governance site (El-sofany et al., 2012).

In another evaluation study, the researchers found that the earlier disconnected websites of the government did not facilitate cross-agency information sharing which is mandatory in citizen-centric e-government (Chatfield and AlAnazi, 2015). A detailed comparative study is thus able to be presented listing three best e-government practices.

a) Variety and Best Practice (VBP) (Owen et al., 2005).
b) CIVIC IDEA (Integrated Delivery of E-government Applications through Digital ID).
c) Strategic framework of e-government (including both front office and back-office components).

These models were used for the evaluation of the UK, UAE, EU and 20 countries' e-government system implementations. It was reported that the third listed strategy of e-government practices were more ideal compared to the first two.

Figure 6 presents the aspects that affect the wide acceptance of the e-governance system according to the citizens of Saudi Arabia (Alateyah et al., 2013). Some of the major issues faced by the Saudi Arabia e-government are technical infrastructure, information and computer literacy, no knowledge about e-services, trust, security and privacy. Furthermore, service quality, culture, DOI and website design are the basic components in the adoption of any e-service. All of these factors contribute to the e-readiness of the site, leading to its adoption. The effect of culture is indirect through the lack of awareness. The Islamic culture of Saudi Arabia may restrict modern thinking itself and thus become one of the main hurdles for availing e-services from any website. According to the doctoral thesis work by Alsaif (2013) and Alrashedi et al. (2015), Saudi Arabia's idea of implementing e-government depends on the perceptions of trust, compatibility, awareness and public service quality. The factors related to culture, traditions and religious belief as effects had a moderating influence. The rapid growth of ICT and the improved infrastructure have contributed to a drastic change within a very short span. The moderating influence of transparency was observed as being related to the e-government acceptance of citizens in Saudi Arabia (Almukhlif et al., 2019).

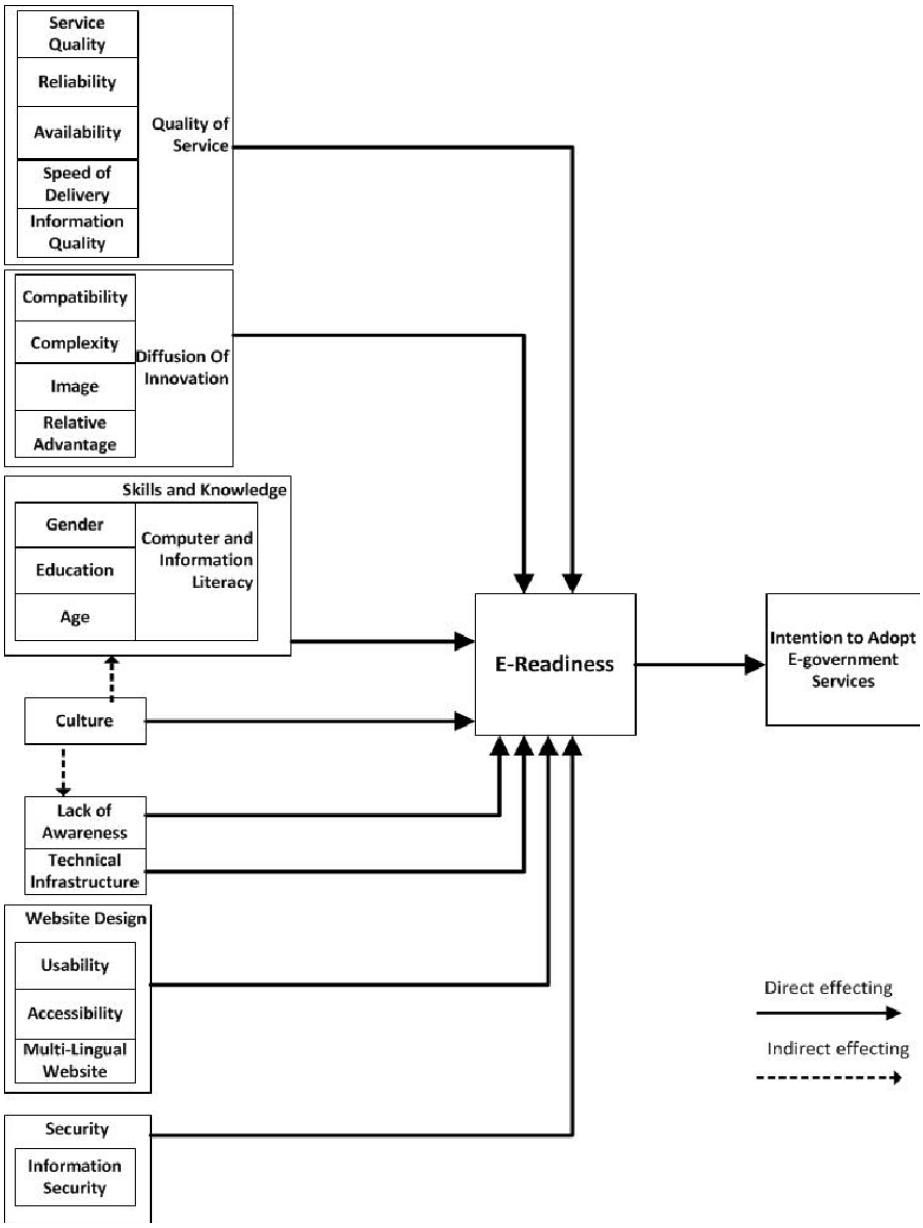

Figure 6: Factors determining the acceptance of the e-government framework (Alateyah et al., 2013)

An e-government framework for Saudi Arabia was presented and discussed using three maturity models to evaluate its status (Al-Mushayt et al., 2009). Figure 7 represents the framework that is self-explanatory as each item is descriptive by itself.

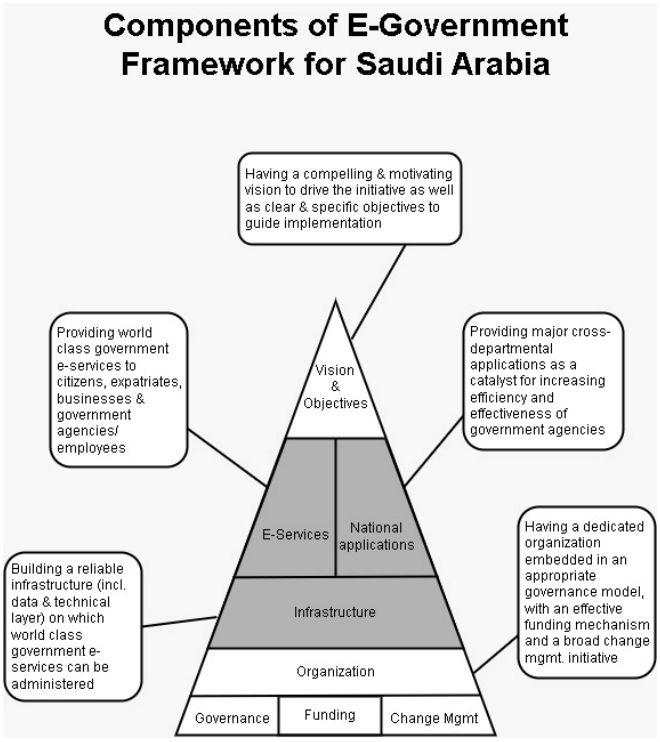

Figure 7: An e-government framework for Saudi Arabia (Al-Mushayt, et al., 2009)

SWOT analysis and the use of TOWS for the strategy formulation of e-governance in the Kingdom was accomplished by Alshomrani and Qamar (2012). Table 3 presents the results yielded.

Table 3: SWOT analysis of e-government in Saudi Arabia (Alshomrani and Qamar, 2012).

Strengths: S1: Constitutional wiliness and public administration. S2: People-centric policies. S3: Improved ICT Infrastructure in Saudi Arabia. S4: Accessible e-government websites	Opportunities: O1: Improved economy. O2: Enhancing the ICT infrastructure. O3: Legal framework. O4: Academic's involvement to support ICT. O5: Better employment opportunities for IT professionals.
Weaknesses: W1: Inadequate technical knowledge. W2: Issue of the digital divide. W3: E-transaction practices.	Threats: T1: Decentralised e-governance. T2: Citizen's mindset and culture. T3: Safety and privacy of personal information. T4: Adoption of mobile technology.

Based on the Analytical Hierarchy Process (AHP) analysis, the TOWS matrix was done and is presented in Table 4. Eight strategies were identified using SO, ST, WO, and WT combinations. All of these strategies may not be equally as important or effective but there is a need to prioritise and discard the strategies which are of a low benefit or have no benefit-cost ratio.

Table 4: TOWS Matrix for the strategy formulation of e-government in Saudi Arabia (Alshomrani and Qamar, 2012)

	STRENGTHS	WEAKNESSES
OPPORTUNITIES	SO Strategies: MaxiMaxi Strategy-1: User-centric (S2/S4/03/04). Strategy-2: Statutory e-governance framework (S2/03).	WO Strategies: Mini-Maxi Strategy-3: Bridging the Digital Divide (W2/W4/O4/O5). Strategy-4: Improving human ability (W1/O3/O4).
THREATS	ST strategies: MaxiMini Strategy-5: Nationalised e-government System (S1/S3//T1/T3). Strategy-6: Dedicated communication (S3/S4/T3).	WT Strategies: Mini-Mini Strategy-7: Promoting awareness (W2/W3//T2/T3). Strategy-8: Planning based on technology and Internet (W1/W2/T2/T4).

We used an evaluation model for Organizational E-Government Readiness (OEGR) to examine the public organisations of Saudi Arabia and the output of the interviews with the officers related to e-government (Alghamdi et al., 2014).

The positive perceptions about e-government and its services and applicability to the disabled, old, sick and women have made the e-government framework very popular in Saudi Arabia (Yamin and Mattar, 2016). The higher efficiency and easy access to government and non-government services are expected to be a further improvement. The adoption of a Cloud computing architecture for e-governance in Saudi

Arabia was attributed to a lack of knowledge and concerns about a loss of privacy, security and governance by the respondents (Al-Ruithe et al., 2018).

In the foregoing discussions, a more detailed treatment of e-governance was done in the case of China, the USA, and Saudi Arabia. Although more work on this aspect is expected from the USA, surprisingly very little research has been reported that has directly dealt with the e-governance of the USA in the literature search and on China. Some randomly selected (developed and developing countries) e-governance/e-government models and frameworks have been discussed in the subsections of the literature review above.

A comparative study is presented between New Zealand, Australia, Sri Lanka and India in terms of their e-government frameworks (Riad et al., 2011). The New Zealand model presented the framework as trend levels consisting of interactions between people and business through access channels with a common foundation for all components as layers of applications, policies, standards, information technology, information and data and services. Sri Lanka described their layers as architectures, that is, the application, data and network. The application architecture contains the various government services. The Indian framework had a middle point between government service portals and e-government partnerships with business and citizens through their home computers and mobile devices. Furthermore, the Australian e-government framework consists of three major layers. Agencies consisting of the commonwealth, state governments and local administrations have an interoperability layer. This layer follows the rules and regulations for authentication, data exchange and integrated web service through channels like the internet, customer care centres and shops.

In the following section, a comparison is made between the frameworks of Saudi Arabia, the USA, and the UK to demonstrate their virtues and shortcomings. The objective of the analysis in this research thesis is to combine the virtues of all three countries' models to propose and evaluate an e-government framework for Saudi Arabia. The USA is an early leader in e-governance and it has security systems integrated into its e-governance framework. The UK is an advanced European country with innovative approaches towards e-governance.

2.6 Issues and Challenges in the Existing E-Governance Scheme

Despite the prosperous employment of the e-government system which is an advantageous step taken and despite the fact that it has achieved great benefits for individuals, governments and businesses, it is plagued with serious issues related to the safety and security of personal data provided by the users online.

It should be noted that some of the e-government frameworks cannot guarantee the privacy of people's information. These real time issues must be dealt with and solved to enjoy *efficient, effective,* and *safe e-government* services. The major issues presented are related to the continuously adopted new policies (Dawes, 2008).

Issues related to technology, management and the change to the e-governance system are the main factors to be considered when planning e-government implementation (Ramadoss and Palanisamy, 2012). The layers of infrastructure, application and integration along with the application software are the main components of technological issues. Political and policy processes are the main components of management issues. Infrastructure funding is another issue to be considered. However, achieving a cost reduction due to the improved services through e-governance is a challenge. Catering to the needs and expectations arising due to the implementation of e-governance is another challenge faced by different countries. Various problems like the application availability, the restriction of finances, political processes, and a lack of trained professionals in ICT also need to be tackled including the organisational changes necessary to do so. Regions with less internet facilities may limit the scope of the intended e-government system expansion. The digital divide is very conspicuous in these countries. Even developing countries face serious challenges due to rapid technological changes, a shortage of skills, private and public administration barriers when it comes to preparing government officials and a lack of awareness of the likely problems due to e-channel management which can collectively hamper the progress of e-governance.

Geographical, social, and economic disparities seriously affect the fully-fledged implementation of e-governance (Shah, 2007). Other challenges dealt by the Indian government during the implementation of an e-government framework for public service delivery included high levels of unawareness, inadequate infrastructure, and unsatisfactory levels regarding the security and privacy of financial data. The front office of the e-government framework caters to the needs of the G2C and G2B services whereas the back office takes care of the G2G and G2E services. For effective e-governance and G2E (Government to Employees) services, employees need to go online before the citizens go online (Rao, 2011).

The four stages of the e-governance framework were studied and presented by Signore et al. (2005). The first stage of e-governance is information availability which includes cataloguing, balancing different amounts of information in different departments on the site, the allocation of resources to different departments, information maintenance and updating the temporal data, format and user-interface consistency, privacy and addressing the limited scope as some of the challenges faced in this stage. The

allocation of responsibility to a competent person and the responsibility of responding to emails need to be fixed properly. The second stage of e-government evaluates the cost, time and integration of legacy systems where the security of politically sensitive information, especially authentication and confidentiality, are some of the major challenges faced. The third stage of e-government is related to establishing remote connections which requires adequate coverage and security. It should be noted that automated systems alienate the direct involvement of government officials in the transaction and the services can be obtained round the clock. The right balance between privacy and a right to access information needs to be maintained. The fourth stage of e-government is the horizontal integration of all government services across the various departments. This faces the challenge of the limitations of the public sector with respect of its functional nature compared to that of the private sector. In an e-government framework, many of the services are available to the citizens irrespective of their location. To ensure a one stop service for all of its citizens' requirements, each department needs to lose some power (not always) to encourage the user to opt for the online services whenever necessary. A considerable change in the mindset of the government officers is mandatory and this is not an easy job to do. The desire for the dominance of one's department over the others with respect of information needs related to transactions is a major hurdle in achieving the desired change in mindset. As citizens have the full right to use or not use any public service, the information about individuals cannot become a tool to watch them secretly. Issues related to technology (ICT), economics (Financial) and society (Public administration) were also discussed in detail (Signore et al., 2005).

In Zambia, a lack of political will, inadequate ICT infrastructure and not using the local language in the content have together delayed the adoption of e-government practices in the country (Bwalya, 2009). Kazmi, (2010) carried out a survey and found that the quality of the website, ICT infrastructure, encouraging government policies and availability of the required technical skills were identified as the challenges faced by Pakistan when looking to employ e-governance successfully in the country. The challenges faced by the e-governance framework in Dubai (No 1 e-city in the Middle East province) included issues of the language used on the government portals, integration, the digital divide and quality websites and e-services (Zhao et al., 2012). A low level of internet penetration, the limitations of the ICT infrastructure, inadequate institutional framework support, inadequate funds, limitations in terms of technical expertise, cultural issues, and a lack of public awareness and participation were identified as the major challenges facing th e-governance enhancement in Botswana (Nkwe, 2012).

To address the challenges of operating in a connected environment, engaging stakeholders and solving societal problems, the so-called third stage of e-government, termed 'lean government' (l-government)

is now presented (Janssen and Estevez, 2013). In e-government, the public authorities operate on platforms which facilitate innovation and interactions with a focused orchestrating role. It simplifies and streamlines the administration structures and processes and stimulates novelty for the stakeholders.

Poverty affecting access to internet, the technical illiteracy of most of the population, English language dominance over the local languages affecting access by those who do not know English, a lack of awareness about e-governance and how it can be used for availing various services, a lack of supportive infrastructure like power and internet connection and the barriers affecting the re-engineering of processes were the challenges faced by the e-governance in India (Malik, et al., 2014). Financial feasibility and the need for a huge amount of funds were identified as the problems when seeking to expand the e-governance in India (Paramashivaiah and Suresh, 2016).

It was observed that only three hurdles, technical, social and financial, have been listed for the Jamaican e-government framework (Waller and Genius, 2015). In the case of Rwanda, the e-government implementation challenges include information infrastructure, social inclusion, trust in the new system and language (Twizeyimana et al., 2018). It should be noted that all challenges do not affect the e-government system to the same extent and the mitigation methods vary.

All of the above literature and survey works to show the general trend of the issues and challenges faced by countries while implementing and taking forward an e-government framework. The relative effects vary with the economic status of the country, its socio-economic structure, technological capabilities and willingness as reflected by the policies and strategies. Having reviewed the issues and challenges faced by various countries when implementing their e-government system, some of the limitations of the current e-government frameworks of particular countries will be reviewed in the next section leading to addressing the limitations by proposing a new improved e-government framework for Saudi Arabia.

2.6.1 Function Limitations in Existing E-Governance Frameworks

Despite the exceptional achievement of public service delivery by e-governance frameworks, the frameworks being developed and implemented by several countries do have some disadvantages and limitations attached. It has been reported that almost one third of the implementation attempts of e-government frameworks result in complete collapse, i.e., the e-government frameworks are immediately abandoned after implementing them. Furthermore, 50% of e-government frameworks are classified as being in a state of partial decline, i.e., the objectives of the framework were not achieved or reached

undesired outcomes. This is mind boggling because it amounts to a waste of resources due to the e-government framework being implemented by a country and not achieving the desired goals.

Studying Jordan's e-government framework, it was observed that it is not ready for an e-government system as the citizens are treated as customers to a business (Ciborra, 2005). This directly means that more privileged members of the society will have better and easier access to the public services. There may also be a need for intermediaries and this can increase the risk of corruption as these intermediaries may demand bribes. Hence, a collaborative and simultaneous (e-government implementation and political change) implementation needs to be done side by side with social and political changes so then the nation can get all of the associated benefits. In addition, the author also presented that a nation's economy needs to grow to the level of being a service delivery state where corruption, political influence, biased markets and other pertinent issues are addressed before implementing an e-governance framework.

The research determined there to be three gaps in the e-government framework viz., hard and soft, private and public and country. Hard and soft gaps refer to the difference between the technology (hard) and what's obtainable in the social context (soft) in which the system is operating. The private-public gap indicates a system that is working fully for one sector that may not work in another even partially (Ciborra, 2005). The country context gaps refer to the e-government framework being obtainable in developing countries that may not allow the use of an e-government framework created for a developed country (Dada, 2006).

Issues related to the e-government framework employment in India were evaluated using a four-stage evaluation model (Paul and Paul, 2011). Although information and communication technologies have facilitated the e-governance implementation by India in a great way, the full potential remains untapped. The possible reasons identified are related to the poor organisational, human, and technological infrastructure. In a multilingual country like India, the language that is to be used in the system and public access points becomes an important issue. A sound policy for cybersecurity ensures secured e-governance transactions.

A lack of funds in relation to the organisational and financial perspectives affecting the development of databases and the quality of the service are just some of the main challenges faced by administrations when implementing e-governance systems. A Cloud-based architecture was proposed as a solution to overcome the issue of an integrated database structure for e-governments (Mosa et al., 2016). Figures 8 and 9 represent web-based and Cloud-based e-government frameworks, respectively.

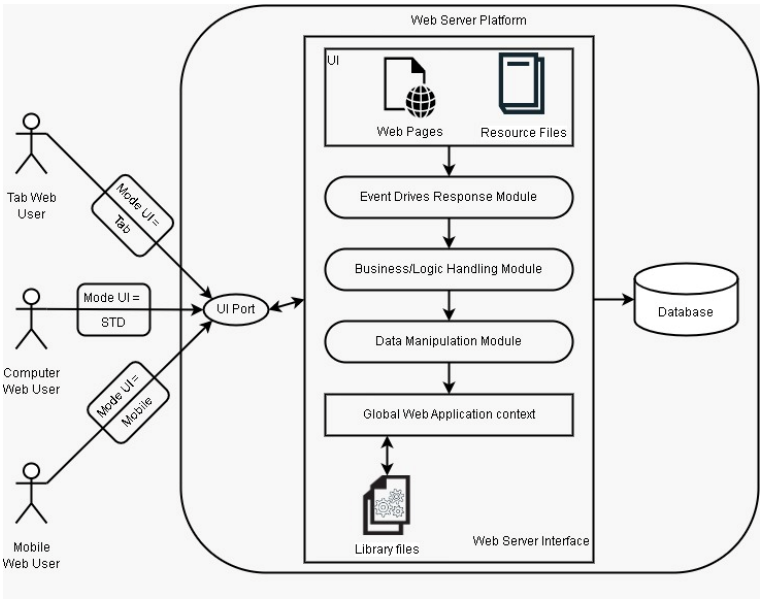

Figure 8: A web-based e-government framework (Mosa et al., 2016)

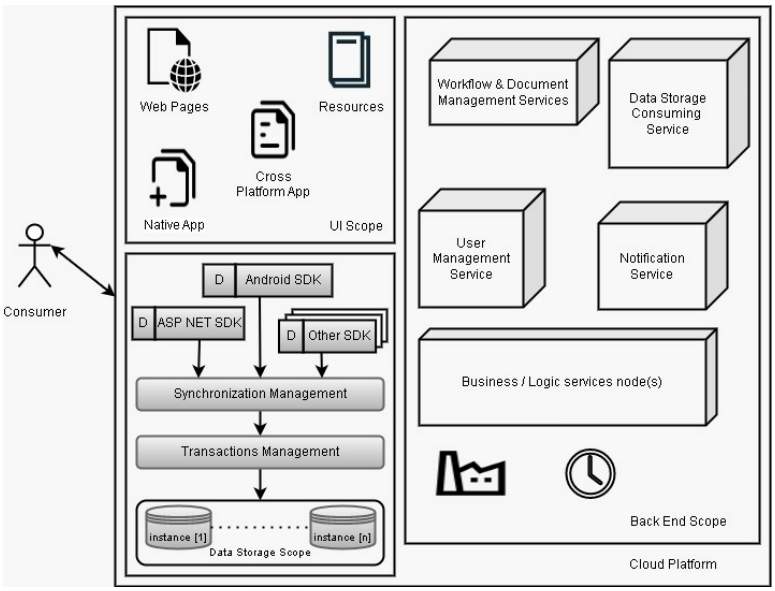

Figure 9: Cloud-based e-governance framework proposed by Mosa et al. (2016)

It should be noted that the Cloud is used for backend support for business and logistics as well as workflow and document management, user management, data storage and notification services. The data storage has transaction and synchronisation management systems in place alongside operating systems and software applications for the user interfaces. Cloud-based services (pricing based on consumption, innovation, agility, resilience, standardisation and upgrades) are provided (a shared pool of computing resources) which delivers the services on-demand over the network situated in the loud.

2.6.2 Security Issues in E-Governance

Various types of information security threats and security measures undertaken in e-government by different countries have been reviewed and discussed by Singh and Karaulia (2011). In 2015, South Africa's Ministry of State Security implemented a National Cybersecurity Policy Framework (NCPF) as an extension of the Protection of Personal Information (POPI) Act 2013 to ensure data privacy (Ewan, 2017). Ghana's e-government system identified a lack of national databases to verify the information, as well as unauthorised access to the systems, service exclusion, illiteracy and little or no internet access as the major security challenges (Botchwey, 2018). Marian et al. (2016) proposed a framework which offers organisations the ability to identify issues and to employ security governance and management processes. Later, a lightweight and robust remote user authentication protocol was proposed to be implemented in smart cities by e-governments for the improved security of secured transactions (Geeta and Sheetal, 2017). A sophisticated framework for the early detection and mitigation of insider threats (stakeholders) in an e-governance IT infrastructure needs to be employed.

The Role-centric Mandatory Access Control (RMAC) system-based access control model has been implemented by Saudi Arabia to provide inadequate security to e-government sites (Albrahim et al., 2018). Normally, for high security information, access is restricted to very few top level officials. It is found to be mandatory to have a collaboration between the information systems and other e-government agencies to achieve the highest potential of e-governance (Alfadhel et al., 2019). It has been observed from so many research articles that have reported about security and privacy issues that Blockchain technology implementation for e-governance provides better and more efficient security services compared to traditional security and privacy approaches.

2.6.3 Research works and critical analysis on why current security measures are not sufficient?

The implementation cost of Blockchain technology in an e-government, the problems for individuals and societies (loss of jobs), payment facilitation and expert background knowledge are some of the issues faced by the application of Blockchain technology (Risius and Spohrer, 2017). It has been challenging to create a commercial application environment with Blockchain technology (Target News Service Washington, 2018). Furthermore, scalability, hardware security, transaction confidentiality, the payment leg and the uptake of editable Blockchains are also considered to be major issues related to Blockchain. Distributed Ledger Technology helps to achieve scalability with faster transactions but currently adapting it to a new market structure in the form of Blockchain should enable a stable link with a centrally backed digital currency. Zero Knowledge Proof (ZKP) or a similar technology may be useful here. In ZKP, an additional layer of cryptography in the consensus algorithm step verifies the transaction without revealing

any information. This will ensure additional confidentiality and security in the successful implementation of Blockchain technology in e-government.

It has been observed that 51% of malicious or dishonest nodes may lead to tampering with the validation process and creating new blocks much faster in a manner that is considered genuine by other active nodes on the network, resulting in honouring the false transaction (Alketbi et al., 2018). When transactions are controlled by dishonest nodes on the network, this leads to compromised transactions. Furthermore, the control by the outsider is minimal and results in the entry of wrong records in the system. The repeated use of SYN flood attacks (DoSs) can make the system non-responsive. A sybil attack controls the nodes to prevent locks or transactions and to alter or disconnect the communications of other nodes. The timing error slows down the acceleration of the system and occurs when inaccurate transactions are carried out. Public and private keys on the network might be manipulated, leading to undesirable consequences. Moreover, if the audit server is compromised, any wrong transactions will pass through the system as legitimate ones. Security flaws often lead to bugs in the system, thus affecting the smart contracts. The Decentralised Autonomous Organization (DAO) can be subjected to this form of vulnerability.

Unauthorised access to the private keys of users (weak encryption of the keys makes them vulnerable) is possible using conventional malware attacks which questions the confidentiality, integrity and authenticity of transactions. Standardisation, collaboration, a management system and the security of physical data, as well as application systems, secret keys and the management of various risks have all been suggested as solutions to the challenges in the given context.

The limited adoption of Blockchain technology by the e-governments of developed countries and the lack of empirical evidence are major concerns when seeking to arrive at any conclusion (Batubara et al., 2018). Technological challenges pertaining to scalability, security and flexibility do not need special mention. The adaptability and acceptability of a novel e-governance framework is challenging in the organisational context of the government whereas the environmental barriers are lacking legal and regulatory support.

Data governance and privacy, as well as resistance from officers, needs to be considered as among the difficulties found in the application of Blockchain technology in under-developed countries and developing countries. Technology-related issues are more challenging when using Blockchain technology to prevent corruption including using it in e-government platforms (Kim and Kang, 2017).

2.6.4 Why Blockchain?

Blockchain as an emerging technology has directly or indirectly affected human life in various ways. The advancements in Blockchain technology have led to tremendous reforms in the public sector domain especially. Government leaders and policymakers around the globe have already set themselves on a path to seize the opportunity of utilising the potential of distributed ledger platforms. To deliver the promise of making public digital platforms robust and transparent, it is imperative for governments to adopt a decentralised platform for their information management services. Globally, there are a variety of providers of information technology services that have come up with solutions designed to improve the reforms in the public sector. Any government is typically a formation of bureaucratic fabric governed by certain laws and regulations. Therefore, its basic building blocks are regulated by a set of well-defined administrative standards that can be translated into an ideal digital platform such as Blockchain.

Information and services are typically dispersed to businesses and individuals by the e-government which is usually implemented in a top-down fashion. The second political aspect of such reforms is regarding the bottom-up electronic participation in order to create a platform for a wide range of services to be provided to the public. Blockchain represents the third and latest dimension of these public sector reforms by taking a peer-peer approach to cater to the requirements of the businesses and citizens, providing them with a better service platform. All three dimensions create a strong basis for the automation of typical government functioning. The fact that governments are by nature bound to provide services to public and enterprises through various technological means relates to the automation of public information services on a more sophisticated platform due to it being highly required in the current era of *Internet plus*. The public understanding of e-government is shaped by the centralised characteristic of publicly available datasets with all of the pros and cons of an e-government. Such a centralised approach advocated by the government officials and managers is solely responsible for determining the fate of an e-government system though a wide range of public services provided through different electronic platforms. The highly centralised nature of e-government and the centralised control of public databases is related to the total aggregation of public information which in turn puts all of the burden on one centralised place. This aggregation of information can lead to distrust between the public and enterprises irrespective of how efficient and robust the services are. As a matter of fact, citizens doubt the credibility of the information that is being dispersed through the centralised e-government platforms particularly when it involves financial service delivery. Public trust deficiency in a digitally transforming environment where social media platforms are being used at an enormous level may lead to the exaggeration of misinformation and suspicion on the internet.

Blockchain and its decentralised nature provides a better solution to the aforementioned cases. It is an alternative for making public information more transparent in a highly distributed fashion, potentially putting an end to the public distrust problem in conventional e-government platforms. It is not just a highly reliable technology for data storage. Blockchain networks also prevent the issue of public distrust because of the fact that Blockchain network peers equally trust the distributed ledger ecosystem. There is no centralised tracking system that records the history of changes as a frequently updated registry version gets distributed in an extremely interactive peer to peer approach. To add to that, no other party is required for the verification of newly created blocks since the transaction is automatically subjected to a self-cross-referencing process, thus improving the credibility of network with each newly created block, making data manipulation extremely difficult.

Another prospective regarding the advantage of using a Blockchain network is that the memory requirement increases when there is a hefty amount of data added to the databases every single day, making the data processing more complicated and costly with the currently available data storage techniques in place. It is therefore important to shift to an energy and cost-efficient and more importantly, an open source peer-to-peer distributed ledger technology with Blockchain being an unopposed contestant on the list.

2.7 Blockchain Background

Blockchain technology is one of the considerable achievements of technological advancement for data management and it is widely accepted by almost every business model. The primary objective of Blockchain technology is to enhance the integrity, reliability and privacy or security of any transaction in a decentralised structure of data management. In the earliest stages, Bitcoin implemented Blockchain technology during the year 2008 which involved the extensive encryption and management of transactional data to avoid unauthorised access (Cheng et al., 2017). Data encryption and the decentralisation of the data management are the driving forces behind the transaction becoming reliable and secure without having a third party in place. Blockchain technology is observed to be in a young stage as it has not been explored fully regarding its capability to manage large amounts of transactional data and being transparent and secure (Huumo et al., 2016). This section presents an extensive literature review pertaining to Blockchain technology and e-governance. After encouragement from the UN, every country is planning to employ Blockchain technology to provide safe and secure public services including health and public security management (Jun, 2018; Brodersen et al., 2016).

Blockchain technology is broadly categorised into *Public, Private* and *Federated* based on its access to the public and the permission needed to access it. Public Blockchain (Bitcoin is the most suitable example) is open source and doesn't need any specific permissions to access them. It is ideal when data is generated en-mass and the individual's identity needs to be kept confidential where no one has the privilege to edit or remove anything from the Blockchain (Kiviant, 2015). Private Blockchain allows only a limited number of persons to validate the transaction like in relational database management systems where privileges are given to some users to edit and remove data. Others can only access the information from the database (Zhang et al., 2017). In an exclusive private Blockchain, the public is not even given the privilege of being able to read the data. Federated Blockchain is largely employed by banking and financial institutions to cater to the need for huge transactions. Using federated Blockchain, authorised individual(s) are given the authority to validate the transactions whereas private Blockchain has only one validating entity. Furthermore, it reduces the cost, improves document handling and ensures quality as well. Figures 10 and 11 represent the structure of public and private Blockchain, respectively.

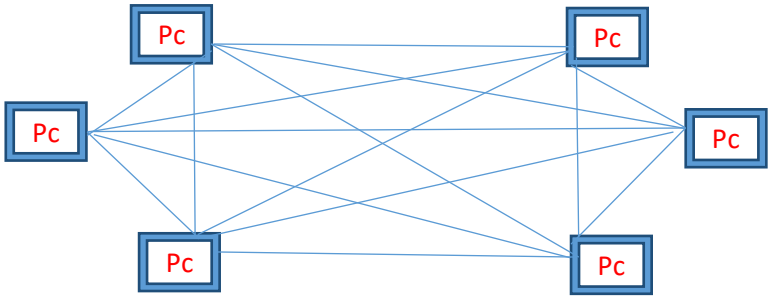

Figure 10: Public Blockchain structure (Kiviat, 2015)

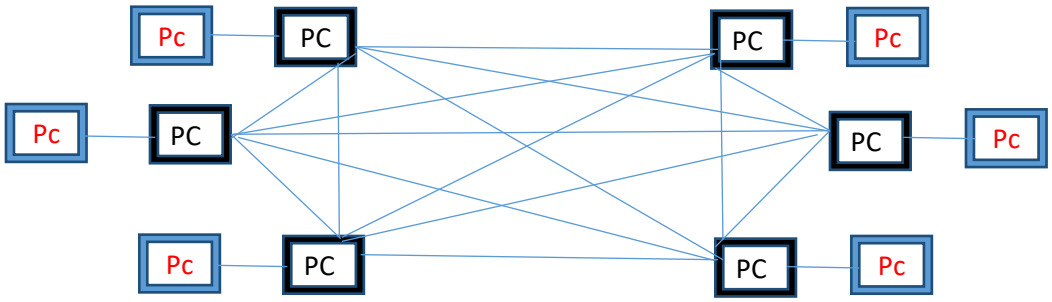

Figure 11: Private Blockchain structure (Zhang et al., 2017)

It is evident that data sharing has become efficient and secured by Blockchain technology because it is decentralised, transparent, distributed and time saving. Blockchain technology is employed as a large public and private data management system including by federal, government, healthcare, scientific research, and law enforcing agencies. Many countries implement Blockchain technology to achieve better (improved) e-governance which is safe and secure due to enforcing regulations and prohibiting violations (Larsen et al., 2014).

Blockchain technology does not follow any specific standard regulation and the privacy and confidentiality of the transaction is a major challenge dealt with by Blockchain technology (Bergquist, 2017; Marr, 2018). Furthermore, vulnerability, redundancy, distribution, implementation cost and compliance with the regulations are also considered to be challenging. Excessive cybercrime and increasingly skilled hackers have raised the credibility of implementing Blockchain technology (Kothe et al., 1991). Implementing Blockchain technology completely depends on its privacy preservation ability. Blockchain technology requires a huge infrastructure investment initially, as well as during use and after implementation to manage the huge amount of data going over the network (Huumo et al., 2016). The increased number of users over the internet invites the possibility of data redundancy that sometimes results in the slowness of the system overall.

Transactional data replicates to inform the receiver about the transaction which raises privacy concerns over the internet despite implementing the signatures of the sender/receiver to validate the data (Zhang et al., 2017). The complex structure of Blockchain technology ensures the security of the transaction but to interfere, a hacker could gain more access than just to the actual node i.e., a 51% attack phenomenon (Hummo et al., 2016). However, it was observed that cryptographic technology provides the best security and integrity for transactions and that the full potential of this technology has yet to have been explored and reported (Kiviant, 2015).

DAH minimises the counterparty risk and eases the transaction. Hyper ledger is based on the UTXO script and distributed in nature. Hyper ledger employs a proven consensus algorithm that can carry a huge number of transactions every sec (Peters et al., 2015). Chain is an open sourced Blockchain protocol that is widely implemented and accepted by the financial industry including Citi, Visa, CapitalOne, Fidelity etc. Role-based permissions, selection privacy, immediate transactions, smart constructs, and integration with the current protocol are some of the major reasons behind its wide acceptance. R3CEV is a proposed protocol for industry where banks all over are collaborating with each other with the purpose of finding common standard procedures. Businesses other than banking also encourage and look forward to

integrating Blockchain technology due to the current production and shipping industries improving upon their secured services. It can be observed that production-based establishments find it difficult to engage in logistics manually. Blockchain technology helps production-based industries to maintain and track their logistics for a competitive advantage (Niforos et al., 2017). Unlike traditional data management, Blockchain technology integration helps the businesses make more secure and transparent transactions that are immutable later. It also provides a continuous storage of transactions in real-time using smart contracts which helps in the execution of the transaction by meeting certain parameters (Bergquist, 2017).

It is mandatory to solve a cryptographic puzzle to include a block (verified blocks only) which takes an enormous amount of energy and computational power. This provides an opportunity for the participants to validate their transactions. It should be noted that the validation is also rewarded based on the number of blocks that they add to the chain (Lin and Liao, 2017). This further simplifies the work over Blockchain where more individuals team up with others to balance out the power of the larger stakeholders. It offers a greater centralised network. Every participant in the Blockchain validates the true and valid Blockchain network which stops the double spending of crypto coins. It enables every node over the Blockchain network to give away a public key. Messages go through every node after verification by the organisation. It authenticates the user over the Blockchain using the primary keys that they have. Every node is bound to attach its identity to the transaction to be validated and it is accepted by others on the network. Every node is required to wait its turn (randomly picked by the network) to get a block, resulting in the optimal utilisation of resources. It has been proven to be very efficient at granting access to the blocks.

E-governance provides services with the minimum involvement of the government in online mode and it helps the government to keep track of the transactions related to land, vehicles, finances, taxes and penalties etc. Blockchain technology serves e-government by inducing effective communication between the citizens and the government authorities. The system is automated to make decisions according to the requirements at any level and to keep the communication happening (Hou, 2019). The list below includes the services offered by the government to their citizens.

1. Land/property record management
2. Vehicle record management
3. Financial transactions
4. Citizens record management
5. Taxation and fines

6. Benefits/fund disbursements
7. Payroll management
8. Educational data management

Despite having adapted to new digital technology, some of the areas related to record management and financial transactions are not fully monitored. The implementation of Blockchain technology enriches the government to carry out error free transactions. Improved ICT and distributed governance systems have brought the government and citizens closer to offering and seeking public services easily, respectively. Blockchain technology offers not only reliability and data safety with compatibility and efficiency related to the concepts of e-government. It also stores every activity of the citizens and the wider e-government. All of the information about the public services is provided on the official websites of the government which is automatically updated whenever and wherever necessary. The users of these systems also maintain their security by avoiding data sharing and abuses and provide accurate data. E-government systems implementing this technology are also updated about the requirements of the services and decisions are taken accordingly. One of the major services offered by Blockchain technology is impossible data manipulation which results in better and more timely information and services. Everyone on the network contributes to the overall development of the country. Blockchain technology also encourages end-to-end transactions without a third party present. In other words, it offers decentralised governance. With no intermediate third party in place, the cost incurred regarding the state duties and intermediaries is reduced. It is evident that Blockchain technology enhances more transparent, quick, safe and secure transactions for citizens (Ølnes and Jansen, 2017).

The most important features of Blockchain technology that inculcate efficiency in e-governance systems are listed below.

- The technology does not need any central authority to run the system. Thus, there is no need to administer the system and no one has any control over correcting the data.
- The system operates continuously as the data (after being uploaded) is copied to many computers. The system will keep working even if 99% of the total computers go offline.
- The data embedded in the block technology is totally safe and secure.
- Only cryptographic edited data goes in the system which makes the data more safe and secure.
- The cryptographic codes are not privatised for use and are not owned by any agency.

2.8 Blockchain Technology for the Security Management of E-Governance Systems

The security threats can be physical connectivity, Wi-Fi, hardware, a large attack surface, bandwidth consumption, applications, interception etc. (Yang et al., 2019). The current security system of the e-government framework depends on human experts, meaning that there is a high chance of cybersecurity compromise and corruption. However, Blockchain technology is proposed and implemented to address these issues easily and successfully (Diallo, et al., 2018). Blockchain technology can be implemented for digital ID management and secure document handling using distributed ledgers (Ølnes and Jansen, 2017). Improving the transactional transparency, preventing fraud and establishing trust in the public services has invited the interest of the ICT community.

Blockchain technology can also be used as an access control monitor only and for the storage of data somewhere outside of the Blockchain to avoid the sharing of sensitive government information to third parties. However, with later enhancements to Blockchain technology, it is acknowledged that using encryption and distributed data means that a highly secure and privacy preserving decentralised Blockchain system can be developed as presented in Figure 12.

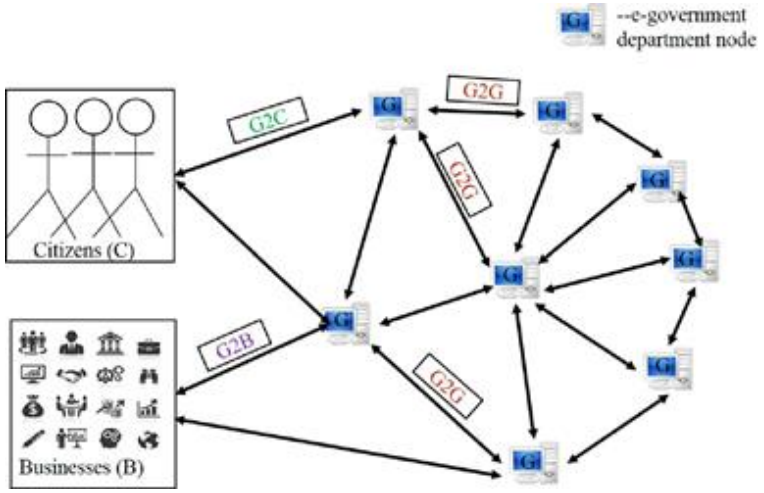

Figure 12: A Blockchain-based e-government system

A Blockchain technology-based decentralised e-governance framework for smart cities with enhanced security and the privacy of its citizens can be implemented (Yang et al., 2019). A Blockchain-based security system in a decentralised framework proposed by the authors is given in Figure 13.

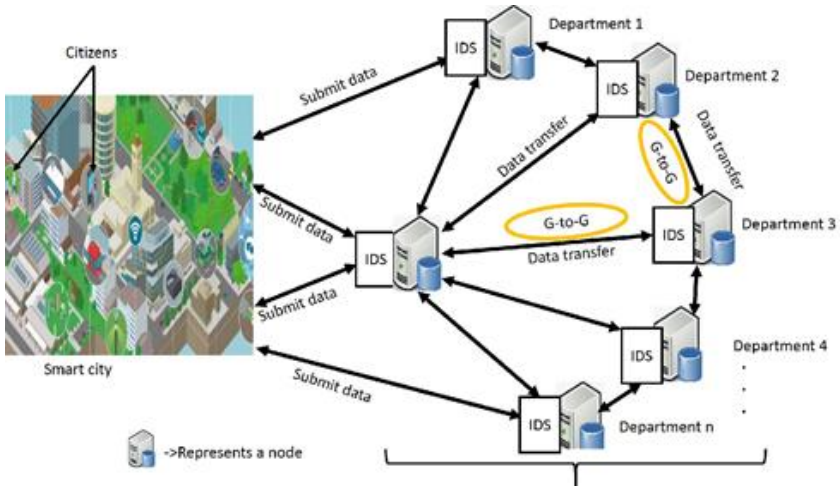

Figure 13: Blockchain-based decentralised e-government system (Yang et al., 2019)

Public key cryptography provides security against unauthorised access. Every node on the network is assigned a private key for validating transactions on the network. To alter the record on the Blockchain, the attacker needs at least 51% of the network peers to allow the modification which is highly unlikely. In the proposed system, the availability of the system is ensured by avoiding any single point of failure. Attacks become almost impossible with node registration which allows the user to share data to other peers on the network. Figure 14 depicts the layered distributed ledger system and Table 5 presents the security requirements and countermeasures (Yang et al., 2019). Every transaction on the network is validated by its peers on the network which leads to the safety and security of the transaction.

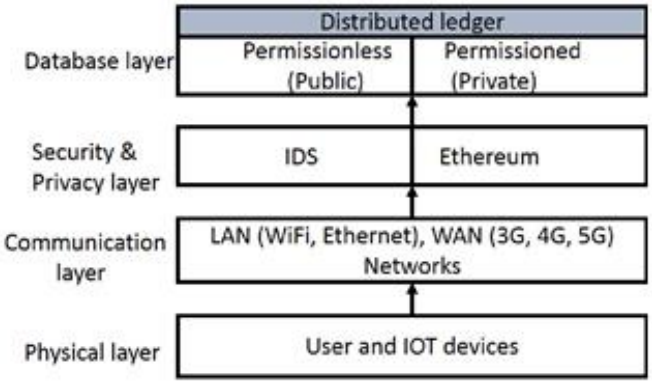

Figure 14: The layered distributed ledger system (Yang et al., 2019)

Table 5: Security requirements and countermeasures (Yang et al., 2019)

Security service	Countermeasure (s)
Authentication	Blockchain address and digital signature
Access control	Digital signature and encryption
Confidentiality	Encryption
Integrity	Encryption and digital signature
Non-repudiation	Encryption and digital signature
Availability	Distributed/decentralised
Trust	Decentralised, encryption and digital signature

The Elliptic Curve Cryptography (ECC) procedure for encryption and digital signatures is suggested for security in Blockchain technology-based e-governance systems (Ølnes and Jansen, 2017). Table 6 presents the comparison of conventional internet and Blockchain layered structures when it comes to added security features.

Table 6: Comparison of conventional internet and Blockchain layered for added security features (Ølnes and Jansen, 2017)

Internet	Blockchain technology
Applications	Applications
HTTP/HTML/…	Bitcoin/other currency
TCP/IP	Consensus rules, peer-to-peer, security
Physical and logical link	Distributed Blockchain database

2.9 Case Study: Existing Blockchain Technology-Based E-Governance

Blockchain technology is being used in various countries for the registration of different types of assets (movable and immovable). The registration of intellectual property and regulating pension systems have

become easy with the advent of Blockchain technology (Jun, 2018). Blockchain technology has been successfully employed by multiple countries for the purpose of conducting auctions and to ensure transparency in budget making and budget execution. It is also widely used at the time of elections for fair vote counting at the election booths (Kshetri and Voas, 2018). Here we mention some of the prominent examples of Blockchain technology in e-governance.

2.9.1 The KSI Blockchain and the X-Road in Estonia

Estonia is one of the topmost states offering almost 99% of its government services online. When evaluated, it was observed that the equivalent of 800 years of working time has been reduced (https://guardtime.com/technology). Internet services as human rights, digital signatures valid for authentication services and the duplication of data is also avoided. Blockchain technology easily detects data manipulation either external or internal (https://e-estonia.com/solutions/e-governance/). The Keyless Signature Infrastructure (KSI)-based Blockchain application is employed by the Estonian government. It has been successfully implemented at every level of the government to be uninterrupted and to offer both speedy and secure services. The KSI Blockchain was found to maintain the integrity of records and the detection of unintended modifications. KSI Blockchain employs secure signature services to provide secure e-services and full data privacy. A block, once it is appended to the chain, can never be modified. KSI signatures don't need to be reverified. Figure 15 depicts the integration of the KSI Blockchain within the e-governance framework using the X-Road procedure.

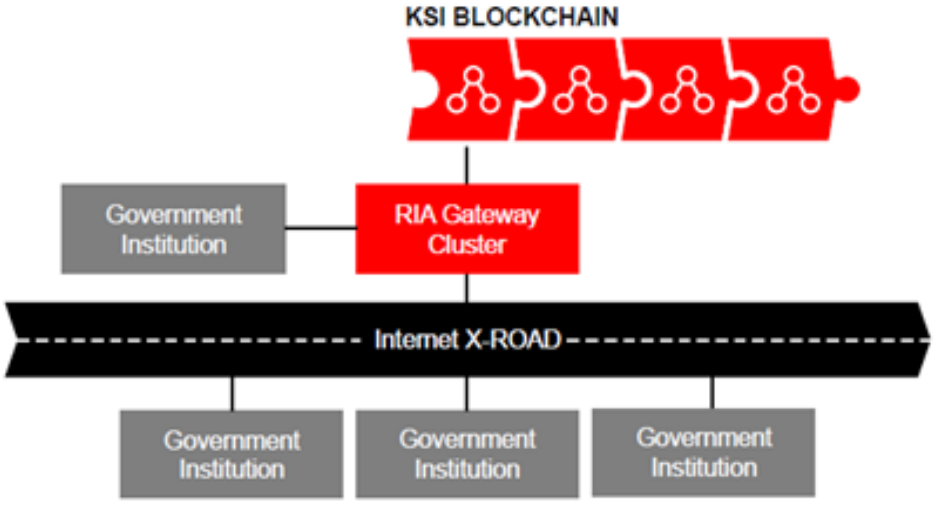

Figure 15: Integration framework of the KSI Blockchain within the e-governance systems using the X-Road (Source: Ivo Lõhmus, Guardtime)

The X-Road is Estonia's interoperability platform that combines various security services (registration services, an e-health system, judicial and police functions etc.), e-facilities and different frameworks. The KSI Blockchain technology-based Audit Logs architecture followed by Oracle is presented in Figure 16.

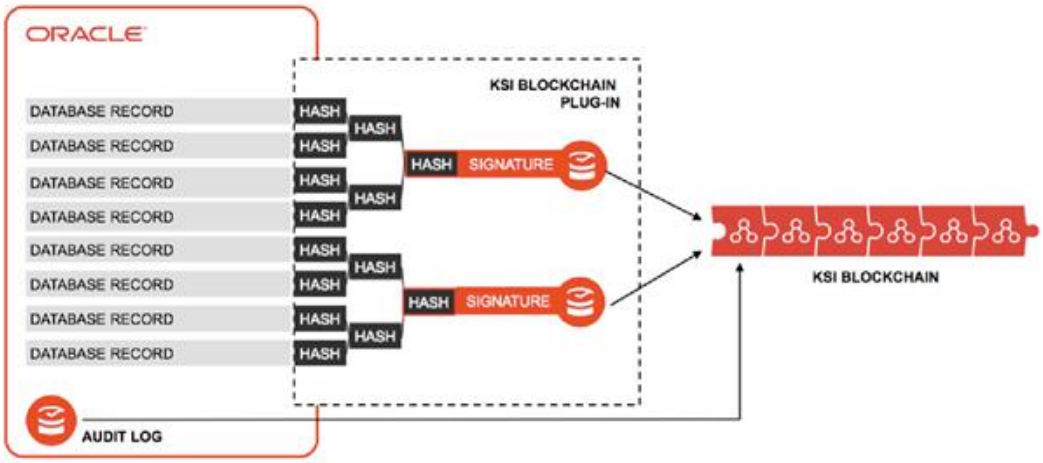

Figure 16: KSI Blockchain technology-based Audit Logs. Source: (Jun, 2018)

Estonian State Agencies employed KSI Blockchain technology to offer better and improved registries for healthcare, property, business, succession, digital courts, surveillance, tracking, administrative laws, political regulation and official announcements. It can be observed that many countries have implemented Blockchain technology using the KSI architecture for their e-governance systems at various levels, which is possible. The organisations implementing KSI Blockchain technology include NATO, the US Department of Defence, Boeing, Ericsson, SAP, and GE for the purpose of securing and distributing data.

The advantages of the KSI Blockchain architecture include the following:

1. Original data is never shared over the network.
2. Ownership of the data remains with the owner only.
3. Only the irreversible hash of a file is shared (SHA 256 or SHA 3 is currently supported).
4. The generated hashes are encrypted and added to the Blockchain.
5. KSI Blockchain uses hash calendar techniques that enable it to be highly scalable.
6. It is much faster and can cover and update all generated data worldwide within a second.
7. It takes the least time possible (less than a second sometimes) to cover and update all generated data.

In August 2017, a vulnerability was reported that compromised the security of millions of eIDs used in the E-Estonia system that were using the KSI Blockchain. Later, it was revealed that the flaw was in the

security chip used in the eIDs and that KSI has nothing to do with it. To date, no known attack is available against the KSI Blockchain.

2.9.2 BROP: Blockchain Technology in e-government in China

Zhongchao Blockchain Technology Research Institute's (ZBTRI) Blockchain Registry Open Platform (BROP) Version 1.0 was recently launched by China to standardise the Blockchain applications and to encourage its mass level application. BROP has been developed to provide a digital id, secured data and digital certificate services (http://www.zcBlockchain.com/epc_html/index.e.html). The BROP is designed to protect and enhance intellectual property rights such as patents and copyrights using a Smart Contract document that is written as a decentralised application (DApp) that operates on a Blockchain platform as presented in Figure 17 (https://seekingalpha.com/instablog/22912651-daniel-jennings/5137878-china-s-central-bank-testing-Blockchain-platform).

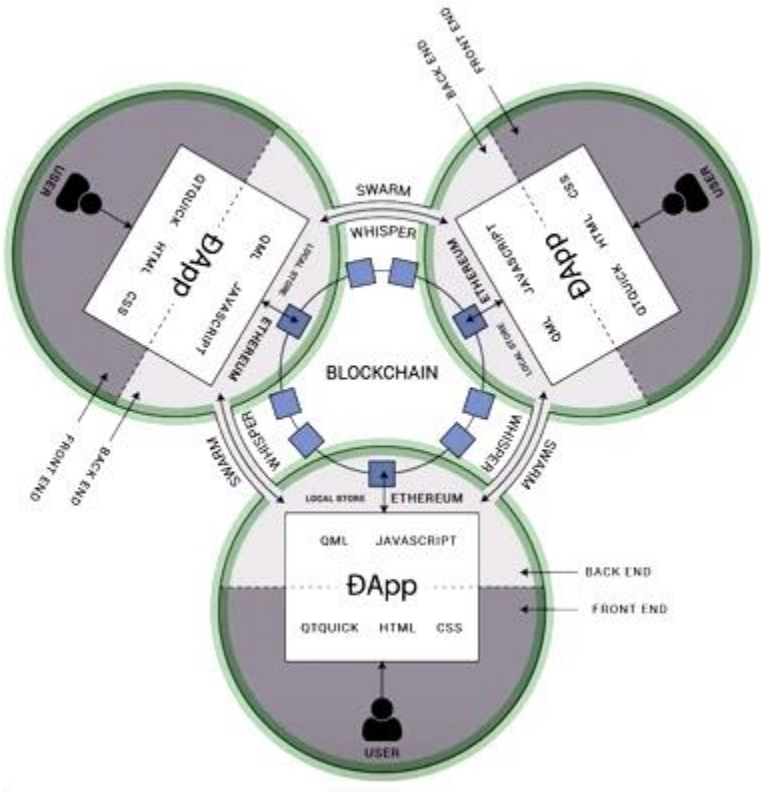

Figure 17: DApp Architecture

2.9.3 DayOne.swiss (Swiss government healthcare block chain program)

The DayOne.swiss Blockchain initiative supports precision medicine to ensure data integrity, compliance and a secured data exchange. Genome data management and clinical trial data storage were the main concerns of this project. Genome data management in biobanks was proposed by Jun (2018) as shown in Figure 18.

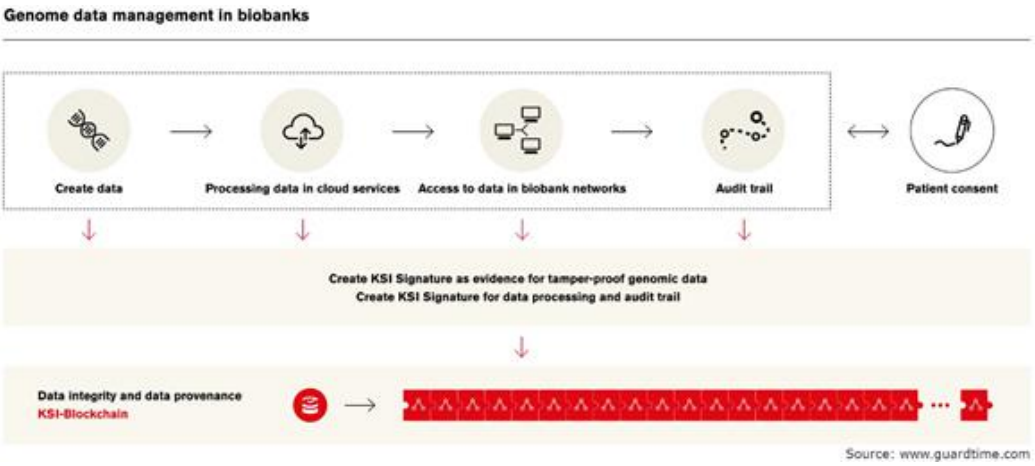

Figure 18: Genome Data Management in Biobanks (Jun, 2018)

The use of Blockchain in genome data management ensures data integrity, the security of audit records and taking patient consent prior to its use in future. At the same time, Blockchain technology can also help to ensure the adherence to the ALCOA standards (Attributable, Legible, Contemporaneous, Original, Authentic, Complete) related to the use of any electronic device on anybody. A new audit trail record is generated in the database for every operation/procedure performed. These are secured using a KSI signature that serves as proof of evidence that the data (neither in terms of time nor authorship) was not tampered with.

2.9.4 National Agency of Public Registry (NAPR)

The NAPR in the Republic of Georgia is one of the first Georgia Blockchain technology projects which converted the entire land records to digital. The NAPR provides its citizens with a digital certificate of their assets that are cryptographically proven and published to the Blockchain. The primary objective of the NAPR was to employ a secure solution for data security, transparency and for the auditable processes for both its citizens and the governments. This has resulted in a 400 times faster land registry process and a fully tamperproof record management. Figure 19 below depicts the proposed NAPR Architecture for the Republic of Georgia.

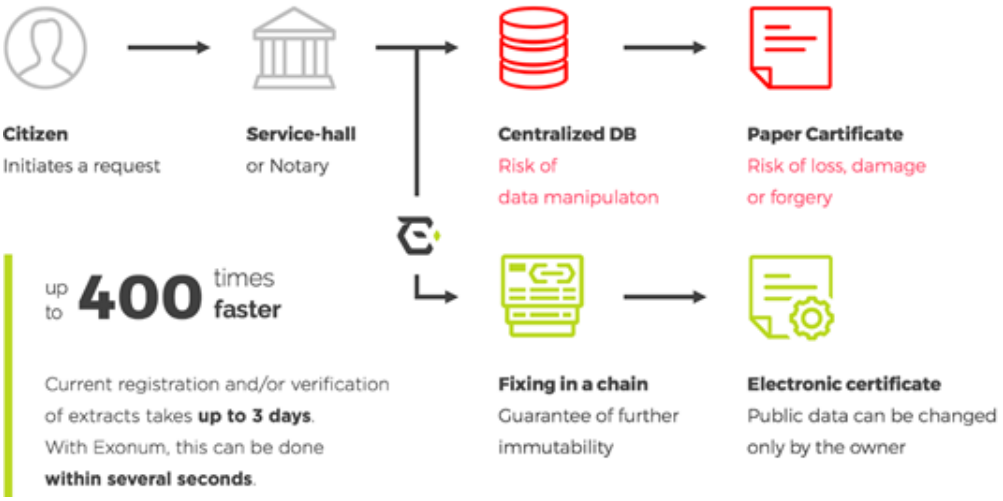

Figure 19: NAPR Architecture (KSI Technology)

2.9.5 Project Ubin: Monetary Authority of Singapore (MAS)

The Monetary Authority of Singapore (MAS) has initiated "Project Ubin: Singapore Dollar (SGD)," a distributed digital cash ledger project based on a Distributed Ledger in collaboration with MAS and R3. The participating banks in this project include BoA Merrill Lynch, Credit Suisse, DBS Bank, HSBC, J.P. Morgan, OCBC Bank and United Overseas Bank where the BCS Information Systems provides the necessary technology (http://www.mas.gov.sgp). The Ubin project supports MEPS+ payments that are RTGS systems which makes the transfer of interbank funds of larger valuations easier. Currently this project covers transactions within the Singapore region and it is expected to be extended to international level transactions in the next stage. Figure 20 depicts the high-level architecture of Project Ubin implemented by the Monetary Authority of Singapore (MAS).

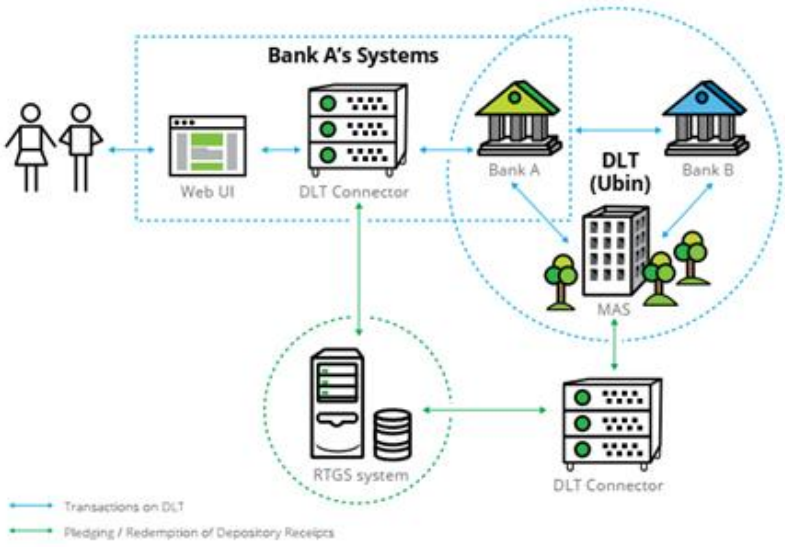

Figure 20: High level architecture of Project Ubin

2.10 Summary

The extensive analysis and comparative study of the various proposed e-governance frameworks is presented in this chapter. A detailed survey was carried out to understand how developed, developing and underdeveloped countries implement e-governance using Blockchain technology, as well as the challenges faced by the countries implementing it. From the literature review of e-governance using Blockchain technology on the issues and challenges related to it, it was found that none of the e-governance frameworks are completely apt for Saudi Arabia. It is advised to integrate the significant aspects of a fully functional e-government framework and to propose a novel e-governance framework that assimilates Blockchain technology for the security and safety of transactions in an e-governance framework. In this research, we have proposed and evaluated one such novel e-governance framework specifically for Saudi Arabia. The proposed methodology is presented in detail in the upcoming chapters with the aim of achieving the objectives listed in the earlier chapters.

Chapter 3: Research Methodology

3.1 Introduction

In the previous chapter, the available literature on e-governance, the threats to the security of information and the scope of using Blockchain technology to address security problems were discussed leading to the development of a framework for e-governance in Saudi Arabia in which Blockchain technology was incorporated. Most frameworks and models of e-governance have poorly addressed the issue, although the problem was at least mentioned by previous researchers. Some of the papers explored the scope of using Blockchain technology applications to ensure secure transactions and the protection of security. Some models were also suggested but there was a high degree of tentativeness to the whole approach. The protection of the security of the Saudi Arabian e-governance framework was found to be at a lower level compared to those of the USA and the UK when Blockchain technology was not used. In this chapter, the methods used for translating the framework into an actual e-governance system for use by the stakeholders are described. Figure 21 gives a flowchart of the work processes carried out in this work, it follows a rational, logical approach and process in a top-down manner as shown in the below figure.

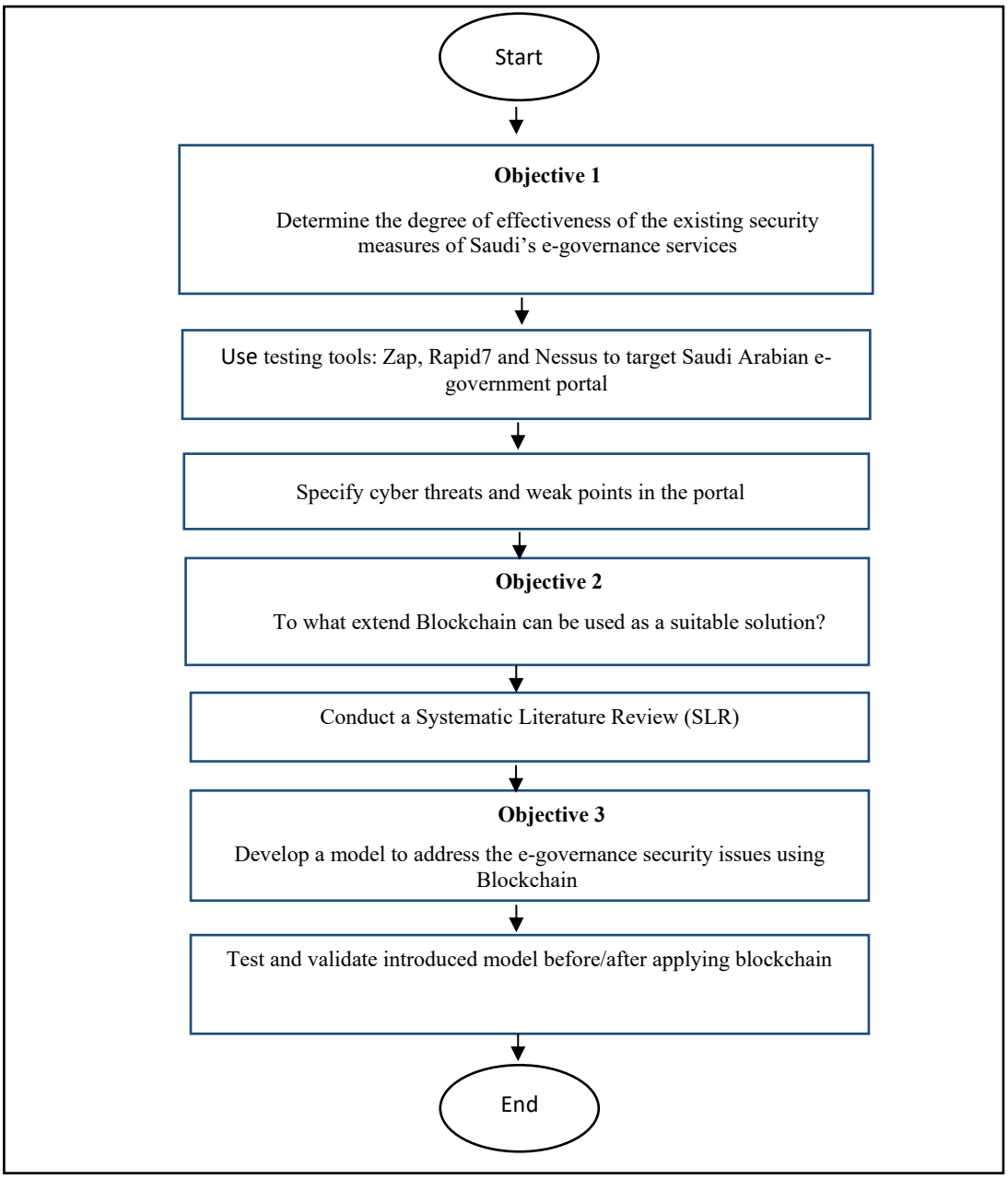

Figure 21. Research methodology processes

3.2 Overview of the Research Tasks and Proposed Approach

The methods of analysis used to address each objective are explained below.

3.2.1 Objective 1

Objective 1: To determine the degree of effectiveness of the existing security measures of Saudi's e-governance services

The first objective was achieved by the literature review. Some of the details of the UN survey of e-government systems in different countries (UN, 2018) have been discussed in the Introduction chapter.

The review of the literature was done using search terms like “e-governance”, “vulnerability of e-governance sites”, “Saudi Arabia”, “cyber threats in e-governance”, “trust in e-governance”, reliability of e-governance”, security and privacy of e-governance” and any other suitable terms. The databases of Eric, Springer, Sagepub, ACM, IEEE and others from the social sciences were also searched using the same terms. A large number of published works were obtained by these searches. The contents of the works relevant to this research were analysed and tabulated for use.

The modern method of governance is the e-government model. It has made effective use of information and communication technology to increase the transparency between the public and governments. The Kingdom of Saudi Arabia is looking for ways to implement new Blockchain technology that is both resilient and efficient as a form of e-government. It does, however, come at a price. The implementation of Blockchain technology in e-governments is confronted by a number of hurdles ranging from security concerns to privacy and scalability concerns. This study has examined and discussed the literature on the obstacles and issues that may arise as a result of the use of Blockchain technology. The findings revealed that the adoption of Blockchain technology by e-governments is limited owing to the lack of practical work. Besides that, a few articles have mentioned complex governance models and regulatory rules as impediments. In the Kingdom of Saudi Arabia and its adjoining regions, a lot of scientific studies have been performed to examine the advantages and concerns associated to a Blockchain-enabled e-government systems. Several studies have demonstrated the importance of the appropriate handling of sensitive data that is held by governments. Data manipulation, unauthorised access, identity disclosure and tampered data integrity are all hazards regarding the data possessed by governments around the globe. Despite the fact that Blockchain addresses this issue to a larger extent, it is yet to be fully adopted by countries around the world due to specific restrictions.

In his paper, Nakamoto (2008) coined the term and explained the concept of Blockchain technology as a safe and transparent platform that allows the government to function without the need for a central authority as a platform enabling citizens and governments to interact in a completely transparent manner. Another study by Ølnes, Ubacht and Janssen (2017) demonstrates the utility of Blockchain in the government and other government departments. The departments require technology that allows them to transmit information in a safe manner without the risk of unauthorised access.

In his paper, Al-Garni (2015) identified the hacking, software dangers and faults that Saudi Arabia's e-government systems face. There seems to be a lack of professionalism and knowledge, outdated

infrastructure and not enough regulations to efficiently utilise the e-government systems from the viewpoint of a common citizen looking to those services. Cyberattacks and scams in Bhutan, according to Choejey (2015), were caused by the inefficiency of the web security protocols. Alsmadi and Abu Shanab (2016) ran a test to demonstrate the ineffective security of the systems with the result that the majority of the websites were vulnerable to attack. In another instance, Al-Sanea and Al-Daraiseh (2015) put 150 websites from various areas such as education, health and finance to the test in order to assess the security of Saudi Arabia's e-government websites. Because of their inadequate configuration and programming, the sites were vulnerable to attacks according to the findings. Surprisingly, commercial websites were found to be more secure than government websites.

Riad et al. (2011) presented a comparative analysis of the e-government frameworks of Australia, New Zealand, India and Sri Lanka. The framework was presented in the New Zealand model as trend levels which consisted of the interactions between people and businesses via access channels, a common basis for all components as the layers of applications, regulations, standards, ICT, data and information and services. Sri Lankan layers are referred to as architectures and they include network, data and application. Various government functions are included in the application architecture. Through home computers and mobile devices, the Indian framework provided a middleware connecting the government service platforms and e-government partnerships with businesses and citizens. Furthermore, there are three primary layers to the Australian e-government framework. An interoperability layer exists for agencies such as the Commonwealth, state governments and local administrative councils.

To establish the degree of vulnerability of the Saudi Arabian e-government website (www.yesser.gov.sa) to cyberattacks, this study employed three penetration testing tools. Rapid7, Nessus and Zap are the three tools employed. The security testing tools are utilised because they make it simple to scan from an external IP address while evading the restrictions put forward by the local network. They also allow for the creation of reliable proof-of-concepts that demonstrate the risk of vulnerabilities. The Yesser website includes severe and medium-level vulnerabilities according to the findings. This experimentation demonstrates that the existing e-government framework has not been able to adequately handle a number of security and privacy challenges (especially in terms of trust, confidentiality and integrity). Although several researchers have worked to address the security issues in the e-government system, our research demonstrates that there are still certain gaps that need to be filled. Most of the existing frameworks and models, for example, do not reflect the critical e-government security requirements such as the distrust in online transactions and unlawful access to systems through insiders. The Yesser website in particular has

a few security concerns that are mostly classified as severe, medium and low-impact vulnerabilities, according to this work.

3.2.2 Objective 2

Objective 2: To find out the suitability of Blockchain as a solution to cyber threats and to achieve security in Saudi's e-governance services.

This objective was achieved by a review of the literature using search terms related to Blockchain technology, the application of Blockchain technology in e-government and how Blockchain technology enhances the protection of e-government sites for the purpose of security and privacy. The same methods of searching as given in Objective 1 will be undertaken here using these search terms. The literature collected will be used for content analysis and tabulation as above.

Because Blockchain is designed to be decentralised, it is an excellent contender for authenticating data and ensuring transaction integrity. Currently, the industry's methods for accomplishing this are not decentralised. Instead, they make use of the help of a trusted third party. Of course, this is a less-than-ideal system for accomplishing the intended outcome. How can we be certain that our trusted third party is really trustworthy?

Of course, the obvious answer is that the trusted third party can never be trusted completely. The system is vulnerable so long as we rely on a trusted third party. What if the third party isn't trustworthy at all and is actually malicious? What will happen in a case where the third party is compromised even though it was acting in a good faith? Both of these issues have obvious answers. If, for any of the reasons mentioned, a trusted third party is not trustworthy and the entire transaction that is based on that trust is in fact compromised, Blockchain truly shines in this type of scenario since it enables us to provide a way to ensure the validity and integrity of whatever we're trying to accomplish without getting concerned about jeopardising the integrity of the third party.

The adoption of the idea of "smart contracts" is one way to ensure transaction integrity. The purpose of smart contracts, as the name implies, is to facilitate the use of Blockchain to validate the contract signed by the two parties. The contract's contents would be given in the electronic version with both parties signing it digitally. In his approach, the Blockchain component would use it to validate that the contract's signatures are genuine. If necessary, the Blockchain may be utilised to resolve any disputes that may occur by confirming the validity of the digital signatures in a secure and decentralised manner (Abdelhamid and Hassan, 2019).

While the integrity and legitimacy of a transaction is vital in business transactions, they are probably even more important in the context of government functionalities. Blockchain-based systems and their integration with e-government will have a good impact when it comes to dispersing effective public services, cheaper transactions and a problem free way for individuals to communicate with the government. It provides a variety of services ranging from education to healthcare services and from businesses to centralised citizen information systems. Physical interactions and the response time are kept to a bare minimum. The e-government services merged with a Blockchain are responsible for ensuring safe data transmission, e-voting, tax return filling and the identification procedure, to name a few. The sole objective is to digitally combine the public services and reduce the weight of bureaucratic tasks, all while maintaining confidentiality and security. As per our analysis of the literature based on Blockchain e-governance, public sector operations can be studied at three levels: micro, meso and macro. In our opinion, governance policies at one level do not exist independently; they are interrelated. Governance practises at all three levels are interconnected within public administration and it is difficult to predict any degree of governance without having a proper understanding of the others. Some research focuses on the use of Blockchain to achieve policy goals in governance. The objectives of these policy goals include public participation, the role of the media and value exchanges among social, political, economic, legislative and business organisations (Hsieh, Vergne and Wang, 2017; Meijer and Ubacht, 2018; Paech, 2017). These features are not counted as a discrete category in the paradigm but they are presumed to be influencing factors at each level of governance due to their extensive importance. Decisions taken at one level have an impact on other levels in this system. In a Blockchain network, the distribution of tasks plays a role in the decisions taken by any government body. Centralised, semi-centralised, decentralised and polycentric governance structures are the four types of governance structure. The term "centralised" refers to a form of government in which decision-making is delegated to a group of people or an institution. In semi-centralised governance, a centralised management board makes only a few decisions, while the other decisions pertaining to governance are determined completely on the basis of the platform’s user vote. As a result, Blockchain is seen as a unique technology that can help with the robust and automated dispersion of most administrative services, as well as better transparency and e-government.

The incorporation of Blockchain into e-government systems has attracted a lot of attention. However, it continues to face numerous unsolved problems, providing researchers with the opportunity to investigate and contribute to future research gaps in this domain. Several papers confirm that the public sector domains have little interest in incorporating Blockchain into their systems. One reason could be because there isn't much experimental proof in this area yet. As a result, more work must be done to persuade

governments to employ Blockchain in e-government systems. The literature research revealed that there are still numerous technological difficulties to be addressed including reliability, security, interoperability, configurability and scalability. However, it is unclear as to what extent these challenges will demand improvisation. As a result, there is a critical need to set technological standards in Blockchain and to carefully determine their design characteristics in accordance with the objectives of the public sector. Furthermore, Blockchain has gained a lot of attention recently and there are no clear standards stating that Blockchain is the best solution, particularly in terms of e-government applications. As a result, a strategy is needed to examine the acceptability of Blockchain technology as a solution based on a a logical understanding of public processes, regardless of where it is implemented. This will lead to the creation of Blockchain design protocols that take into account the technological and organisational aspects of such operations.

3.2.3 Objective 3

Objective 3: To develop a model to address the e-governance security issues using Blockchain design with validation through implementation

This section highlights the implementation of a secure scheme for Saudi e-governance that uses Blockchain to protect e-governance services in order to meet study objective 3.

Flexibility, scalability and security are among the hurdles impeding Blockchain implementation in e-governance, according to Carter and Ubacht (2018). The problems are related to acceptability and the need for a new governance model from an organisational viewpoint. Meanwhile, the greatest difficulty from the perspective of the environment is a lack of laws and regulations. The lack of an entire application framework where the scalability, reliability, flexibility, security and interoperability of Blockchain for e-governance systems is addressed necessitates the creation of an appropriate design solution. Furthermore, the implementation of Blockchain technology will result in major organisational transformations in terms of process, culture, strategy and structure.

According to Heng (2017), the use of Blockchain technology in the e-government system of China has several advantages, including greater access to and transparency regarding the government data, improved quality and quantity of government services, and improvements in information dispersion across the different organisations. However, the system still has issues with reliability and data security.

As a result, it is critical to design a generic application platform for Blockchain, as well as management standards, to ensure that the Blockchain is effectively integrated into the e-government system.

Because of the many reasons addressed thus far in this analysis, e-government systems are vulnerable to internal and external threats and attacks. It is vital to keep an eye out for such threats and to take proper countermeasures. Based on this, we have proposed a framework that integrates Blockchain technology with e-government in Saudi Arabia for the system and users' security protection. This is a direct response to study objective 3.

Saudi Arabia's existing e-government platform (Yesser) uses a centralised database, resulting in a lower degree of confidentiality and distrust (Al-Mushayt et al., 2012). Because it is entirely based on a decentralised database, the proposed architecture provides more security. The proposed framework leverages Blockchain to secure e-governance, using Saudi Arabia as a case study. The proposed model brings in decentralisation, access control, confidentiality, privacy and trust into the e-government services. The researchers have not leveraged Blockchain technology to secure the Saudi e-government system in the past.

3.3 Summary

The methodology of this research has been described as per the objectives so then the findings can be connected to the achievement of the objectives in response to the research questions and the aims of tis research. The first and second objectives can be achieved using the literature review and the third one is implemented to achieve security. For all LR works, suitable search terms relevant to the specific objective were used in the search engines and databases. Content analysis was done to extract the relevant information from the collected literature. Implementation at the researcher level to test whether the required security enhancements worked was achieved by the proposed model compared to the current model.

Chapter 4: Risks and Vulnerability Assessment of the E-Governance Framework

4.1 Introduction

Technology has shaped the world and turned the universe into a global village. The developments in information technology have cut across both public and private sectors. Basically, the integration of IT into business to provide public services online as well as to increase the government's efficiency is called e-government. However, as promising and as great as e-government is, it faces the challenge of cyber threats. According to Rehman et al. (2016), concerns about cyberthreats have affected the user acceptability of e- government systems. Users perceive that hacker(s) or third parties may have access to confidential information like their credit card details. Meanwhile, it is the government's responsibility to protect the user data and strengthen the e-government system against any form of security threat.

The primary aim of e-government is to make the government services more seamless, efficient, and timely for every citizen and organisation. However, e-government systems are now faced with security threats and cyberattacks, and these challenges have raised concerns about their users' privacy as well as the confidentiality and integrity of the user data.

End users encourage the e-government structure to ensure that the online government services are comfortable to use by avoiding long waits in queues which saves both time and money. It was observed that communication between the government departments is far better than any private business network as many of them are connected and do not need to compete with each other to provide information to the end users. The fast evolution and adaption of smart technologies includes smartphones, IoT (Huh et al., 2017), smart homes (Dorri et al., 2017), smart societies, smart cities and other organised networks will certainly increase the use of e-government services (Biswar and Muthukkumarasamy, 2016; Yang et al., 2018). The most commonly observed threats by the countries implementing the e-government set-up are Denial of Service (DoS) and malware directed against the network (Pau, 2010). During the year 2015, the US government observed the disclosure of confidential information related to social security numbers, passwords and security clearance information for almost 5 million government employees (Cryptomathic, 2015).

The key features of an e-government setup:

1. Safe: Prior authentication of the nodes and users of the network.
2. Secured: Authenticated users have enough control over the information.
3. Scalable: New nodes (easily added to the network) automatically follow the consensus mechanism of the network.
4. Reliable: Distributed data storage
5. Resilient: The e-government system is robust against single point failure.
6. Auditable: Accessing the previous version of the network is effortless.
7. Verifiable: Every node verifies each transaction in the network.
8. Right to information: Users on the network have the authority to authorise users to access their information.
9. Quality data: Only validated information is stored in the system.
10. Transparent: The transaction information shared by the nodes is identical.
11. Low operational cost: No need for a third party in place.
12. Fast and efficient: Anyone who is authenticated is eligible to add new records to the network.

Currently, e-government websites and eID management systems implement centralised database systems which store and retrieve the information requested by the user (Seltsikas and O'keefe, 2010; Ali et al., 2014). It should be noted that centralised databased management systems are highly vulnerable to DDoS, DoS and malware attacks. Therefore, a e-government system implementing a centralised database structure becomes highly vulnerable to attacks and needs to adopt better and reliable security measures. A Blockchain technology framework can be public (permissionless) or private (permissioned) (Swan, 2015). A public Blockchain allows every user over the network to create, join, and participate in the network activities whereas a private network restricts the number of nodes able to join the network.

It is observed that for 51% of the attacks, phishing, sybil and routing are four very crucial ways that a hacker will try to get unauthorized access to the information in the Blockchain. It is necessary to secure the Blockchain design as well as its environment. Svein and Arild (2017) noted that Blockchain technology can be easily mastered, adopted, and adapted by many people. The study revealed that Blockchain technology is now an emerging technology for new innovations and development, not only in the financial systems but also in government agencies and organisations.
The specific objectives achieved in this chapter include the following:

a) To determine the degree of vulnerability of e-government services to breaches of privacy, trust, confidentiality and security.

b) To determine the degree of vulnerability of the Saudi e-government system (Yesser) to cyberattacks.
c) To propose a new framework that can secure the Saudi e-government system.

In this chapter, we take a closer look at identifying the vulnerabilities and risks associated with the present e-government systems around the world. As an example, case study, we have looked into the e-government system created and implemented by the government of Saudi Arabia. In Saudi Arabia, the government has embraced a new technological era in which technology is utilised as an instrument to make communication, government services and connectivity more seamless. Saudi's e-government system, Yesser, is pivotal in the realisation of the Saudi Vision 2030. As a result, it is important that the Yesser website has adequate security. This chapter aimed to determine the level of security of the Yesser website by utilizing three penetration test tools to scan the website. The tools included Zap, Rapid7 and Nessus. Based on the analysis, this chapter proposed a new framework for use by Yesser. However, in this chapter, we also assessed the degree of risk and vulnerability associated with the websites used for e-government functions. The results show that the Yesser website does not have critical vulnerabilities but has severe and medium-level vulnerabilities. This chapter presents a new framework which can be based by the Saudi government system.

4.1.1 Vulnerability of e-Governance Services

It is necessary for the e-government framework to achieve and maintain the confidentiality (authorised information sharing), integrity (information protection) and availability (information retrieval) of the services that are also safe from and secure against vulnerabilities. Records are protected using public key cryptography which provides the security and identifies unauthorised access, whereas the other nodes on the network have private keys for approving transactions. Furthermore, an attacker needs at least 51% of the network nodes in his/her favour to modify a record in the Blockchain, which is almost impossible to achieve (Swam, 2015). All of the nodes over the Blockchain framework are hashed and an incomprehensible hash is stored for every transaction in the Blockchain.

According to AlGarni (2015), hacking, terrorism and software error constitute the major types of vulnerabilities of Saudi e-government systems. On the part of the government and employees dealing with e-government services, there were found to be issues like a lack of professionalism and accountability, poor IT infrastructure, a lack of awareness of security perspectives at the customer level, and inadequate laws and policies guiding the e-government services.

Choejey et al. (2015) noted that the lack of or limited use of a standard web security policy and risk

management practices have led to cybersecurity threats like malware, phishing scams and hacking in Bhutan. Alsmadi and Abu-Shanab (2016) used Rapid7 security and penetration testing tools to explore the vulnerabilities of major e-government websites in Jordan. The outcomes of the tests carried out indicated that most of the websites are prone to attacks.

Also, having realised that only a little effort was made in the direction of evaluating the security level of Saudi Arabia's e-government websites, Al-Sanea and Al-Daraiseh (2015) assessed 150 websites owned by financial, governmental, academic, and commercial organisations. The paper noted that the vulnerabilities in e-government websites are caused by the wrong configuration, weaknesses in the programming, or a lack of updates. The results of the assessment revealed that the websites are faced with low, medium, and high impact vulnerabilities. For instance, 61% are vulnerable to clickjacking, 17.5% are vulnerable to SQL injection and 13.5% are vulnerable to shell injection. Based on the number of vulnerabilities found, a comparison was made between government and commercial websites. The result of this comparison showed that commercial websites are more secure than government websites.

Using tools like Google Speed Insight, Pingdom, Acunetix and w3c Checker, Elisa (2017) assessed the accessibility, usability and web security vulnerabilities of 79 e-government websites in Tanzania. The outcomes for the presence of web security vulnerabilities showed that 40 (50.6%) out of the 79 websites assessed had one or more high-severity vulnerabilities (cross site scripting-XSS or SQL injection) while 51 (64.5%) had one or more medium severity vulnerabilities (Denial of Service or Cross-site request forgery).

Bissyandé et al. (2015) carried out an empirical assessment of e-government website security in Burkina Faso. A systematic scanning of the sample websites for simple and well-known vulnerabilities showed that there were serious security issues calling for urgent attention. For example, it was possible to crawl all information (including hostname and password) from the temporary backup files on a government website to thus read and write directly into the database, thereby impersonating the website's administrator.

Murah and Ali (2018) evaluated 16 Libyan e-government websites using a penetration testing framework. Content analysis was also carried out to determine how far the privacy and security policies on the websites have been implemented. The results of the testing revealed that nine out of the 60 websites have high to medium vulnerabilities. Most of these vulnerabilities were due to the misconfiguration of the systems and the use of outdated software. Only two of the websites had their privacy and security policies published on their websites.

Pandya and Patel (2017) explored the relationship between technology in relation to the vulnerability severity and vulnerability types found in 26 e-government applications and websites from Gujarat, India.

Most of the websites made use of Microsoft technology while some used Apache technology. It was observed that there were more medium to low vulnerabilities found on the websites using Apache technology compared to those using Microsoft technology. Meanwhile, informational vulnerabilities and validation-type vulnerabilities were higher in Microsoft technology than Apache technology.

4.2 Analysis Methods

This section provides the complete analytical study that was carried out in this chapter to evaluate the e-government framework adopted by the government of Saudi Arabia. Keeping the analytical report in mind, a novel Blockchain based e-government system is proposed for Saudi Arabia (the upcoming section discusses the proposed framework in detail).

4.2.1 PRISMA format for a Systematic Literature Review (SLR)

To determine the degree of vulnerability of e-government services to breaches of privacy, trust, confidentiality and security, this research leveraged the outcomes of the existing related literature by carrying out a Systematic Literature Review. The SLR follows the PRISMA format (Mohrer, 2009). The steps adopted include a Database Search, the use of an Exclusion and Inclusion Criteria, Quality Evaluation and Data Analysis. The search sources used were EBSCO Information Sciences (www.ebsco.com/), IEEE Xplore (www.ieexplore.ieee.org/Xplore/), Elsevier ScienceDirect (www.sciencedirect.com/), and Google Scholar (www.scholar.google.com.au/). The search terms entered into the databases include "e-government frameworks", "effectiveness of e-Governance", "cyber security of e-Governance systems", "Blockchain technology," and "Blockchain in e-Governance."

4.2.2. Use of penetration testing tools on Yesser's website

This research leveraged three penetration testing tools to determine the degree of vulnerability of Yesser's website (www.yesser.gov.sa) to cyber threats and attacks. The three tools used included Rapid7, Nessus and Zap.

These penetration testing tools were used because they make it easy to bypass the local network restrictions to scan from an external IP address. They also make it possible to create reliable proof-of-concepts to prove the risk of vulnerabilities. After scanning the Yesser website using each of the three tools, the results were collected and analysed.

4.3 Results and Discussion

In this section, we discuss our research findings that directly address the three research questions mentioned in Section III of this chapter. The first research question relates to our finding following the analysis of various works on the e-government approach adopted by different countries. This gives us the scope to move to the next research question in which we demonstrate how different penetration tools are being used to assess the risks and vulnerabilities of one specific e-government website, Yesser. Based on our findings, we then propose a new e-governance framework to address our third research question.

4.3.1 PRISMA format for a Systematic Literature Review (SLR)

After the search terms were entered into the search sources, 138 papers were identified. Out of these papers, 36 duplicates were found, thereby reducing the number of papers to 102. The remaining papers were then screened to determine their relevance based on the titles, abstracts, and full texts. At the end of this screening, 66 studies were eliminated resulting in 36 articles. These 36 papers were then evaluated for quality and the result was the 10 papers that were ultimately included in this SLR.

Table 7: Summary of the papers on security in e-governance

Paper	**Description**	**Method**	**Weakness & Limitations**	**eGov Security Requirements**		
				Confidentiality	Trust/ Privacy	Integrity
Zhao, J. and Zhao, S. (2010)	Carried out an assessment of e-government sites owned by the United States to look for the opportunities and threats that the sites offer to the users. Less than half of the sites clearly stated their security measures and 98% of the sites used SSL encryption to secure its user accounts.	Information security auditing, computer network security mapping and web content analysis.	The paper identified a lot of security lapses but failed to provide solutions for all of them.	No	Yes	No
Alshehri, M., and Drew, S. (2010)	The paper identified the challenges and barriers affecting the adoption of e-government by Saudi citizens.	Online survey and data Analysis.	The paper did not explore the security requirements of e-govt. in detail.	Yes	Yes	No
Bertot, J., et al. (2014)	The paper examined the ways that the current information policy framework failed to address different	Survey.	The paper is limited to the US only.	No	Yes	No

Paper	Description	Method	Weakness & Limitations	eGov Security Requirements		
				Confidentiality	Trust/ Privacy	Integrity
	policy challenges in relation to e-government. The paper then offered recommendations as a starting point to revise the policy.					
Rehman, M., Esichaikul, V., and Kamal, M. (2012)	The study explored the factors that promote the end-user adoption of e-government services in Pakistan. The factors revealed by the findings include user data privacy, performance expectancy, awareness and social influence.	Unified Theory of Acceptance and Use of Technology (UTAUT) model. Online survey. Statistical descriptive analysis.	The data sample used was small as the survey had only 115 respondents.	No	Yes	No
Rodrigues, G., Sarabdeen, J., and Balasubramanian, S. (2016)	The research identified the factors that influence the adoption of e-government services in the UAE. The factors identified include confidentiality, user attitude and trust.	UTAUT model, Exploratory factor analysis, regression analysis and correlation analysis.	The study failed to provide the ways that the factors identified can be addressed.	Yes	Yes	Yes
Osman, I. H., Anouze, A. L., Irani, Z., Al-Ayoubi, B., Lee, H., Balcı, A., and Weerakkody, V. (2014)	The study proposed a COBRAS (Cost; Opportunity; Benefit; Risk; Analysis for Satisfaction) framework which balances the user's risk and cost of engaging with an e-government service with the associated opportunity and benefit.	Proposed the COBRAS framework. In total, 79 questionnaires were filled from among the 2785 users of the Turkish e-govt portal. Utilised structural equation modelling and confirmatory factor analysis.	The security requirements of e-governance were not thoroughly explored.	No	Yes	No
AlKalbani, A., Deng, H., and Kam, B. (2015)	This examined how organisational security culture affects information security compliance in public agencies and organisations in terms	Developed an information security model and hierarchical	No insight was provided on how to improve accountability,	Yes	No	Yes

Paper	Description	Method	Weakness & Limitations	eGov Security Requirements		
				Confidentiality	Trust/ Privacy	Integrity
	of e-government development. The study showed that information security awareness, accountability, social pressure and management commitments positively influence information security compliance in public organisations.	regression analysis.	information security awareness and management commitments which were the factors identified to have a positive influence on information security compliance.			
Gabriel, B. (2018)	This paper assessed the level of public trust and confidence in the integrity of the data and systems exchanged on Ghana's e-government platform, with a specific focus on data protection and integrity. The study showed that there is a huge weakness concerning the issues of confidentiality, the continuous availability of services and the data integrity of e- government platforms.	Cross-sectional survey with respondents drawn from four regions with a high concentration of e-government services.	While the study identified major challenges that need to be addressed like a lack of a national database to verify information, service exclusion, poor internet etc., it did not provide any solutions.	Yes	Yes	Yes
Mohamed, R. and Rajandran, K. (2017)	The study examined the cause of low participation in e-governance in Thanjavur district and found out the causes include level of awareness, acceptance, attitude towards sustainable development and the securityof e-governance.	120 respondents selected on the basis of random sampling, regression and correlation analysis.	The sample is small; the study noted that e-government web security needs to be improved but did not state the specific improvements to be made and how.	No	Yes	No

Paper	Description	Method	Weakness & Limitations	eGov Security Requirements		
				Confidentiality	Trust/ Privacy	Integrity
Haran, M. (2016)	This study identified the relevant stakeholders who are insiders as far as the e-government IT infrastructure is concerned. It listed the threats that may be caused by said insiders. The paper then provided ways to mitigate such threats.	Proposed a robust framework mechanism for the early detection and mitigation of insider threats.	The paper is limited to insider threats alone.	No	Yes	No
Choejey, P., Fung, C. C., Wong, K. W., Murray, D., and Xie, H. (2015)	An assessment of the factors affecting the implementation of a cybersecurity program in government agencies in Bhutan. The research showed that several organisations are affected by cybersecurity threats like hacking, phishing scams and malware. The recommendations provided include technological and managerial practices to improve people's level of confidence and trust in e-government services.	Survey with 157 respondents.	The sample for thesurvey is small.	Yes	Yes	No

4.3.2 Use of three Penetration Testing tools on Yesser's website

We used three different penetration tools - Rapid7, Zap and Nessus - to analyze the risks and vulnerabilities associated with e-government websites.

- Rapid7

The Yesser website was scanned using InsightVM from Rapid7 LLC on February 24th, 2020. The website was found to be active and its vulnerabilities by severity are represented in Figure 22. The vulnerabilities by severity are divided into three categories: critical, severe, and moderate.

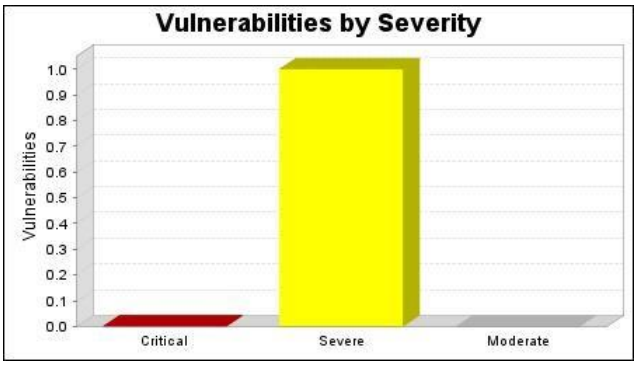

Figure 22: Yesser's Vulnerabilities by Severity

As shown in Figure 22, there were no critical vulnerabilities found during the scan of the Yesser website. Also, there were no moderate vulnerabilities discovered. However, there was one severe vulnerability. The severe vulnerability detected was where the subject common name (CN) field in the X.509 certificate was different from the name of the entity providing the certificate.

Referring to the vulnerability categories, the Rapid7 scan found one vulnerability instance each in the HTTP and Web categories, thereby making them the most common vulnerability categories as shown in Figure 23. HTTP and HTTPS services were both found on the Yesser website, making them the most common services (Figure 24).

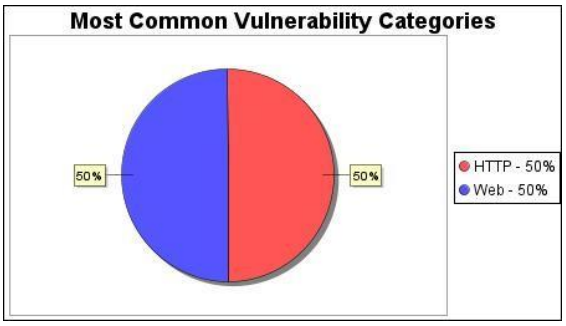

Figure 23: Yesser's Most Common Vulnerabilities

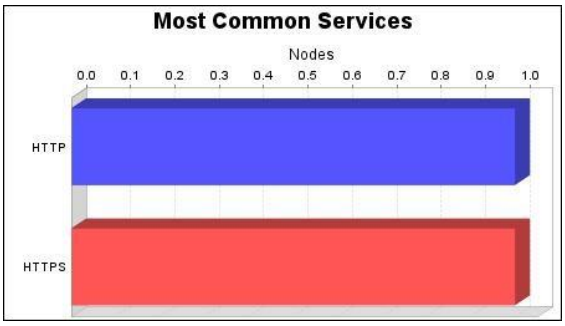

Figure 24: Yesser's most common services

- Zap

The Zap scan of the Yesser website was carried out on June 13th, 2020. The summary of the scan is provided in Table 8 below.

Table 8: Summary of the Zap Scan of the Yesser website

Risk Level	Number of Alerts
High	0
Medium	1
Low	10
Informational	2

The medium alert received showed that the X-frame options header is not set. The simple solution to this is to ensure that the X-frame options HTTP header is set on all pages on the Yesser website. The low impact vulnerabilities detected by the scan include an Absence of Anti-CSRF Tokens, Cookie Without SameSite Attribute, Cross-Domain JavaScript Source File Inclusion, Cookie Without Secure Flag, Cookie No HttpOnly Flag, Web Browser XSS Protection Not Enabled, Incomplete or No Cache-control, Secure Pages Include Mixed Content, and Private IP Disclosure.

The following are the two informational vulnerabilities that were detected by the scan:

a) Information Disclosure - Suspicious Comments. The solution to this is to remove all comments that return information capable of solving any underlying problems.
b) Timestamp Disclosure – Unix. Here, the solution is to manually confirm that the timestamp data is not sensitive and thatthe data cannot be aggregated to disclose exploitable patterns.

- Nessus

The Nessus penetration test tool was used to scan www.yesser.gov.sa on February 24th, 2020. The

results (Figure 25) show that there were no critical or high vulnerabilities on the Yesser site. However, two medium-level vulnerabilities were found and 22 informational vulnerabilities.

Figure 25: Results of the Nessus Scan of the Yesser Website

The first medium vulnerability is F5 Big-IP Cookie Remote Information Disclosure. The remote load balancer suffers from an information disclosure vulnerability. The second medium vulnerability is that the web application is potentially vulnerable to clickjacking.

4.3.3 Proposed e-Governance Framework

E-governance systems are vulnerable to external and internal threats and attacks for various reasons as discussed before in this review. Watching for such attacks and taking appropriate remedial steps is necessary. Based on this, we have proposed a new framework which can be integrated into e-governance for the security and protection of the system and users as shown in Figure 26.

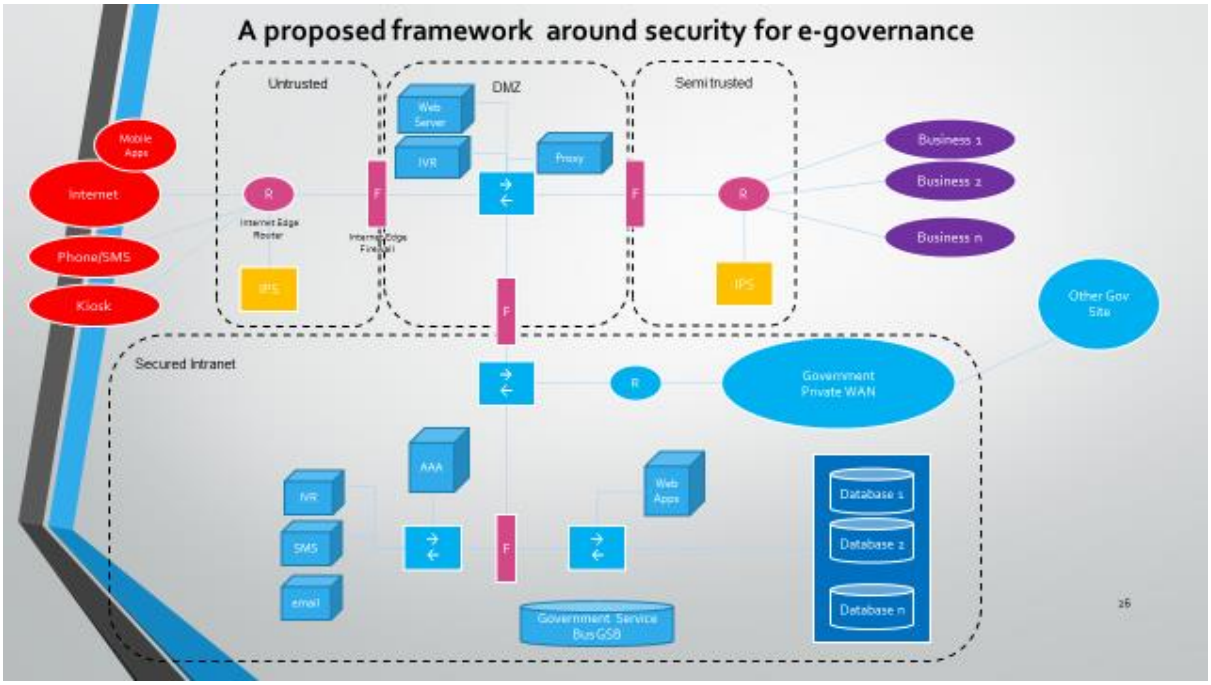

Figure 26: A proposed framework for e-governance

4.4 Summary

The study presented in this chapter explores most of the existing literature on securing e-Government systems in different countries. Our study reveals that there are several security issues (particularly regarding confidentiality, trust, and integrity) which the existing e-government frameworks have not been able to address thoroughly. While many researchers have made an effort to address the security challenges in different e-government systems, our study shows that there are still some loopholes that need to be blocked. For example, most of the existing frameworks and models do not capture the necessary e-government security requirements, they have a lack of trust in internet-mediated transactions and there is the potential for unauthorised access to systems with the help of insiders. This paper shows that the Yesser website has a few security issues which are majorly categorised as severe, medium-level, and low-impact vulnerabilities. This chapter also proposed a new framework to secure the Saudi e-governance system. This proposed model brings in an easy information flow, improved access control, confidentiality, and trust into the e-governance services.

Chapter 5: Use of Blockchain in E-Governance Framework

5.1 Introduction

TRANSFORMATION and reorganisation across public sector domains can be navigated by making use of the latest technological advancements. ICT (Information and Communications Technology) can be pivotal when it comes to improving the public sector domain and it is often referred to as e-government. [1] The e-governance system is extremely useful at making government services available to citizens and private organisations efficiently. It has contributed tremendously to the governance of the state machinery and emerged as an effective and efficient tool for citizens and businesses. Apart from offering an easier approach to the information held, e-government provides efficient and transparent services [51]. A fully developed ICT system integrated with e-government services is the predictor of a country's holistic growth [52]. With the advent of technology in every field, it is necessary for governments to digitise their public sectors and to ensure that they provide the utmost accountability and transparency. E-government is the most hailed practice of modern times that has dynamically shifted the structure and working of organisations around the world. It's not just a communicating link between citizens and the public sector. It is comprised of households, firms and the government. E-government is now seen as a stepping stone towards a positive change in the way that government systems work. It's the much-needed basic change that has affected the already used methods, the approach towards the public sector and has influenced cultures and values alike. Government systems need to make full use of the resources and information and technology tools that are handy, all of which can ensure effectiveness, correctness and timely information delivery [61].

To achieve the already set standards of information dissemination and to maintain the decorum of security, Blockchain seeks to establish quite a developed infrastructure and extensively used security protocols. Ensuring the security of the data is the fundamental job of the Blockchain regarding e-government. Security has to be the primary goal and no element should be allowed to compromise this. Since the information is accessible to all, anyone on the network can access it illegally. This issue of Blockchain needs to be addressed while it is being implemented.

The e-government system can be categorised into three forms viz. the one that links citizens directly to the government (G2C), the one where employees directly connect with the government (G2E) and the last one where the government communicates with the government (G2G) [62]. This system could prove

to be of much use but it has more complexity than usability. It has its share of challenges and limitations as well. Many countries along with Saudi Arabia have made use of these technologies but all of them are still in their nascent stages of adoption. However, e-government websites are facing various setbacks caused by several information security breaches. To address the security lapses in e-government, several researchers have proposed the use of Blockchain to secure the e-government system. Reference [2] demonstrated that the e-government improved when using Blockchain and decentralised autonomous organisations (DAOs) for government contracting. He introduced the concept that using Blockchain made the service immune to both internal and external attacks. In addition, the program ensured that the operations would be controlled by predefined rules, thereby reducing the number of uncertainties and errors caused by human intervention.

Gordon [3] leveraged Blockchain to prevent potential breaches of data privacy and security in e-government healthcare services. They noted that data integrity is being undermined when the data traverses through unknown communication networks. As a matter of fact, malicious attackers may exploit these security flaws to compromise the valuable information sent by healthcare providers through the healthcare network. To solve the problem, they proposed five mechanisms based on Blockchain. These included digital access rules, data aggregation, data liquidity, patient identity and data immutability. By using Blockchain, the paper noted that the privacy and security issues faced when handling e-government data in healthcare became extremely low. In Saudi Arabia, the kingdom operates an e-government system called Yesser. Reference [4] assessed the degree of vulnerability of Yesser by carrying out a penetration test using three tools, Rapid7, ZAP and Nessus.

The outcome of the tests showed that Yesser is prone to severe and medium-level vulnerabilities. Can the Kingdom of Saudi Arabia utilise Blockchain technology to secure its e-government service? This is the major question to be answered as this paper takes a deep dive into the subject matter.

5.2 Blockchain and e-Governance

Unlike a traditional database, Blockchain stores the data in a decentralised form in blocks. These blocks, once full, are connected to each other through chains. It was introduced by [5]. Although a variety of data can be stored in Blockchain, it found its first use in cryptocurrency with being a ledger for transactions being the most common so far. These decentralised Blockchains are then distributed across peer-to-peer networks [6]. The blocks in the network have unique identifiers which are attached to the blocks as headers. The block headers store information such as the timestamp, transaction details and contents of the block. The transactions in the Blockchain of cryptocurrency are those of records, contracts and other

information [7]. Like a traditional public ledger, Blockchain is a series of blocks that carry a comprehensive list of transaction information. A block has just one parent block if the block header contains a preceding block hash. The hashes of previous blocks would likewise be preserved on the Ethereum Blockchain. The genesis block is the initial block in a Blockchain that has no block prior to it. Each node in a public Blockchain might engage in the consensus protocol. In a consortium Blockchain, only a limited number of clusters are accountable for maintaining the block. In the perspective of the private chain, one organisation is accountable and has complete control of the situation and can make a final decision [55]. There are three types of Blockchain systems now in use: public Blockchain, private Blockchain and consortium Blockchain [57]. All records are exposed to the public in a public Blockchain, and any user can engage in the process of negotiation. In contrast, just a small number of already selected nodes are able to take part in a Blockchain's consensus process. Unlike public Blockchains, in private Blockchains, only the nodes that are part of the same Blockchain are made to participate. The major distinction between the three types of Blockchains is that public Blockchains are decentralised, consortium Blockchains are somewhat consolidated and private ones are completely consolidated because they are managed by a single entity [55]. Maintaining and registering land records is one of the potential government applications of Blockchain, along with its use in the education health sector and information and communication systems. Kirkman and Newman (2018) offer a block-chain-based land management mechanism which stores information about the lands, the details of its owner and mortgage status if any; all of this is stored and made public. Usually governments work in isolation and fail to share data, retaining only redundant information. Blockchain has made it easier to maintain and share all information and data related to its stakeholders. This publicised information across the departments improves the operational success, effectiveness, transparency, responsibility and decisiveness [60].

In the case of cryptocurrencies, Blockchains store data in such a way that the data does not remain confined to a single user. In fact, all users can have access at a single instance in time, owing to the distributed nature of Blockchain [6]. By making use of public and private keys, Blockchain can ensure some amount of privacy. The end users would make transactions with the private and public keys assigned without revealing their true identities. Both permissioned and permission-less ledgers confront problems such as responsibility for the participant’s duties and the terms of usage as well as ownership for automatic permission execution by the ledger; and so on owing to the user's position (particularly in the case of anonymous users). The ledgers in those Blockchains are maintained in such a way that every update in the form of a transaction and any other digital event whatsoever is to be recorded and validated using certain consensus mechanisms. These mechanisms have certain rules set that ensure that there is no meddling with the transactional data [7]. Based on different attributes such as the time taken to

complete a transaction, energy regularisation, configurability and oversight, the Blockchains have varying advantages and disadvantages. Since there are many nodes available on the network, if a transaction that takes place between the nodes is valid, a timestamp is applied. The Blockchain stores the current time, in the form of a timestamp, of the moment when the block was being mined and validated by the network. The newer blocks are linked to older blocks using a hash pointer as a link [8]. Blockchains, apart from being decentralised, are inflexible and not open to transaction reversal. This feature of decentralisation in Blockchains provides a secure, resolute and impervious policy for transactions to take place directly, following the core concept of Blockchains [9].

The major aspects involved when using Blockchain are presented in the figure below.

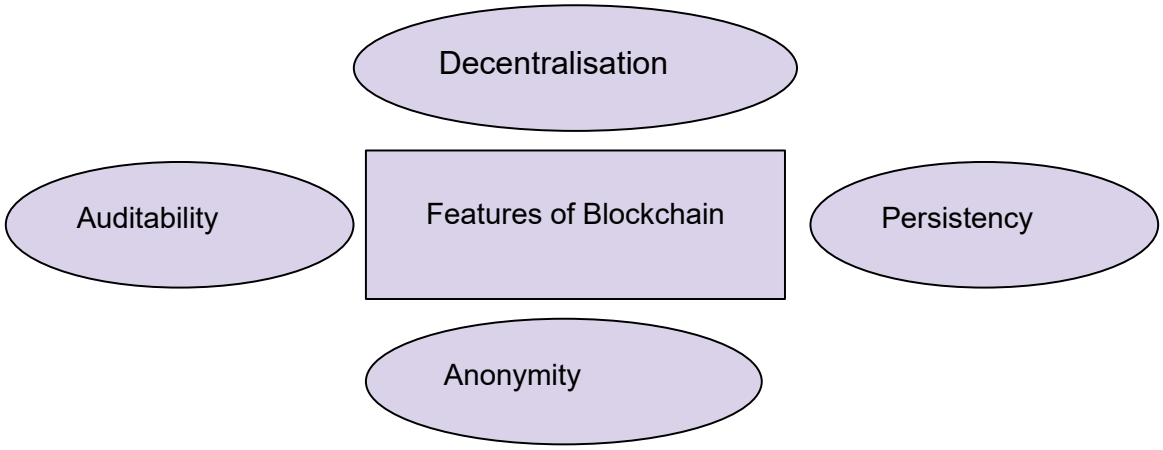

Figure 27: Overview of the features of Blockchain

5.2 1 Decentralisation

Decentralisation is the main feature of Blockchains. Decentralisation in Blockchain technology includes the dispersion of services across a network instead of having all elements connected to a centralised authority. There is no single point of control and this is what makes Blockchain highly secure compared to other technologies. A unique transaction account is provided to each Blockchain user, known as a miner, and more blocks are created once the miners have been validated. Blockchain technology's revolutionary quality is exemplified by the decentralised nature of the data records that it uses; Blockchain networks employ consensus procedures to safeguard the nodes. Every transaction gets validated and in no way can the data be altered. Decentralisation in computer networks has actually shifted the typical architecture of the client-server model to a node-to-node network wherein all nodes have equal

importance and niches. This is shown in the application layer in the Blockchain and makes use of the consensus protocol. Even public Blockchains networks that don't require any permission to freely play and join are somewhat decentralised based upon the nodal neighbours that each node has created in the network. These nodal connections affect the propagation of the transactions on the network. Since the Blockchain is scattered over the network, every transaction must be validated by each node on this network and all the nodes have a record kept of the ledger already [10]. This makes the whole process of using Blockchains fault tolerant and protected from government meddling, rendering any third-party interference useless, ensuring faster transactions, maintaining data consistency and integrity and lastly creating attack resistance. Despite being decentralised, Blockchain data seldom loses its credibility owing to the consensus algorithms used.

5.2.2 Persistency

A distributed or dispersed Blockchain is rigid and unyielding. The transactions, once recorded, cannot be rolled back. Blockchain provides better clarity and lucidity for projects that are large enough to keep a record of. No invalid transaction is entered by the Blockchain, and any transactions that are already added are impossible to delete, copy or edit, thus maintaining the integrity of the data. Since many people retain control of the data in these Blockchains, data consistency is a must. Once a transaction is incorporated into the Blockchain, it is hard to erase or rewind the transaction. Blocks containing incorrect transactions might be identified right away.

5.2.3 Anonymity

The users on the Blockchains have unique codes called public keys. Whenever a user makes a transaction, the public key is recorded into the Blockchain and not their personal information, thereby securing their identity and maintaining anonymity. Confidentiality is a very much sought-after feature of Blockchains and that of cryptocurrencies for that matter. The creators of [58] choose the intrinsic data integrity of Blockchain technology which guarantees that the stored data is resistant to mutation or deletion, with the intention of promoting privacy. It opens up the door to the idea of a future Blockchain that has the provision to change or eliminate transactions in a safe manner while keeping the identity of the individuals involved anonymous. It provides an optimised and adaptable Blockchain-based memory for this purpose. Blockchain technology also aims to eliminate the ambiguities that come with people's identities and the correctness of shared resources. This unpredictability can be avoided by making use of Blockchain technology which provides shared information on virtual identities and events that are transparent to all users while still keeping it rigorously disguised by making use of high end cryptography.

5.2.4 Auditability

All transactions in the Blockchain should be valid and verified for auditing. To make a Blockchain auditable, the transactions must be stored in chronological order. This is done by keeping account of the previous block's hash and that of the present block which holds the address of the next block to be added. Hashing techniques are used as a protocol to connect two nodes.

A trend in technology today is digital currency. Since Blockchain is an important aspect of cryptocurrencies, the key characteristics of Blockchain have proven to be a boon for the public sector as it provides some benefits in the form of secure transactions, data integrity and security. Once a monetary transaction is performed, it needs to be verified and audited. This is done by making use of the timestamps created by the Blockchain itself. These timestamps allow the user to verify whether or not the services were conducted in the manner they were presumed to be. If the timestamps verify the occurrence of events in the same chronological order, the system can be thought to be error free. However, in the case where the verification process fails, it signals the presence of a malicious entity on the network. This feature of Blockchain ensures non-repudiation and fiddling even by the maintainers of Blockchain, and all of this is done by making use of the public key system. In the case of Blockchain, the auditable evidence lies within the Blockchain i.e., within the hash itself. These are immutable when it comes to the data transparency and distributed structure of the data which helps to eradicate fraud and corruption in the public sector as well [11], [12]. Since Blockchains are irreversible and no data can be fiddled with, it ensures better data transparency and thereby increases the level of public trust. It is expected that the concept of Blockchain might gain worldwide popularity and acceptance by its stakeholders, replacing the traditional databases if the benefits it is assumed to offer are provided.

Despite a lot of conceptual work done on the same, the potential benefits of Blockchains have yet to be proven by any factual evidence whatsoever [13]. Thus, a wide range of research on Blockchain that covers all e-government systems, influences and threats is the need of the hour. Here, we have conducted a systematic literature review on how the adoption of Blockchain would affect government bodies and what challenges it might face. In the following section, we put forward the methodology used while looking for the appropriate literature.

4.3 Methodology

Taking into consideration the potential significance of Blockchain in the public sector domain, we performed a logical narrative review to discover the present trends in Blockchain with respect of e-

governance systems. The following research question was formulated to achieve this goal: *What problems are faced when adopting Blockchain technology as part of a secure Saudi e-governance system?*

The following keywords were used which were derived from the research question above:

(Blockchain OR "Blockchain technology") AND (Saudi OR "Saudi Arabia") AND (governance OR e-Government OR "public sector") AND (Challenges or Limitations)

Three major electronic databases were used to search and download the research articles: IEEE Access, Springer and Google Scholar. The keywords, titles and abstracts were used to search the publications, events and conferences. After a logical literature survey, we ended up with 226 articles up to March 2020. Various additional criteria were used for the selection of appropriate research articles in order for them to be included into the literature review as illustrated in Figure 28. A full-text article reading brought down the number of research articles to 28.

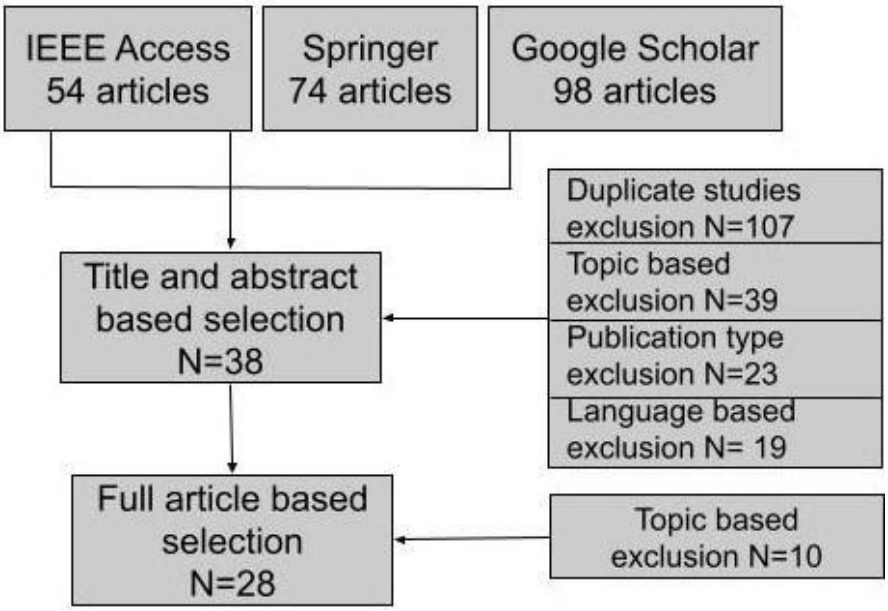

Figure 28: Article search and selection

4.4 Comparison Analysis

Since an array of intangible factors must be taken into account when an attempt is made to add value to society through such reforms, automating *the* e-government operations has remained a major challenge and an elusive aspect of technology-driven reform within the public sector, even if the use of Blockchain technology is promoted by government representatives and policymakers already. Blockchain technology

could be a significant opportunity for e-government officials to increase their public sector service delivery by providing greater transparency in all services involving distributed ledger technology. For instance, e-participation, e-administration, telemedicine, e-health, open data, e-voting, smart cities, and many other e-government areas are now starting directly to benefit from the development of more decentralised solutions, all of which are assured by Blockchain technology. Many academics are researching how Blockchain technology can be used in e-government projects including various administrative and political reforms, but very few focus on how distributed ledger technology can be used to automate government processes. The purpose of this study is to bridge this knowledge gap and to build a foundation for future research in this area. In this session, we will explore how emerging technologies can be harnessed for improved governance, transparency and efficiency. This study considered 28 research papers that have examined the potential of using Blockchain technology as a solution to solve Saudi Arabia's e-government services' security problems. Besides demonstrating the potential uses of Blockchain, they show other ways that the Saudi government can leverage it to create more e-Government services. Below you will find a table that summarises all of the conclusions reached and the method they used to determine them.

Table 9: Summary of the Derived Conclusions

Reference	**Type of study/ Research method**	**Findings**
a) [14]	Framework	Combines Blockchain and artificial intelligence to preserve the infrastructure against a breach of security and privacy. Integrated technologies identify any encroachments and avoid the attacks that could possibly take place while maintaining anonymity and encryption, scaling out to allow the users and government authorities to get linked with the network and creating unique keys and Blockchain labels for citizens.
b) [15]	Diagrams and SWOT analysis of Blockchain	The paper introduces SWOT analysis for the Bitcoin protocol.) Quantum attacks prevented by lattice cryptography suggested. They listed Blockchain cons (Performance; Unique keys with separate signatures that ensure authentication. These signatures help to secure transactions in a cryptic manner; Redundancy for huge storage; Nascent technology for resolving challenges; Uncertain regulatory status; Integration concerns of Blockchain applications)

Reference	Type of study/ Research method	Findings
c) [16]	E-voting	A lack of auditing capabilities and system verification methods affect the acceptability of e-voting systems as a transparent and tamper-proof method. Proposed an Auditable Blockchain Voting System (ABVS) as a solution with a supervised internet voting system. Voting systems powered by Blockchain could be used as in several use cases in e-government systems.
d) [17]	Framework	Blockchain can be used for electronically generated and managed IDs and the errorless handling of documents and as a venue for different purposes in government systems. It can also serve as a support infrastructure for verifying different kinds of resolute documents. Currently, there is IPFS and Swarm which is represented as an alternative to AWS S3 but in a decentralised manner. Both of these solutions could be considered decentralised storage systems that can be used in government systems.
e) [18]	Framework	A distributed e-government node-to-node system that makes use of Blockchain technology. This ensured both information reliability and confidentiality with a simultaneous increase of trust. Security and privacy aspects were analysed. They suggested using Ethereum as a private Blockchain.
f) [19]	E-voting	Secrecy violated by various agencies. A concept of crypto-voting as a method of e-voting was proposed. Blockchain was used for integration of the management processes and election events. The paper only introduces the voting concept.
g) [20]	E-voting	

Reference	Type of study/ Research method	Findings
		Made use of Blockchain as a ballot box with transparency, decentralisation and the facility to change or update votes based around a permissible time duration during voting. Thus, Blockchain proves to be a boon for transparent voting.
h) [2]	Framework	Leveraging Blockchain technology with DAO (decentralised autonomous organisation) makes the e-government system immune to both internal and external attacks, as the operations are controlled by predetermined rules. Reduces uncertainty and the errors caused by human mediated processes. Using DAO is very important for automating actions in Blockchain through smart contracts.
i) [21]	Framework	Blockchain's Hyperledger fabric helps to minimise the threat to the private information of citizens and to the government bodies that share data. The hyperledger fabric meets the various needs of the government, such as a low number of transactions per second.
j) [22]	Various countries	Used Blockchain as an internet infrastructure with examples from countries that have applied it to various e-government services related to tax administration, welfare, land titles and academic certificates.
k) [23]	Healthcare sector	Differentiated data privacy (ensuring control of the access to information only by users) and data accessibility (ensuring unrestrained information access). Conflicts between the privacy and accessibility of data are particularly visible in the healthcare sector. Combining Blockchain technology with smart contracts as a solution.
l) [24]	Healthcare sector	Provided the Blockchain technology requirements for the Office of the National Coordinator for Health Information Technology (ONC) in the

Reference	Type of study/ Research method	Findings
		USA, which are recognition proofing and authentication, secure storage and exchange of data, the scalability problem in Blockchain, accurate and trustworthy permission authorisation to receive and access patient data and consistent data formatting for interoperability and modularity. The Fast Healthcare Interoperability Resources (FHIR) framework was proposed as a solution.
m) [25]	Healthcare sector	Possibility of increased security and privacy problems if the request for data retrieval is initiated and mediated by the patient as per recent trends. Five mechanisms were proposed to address these problems: digital access rules, data accumulation, data interchangeability, patient verification and data irreversibility. Whether these problems will be solved, and the barriers involved in Blockchain-enabled information sharing that is initiated by a patient themselves, with respect of the transactions made using clinical data, privacy and confidentiality, the engagement of patients and the incentives, have also been evaluated. Privacy and security problems were lower when Blockchain was used.
n) [26]	General survey	No safety or security problem on the Blockchain technology protocol side. The user side was susceptible if the safe storage and use of private keys was not ensured. If the private key is leaked, stolen or lost, security becomes compromised.
o) [27]	e-voting	Blockchain can address some, but not all, of the security concerns which include anonymity, confidentiality, integrity and non-repudiation. Some of the possibilities regarding the security and privacy threats when involving the use of Blockchain for e-voting were compared with other methods of protecting privacy and security.
p) [28]	e-voting	Introduced the use of an open source Blockchain which is basically a cryptocurrency, i.e., Ethereum, testing it for its functionality on a smart contract on the Ethereum network using Ethereum wallets and its reliable language as an e-voting system. Those who do not have an Ethereum wallet can use the Android platform for the same purpose. Once an election is conducted, this Ethereum Blockchain stores the votes

Reference	Type of study/ Research method	Findings
		and ballots. All Ethereum nodes manage the voting transaction requests. This consensus ensures transparency in e-voting. This system was proven to have high reliability and efficiency.
q) [29]	Political referendums and other participative democratic processes.	When Blockchain is used for political referendums and other participative democratic processes, with an increasing reliance on private-friendly, secured and encrypted networks, it needs to be increasingly more open, inclusive, ethical and transparent.
r) [30]	Framework	Blockchain-based electronic evidence preservation model to take care of the rapidly increasing large amounts of internet data.
s) [31]	Columbia	Pitched the idea for a secure national identity digital document in Columbia. It required the use of smart cards since it was based on the concept of Blockchain. It took on the benefits of conventional authentication methods such as biometry (to authenticate users) and their documents so then the threats to the security of the currently used Identity Document can be minimised.
t).[32]	General	Blockchain employed for state-owned public registries by using data hashing (anchoring) on the Blockchain. Identification and analysis of scenarios for when such hashing is beneficial and when it is not. This method was compared with signatures using PKI (Public Key Infrastructure).
u) [33]	e-voting	Blockchain technology used for e-voting using the example of an application, CongreChain, developed as a Ruby implementation of an open asset protocol for coloured coins, which are Bitcoins with metadata attached to them. They can be used to represent many types of assets like

Reference	Type of study/ Research method	Findings
		stocks, bonds, coupons and even votes without fear of counterfeiting. Coloured coins require special wallets that can read and understand the metadata attached. When used for voting, the application is used to create an address to represent the election candidates. A vote is done as a transaction by sending the asset to the address of the preferred candidate. It is verified by the usual processes and valid elections are added to the block. The votes are counted by reviewing the balances of the addresses of each candidate. This system was tested and validated by the authors and was found to have all of the required strengths in terms of security and privacy.
v) [34]	General	Used Blockchain in e-government services to strengthen the services, clarity and accessibility, interoperability between different organisations to prevent any attacks via network, publicly available transactions and impossibility of adding transactions to modify or delete others, thus ensuring safety and security while being open to all.
w) [35]	General	Leveraged Blockchain technology to solve the current problems and challenges of data security and the level of trust in Cloud computing. The security mechanism of Blockchain was integrated with the secure storage mechanism of Cloud computing. A virtual machine agent model with mobile agent technology was used.
x) [36]	EGS stages	Explained the staging of e-government (EG) into 1.0, 2.0 and 3.0. Thus, EG 1.0 made use of Web and ICT to refine the orderliness and efficiency. EG 2.0 was supported by Web 2.0 technologies to become more citizen-dependent through portal services, promoting citizen participation and e-democracy. EG 3.0 uses Web 3.0 ICTs which include shared ledger technology, AI, Neural Net and the Virtual Web. The combination of Blockchain and AI can solve many of the current problems of privacy and security like the control of personal data. The

Reference	Type of study/ Research method	Findings
		authors used energy and healthcare sector data to support their contentions.
y) [37]	Bangladesh	There is a higher incidence of cyberattacks in Bangladesh compared to the rest of the world, and mor varied forms and types. Although Blockchain was mentioned as a solution to enhance the security of e-government services, it was not pursued further due to no specific recommendations to use it. Only the policy, regulatory and strategy levels of cybersecurity were examined for improvements.
z) [38]	Device-to-device communications	Blockchain technology to secure IoT authentication and authorisation for device-to-device communications. For this purpose, the IoT network was divided into a multilayer decentralised system. A local authentication mechanism and cluster head authorisation purpose within each cluster were used for which Blockchain was used for the local implementation without a central authority.
a.i) [39]	Indian Aadhar	A decentralised system to allow access to personal records by registered users was suggested. The example chosen was the Indian ID card, Aadhar. It involves the user, authority and a third person. The personal information of the citizens was recorded in the Blockchain digitally. Individual identity keys were generated and the system increased the level of trust in the genuineness and reliability of the data.
a.ii) [40]	Nigeria; interviews and a document review	A scalable framework which uses Blockchain technology to address the privacy, information sharing and record keeping issues in the health sector of Nigeria.

4.5 Research Challenges

Among the various challenges faced when seeking to integrate Blockchain into an e-governance system, the SLR carried out by this work revealed the following:

5.5.1 Security

Only four papers reported this issue: [11], [9], [41], [42]. Both problems related to Blockchain and those not completely solvable were identified in these papers. There are a few instances where using Blockchain to solve the security and privacy problems of e-government services could lead to even greater problems. Saudi Arabia needs to examine whether any such factor exists in their context. If yes, Blockchain cannot be implemented at all. The implementation of Blockchain technology is a promising one. However, some challenges are correlated with its application. The most critical issue is the privacy and confidentiality of the information being transacted through the system. There is no standard set of regulation that governs the transaction or whole system of information exchanged through the system, leaving it to be volatile. Some of the areas where Blockchain is prone to attacks and security needs to take the centre stage:

i) Broken Authentication: A large surface of the Blockchain will be vulnerable to attacks if the proper execution of the authentication functionality is ignored.

ii) Insecure Deserialisation: If the Blockchain comes under attack, malicious users can interfere with the deserialisation code and thus compromise the Blockchain system.

iii) Making use of components that already have vulnerabilities. This happens due to the reuse of code.

iv) The exposure of sensitive data; this security threat has the highest potential for damage in a Blockchain.

An extensive research study conducted by [82] identified potential threats like endpoint security, Denial-of-Service, vulnerabilities in the code and the deliberate misuse of code. Some of the research work showed the possibility of hijacking the BGP (border gateway protocol) which is done by compromising the routing process of the Blockchain as another potential threat to Blockchain. Man in the middle attacks, EREBUS attacks and DNS attacks were among the other identified threats. However, these attacks were categorised as a high level of cyberattack against Blockchain.

Other significant challenges include vulnerability, redundancy, the distribution and replication of data, the cost associated with implementation and compliance with the regulations. The nodes could only be accessed by authorised personnel included in the transaction, making it nearly impossible for any other person even in the same organisation to know about the marketing. In this way, billions of cryptocurrencies can be issued with only two persons having the information.

5.5.2 Privacy

Blockchain has recently attracted a lot of interest as a decentralised and distributed public ledger technology used in peer-to-peer networks. It uses an interlinked block structure to validate and store data, as well as a trusted consensus protocol to synchronise any data changes, allowing for the creation of a secure digital platform for data storage and sharing. However, the issues of privacy and safety always appear with the use of the internet and networking. With the emergence f cybercrime and increased number of skilled hackers, it has become more difficult to track or locate safety breaches. Almost every organisation that adopts this method also raises the question of privacy. With the implementation of the Blockchain system into an organisation where centralisation is also considered, privacy concerns dominate the benefits of using Blockchain technology. The confirmation of the order being trustworthy and safe depends on the possible adaptations, thus increasing the probability of risk. It is a common challenge for nearly every business that incorporates or intends to implement Blockchain. Though Blockchain can be a useful framework for the development of distributed systems, privacy concerns (such as the disclosure of a user's true identity and transaction amount) should not be overlooked in the protection of the users' interests. When the Blockchain is linked into a supply chain management (SCM) system, for example, if the buyer-supplier relationships or extra information for each conversation are not protected, trade secrets of suppliers may be leaked. That is, by evaluating the transaction records, the cost of the products from various vendors can be calculated. As a result, the suppliers' incentive to use the Blockchain-based platform will be reduced because their interests will have been jeopardised, severely limiting the use of Blockchain in SCM systems. Hence, it is necessary to perform an evaluation of the privacy preservation in such a Blockchain-based network. International technological corporations and service providers are potentially trusted parties with access to and control of user data and information. While this can help users, it can also be used as a tool to implement monitoring or censorship or it can even lead to the abuse of user trust.

5.5.3 Vulnerability

The complexity of the Blockchain system makes it less visible from the end-user point of view but this also enhances its security. The mechanism ensures that the authorised person uses the nodes to control the transaction but in case of any hacker approaching with more access than the actual node, the network will become vulnerable. Therefore, it is more common in large centralised systems of Blockchain used by organisations. Blockchain is vulnerable to selfish miner attacks. It was shown by Eyal and Sirer [56] that even if only a small section of a hash is compromised, the whole network is at risk. If the transactions are carried out using randomly generated addresses rather than personal information, the Blockchain is thought to be secure. As mentioned already, if the Blockchain comes under a miner attack and the miners

get access to more than 50% of the Blockchain, the threat would be of a greater intensity and potential. The miners would use most of the available computing resources to meddle with the data present on the blocks.

Another significant challenge that the Blockchain may have to deal with are the errors committed by the end users in terms of losing their keys. If an unauthorised user gets their hands on these keys, the information present on Blockchain is vulnerable to meddling or theft. Apart from this, regular software updates and installations might become a potential cause of data breaches.

5.5.4 Redundancy

With enhanced and fast internet technology, more individuals and organisations are using Blockchain technology. This has led to massive amounts of data being processed at once. In order to maintain the concurrence of such large amounts of data, a broadcast algorithm is put to use by the Blockchain technology. This algorithm in turn has some disadvantages, the first one being the redundancy of the data traffic. When the nodes communicate with each other to send information over the network, it creates a havoc of replications which is nothing but data redundancy. The system of Blockchain can often be slow due to a transaction and the enormous set of information as a result. Due to the amount of complex data, such transactions can take time to be processed and completed. Since Blockchain has no intermediary or central authority, the scattering of the same information over a range of blocks makes it redundant.

5.5.5 Data Distribution and Replication

The approach used in the Blockchain-based system confirms the privacy of the data. However, the system used for transactions employs the data replication method for it to be sent on the other end. It again raises the challenge of data privacy. Due to its disseminating nature and the presence of many copies of a particular ledger, a cyber threat that happens at one instance might pose a threat to all copies kept at various blocks [59]. This distributed feature of Blockchain is an energy exhaustive job especially in the case of transactions where multiple copies get affected at once. However, the specific signature can be used to validate the data and avoid any cyberattack leading to unauthorised access. The distribution of data over other chains also increases the chance of data integrity violations.

5.5.6 Regulatory Compliance

The lack of regulation for Bitcoin or other Blockchain transactions has made it quite a risky network. Many interested individuals and organisations opting for this technology must run the risk for many months due to the system's vulnerability. Moreover, it can also result in multiple scams and fraud cases.

Many internet schemes are discovered to be scams and like other networking crimes, law-making bodies are not entirely successful at tackling this issue. Another big limitation are the constraints to its scalability. It has comparatively less throughput than traditional databases which hinders its application on a much bigger level. Both Bitcoin and Ethereum have a lower throughput than the existing traditional payment systems. To avoid certain attacks that are prone to being used against Blockchains like Byzantine attacks, the consensus data algorithms make use of additional mechanisms which in fact puts a limitation on the computing power and throughput of the network [53]. The consensus algorithm is a kind of protocol that both nodes communicating on the network follow. The protocol is based upon both of the nodes agreeing whether or not to share information.

5.5.7 Implementation Cost

An important feature of Blockchain is its high consumption of energy. The huge amount of energy is used to keep the transactions in the ledgers updated. A new node is created on the initiation of every new transaction. This creation of new nodes every transaction is both time and power consuming. Each created node makes sure that there is no interlude and remains active until a transaction is ended. All of these mechanisms require a considerable amount of computing power, thus increasing the various costs of implementation [54]. The practical and easy-to-use transaction method is also associated with increased costs. The Blockchain network demands careful monitoring and a continuous supply of energy. The amount of data and information being transacted and stored on the network is also significant, marking the fact that the estimated cost could be high initially and during implementation. Besides, the data that is sent or received accounts for a lot of the storage on the server. These facts indicate that the costs at the start, during and after the application of Blockchain technology are very high.

5.5.8 Limitations

This problem was reported in six papers as listed below. Some of the problems can be solved sometimes, and others remain unsolved even if Blockchain is used. Some of the papers [15], [43] have discussed the limitations where Blockchain cannot solve certain existent problems. Some researchers [44], [24] are of the opinion that the implementation of Blockchain is not feasible in Saudi Arabia yet. However, some researchers [26], [27] have suggested that the implementation of Blockchain should go ahead in areas such as healthcare. A few of them have restricted their opinion of implementation in areas such as e-voting in Saudi Arabia [26], [27]. The majority of the research in Blockchain application in e-governance is still in progress or at the pilot implementation level and propriety-based. Detailed information and architectures are rarely available in the academic area which is a significant issue when seeking to

understand and review the existing architectures. A significant amount of studies have shown the inability of Blockchain to adapt and implement smart contracts, a tool that is activated on the initiation of every transaction and is helpful as it removes differences and bias. Smart contracts are nothing but a protocol given by Nick Szabo. It's a piece of code that's used when two entities need to exchange information over the network without having to necessarily introduce each other. This contract protocol remains active until the end of the transaction. It's pre-fed to both nodes already. It can even get cancelled if any one of the conditions is not fulfilled by either of the nodes [64].

Another researcher named Alrebdi (2020) declared there to be three main hindrances to adopting Blockchain in KSA's e-government. These were the dearth of technically sound experts needed to manage and run the Blockchain systems, a lack of knowledge on the usability of Blockchain, and it being still in its initial stages. Moreover, scalability and low speed were identified as challenges faced by the kingdom of Saudi Arabia by Ashmawi (2020).

There were other constraints like time and money as all of the current implementations of Blockchain-based e-Governance systems are far away and considered to be secret. Therefore, the respondents were not available through online mediums to explain and answer queries.

5.6 Analysis and Research Findings

A vast amount of research has been done regarding the privacy policy for e-governance in Saudi Arabia. Studies identifying the major issues that influence e-governance both in a negative and positive way in Saudi Arabia were conducted by Rayed Alghamdi et al. [63]. These studies found that Saudi Arabia has great scope for growth and adoption of Blockchain technology and ICT.

In this section, we analyse the results found by the SLR presented in the previous section. Many of the papers address utilising Blockchain as a voting application to make use of the digital identity of the Blockchain. Then they expose the Blockchain features like the sharing of data from the Blockchain between several organisations. The Blockchain platform is a shared ledger between organisations where each organisation has their own smart contracts with which to sign transactions in the Blockchain which increases the security of the Blockchain as a whole. There are several factors that need to be considered when selecting the best Blockchain framework.

Firstly, there is the integration between the Blockchain framework and the current system. As Blockchain integrates with the current system, it does not replace the current system. One can think of Blockchain as integration rather than as a migration. Secondly, there is the number of transactions per second. Lastly,

the ease of use adds more organisations to the system. Table 10 shows the trends of each selected paper with respect of the use of Blockchain to strengthen the security of e-government.

Table 10: Common Trends Using Blockchain

Type of study/methods	No	References
General and frameworks	9	14, 17, 2, 18, 21, 35, 30, 26, 32
SWOT analysis of Blockchain	1	15
e-voting (including political referendums and participative democracy)	7	16, 20, 19, 27, 28, 29, 33
Estonia, Turkey, Columbia, Bangladesh, Nigeria, and India	4	31, 37, 39, 40
Country groups (including the EU, D5 etc.)	1	22
Healthcare	3	23, 24, 25
EGS Stages	1	36
Device-to-device communications	1	38

5.6.1 Recommended Solutions for e-Governance Services

i. Infrastructure-related issues are more important in the case of smart cities. Blockchain with AI appears to be a good solution as testified by five papers.

ii. In the case of e-voting, verified voting for genuineness, secrecy and tamper-proofing are the issues. These problems can be solved using applications like Crypto-voting, ABVS, CongreChain or coupling Blockchain to use the smart contract system of the Ethereum network. Four papers suggest each of these.

iii. Blockchain with an SSL layer for the encrypted information that is only to be transmitted was preferred to deal with all malicious direct and indirect attacks as stated by a paper.

iv. In the healthcare sector, privacy versus accessibility can be dealt with using smart contracts integrated Blockchain. FHIR and Ancile frameworks were also suggested.

v. To ensure data security and trust in Cloud computing, the security mechanisms of Blockchain can be integrated with the secure storage mechanisms of the Cloud.

vi. For addressing the security issues of device-to-device communications, Blockchain can be used for secure IoT authentication and authorisation with IoT as a multilayer decentralised system.

vii. In Nigeria, scalable Blockchain technology was found to solve the problems of privacy, information sharing and record keeping issues in the health sector.

Our research findings focus on identifying the scope of using Blockchain technology to improve the confidentiality and reliability of e-government services and these are presented in Table 11.

Table 11: Problems and their Solutions in e-Government Services

Problems and challenges of e-Government services	Solutions	References
a. Information security and privacy in general b. Current problems of security and privacy c. Indian Aadhar d. Internal and external attacks e. Risk of private information disclosure f. Quantum attacks	a. A distributed e-government terminal-to-terminal system making use of Blockchain. b. Combine Blockchain with AI, ensuring proper authentication and the proper use of public keys, ensuring cryptography in the public Blockchain. c. A decentralised system to allow access to personal records by registered users was suggested. d. Blockchain with DAO (decentralised autonomous organisation). e. A hyper-ledger Blockchain. f. Lattice cryptography.	[18](a) [36](b) [39](c) [2](d) [21](e) [15](f)
Smart cities - a. Infrastructure vulnerability, especially smart cities b. Security and privacy	a. Combine Blockchain with AI. b. Blockchain support for ID management and the secure handling of documents.	[14](a) [17](b) [22](c)
e-Voting a. Lack of auditing capabilities and system verification methods affecting the acceptability of e-voting systems as a transparent and tamper-proof method.	a. Auditable Blockchain Voting System (ABVS). b. Crypto-voting c. Use of Ethereum cryptocurrency wallets and reliable language as an e-voting system.	[16](a) [19](b) [28](b)

Problems and challenges of e-Government services	Solutions	References
b. Secrecy violation by various agencies c. Valid votes	c. CongreChain developed as a Ruby implementation of the open asset protocol for coloured coins.	[33](c)
Conflicts between privacy and the accessibility of data, particularly that which is visible in the healthcare sector	Combine Blockchain with smart contracts.	[23]
High incidences of cyberattacks in Bangladesh	Blockchain policies, regulations and strategies.	[37]
Healthcare security and privacy problems- a. ONC requirements b. Privacy and security	a. Fast Healthcare Interoperability Resources (FHIR) framework.	[24]
Security issues of the currently used Identity Document in Columbia.	Introduction of an electronically developed national unique Identity Document using the concept of a Blockchain network.	[31]
Data security and the trust in Cloud computing.	The security mechanism of Blockchain was integrated with the secure storage mechanism of Cloud computing.	[35]
Security of device-to-device communications.	Blockchain for secure IoT authentication and authorisation with IoT as a multilayer decentralised system.	[38]
Privacy, information sharing and record keeping issues in the health sector of Nigeria.	A scalable Blockchain framework.	[40]

5.6.2 Blockchain as a Solution

Apparently, Blockchain-based solutions and their incorporation into e-governance will produce a positive impact in relation to effective public services, low-cost transactions and a trouble-free method of interaction between the citizens and the government. It offers its range of services from healthcare to education, and from business organisations to the centrally stored

information of citizens. There is minimum physical interaction and a minimum response time. Ensuring secure data transmission, electronic voting, e-procurement, filing tax returns and identification process are some of the tasks undertaken by the e-government services incorporated within a Blockchain. The sole purpose is to amalgamate the public services electronically and to minimise the bureaucratic roles involved, all of which would be done in a confidential and secure manner [69].

In this section, we look at the governance decisions that must be made in order for Blockchain technology to be used in the public sector. According to our review of the literature on Blockchain governance, activities in the public sector may be studied in a three-tier way, i.e. the micro, meso and macro levels. Governance policies on one level, in our perspective, do not stand independently. Rather, they are interconnected. [84] emphasises that in public administration, governance techniques at all three levels are intertwined and it is difficult to foresee one level of governance without understanding the others. Some studies focus on policy goals in the conducting of governance with the help of Blockchain. These policy goals include the involvement of the public, the role of the media and the value exchanges across political, social, economic, law-making, and business organisations [85][86][87]. These aspects are not counted as a discrete category in the paradigm but they are assumed by their widespread significance to be influencing variables at each level of administration. In this framework, decisions made at one level affect the other levels as well.

Governance structure: There are distributed roles in the decisions made in any government organisation in a Blockchain network. The structure of governance is categorised into four categories which are centralised, semi-centralised, decentralised and polycentric. Centralised administration pertains to governance where the decision-making is under the control of a group of people or an institution. In case of semi-centralised governance, a few choices are made solely by a centralised management board, whereas other governance decisions are made purely on the basis of the voting done by the platform users.

Therefore, Blockchain is viewed as a distinctive technology helping to deliver efficient and automated administrative services with an increased transparency within an improved e-government system. We present our research according to some of the points presented below.

5.6.2.1 Potential to solve security problems using Blockchain

As many as 19 papers found Blockchain to be useful when solving security and privacy problems in a variety of situations. The list of papers based on the use-case scenario

classification is given in Table 12. It is highly encouraged to implement Blockchain technology in the Saudi Arabian e-government system. Blockchain can offer a possible course of action when creating data assurance issues. The development presents security and anonymity to empower the affirmation of our individual information. The key incorporation of insurance inside the Blockchain is a self-assertive series of numbers known as private and open keys.

Table 12: Security and privacy issues solved by Blockchain

CLASSIFICATION BASED ON USE-CASE SCENARIOS

Papers	**Area**
[45], [13], [17], [22], [46], [25]	Healthcare
[47]	Smart Cities
[48], [29]	Participative democracy
[30], [49], [50], [31], [50], [32], [33]	e-voting
[34], [39]	Indian Aadhar
[40]	Nigerian e-government system
[16]	Future scope

5.6.2.2 Business Transactions

Blockchain has quite a good scope in relation to businesses as well. It has been identified that the contemporary technology would help by removing the intermediaries between various business agents. Blockchain has the ability to disrupt a variety of sectors and to drastically affect the fields in which it can be used. The focus of this study now is mostly on three aspects. [70] and [71] identified some fields within financial services that have been the most affected by Blockchain. These services were bank transactions, accounting at the bank and auditing. Blockchain has removed the involvement of a third party in the process of business transactions. The elimination of the third party minimises the cost of transactions. One of the most important uses of Blockchain in financial service is to do with cross-border transactions. International transactions can be done in a short span of time without having to pay a surcharge

on the exchange of currency. These changes have completely turned the traditional means of business upside down [72]. Customers can make payments using their open and private keys in a distributed shape without giving individual information to an outsider application. Blockchain will moreover accompany the included security into the budgetary data. With the advent of peer-to-peer transactions, users having a lesser or no formal approach to any financial services could get their hands on all financial services that they want to, even if they were initially categorised only for those with authentic financial records [79].

The supply chain has been declared to be another main non-finance application in Blockchain in business organisations [73]. Blockchain's formal registry allows each party of the system to identify and monitor a flowing item across the supply chain [74][75]. The use of a transparent, verifiable and shared database lowers the presence of redundancy regarding each stakeholder's database operation and updates. Another benefit of Blockchain is the use of linked gadgets in cars or storage refrigerators which would help to keep a track of the temperature during the supply chain, thus ensuring that the health standards aren't violated [76]. Blockchain has the capability to bring about a change in industrial services. Apart from the elimination of intermediaries that we have already mentioned, it lets its users track their transactions and assets anonymously. [77] and [78] talked about some uses of Blockchain in the manufacturing industry and the role of Blockchain in facilitating security and accuracy in 3D designing. A wide range of industries around the world have switched to this technology by taking inspiration from such firms. Saudi Arabia still has room to make changes in its business models, facilitating capitalisation and thereby improving operational coherence [79]. Initial coin offerings (ICOs) are one of the widely used applications of Blockchain that the finance sector can use to help sending value across all dimensions, reducing the cost and asymmetries found in the information [80][81].

5.6.2.3 Healthcare Data

The role of Blockchain in healthcare is predominant among all of its other functionalities. The features that encourage the use of Blockchain in healthcare are immutability, anonymity and autonomy. It pushes to build a secure and immutable database consisting of all healthcare records in the state. The decentralised and peer-to-peer properties help by sharing information between the concerned patient and the consultant without the intervention of a third persona and in the meantime delivering the information in real time. A prototype by the name of MedRec was suggested by [65] for use by the healthcare systems in Saudi Arabia. MedRec along with Blockchain addressed four main problems. The first one being the scattering of the

patient's illness history across different departments and hospitals that they have ever been to. These hospitals used to operate the traditional way and didn't share information whatsoever with other hospitals. Thus, every time a patient made a new appointment, a new record was maintained, making the information redundant and resulting in a waste of resources [66]. This scattered information delays the retrieval of information. This delay doesn't work with the patient and this is the second issue that MedRec targets. The last target was to remove the barriers between one-to-one communication between a patient and his doctor and to channel the flow of data through the different departments [67][68].

Blockchain innovations can offer better control to patients over their medical service information. They can store their medical service information on the Blockchain. Once the information is recorded, the patients can hold the data securely and make it accessible to just the required specialists. They can encourage the delivery of a specific segment of the data to the medical care supplier for the purposes required.

5.6.2.4 Integrating Blockchain with other applications

Blockchain may be useful, sometimes with synergistic effect, if another application is integrated with it. AI, IoT, drones, big data etc. can be coupled with Blockchain for enhanced effects as was indicated specifically in the three papers listed below. Saudi Arabia can explore the possibility of using any of these other applications for such an enhanced effect in relation to Blockchain [35], [36], [38]. Blockchains are rapidly gaining recognition and popularity owing to their distributed and decentralised features. It can open up new avenues and opportunities and has been proven to be a boon for businesses because of its high transparency, secure transactions, high reliability and clearer immutability. Blockchain is the most popular technology used in current transactions. It possesses various features that have led to making it accessible. The features include decentralisation, transparency, resilience, time reduction, reliability, atomicity in transactions, collaboration, fraud prevention, security and so on. Today, Blockchain technology is widely used in various sectors including finance, accounting, markets, e-governance, health care, Internet of Things (IoT), science, art and so on. Blockchain is the basis of modern record keeping and recording transactions concurrently and in a permanent fashion in different positions. The entries are encoded to limit changes.

E) E-voting. Blockchain has found use in electronic voting systems. For each election, every registrant has his or her own identity wallet. The election supervisor produces a voting shared ledger for each related node within the districts, after which the voter can begin voting. The

data of the vote is confirmed by the majority of district nodes and the ballot is stored on the Blockchain. Each voter acquires a polling ID which may be used to check that his or her vote is recorded on the Blockchain and accurately tabulated. To meet the privacy standards, any personal information related to the voter is not contained in the voting transaction on the Blockchain. Ethereum is found to be the most suitable Blockchain for e-voting. It helps to conceal the identity of the voter by using hash values. Multi-factor authentication is done to verify the voter details [89].

5.7 Summary

This chapter presents the results of various studies in the literature and analysed the challenges faced in the integration of Blockchain into e-governance models. Through our systematic analysis, we conclude that the theoretical research in this domain has only just begun and that the risks have not yet been thoroughly identified. More research is required with a focus on integrating Blockchain into the public sector domain. Research with empirical evidence in the government context needs to be carried out to study the potential benefits of integrating Blockchain technology into e-government systems. Judging from the common trends in the findings reported in the selected papers, there is a high potential related to using Blockchain as part of enhancing the security of systems like Yesser and other e-government services in Saudi Arabia. However, there may be certain services (like e-voting if implemented) which require a slightly different approach. There is a need to identify the elements that are favourable and those which are unfavourable for Blockchain implementation in the Saudi context. Although not reported in the reviewed papers, cultural aspects may be a factor here as well. Research needs to be undertaken in the Saudi context to work out what is best for the country.

Chapter 6: A Novel Design of an E-Government System Using Blockchain

6.1 Introduction

Fundamentally, a distributed record database or a public ledger has a history of all transactions carried out between the participants. Authentication in every step is required via the consensus of the majority of parties that are participating in the transaction. Once recorded, the information can never be removed. Blockchain contains the authenticated records of every single transaction. The main idea behind this to create a distributed consensus in the online world allowing all participants to recognise the digital events executed by developing irrefutable transactions on a public ledger platform. There is a huge scope for a paradigm shift as part of developing a scalable distributed and decentralised e-government system.

To understand the working of Blockchain, its positive effects and its relevance in relation to e-government systems, we need to have a thorough knowledge of Blockchain and how its adoption has changed the dynamics of technology today. E-government has widely replaced traditional and conventional means of governance in all public sectors. [1,2]. The idea of e governance is accepted as the centre of every new innovation in information, technology and communication systems. E-government systems are programmed to automate public service models around the world [3-5]. Due to its transparency and lower level of fraud, it is described as the electronic mirror of the real government which has made use of numerous digital technologies for conducting tasks like recording, processing and addressing the key stakeholders, as well as disseminating information to its citizens, enterprises and government bodies. Blockchain is a unique way of storing information at distributed locations as a part of the distribution ledger technology. It is an unconventional way of recording data in such a way that the data is secure from any fiddling or modification [6-8]. It stores information in a sequential pattern. The decentralised way of storing information has made Blockchain much more reliable at storing and retrieving information. Blockchains are said to be attack repulsive, i.e., they are less prone to corruption and attacks because the information blocks follow a pattern for storage which has to be in chronological order. This mode of encoding

Blockchains has proven to be beneficial unlike traditional stored information which would wear out and disappear with time due to the logic of the conservation of energy and the process of entropy in any environment that it is stored in. [9-13]

The ledger that stores the data is shared by all stakeholders, making it a one system with many users concept. Since many users access the Blockchain at once, the systems have to be very reliable and robust. The new data added gets recorded in the newer blocks, along with the status of the previous blocks as hashes which contain a summary of the previous block's data. When the block is completely written with the data to be stored, it gets sealed and becomes a permanent part of the Blockchain. This block is then unavailable in terms of meddling and modifications. The Blockchain is presumed to have a hypothetical infinite storage because newer blocks can be continuously written along with a hash which has the information of the previous block. Essentially, the Blockchain can be considered a living process that will continue to exist as long as the code from one block is copied to the next. There is a hash in every new block which contains information about the previous block as well as a register of the entire Blockchain in every new block. There are millions of blocks in the Blockchain that represent citizens, businesses and governmental organisations, therefore it is the entire block that in theory enables anyone connected to the network to identify the information available within any block on the Blockchain. This would be theoretically impossible otherwise since there are millions of blocks on the Blockchain.

Thus, manipulating the recorded data of a Blockchain is possible only if some of the peers are corrupt and are willing to change and update systematically in a sequence without interruptions. In an independent Blockchain that can be monitored individually because of the thousands of individual block owners it has, this is not possible because of the integration of the following: a) In a distributed ledger, all blocks are recorded over multiple memory locations in a decentralised manner, therefore no one has control over the ledger. b) Any peer on the network can have access to a copy of a single ledger. c) Writing data to a block cannot be changed or updated unless all sequential blocks are changed. Therefore, Blockchain is the optimal solution for better transparency, security as well as flexibility when dealing with government systems. The results so far are enough to increase the public confidence in e-government systems, whether it is in the management of government databases or keeping an account of public transactions.

6.2 Relevance of Blockchain Technology in E-Governance

The network, which was first announced as Bitcoin, refers to a peer-to-peer network that provides transparency through transaction consensus. Blockchains immutability and consensus role minimises the need for the central authorities which makes it an ideal solution for dispersed environments. Because data is today's most valuable asset, the use of Blockchain in data-driven architecture can bring about decentralisation, anonymity and other benefits such as audibility and persistence. The most frequently encountered terminologies used in Blockchain technology are explained below. Node and Block: In a peer-to-peer network, a node is a computer that represents the landlord of transactions carried out by a certain user. A block is a page that cannot be changed. A block in the Blockchain is added when a transaction is approved which makes it a distributed ledger.

i. Node and Block:

In a peer-to-peer network, a node is a computer that represents the landlord of transactions carried out by a certain user. There is no way to change a block. When you arrive at the Blockchain, a transaction is approved and a new block is added to the chain.

ii. Consensus:

Through the approval of the node decisions, the consensus method was applied to process and validate transactions. A number of common consensus algorithms have been discovered such as Byzantine Fault Tolerance, Proof of Stake and Proof of Work.

iii. Scalability:

Node scale or performance scalability is offered dependent on the accesses available in terms of the currently available solutions. Node scalability is funded by government Blockchains like Ethereum and Bitcoin as performance scalability is provided by state Blockchains.

iv. Smart contract:

Apart from investment management and cryptocurrency, the third generation Blockchain revolution has broadened the application of Blockchain in terms of its application areas. Smart contracts may command complicated functions by defining arbitrary rules. The functions in an Ethereum smart contract have a "gas" cost that is determined by the number of computing steps and the amount of available space. The value of gas is paid in cryptocurrency.

Blockchain technology is a growing platform for matching the standards of present-day technology and innovations. It has found use not just in financial systems but in the public

sector as well due to its robust nature, its built transparency and global reach. Although these characteristics are not of equal importance to all governments, they are a big deal for countries with a higher percentage of corruption and distrust present, for example, Columbia. Blockchain technology, owing to its transparency features, has upgraded the e-government in Columbia [21]. Other than Columbia, other countries viz China, Japan, Singapore and South Korea were the first from Asia to leverage the intensity of all activities and innovations related to Blockchain. This is evident from the technological infrastructure and capital investment. Many start-ups based on Blockchains have been started [27]. A survey conducted in 2018 showed that Asian countries such as China, Japan, South Korea and Singapore have the highest number of stakes in the top ten Fortune 500 companies. These companies only have projects that are done in Blockchain. In China alone, 38% of companies work on Blockchain and they come from a variety of branches from IT to banking and from energy to motors. Well-known companies like Sony and Fujitsu from Japan have not fallen behind in terms of trying their hand at Blockchain [27].

In 2016, the Chancheng provincial government in China established an e-government platform providing services using Blockchain technology. An e-governance platform based on Blockchain technology is being introduced in Guangdong province in collaboration with a Chinese software company named 21ViaNet China. It was the first Blockchain-based e-governance platform in China and a next-generation open platform designed to improve trust between its citizens and the government [22].

A good number of South Korean companies that were a part of Fortune 500 have explored their means in relation to Blockchain. A statistics report related to Blockchain presented China as the first country wit the highest number of patents based on Blockchain (41%) which is a clear indication of growth of Blockchain in these countries. Half of the top 100 Global companies were Chinese and had patented projects on Blockchain. Several government bodies in China have prohibited the trade of cryptocurrency. This didn't hinder the development or growth of Blockchain which was a building block of Bitcoin. In fact, the Chinese government played a vital role in letting Blockchain take the lead in the market by making several initiatives. Blockchain technology was used by China for the first time in December 2016 in the 13th five-year plan that aimed at building its national strategic technological advantage.

In 2017, certain banks in China viz. the Chinese central bank offer to help promote research and innovation in advanced technologies like artificial intelligence and Blockchain as part of

its Five-Year Financial Industry Plan. The plan was accepted and nearly a year later, the Ministry of Industry and Information Technology (MIIT) published China's Blockchain Technology and Application Development as the first official guidelines on the technology. In addition, Hong Kong's government and economic, financial and legal affairs were governed by the rule of "one country, two systems." In doing so, Hong Kong promoted Blockchain across Asia. As part of its commitment to adopting and developing Blockchain technology, the South Korean government plans to invest more than US $900 million by 2019. For example, the government updated its tax duties to allow companies to focus more on innovations and developments such as Blockchain. [9], a company in South Korea, hoped to create an encrypted valley for the Blockchain industry. A Blockchain-based auxiliary platform, GroundX, was introduced to the Kakao company in March 2018. Blockchain services are created and made available by millions of developers. Blockchain-based start-ups have been promoted by all of the governments discussed above in a wide range of fields, including social media and FinTech.

The first Chinese Blockchain research centre known as Wanxiang Blockchain Labs were set up in Shanghai in 2015 to initiate and develop research and application of the Blockchain technology. Bubi Chain and Juzix are among the projects that worked on promoting Blockchain infrastructure to create an ecosystem. China outgrew all other Asian countries when it came to adapting Blockchain. Japan, on the other hand, has a relatively lesser number of businesses involved in Blockchain [30].

Dubai’s economic department uses Blockchain to register land effectively, improving the registration process and reducing the probability of fraud and corruption. This technology has been adopted due to its decentralised nature, making it an ideal tool for storing records, contracts and other documents related to customers. Furthermore, Blockchain technology is used to provide seamless, safe, efficient and impressive city experiences. Dubai also intends to use Blockchain technology to improve government services in 100% of cases [23].

In the Republic of Moldova, Blockchain has come up with increased inward capital investment flows and reduced corruption practices. In the tourism sector, Blockchain technology has solved the problem of double spending with the use of modern cryptographic techniques. Also, tourism is promoted using loyalty programs which are based on loyalty cryptographic tokens. Using the Blockchain technology, a Blockchain-based voting system and zero % fee booking systems help clients to vote for the best hotel or tourism destination. Blockchain is also

implemented in government ledgers and databases. Blockchain has proven to be an incredible and unforeseen power to end poverty [24]. Moreover, a Blockchain-based pilot project, a digital identity system for undocumented children, has been developed by the United Nations along with the World Identity Network. The Estonian government is using Blockchain technology to secure its public health records and it has become one of the world's leading governments to do so. Additionally, scattering data over a distributed ledger reduces the vulnerabilities as opposed to having the data aggregated and consolidated in a single location [25]. A Blockchain-based titling system has been developed in the Republic of Georgia, enabling real-time audits and reducing the transaction costs associated with land registration. A pilot project in West Virginia used mobile voting to secure the ballots directly onto a Blockchain-based system for military personnel deployed overseas. To help workers and to prevent forced labour everywhere, the U.S. Department of State, Coca-Cola, and many other private companies have developed Blockchain-based secure registries [26][28].

6.2.1 Blockchain Architecture

In a Blockchain, data is stored, shared and synchronised between different nodes in a network. It was first introduced in 1980 and has been a very well learned research domain since then. [14] In order to fulfil various needs and requirements, two distribution solutions have been proposed, namely Dynamo and Cassandra [15] [16]. Data consistency, integrity and immutability are just some of the benefits achieved by distributed ledger technologies (DLTs) [17] and Blockchain systems. There are two primary types of DLTs: basic DLTs that belong to the Blockchain family and more advanced DLTs that don't belong to the Blockchain family. With the support of cryptographic techniques, Blockchain records and synchronises data in blocks. Every block has the cryptographic hash of the previous block, i.e., each block is cryptographically linked with the previous one. Each block has a timestamp and the transaction data. The records inside the blocks are immutable and changing them would mean the recalculation of the hashes. This is impractical from an organisational and computational point of view.

In Blockchain, transactions submitted to a peer-to-peer network by the end users are validated by particular types of node and then inserted into a new block. It is later propagated to all other participants. The digital signatures are also made by the user using a private key so then the other entities are not able to claim authorship of such transactions. This cannot be rejected by the users.

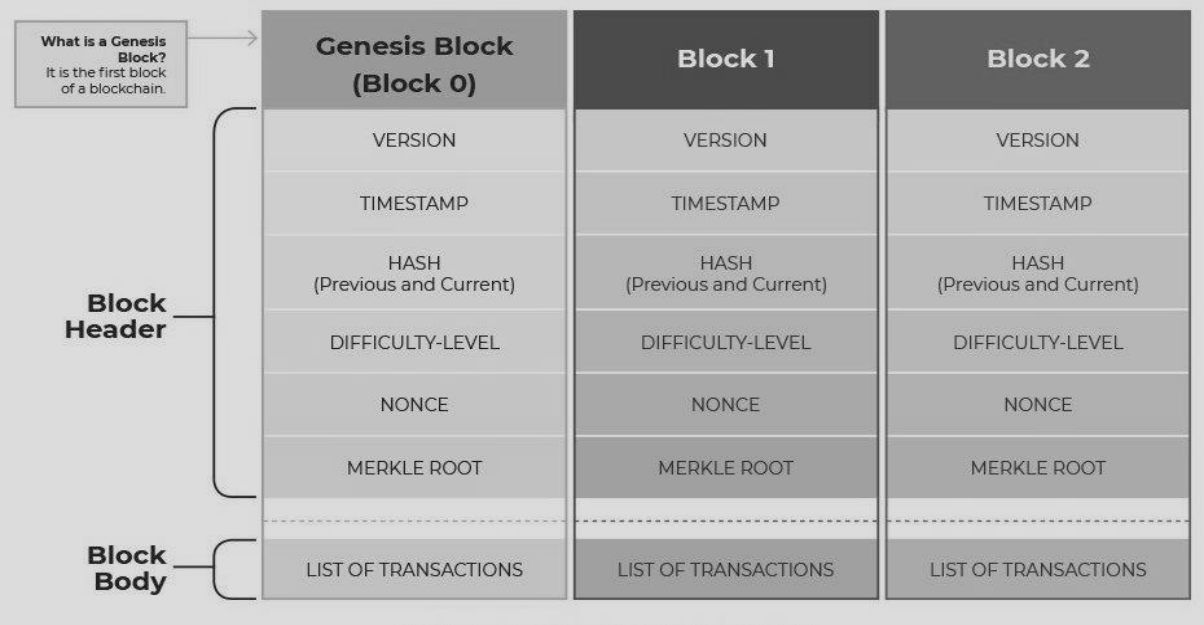

Figure 29: Blockchain architecture

A copy of the data is held by each participant and they can calculate the current "state" of the system independently. In this way, there cannot be any one point of failure. A synchronisation mechanism allows the users to resume the latest state of the system when a participant fails. This can be done using Byzantine fault tolerance (BFT) [18] like proof of work [19] and proof of stake [20].

Blockchain is classified as public if it can be read and accessed by the users. The entire Blockchain can therefore be retrieved by anybody and read by anyone. A private Blockchain can be accessed by a very select group of entities only when it is categorised as such. Depending on who can submit and validate transactions, a Blockchain can also be called permissionless or with permissions. Additionally, Blockchain systems have introduced the concept of "smart contracts" which act to enhance the efficiency of operations. Using Blockchain software, a smart contract performs or enforces a predefined function in accordance with the predefined rules and policies. In summary, the inherent properties of Blockchain technology enable it to be used to deploy a service so then it is reliable where even "trustless" entities can rely on it.

6.2.2 Management system

Any user (Subject) should be able to generate their claims. If a user originates their claims, any cryptocurrency gateway (identity provider) or even another user supporting the Transformation and Verification oracles can validate the statements. There are two types of trust anchors:

strong trust anchors and weak trust anchors. A strong trust anchor gives you the ability to engage with at least one strong claim (G, T, and V). A weak trust anchor, on the other hand, only provides functionality (G, T, and V) for weak assertions. Users are exclusively responsible for claiming storage. As a result, users are in command of two of them, who also have the advantage of having control over their claims and the risks that come with them.

The designs for the Blockchain gateway and Blockchain infrastructure were not picked at random. In actuality, the design was meant to closely reflect how people verify each other's identities everyday. A person or a group of people's identities can be described as the sum of their traits [MW]. These attributes are normally uncountable by this definition and some may be tangible while others are insubstantial. The fundamental aspect is that the aggregation of these attributes gives an individual or organisation individuality.

6.3 A Case Study on the Saudi e-Government Portal (Yesser)

In Saudi Arabia, the information security policy requires all government agencies to post adequate security measures in accordance with Saudi laws, laws, policies, rules and standards. It remains the most challenging task to determine a relevant mix of security controls despite all of the security standards being met. Information systems can be better secured according to the national security policy recommendations. When the Yesser [33] program was launched back in 2007, this document was developed. Over time, it has been able to safeguard the e-government structure but cyberattacks cannot be avoided. Saudi Arabia's electronic government system will be examined and evaluated in this paper.

According to the Kingdom of Saudi Arabia's e-government security policy, the kingdom's information resources will be secured by implementing a triple set of measures such as data integrity, confidentiality and availability. To ensure that the information we hold is protected from hazardous threats, to maximise business sustainability, to diminish damage costs and to ensure that we are utilising our information systems effectively, we need information security. This should not be confined to daily operations. Cybersecurity is a powerful tool. Firstly, it gives consumers enough confidence in the Yesser program to increase the likelihood of them receiving a better service. Secondly, the government must realise the importance of information security to have effective and stable relations with other economic sectors. A complete information security system in Saudi Arabia is needed since it will enable the achievement of multiple objectives such as optimising internal business structures and ensuring the free trade

of information. Keeping track of taxpayers, offenders and defaulters has been made easier by sharing personal identification numbers with the appropriate government departments. By improving the business conditions, curtailing social ills and improving the country's external relations, the ease of doing business has improved. By bringing foreign investments into a country, foreign investors strengthen the country's competitive position in the international markets.

Security in e-government improves the government's effectiveness and ability to deal with economic issues. The government can adjust its policies more effectively with verifiable information if secured information is shared. In this way, the government's Ministry of Health can develop advocacy and sensitisation campaigns for college students who suffer from diabetes. As a result, the students can live a healthier lifestyle. The government Ministry of Higher Education can also improve the curriculum based on information regarding graduate employability. Furthermore, if implemented properly, the country will benefit both globally and regionally from this information security policy.

6.4 Security Assessments on Saudi e-Government Website (Yesser)

A comprehensive technical performance analysis of the Saudi e-government website was carried out between February 2020 and July 2020. The evaluation was performed on the basis of the number of vulnerabilities detected during each scan. The tools used to scan Yesser were Rapid7, Zap and Nessus. The status of the website was active, and the severity of the vulnerabilities are represented in Figure 30. The scale of the vulnerability severity has been categorised into Critical, High, Moderate, Low and Informal. No critical vulnerabilities were found during the scans as such. A high vulnerability was detected during the Rapid7 scan where the CN (Common Name) field in certificate X.509 varies in terms of the entity name from where the certificate was provided. One moderate vulnerability was discovered using the Zap scan and two moderate vulnerabilities were found with Nessus. The Zap scan showed 10 low vulnerabilities whereas 10, 2 and 22 informal vulnerabilities were found using Rapid7, Zap and Nessus, respectively. During the Zap scan, a medium level alert was received, detecting the absence of a header in the X-frame options. The X-frame HTTP header should have been set at all time son all the Yesser web pages.

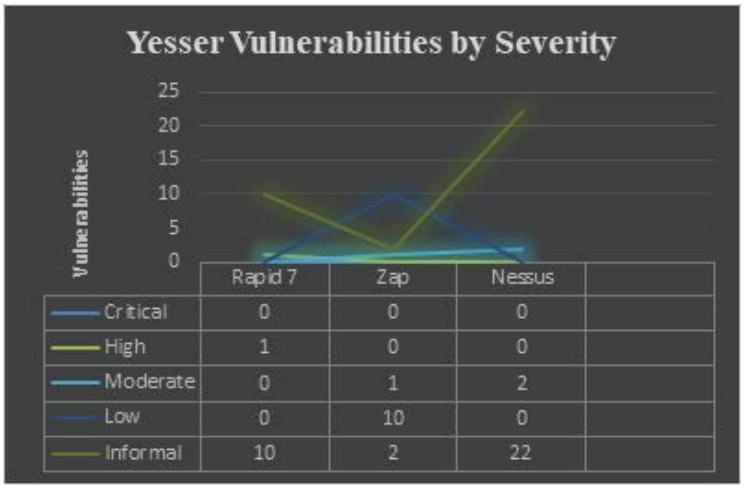

Figure 30: Saudi e-Government website (Yesser) vulnerabilities study

6.5 Integration of E-Governance Functions into Blockchain

The integration of the proposed Blockchain-based e-government framework is illustrated in Figure 31. The proposed framework has five layers that include the Application or Service Layer, the proposed Blockchain Access Layer, the Network Layer and the Ledger Storage Layer. The Application is responsible for hosting the devices that give access to the computational resources and storage. The Blockchain Access Layer is responsible for giving access to the actual Blockchain layer by reviewing, accepting and generating new requests. The Blockchain Layer is responsible for hosting users from the e-government organisations for validating the transactions and giving access to the users after authentication. The Network Layer acts as a communication channel between the users, government organisations and ledger storage. Finally, IPFS (Interplanetary File System) is added to overcome any storage issues. On/off chain data such as documents, images, PDFs and smart contracts are stored in the Blockchain Shared Replicated Ledger that can be deleted or updated in future.

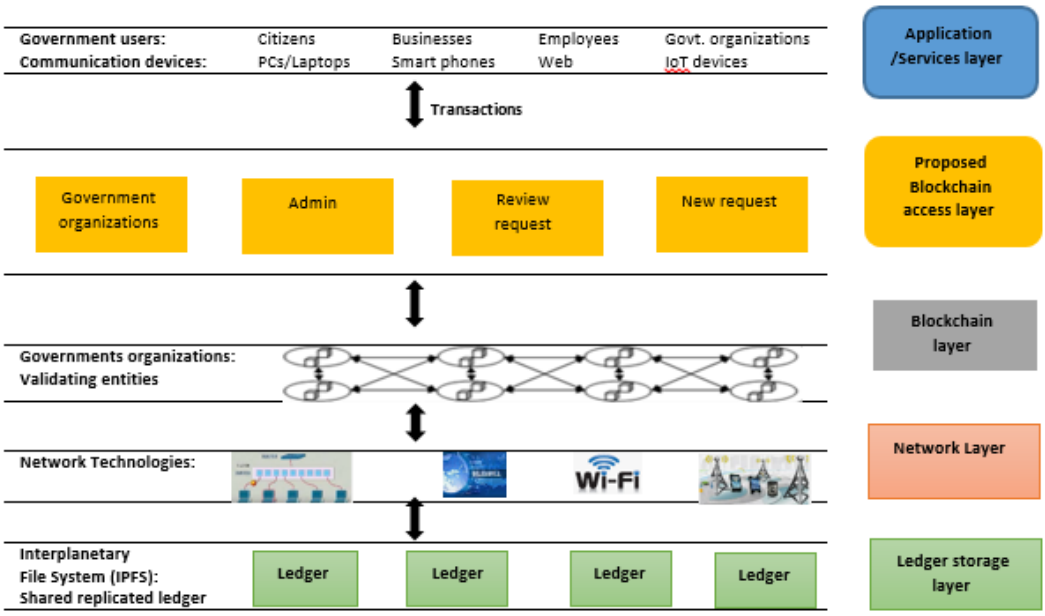

Figure 31: Layers of the Blockchain-enabled e-government system

6.6 Enhanced Secured E-Governance Framework

E-governance systems are highly vulnerable to threats and attacks both internal and external for the many reasons already discussed. Keeping an eye on these vulnerabilities and taking the correct precautionary measures beforehand is extremely important. One of the major objectives behind the integration of Blockchain into the existing e-governance system is to provide security and facilitate trusted transactions across the system. Figure 32 is an illustration of the security perspective of the integration of Blockchain into the Saudi e-governance system.

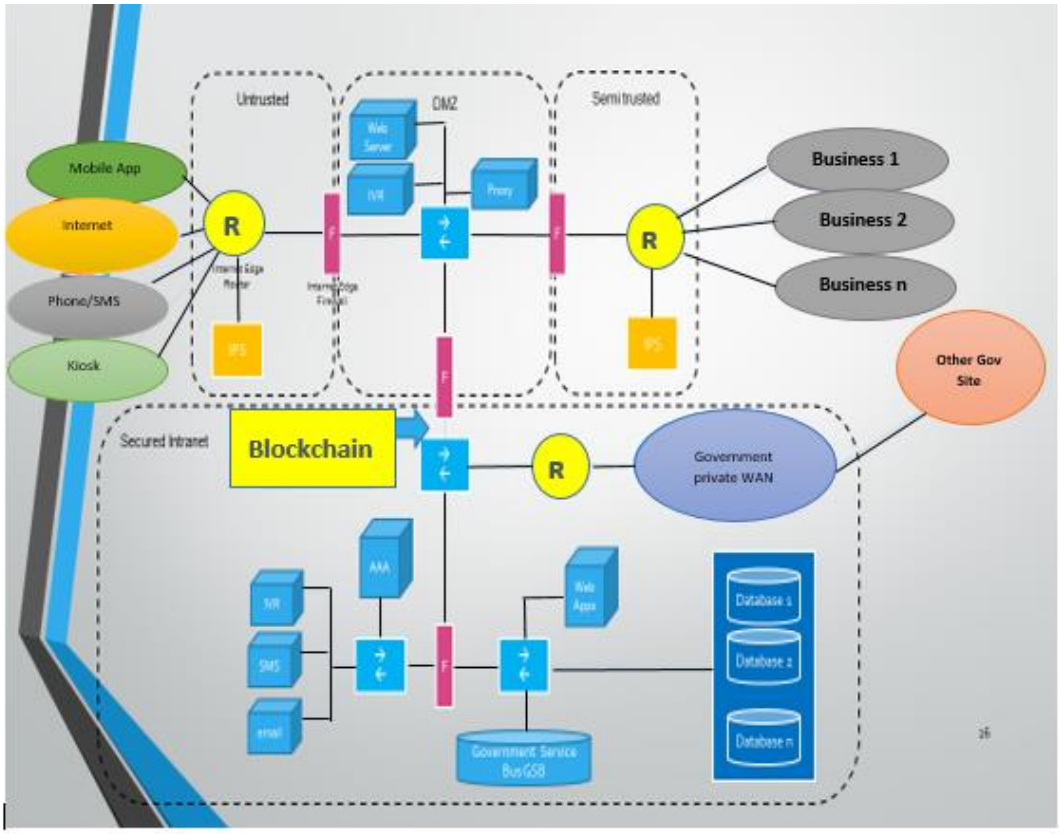

Figure 32: Enhanced secured e-governance framework

In the figure above, the blocks are represented by the letter 'R', the router firewall is represented by letter 'F' and the switches are represented by an arrow sign '→'. IPS represents the standard "Intrusion Prevention System". The left-hand side is labelled as untrustworthy since it is the public network where the end users' network security policies are open and can't be monitored according to government mandates. The right-hand side is connected to various firms in order for the e-government system to fulfil the users' service requests. The DMZ (demilitarised zone) is the zone in between, serving as a communication termination point for both the semi-trusted and untrusted zones. The DMZ is protected by three perimeter firewalls and two unique intrusion prevention systems (IPS) to deal with any hostile traffic. Blockchain has been deployed between the DMZ and the Secured Intranet zone. By incorporating Blockchain technology between the two secure zones, a high level of data confidentiality, data integrity, privacy, trust and access control can be achieved. Separate private and public keys for access, decentralised blocks in the database, consensus protocols for authentication, peer-to-peer approvals and decentralisation are all features of Blockchain technology that preserve security.

A Blockchain-based framework using Hyperledger fabric has been proposed as an outcome of this research, whereby each organisation represents a government organisation. A Blockchain

access layer that acts as an intermediary layer between Blockchain and the application layer has been developed. It connects the Blockchain connection string for a specific organisation with the application layer that represents the application service of each organisation. Hence it is not required to migrate to a new system rather than integrating with the current system where Blockchain is utilised as an integration layer by a specific business use-case, thus solving one of the major issues of Blockchain. One of the major drawbacks of Blockchain is that every participating node requires authentication which makes it slow, hence we differentiate between on/off chain data. We have added a database as a service layer connected to the current system. Another drawback is addressed in this architecture, which is having a huge amount of data. We have added IPFS to overcome any storage issues. An active directory has been added to engage in user authentication and authorisation. Other services have been added related to either the application or the service layer. Unlike the existing Saudi e-governance, the proposed model has better security as it relies on a completely decentralised database.

In the proposed framework, there are three different access scenarios. The three access scenarios characterise the proposed system as Consumer to Government (C2G), Business to Government (B2G) and Government to Government (G2G).

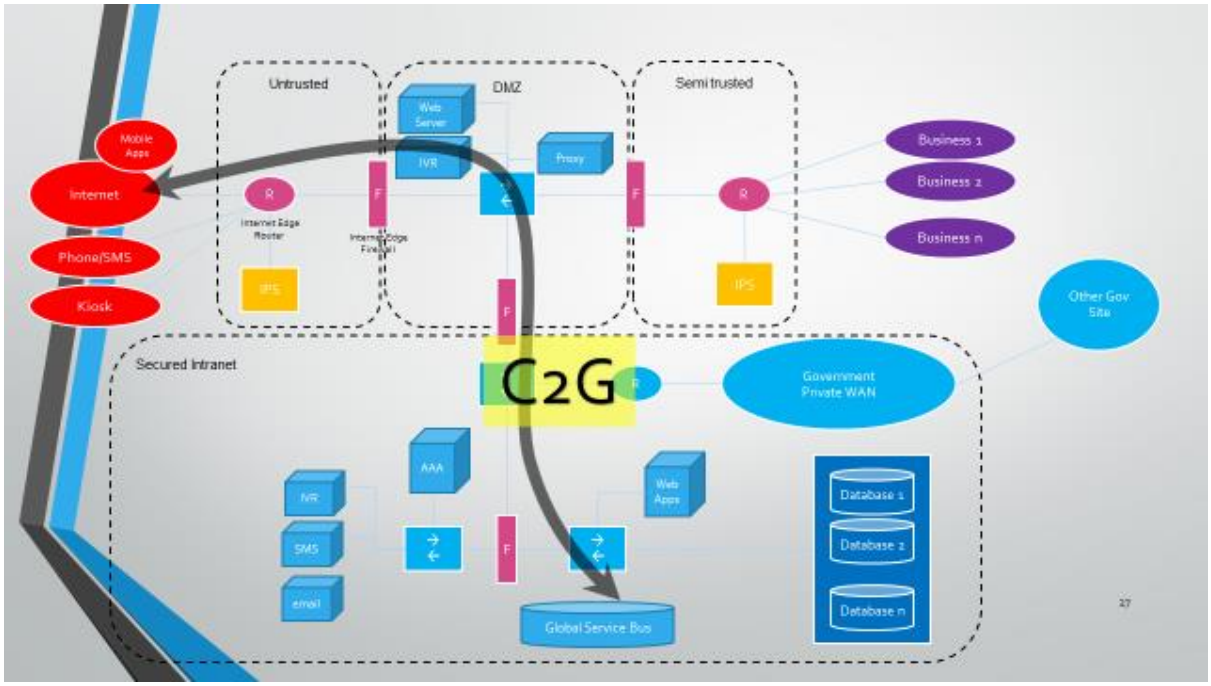

Figure 33: Consumer to Government

i. C2G (Consumer to Government) delivers government services directly to consumers via the internet, public kiosks, mobile applications etc as shown in Figure 33.

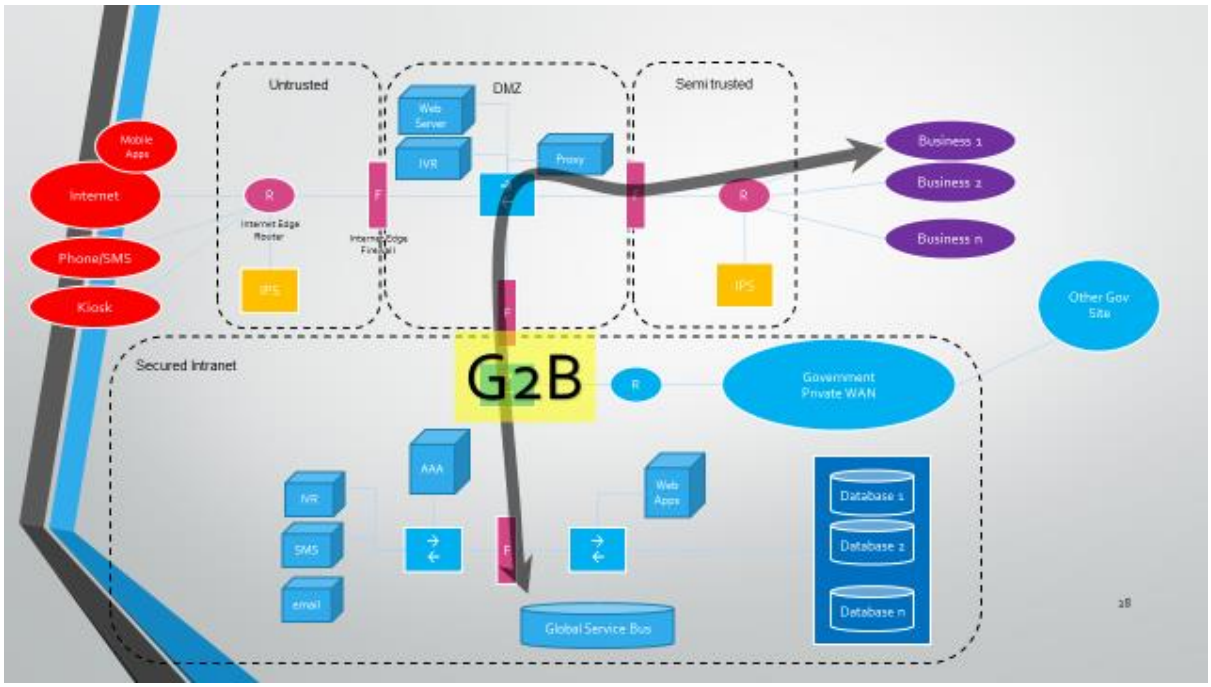

Figure 34: Business to Government

ii. G2B (Government to Business) connects governments directly to businesses as shown in Figure 34.

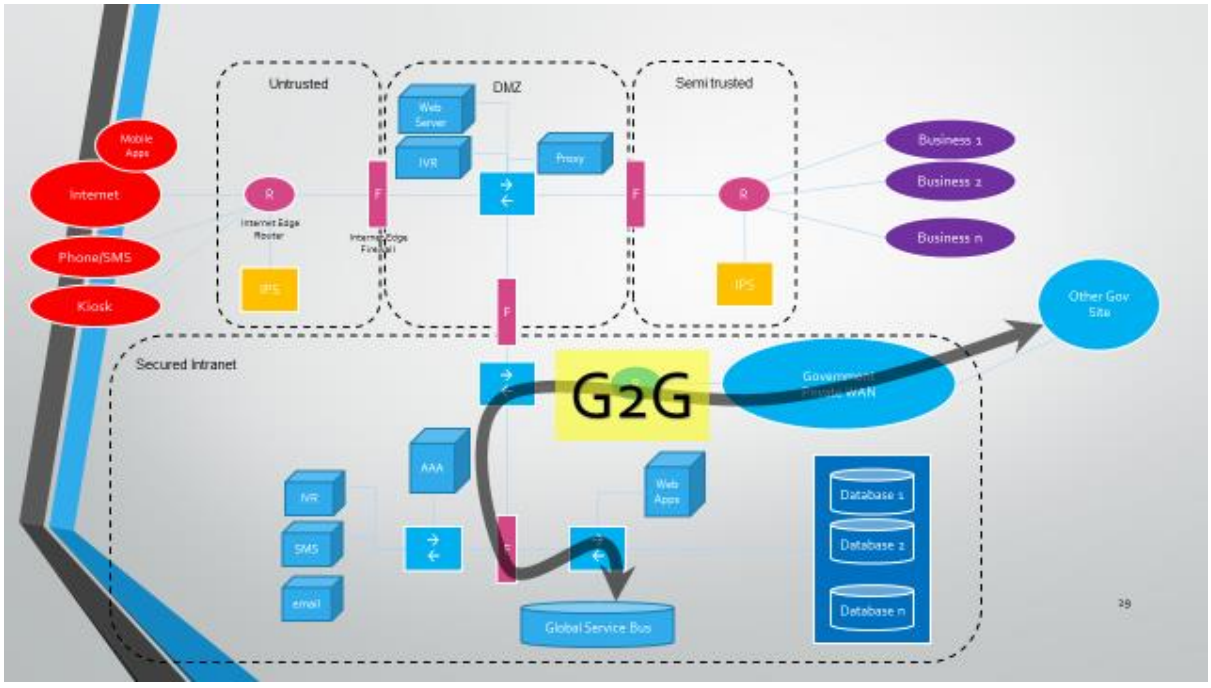

Figure 35: Government to Government

iii. G2G (Government to Government) connects to other government websites that are owned by government organisations or ministries as shown in Figure 35.

6.6.1 Validation and Research Findings

In the beginning, the Blockchain was used exclusively for cryptocurrencies. Since its inception, Blockchain technology has attracted the curiosity of many academics interested in using it for purposes other than financial transactions. Its features including transparency and security have drawn a lot of attention. E-governance is one of these fields with the goal of providing better and more secure services to citizens, corporations and governments. The number of articles involving Blockchain research has risen dramatically in recent years. The majority of suggested Blockchain solutions are in the early stages of development with just a tiny fraction having progressed to system evaluation and prototype implementation.

1. Yesser Vulnerability Scan before applying Blockchain

The results obtained by subjecting the Saudi e-Government website (YESSER) to penetration testing using NESSUS, Rapid7 and ZAP are presented below. Table 13 depicts the results obtained from the NESSUS scan, Table 14 depicts the results obtained from the Rapid7 scan and Table 15 depicts the results obtained from the ZAP scan. The results represent assessment of threat levels based on the three tools we used determining threat levels for a range of vulnerabilities described in a number of documents as referenced in the Tables below. It is important to note that, the table data is based on the reports generated using the three tools.

Table 13: Yesser Nessus scan

High	Medium	Low	Info
0	2	0	22

	Vulnerability	Description	Threat Level
1.	F5.BIG-IP Cookie Remote Information Disclosure	"The remote load balancer suffers from an information disclosure vulnerability." [111] "The remote host with F5 BIG-IP load balancer encodes the IP address on behalf of actual web server within a cookie. Investigating information after 'BIGipServer', it is found that, they are configured by the user and may contain logical name of the device which may disclose sensitive information such as internal IP addresses and names." [Ref 111, https://www.tenable.com/plugins/nessus/20089]	Medium
2.	Web Application Potentially	"The remote web server may fail to mitigate a class of web application vulnerabilities." [112]	Medium

High	Medium	Low	Info
Vulnerable to Clickjacking	“The remote web server does not set an X-Frame-Options response header or a Content-Security-Policy 'frame-ancestors' response header in all content responses. This could potentially expose the site to a clickjacking or UI redress attack in which an attacker can trick a user into clicking an area of the vulnerable page that is different than what the user perceives the page to be resulting in a user performing fraudulent or malicious transactions. X-Frame-Options have been proposed by Microsoft as a way of mitigating clickjacking attacks and it is currently supported by all major browser vendors. Content-Security-Policy (CSP) has been proposed by the W3C Web Application Security Working Group, with increasing support among all major browser vendors, as a way to mitigate clickjacking and other attacks. The 'frame-ancestors' policy directive restricts which sources can embed the protected resource.” [Ref 112, https://www.tenable.com/plugins/nessus/85582]		

Table 14: Yesser Rapid7 scan

High	Medium	Low	Info
1	0	0	0

	Vulnerability	Description	Threat Level
1.	Certificate-common-name-mismatch	“The subject common name (CN) field in the X.509 certificate does not match the name of the entity presenting the certificate.” [113] “Before issuing a certificate, a Certification Authority (CA) must check the identity of the entity requesting the certificate, as specified in the CA's Certification Practice Statement (CPS). Standard certificate validation procedures require the subject CN field of a certificate to match the actual name of the entity presenting the certificate. To detect and prevent active eavesdropping attacks, the validity of a certificate must be verified or else an attacker could launch man-in-the-middle attack and gain full control of the data stream. A CN mismatch most often occurs due to a configuration error, although it can also indicate that a man-in-the-middle attack is being conducted.” [Ref 113, https://www.rapid7.com/db/vulnerabilities/certificate-common-name-mismatch/]	High

Table 15: Yesser Zap Scan

High	Medium	Low	Info
0	3	6	2

	Vulnerability	Description	Threat Level
1.	Absence of Anti-CSRF Tokens	"No Anti-CSRF tokens were found in the HTML submission form." [114] "CSRF exploits the trust that a website has for a user which is in contrast to cross-site scripting (XSS) which exploits the trust that a user has for a website. Like XSS, CSRF attacks are not necessarily cross-site but they can be." [Ref 114, https://www.zaproxy.org/docs/alerts/10202/]	Medium
2.	Content Security Policy (CSP) Header Not Set	"Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks including Cross Site Scripting (XSS) and data injection attacks." [115] "These attacks are used for everything from data theft to site defacement or the distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page. Covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files." [Ref 115, https://www.zaproxy.org/docs/alerts/10038/]	Medium
3.	Missing Anti-clickjacking Header	"The response does not include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options to protect against 'ClickJacking' attacks." [116]	Medium
4.	Cookie: No Http Only Flag	"A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page, the cookie will be accessible and can be transmitted to another site. If this is a session cookie, attacker may launch session hijacking attack." [Ref 116, https://www.zaproxy.org/docs/alerts/10010/]	Low
5.	Cookie Without Secure Flag	"A cookie has been set without the secure flag which means that the cookie can be accessed via unencrypted connections." [Ref 117, https://www.zaproxy.org/docs/alerts/10011/]	Low
6.	Cookie without Same Site Attribute	"A cookie has been set without the Same Site attribute which means that the cookie can be sent as a result of a 'cross-site' request." [118] "The Same Site attribute is an effective counter measure against cross-site request forgery, cross-site script inclusion and timing attacks." [Ref 118, https://www.zaproxy.org/docs/alerts/10054/]	Low
7.	Cross-Domain JavaScript Source File Inclusion	"The page includes one or more script files from a third-party domain." [Ref 119, https://www.zaproxy.org/docs/alerts/10017/]	Low

High	Medium	Low	Info

8. Timestamp Disclosure – Unix	"A timestamp was disclosed by the application/web server – Unix" [Ref 120, https://www.zaproxy.org/docs/alerts/10096/]	Low
9. X-Content-Type-Options Header Missing	"The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'." [121] "This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current and legacy versions (early 2014) of Firefox may use the declared content type (if one is set), rather than performing MIMEsniffing." [Ref 121, https://www.zaproxy.org/docs/alerts/10021/]	Low

2. *Vulnerability Scan of the Proposed Architecture after applying Blockchain*

The results obtained by subjecting the proposed architecture to penetration testing using NESSUS, Rapid7 and ZAP are presented below.

This section contains Table 16 (depicting the results obtained from the NESSUS scan), Table 17 (depicting the results obtained from the Rapid7 scan) and Table 18 (depicting the results obtained from the ZAP scan).

Table 16: The new proposed Nessus scan

High	Medium	Low	Info
0	0	0	6

Table 17: The new proposed Rapid7scan

High	Medium	Low	Info
0	0	0	0

Table 18: The new proposed Zap scan

High	**Medium**	**Low**	**Info**
0	**0**	**2**	**2**

Vulnerability	**Description**	**Threat Level**
1. Timestamp Disclosure - Unix	"A private IP has been found in the HTTP response body. This info is useful when seeking to carry out attacks on internal systems." [122]	Low

High	Medium	Low	Info
	A timestamp was disclosed by the application/web server – Unix [Ref 122, https://www.zaproxy.org/docs/alerts/10096/]		
2.X-Content-Type-Options Header Missing	"The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'." [123] "This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing." [Ref 123, https://www.zaproxy.org/docs/alerts/10021/]	Low	

A comparison of the results obtained from the penetration testing of both YESSER and the proposed Blockchain-based architecture is presented in Table 19. A high degree of contrast can be seen by comparing the vulnerability persistency in YESSER to the vulnerability persistency in the proposed architecture. Figures 36 and 37 present the graphical representation of the results obtained before and after scanning both websites. Based on the scanning, the proposed Blockchain-based architecture possesses a very low degree of vulnerability compared to YESSER with only two threats of least intensity. This indicates its capability of the proposed framework to prevent any type of vulnerability.

Table 19: Yesser and the new proposed vulnerability persistency

Vulnerability	Threat Level	Yesser	New Proposed
1 Certificate-common-name-mismatch	High	✓	✗
2. F5.BIG-IP Cookie Remote Information Disclosure	Medium	✓	✗
3. Web Application Potentially Vulnerable to Clickjacking	Medium	✓	✗
4. Absence of Anti-CSRF Tokens	Medium	✓	✗
5. Content Security Policy (CSP) Header Not Set	Medium	✓	✗
6. Missing Anti-clickjacking Header	Medium	✓	✗
7. Cookie "No Http Only" Flag	Low	✓	✗
8. Cookie "Without Secure" Flag	Low	✓	✗
9. Cookie "without Same Site" Attribute	Low	✓	✗
10. Cross-Domain JavaScript Source File Inclusion	Low	✓	✗
11. Timestamp Disclosure - Unix	Low	✓	✓
12. X-Content-Type-Options Header Missing	Low	✓	✓

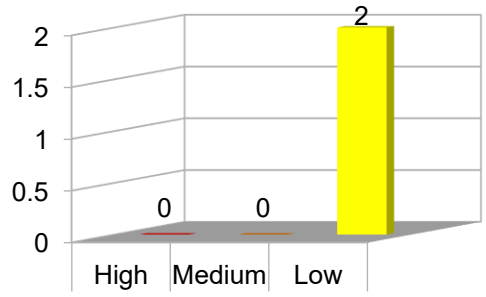

Figure 36: Blockchain-enabled new proposed vulnerabilities graph

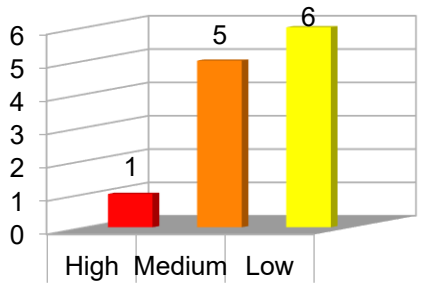

Figure 37: Yesser vulnerabilities graph

In this work, we used the Hyperledger Caliper to measure the performance of the Blockchain implementation with a set of predefined use cases. The main target when using Caliper was testing the number of transactions per second and testing latency. We focused on these two parameters only as one of Blockchain's main drawback is a lack of speed when it is compared to any of the database systems. Hyperledger Caliper indicates that the chosen parameters per Blockchain components (CPU%(max), CPU%(avg), Memory(max) [GB], Memory(avg) [GB], Traffic In [MB], Traffic Out [MB], Disc Write [MB], and Disc Read [KB]). In short, it measures the network, memory, CPU utilisation and disk storage.

When we applied these test cases, we found that when using levelDB, the Blockchain has better results than with couchDB. There was an increase in TPS. As a result, we focused on saving the meta data in the Blockchain and saving the off-chain data for any periodic reports.

Table 20: Hyperledger Caliper results when the peer node uses couchDB

Name	Succ	Fail	Send Rate (TPS)	Max Latency (s)	Min Latency (s)	Avg Latency (s)	Throughput (TPS)
empty-contract-submit-1000	1000	0	248.1	1.93	0.15	1.39	169.2
empty-contract-submit-5000	5000	0	243.1	11.01	0.12	7.64	158.4
empty-contract-submit-10000	10000	0	244.3	24.05	0.10	17.06	154.0
create-asset-1000	1000	0	264.1	3.12	0.13	2.21	145.8
create-asset-5000	5000	0	265.6	16.77	0.18	12.44	140.6
create-asset-10000	10000	0	257.4	33.72	0.15	25.19	137.9
empty-item-1000	1000	0	212.2	2.42	0.10	1.80	144.9
empty-item-5000	5000	0	259.0	11.18	0.15	7.62	164.3
empty-item-10000	10000	0	239.8	23.76	0.12	17.45	152.9
create-item-1000	1000	0	265.0	4.25	0.26	3.53	126.7
create-item-5000	5000	0	263.5	20.88	0.30	17.79	126.4
create-item-10000	10000	0	256.9	41.89	0.28	36.17	124.4
transfer-item-1000	1000	0	279.6	4.72	0.58	3.78	124.7
transfer-item-5000	5000	0	275.7	23.86	0.28	20.18	120.9
transfer-item-10000	10000	0	247.0	50.14	0.31	43.27	111.3

Table 21: Hyperledger Caliper results when the peer node uses levelDB

Name	Succ	Fail	Send Rate (TPS)	Max Latency (s)	Min Latency (s)	Avg Latency (s)	Throughput (TPS)
empty-contract-submit-1000	1000	0	268.8	0.61	0.03	0.14	267.0
empty-contract-submit-5000	5000	0	280.4	0.33	0.03	0.10	279.9
empty-contract-submit-10000	10000	0	294.0	0.27	0.03	0.10	293.8
create-asset-1000	1000	0	223.4	0.46	0.03	0.15	221.9
create-asset-5000	5000	0	287.8	0.38	0.03	0.11	287.2
create-asset-10000	10000	0	284.6	0.29	0.04	0.11	284.2
empty-item-1000	1000	0	298.9	0.28	0.03	0.10	296.2
empty-item-5000	5000	0	283.2	0.29	0.03	0.10	282.6
empty-item-10000	10000	0	295.0	0.32	0.03	0.10	294.8
create-item-1000	1000	0	265.2	2.10	0.22	1.49	193.9
create-item-5000	5000	0	256.5	10.38	0.20	7.05	187.8
create-item-10000	10000	0	246.9	21.62	0.22	14.44	190.4
transfer-item-1000	1000	0	275.7	3.06	0.32	2.10	187.2
transfer-item-5000	5000	0	259.8	14.34	0.27	10.19	184.0
transfer-item-10000	10000	0	257.8	28.09	0.15	20.11	181.4

With the increasing the number of the transaction stress tests, we found that some components (i.e., peer, DB) averaged a resource utilisation level of around 90%, while other components such as the orderer nodes had a fixed percentage of 20-30%. It is important to keep an eye on increasing the CPU utilisation for the DB and peer nodes. We have applied these results to a single channel network. We found that the CPU utilisation of DB is huge compared to other Blockchain components.

Another important factor to enhance the Blockchain speed is where each smart contract should do a single task. As a result, it is stored in the world state as a single transaction. In the aforementioned tables, creating the asset of a smart contract does a simple task, while transferring an item does multiple tasks. We found that with the smaller number of transactions, there was a difference per TPS based on the smart contract complexity.

In this work, we used the Hyperledger Caliper to measure the performance of the Blockchain implementation according to a set of predefined use cases. The main target when using Caliper was testing the number of transactions per second and testing latency. We focused on these two parameters only as one of Blockchain's main drawbacks is a lack of speed when it is compared to any database system. Hyperledger Caliper indicates that the parameters per each Blockchain

component are (CPU%(max), CPU%(avg), Memory(max) [GB], Memory(avg) [GB], Traffic In [MB], Traffic Out [MB], Disc Write [MB] and Disc Read [KB]). In short, it measures the network, memory, CPU utilisation and disk storage.

When we applied these test cases, we found that when using levelDB, the Blockchain performed better than couchDB. We saw an increase in TPS. As results, we focused on saving, in Blockchain, the meta data. This was as well as saving the data off-chain for any periodic reports.

Table 22: Hyperledger Caliper results when the peer node uses couchDB

Name	Succ	Fail	Send Rate (TPS)	Max Latency (s)	Min Latency (s)	Avg Latency (s)	Throughput (TPS)
empty-contract-submit-1000	1000	0	248.1	1.93	0.15	1.39	169.2
empty-contract-submit-5000	5000	0	243.1	11.01	0.12	7.64	158.4
empty-contract-submit-10000	10000	0	244.3	24.05	0.10	17.06	154.0
create-asset-1000	1000	0	264.1	3.12	0.13	2.21	145.8
create-asset-5000	5000	0	265.6	16.77	0.18	12.44	140.6
create-asset-10000	10000	0	257.4	33.72	0.15	25.19	137.9
empty-item-1000	1000	0	212.2	2.42	0.10	1.80	144.9
empty-item-5000	5000	0	259.0	11.18	0.15	7.62	164.3
empty-item-10000	10000	0	239.8	23.76	0.12	17.45	152.9
create-item-1000	1000	0	265.0	4.25	0.26	3.53	126.7
create-item-5000	5000	0	263.5	20.88	0.30	17.79	126.4
create-item-10000	10000	0	256.9	41.89	0.28	36.17	124.4
transfer-item-1000	1000	0	279.6	4.72	0.58	3.78	124.7
transfer-item-5000	5000	0	275.7	23.86	0.28	20.18	120.9
transfer-item-10000	10000	0	247.0	50.14	0.31	43.27	111.3

Table 23: Hyperledger Caliper results when the peer node uses levelDB

Name	Succ	Fail	Send Rate (TPS)	Max Latency (s)	Min Latency (s)	Avg Latency (s)	Throughput (TPS)
empty-contract-submit-1000	1000	0	268.8	0.61	0.03	0.14	267.0
empty-contract-submit-5000	5000	0	280.4	0.33	0.03	0.10	279.9
empty-contract-submit-10000	10000	0	294.0	0.27	0.03	0.10	293.8
create-asset-1000	1000	0	223.4	0.46	0.03	0.15	221.9
create-asset-5000	5000	0	287.8	0.38	0.03	0.11	287.2
create-asset-10000	10000	0	284.6	0.29	0.04	0.11	284.2
empty-item-1000	1000	0	298.9	0.28	0.03	0.10	296.2
empty-item-5000	5000	0	283.2	0.29	0.03	0.10	282.6
empty-item-10000	10000	0	295.0	0.32	0.03	0.10	294.8
create-item-1000	1000	0	265.2	2.10	0.22	1.49	193.9
create-item-5000	5000	0	256.5	10.38	0.20	7.05	187.8
create-item-10000	10000	0	246.9	21.62	0.22	14.44	190.4
transfer-item-1000	1000	0	275.7	3.06	0.32	2.10	187.2
transfer-item-5000	5000	0	259.8	14.34	0.27	10.19	184.0
transfer-item-10000	10000	0	257.8	28.09	0.15	20.11	181.4

With the increasing the number of transaction stress tests, we found that some components (i.e., peer, DB) average a level of resource utilisation around 90%, while other components such as orderer nodes have a fixed percentage 20-30%. It is important to keep an eye on increasing the CPU utilisation for DB and peer nodes. We have applied these results to a single channel network. We found the CPU utilisation for DB to be huge when it is compared to other Blockchain components.

Another important factor to enhance the Blockchain speed is where each smart contract should do a single task. As a result, it is be stored in the world state as a single transaction. In the aforementioned tables, after creating an asset smart contract to do a simple task, when transferring the item (doing multiple tasks), we found that with the small number of transactions, there is a difference per TPS based on the smart contract complexity.

6.7 Security Considerations

The following section presents a subjective idea related to the security concerns of the Blockchain-based e-governance system. The records of the data stored in Blockchain systems are secured with the help of public key cryptography which protects the system from

inquisitorial attempts at alteration and unaccredited access, whereas the users on the network are given a private key for validation and signing transactions. Digital signatures, along with a certain amount of encryption, are used in the network for having secure, private and reliable access to the records. In the case of Blockchain consensus algorithms, for an attacker to alter a record, it requires him to control at least 51% of the network terminals which is usually impossible to perform [31]. Therefore, an attacker would need to alter every copy of any block on the Blockchain and convince all nodes that the new block is valid in order to change a single block. Furthermore, all user blocks on the proposed network are encrypted with hashing algorithms and incoherent hashes of the transactions are stored in the Blockchain to ensure data confidentiality. Rather than being a centralised system, the data of the users is stored on multiple nodes at various locations which ensures that the system does not have any downtime. Because the DPoS consensus protocol prevents DDoS or DoS attacks, it is impossible for an attacker to attack the system because node registration is required for it to share information with its peers. All of the transactions that are obtained from the nodes on the network are verified by witnesses, thus, rendering any malicious actions initiated by malicious nodes useless.

Table 24: Security preserving features of Blockchain-based e-Governance system

Feature	**Justification**
Human error reduction	Identities and devices authenticated before the network is accessed
Public trust improvement	Individuals have direct control of their information and all network participants are authenticated Direct user control and every participant authenticated
More stability	The consensus mechanism allows for the addition of more devices; hence it is scalable
Reliability	Alteration of the data is next to impossible due to the hashing at each block.
Improved resiliency	Point of failure is avoided
Increased auditability	Tracking of the previous transactions is easy

Feature	Justification
Improved verifiability	Before getting added to the Blockchain, all participating peers validate any new transaction that is happening
Information control	Individuals are responsible for authorising who will access their information Authorisation is done only by those who are responsible
Improved information access	Information is stored at multiple locations which enhances its ease of use and speedy access The data should be different
Efficient and quality data	The data is validated in advance, making it more authentic
Improved transparency	A copy of the Blockchain is shared across all transactions using the consensus mechanism
Reduction in the operational costs	There is no third-party organisation needed to process the transactions No third party involved in data processing
Efficient and improved speed	Authorised nodes can access all records

To ensure the security of the electronic transactions within the framework, a few security services and common security measures are provided. Lightweight clients are preferred by users for storing transactions. It is quite expensive to store the entire Blockchain. To store and process information efficiently, e-government devices need quite a lot of storage capacity and computational strength. This technology is also used in the Delegated Proof of Stake protocol which offers a range of benefits such as scalability, speed, interoperability and transparency.

Elliptic curve cryptography (ECC) is used for digital signatures and encryption by most Blockchain technologies like Bitcoin and Ethereum. An ECCA key uses only 32 bits, whereas an RSA key requires 3072 bits. An ECC key offers the same level of security as an RSA key

(Rivest- Shamir- Adleman). Blockchain technology uses 256-bit ECC keys for a higher level of security. Shorter keys also use less CPU power. In addition, it uses little memory and generates keys quickly. As a result, the proposed framework makes it possible to create transactions and seal blocks more quickly.

6.8 Summary

In fact, distributed ledgers can bring many positive elements into the reform of public services, such as increasing the transaction transparency in e-governance systems and improving and speeding up the public information procedures, as well as creating an inclusive platform for a variety of public sector services. As Blockchain tracks all public transactions irreversibly, all information can now be distributed across a wide range of stakeholders in a truly decentralised manner, not only in the public sector but also in the private sector. The unique feature of the Blockchain, based on peer-to-peer communication, can allow the public service delivery models to be refined and enhanced through this peer-to-peer communication characteristic. This way, the confidence of the public in e-governance services is increased as the public services are transparent, accountable and more efficient. However, integrating Blockchain into e-governance services comes with various challenges such as regulatory clashes and security issues (such as confidentiality, integrity and trust). Many researchers have tried to address the security issues of different e-governance systems. We found that the current e-government systems are not trusted for internet-based transactions and are prone to unauthorised access via insider threats. This work proposes a new Blockchain framework primarily aimed at securing the Saudi e-governance system (Yesser), bringing in confidentiality, access control and trust alongside decentralisation.

Chapter 7: Conclusion and Future Works

7.1 Conclusion

It is believed by the authors of this study that the development of e-government is one of the most important aspects of the country's plan to implement information technology. Although governments are investing a significant amount of money, human resources and technology in this field, the size of the population and the complex requirements of the public service delivery makes implementing new technologies into government services extremely difficult. Because Blockchain is safe against internet attacks and is immune to any attempt to meddle with its history, we can look at it as a potential answer to these problems. The research activities have been increasing dramatically over the past few years as Blockchain technology has expanded beyond cryptocurrencies. It is seen as a breakthrough technology in the field of public services and e-governance and allows for simple and transparent interaction between citizens, corporations and governments. Innovative results are achieved when a Blockchain-based system is properly designed through the combination of accountability, transparency, integrity and confidentiality. Additionally, a distributed Blockchain platform fosters greater participant confidence and enhances trust as the transactions are carried out safely without the permission of a centralised authority. Blockchain technology is the backbone of the modern internet. It is widely used for financial transactions due to its immutable, distributed, transparent and decentralised nature.

To directly address the first research question of this thesis, we reviewed the most recent literature on a variety of security issues that the current e-governance techniques are facing that the existing frameworks have not sufficiently addressed, particularly those relating to trust, data confidentiality and integrity. Our findings show that there are still significant loopholes in the existing e-governance models that require considerable attention. Many researchers have already put their efforts into address the security vulnerabilities found in the existing models. However, a number of current e-governance frameworks and models do not take into account the crucial security requirements such as the presence of distrust in online transactions and unauthorised access by insiders. The results of the thorough literature study, as well as the challenges to the adoption of Blockchain into existing e-governance models, have been

summarised in Chapter 2 of this report. Some of our research findings suggest that despite the success of e-governance in disbursing public services, the frameworks being designed and used by many developed and under-development nations possess some drawbacks and restrictions. According to the reports, roughly one-third of all e-governance framework implementations completely fail, depicting that they are promptly abandoned immediately after being put into place. Furthermore, 50% of e-governance frameworks are labelled as being in partial decline, suggesting that their goals weren't met or that they faced unintended consequences. These failures seem problematic since they equate to a country's e-governance architecture wasting resources and failing to accomplish its intended goals.

To answer the first research question, Chapter 4 elaborates on identifying the risks and vulnerabilities related to the current e-governance systems in use around the world. We used the Saudi Arabian e-governance system as an illustrative case study for our research. The Saudi government has embraced and entered into a new technological era where technology is used as a tool to improve connectivity, government services and communication. Yesser, Saudi Arabia's electronic government system, is one such system that is essential to achieving the Saudi Vision 2030. Therefore, it is crucial that the Yesser website has proper security as a result. We evaluated the website using three penetration testing tools, namely Zap, Rapid7 and Nessus. The experimental results indicate that the Yesser website includes vulnerabilities ranging from a moderate to severe level.

The deployment of suitable security protocols by the authorities is one of the requirements of Saudi Arabia's information security policy. Regardless of the government's information security policy, which suggests a variety of security measures to secure the information systems, ensuring an appropriate security control mechanism is difficult. Improvements have been made to the e-governance framework since 2007. However, they have utterly failed to prevent cyberattacks. The goal of the research presented in this thesis is to evaluate how sensitive the Saudi Arabia's e-government services are to cyberthreats. According to Saudi Arabia's e-governance security strategy, data integrity, confidentiality and availability are the most crucial security elements. Any e-government system's daily operations shouldn't be restricted by information security frameworks. Instead, they should minimise the damage costs without engaging in a trade-off with the effectiveness of information security. Information security in turn shouldn't compromise the public services; it should increase the amount of secure and safe transactions, making them easy and efficient. The Yesser program must deliver

efficient and effective services and fill in the gaps across diverse economic sectors. As a consequence, Saudi Arabia must implement its information security policy effectively.

To address the second research question, we determined that the security policy of the Saudi Arabian e-governance framework has been the subject of extensive research for a while. In this study, we conducted research to determine whether the key factors have a significant impact on e-governance in Saudi Arabia, both positively and negatively. The research findings suggest that there is a lot of room for Blockchain technology adoption in Saudi Arabia as examined through the Structured Literature Review results in Chapter 5. Numerous studies discuss using Blockchain technology and possess a lot of contributions such as an e-voting application to use the Blockchain's digital identity, smart cities and its use in the healthcare sector. Furthermore, they demonstrate Blockchain's features by allowing multiple entities to share its data.

Considerable attention has been given to the integration of Blockchain technology into e-governance models. However, there are still a lot of unresolved issues, giving researchers a chance to look into them and investigate any loopholes in this area's future research. Numerous studies support the claim that public sector domains are not particularly interested in implementing Blockchain in their infrastructure. One explanation could be that there hasn't been a lot of experimental evidence in this research area yet. Greater efforts need to be put into convincing governments to employ Blockchain for their e-governance systems. According to our literature review, there are still many technological challenges that need to be resolved, including those related to scalability, interoperability, configurability, reliability and security. However, it is not yet apparent how much improvisation will be needed to overcome these difficulties. Therefore, it is essential to establish technological standards for Blockchain and to carefully choose the design elements in line with the goals of the public sector domain. Moreover, despite the recent surge in interest in Blockchain, there are no established standards indicating that it is the ideal option, particularly for e-governance applications. Therefore, irrespective of where it is used, a strategy is required to assess the appropriateness of Blockchain as a solution that is built on a conceptual knowledge of public procedures. This will lead to the introduction of Blockchain design protocols that take into consideration the organisational and technological aspects of such processes.

Finally, for the second research question, this study found that Blockchain was first solely employed in relation to cryptocurrency-based financial transactions. For the past several years, researchers who have wished to utilise the technology for systems other than monetary transactions have been intrigued by Blockchain's attributes including transparency, data security and its decentralised network. One of

these disciplines is e-governance, which aims to offer citizens, businesses and governments improved and more secure services. Blockchain-related articles have become much more prevalent in recent years. A small percentage of proposed Blockchain solutions have advanced to system evaluation and even prototype implementation, while a handful of them have progressed to the early stages of development. To add to this emerging field of research, this work proposes a novel framework for securing an e-governance model utilising Blockchain, with Saudi Arabia as a case study. Decentralisation, along with security, confidentiality and access control, are all features of our proposed model for e-government services. The experimental results depict a clear contrast before and after the incorporation of Blockchain technology into the e-governance portal with the achievement of a higher degree of security. Due to the variety of factors discussed in this study, the e-governance systems are extremely susceptible to internal and external threats and attacks. It is crucial to keep an eye out for these kinds of vulnerabilities and to take the appropriate safety precautions beforehand. The provision of security and the facilitation of trustworthy transactions throughout the system are two of the main goals driving the integration of Blockchain into the current e-governance framework. Some of the core features of the proposed Blockchain-based Saudi e-governance framework (YESSER) are:

- The design and implementation of an e-governance framework using Blockchain.
- Enhancing the public trust with added security features.
- Enhancing the service efficiency.
- Scalable architecture.

7.2 Future Work

Despite the widespread emphasis given to the potential applications of Blockchain technology, several issues still need to be resolved before this technology can be adopted for a fully functional e-governance model. Researchers now have many chances to contribute to, consider and explore potential research opportunities in this domain. The limited number of scholarly studies demonstrates the little interest in implementing Blockchain in the public sector domain. This is also consistent with the researchers' lack of empirical support which has led many to question the advantages and potential of Blockchain-based systems to enhance public services. Therefore, a more practical study is required to examine the benefits and drawbacks of Blockchain technology adoption in the public sector domain.

Adding Blockchain to the proposed framework will make the public service delivery in Yesser more secure and will prevent the information integrity from being compromised. Since we are dealing with a decentralised system, it is resistant to any unauthorised modifications or

alterations to the data, hence it introduces a high level of trust. The researcher will continue to engage in a qualitative evaluation of the proposed Blockchain framework to determine whether it is able to prevent some of the potential threats to security in e-governance systems presented below:

i. DDOS attack.
ii. Attack on authorisation and authentication.
iii. Threat to anonymity.

References

1. Abdelhamid, M., and Hassan, G. (2019) 'Blockchain and smart contracts' In *Proceedings of the 2019 8th international conference on software and information engineering. ICSIE* 19 New York, NY, USA: Association for Computing Machinery 9195. https://doi.org/10.1145/3328833.3328857.
2. Abdullah, A., Rogerson, N.S., Fairweather, B., and Prior, M. (2006) 'The motivations for change towards e-government adoption: Case studies from Saudi Arabia', *E-government Workshop September 11 2006, Brunel University, West London, UB8 3PH*, 6 (1), pp. 1-21. Retrieved July 8, 2019, from https://www.researchgate.net/profile/Simon_Rogerson/publication/228950754_THE_MOTIVATIONS_FOR_CHANGE_TOWARDS_E-GOVERNMENT_ADOPTION_CASE_STUDIES_FROM_SAUDI_ARABIA/links/58ad5f6392851c3cfda085fc/THE-MOTIVATIONS-FOR-CHANGE-TOWARDS-E-GOVERNMENT-ADOPTION-CASE-
3. Alateyah, S., Crowder, R. M., and Wills, G. B. (2013) 'Factors affecting the citizen's intention to adopt e-government in Saudi Arabia', *International Journal of Social, Human Science and Engineering,* 7 (9), pp. 80-85. Available at: https://eprints.soton.ac.uk/356777/1/81_factors_affecting_the.pdf
4. Albrahim, R., Alsalamah, H., Alsalamah, S., and Aksoy, M. (2018) 'Access Control Model for Modern Virtual e-Government Services: Saudi Arabian Case Study', *International Journal of Advanced Computer Science and Applications*, 9 (8), pp. 357-364. Available at: https://pdfs.semanticscholar.org/ebb0/10ac868b6bb721a9db5d2bc33e24cf48895b.pdf
5. Ali, O., Soar, J., and Yong, J. (2014) 'Impact of cloud computing technology on e-government.' In *International conference on information and software technologies*. Springer, pp.272-290
6. Alizadeh, T., and Shearer, H. (2015) 'A snapshot of high-speed broadband responses at local government level in Australia: a marriage between federally funded initiatives and locally driven innovations?', *Australian planner*, 52 (1), pp. 42-50. doi:10.1080/07293682.2015.1019754
7. Alfarraj, O., Alhussain, T. and Abugabah, A. (2013) 'Identifying the factors influencing the development of e government in Saudi Arabia: The employment of grounded theory techniques,' *International Journal of Information and Education Technology*, 3 (3), p. 319.
8. AlGarni, K. (2015) *Information Security Policy for E-government in Saudi Arabia: Effectiveness Vulnerabilities and Threats.* College of Computing and Information Sciences, Department of Information Sciences and Technologies &Computing-Security. Rochester Institute of Technology. Available at: https://scholarworks.rit.edu/cgi/viewcontent.cgi?article=9788&=&context=theses&&sei-

9. AlGhamdi, R., Drew, S. and Al-Ghaith, W. (2011) 'Factors influencing e-commerce adoption by retailers in saudi-arabia: A qualitative analysis', *The Electronic Journal of Information Systems in Developing Countries*, pp. 47.

10. Alghamdi, I.A., Goodwin, R., and Rampersad, G. (2014) 'Organizational E-government readiness: An investigation in Saudi Arabia', *International Journal of Business and Management*, 9 (5), pp. 14-24. doi:10.5539/ijbm.v9n5p14
11. AlKalbani, A., Deng, H., and Kam, B. (2015) 'Organisational Security Culture and Information Security Compliance for E- Government Development: The Moderating Effect of Social Pressure', *Pacific Asia Conference on Information Systems (PACIS)* (p. 65). AIS Electronic Library (AISeL).
12. Alketbi, A., Nasir, Q., and Talib, M. A. (2018) 'Blockchain for government services—Use cases, security benefits and challenges', *15th Learning and Technology Conference* (L&T), 25-26 February 2018, Jeddah, Saudi Arabia (pp. 112-119). IEEE. doi:10.1109/LT.2018.8368494
13. Al-Megren, S., Alsalamah, S., and Altoaimy, L. (2018) 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), 2018 – ieeexplore.ieee.org
14. Almukhlifi, A., Deng, H., and Kam, B. (2019) 'E-Government Adoption in Saudi Arabia: The Moderation Influence of Transparency', *Journal of Advances in Information Technology*, 10 (1), pp. 1-8. doi:10.12720/jait.10.1.1-8
15. Al-Mushayt, O.S., Perwej, Y., and Haq, K. (2009) 'Electronic-government in Saudi Arabia: A positive revolution in the peninsula', *International Transactions in Applied Sciences*, 1 (1), pp. 87-98. Available at: https://arxiv.org/ftp/arxiv/papers/1205/1205.3986.pdf
16. Al-Nuaim, H. (2011) 'An evaluation framework for Saudi e-government', *Journal of e-Government Studies and Best Practices*, Art ID 820912. doi:10.5171/2011.820912
17. Alrashedi, R., Persaud, A., and Kindra, G. (2015) 'Drivers of eParticipation: Case of Saudi Arabia', *The Journal of Business Inquiry*, 14 (1), pp. 1-22. Available at: http://journals.uvu.edu/index.php/jbi/article/view/120
18. Al-Ruithe, M., Benkhelifa, E., and Hameed, K. (2018) 'Key Issues for Embracing the Cloud Computing to Adopt a Digital Transformation: A study of Saudi Public Sector', *Procedia computer science*, 130, pp. 1037-1043. doi:10.1016/j.procs.2018.04.145
19. Alsaif, M. (2013) Factors Affecting Citizens' Adoption of E-government Moderated by Socio-cultural Values in Saudi Arabia. College of Social Sciences, School of Government and Society, Institute of Local Government Studies. University of Birmingham. Retrieved July 8, 2019, from https://etheses.bham.ac.uk/id/eprint/4851/1/Alsaif14PhD.pdf
20. Al-Sanea, M. S., and Al-Daraiseh, A. A. (2015) 'Security evaluation of Saudi Arabia's websites using open source tools', *First International Conference on Anti-*

Cybercrime (ICACC), 10-12 November 2015, Riyadh, Saudi Arabia (pp. 1-5). IEEE.

21. Alshehri, M., and Drew, S. (2010) 'Challenges of e-government services adoption in Saudi Arabia from an e-ready citizen perspective', *World Academy of Science, Engineering and Technology,* 42, pp. 1039-1045.
22. Alshehri, M., and Drew, S. (2010b) 'E-government fundamentals' In *IADIS international conference ICT, Society and Human Beings.*
23. Alshomrani, S., and Qamar, S. (2012) 'Hybrid SWOT-AHP Analysis of Saudi Arabia E-Government', *International Journal of Computer Applications*, 48 (2), pp. 1-7. doi:10.5120/7317-0065
24. Alsmadi, I., and Abu-Shanab, E. (2016) 'E-government website security concerns and citizens' adoption', *Electronic Government, an International Journal,* 12 (3), pp. 243-255. doi:10.1504/EG.2016.078417.
25. AlZain, M. A, Li, A. S., Soh, B, and Masud, M. (2016) 'Byzantine Fault-Tolerant Architecture in Cloud Data Management', *International Journal of Knowledge Society Research* (IJKSR), 7, pp. 86-98.
26. Assiri, H., Nanda, P., & Mohanty, M. (2020). *Secure e-Governance Using Blockchain* (No. 4252). EasyChair.
27. Avgerou, C. (2010) 'Discourses on ICT and development', *Inf. Technol. Int. Dev*, 6 (3), pp. 1–18. Available at: http://www.itidjournal.org/index.php/itid/article/view/560
28. Azogu, I., Norta, A., Papper, I., Longo, J., and Draheim, D. (2019) 'A Framework for the Adoption of Blockchain Technology in Healthcare Information Management Systems: A Case Study of Nigeria.' *Proceedings of the 12th International Conference on Theory and Practice of Electronic Governance, Melbourne, VIC, Australia*
29. Back et al. (2014) Enabling Blockchain innovations with pegged sidechains.
30. Bannister, F., and Connoiiy, R. (2012) 'Defining e-governance', *e-Service Journal*, 8 (2), pp. 3-25. doi:10.2979/eservicej.8.2.3
31. Baqir, M.N. and Iyer, L. (2010) 'E-Government Maturity Over 10 Years: A Comparative Analysis of E-Government Maturity in Select Countries Around the World' In *Comparative E-Government, Springer, New York*, NY, pp. 3–22.
32. Basahel, A., and Yamin, M. (2017) 'Measuring the success of the e-government of Saudi Arabia', *International Journal of Information Technology,* 9 (3), pp. 287-293. doi:10.1007/s41870-017-0029-4
33. Batubara, F. R., Ubacht, J., and Janssen, M. (2018) 'Challenges of Blockchain technology adoption for e-government', *Proceedings of the 19th Annual International Conference on Digital Government Research Governance in the Data Age* - Dgo'18. doi:10.1145/3209281.3209317

34. Baqir, M. N. and Iyer, L. (2010) *E-government maturity over 10 years: A comparative analysis of e-government maturity in select countries around the world in: Comparative E-Government*, Springer, New York, NY, pp. 3–22.

35. Bayer, D., Haber, S., and Stornetta, W. S. (1993) 'Improving the efficiency and reliability of digital time-stamping', In *Sequences Ii*, Springer, pp. 329-334.

36. Beinke, J. H., Nguyen, D., and Teuteberg, F. (2018) 'Towards a business model taxonomy of startups in the finance sector using Blockchain.' *Paper presented at the thirty ninth International Conference on Information Systems (ICIS),* San Francisco.

37. Bennett, O. (2009) 'Electronic Government (e-Government)', *House of Commons*. Available at: https://researchbriefings.files.parliament.uk/documents/SN01202/SN01202.pdf

38. Bertot, J. C., Gorham, U., Jaeger, P. T., Sarin, L. C., and Choi, H. (2014) 'Big data, open government and e-government: Issues, policies and recommendations', *Information polity,* 19 (1, 2), pp. 5-16.

39. Bergquist, J. (2017) *Blockchain Technology and Smart Contracts: Privacy-preserving Tools*.

40. Bissyandé, T. F., Ouoba, Ahmat, D., Ouédraogo, F., Béré, C., Bikienga, M., . . . Sié, O. (2015) 'Vulnerabilities of Government Websites in a Developing Country–The Case of Burkina Faso' In R. Glitho, M. Zennaro, F. Belqasmi, and M. Agueh (Ed.), *International Conference on e-Infrastructure and e-Services for Developing Countries.*

41. Biswas, K., and Muthukkumarasamy, V. (2016) 'Securing smart cities using Blockchain technology' In *2016 IEEE 18th international conference on high performance computing and communications; IEEE 14th international conference on smart city; IEEE 2nd international conference on data science and systems* (HPCC/SmartCity/DSS) (pp. 1392–1393).

42. Blockchain technology. (2016) 'Advantages & Disadvantages of Blockchain Technology' [Online]. Available at: https://Blockchaintechnologycom.wordpress.com/2016/11/21/advanta ges-disadvantages

43. Block J. H., Colombo M. G., Cumming D. J., and Vismara S. (2018) 'New players in entrepreneurial finance and why they are there', *Small Business Economics*, 50 (2), pp. 239–50.

44. Bracamonte, V., Yamasaki, S., and Okada, H. (2016) 'A Discussion of Issues related to Electronic Voting Systems based on Blockchain Technology', *Computer Security Symposium*, 11-13 October 2016, (pp. 684-687). Available at: https://ipsj.ixsq.nii.ac.jp/ej/?action=pages_view_main&active_action=repository_view_main_item_detail&item_id=175800&item_no=1&page_id=13&block_id=8

45. Brodersen, C., Kalis, B., Leong, C., Mitchell, E., Pupo, E., Truscott, A., and Accenture, L.L.P. (2016) Blockchain: Securing a New Health Interoperability Experience. ed: Accenture LLP.

46. Business Jargons. (2019) 'E-Governance' [Online] *Business Jargons.* Available at: https://businessjargons.com/e-governance.html

47. Buterin, V. (2014) *Ethereum White Paper: A next-generation smart contract and decentralized application platform*.

48. Bwalya, K.J. (2009) 'Factors affecting adoption of e-government in Zambia', The Electronic *Journal of Information Systems in Developing Countries*, 38 (1), pp. 1-13. doi:10.1002/j.1681-4835.2009.tb00267.x

49. CabinetOffice. (2000) 'e-government: a strategic framework for public services in the information age', *The Cabinet Office, UK*. Available at: https://ntouk.files.wordpress.com/2015/06/e-government-strategy-2000.pdf

50. Çabuk, U. C., Adıgüzel, E., and Karaarslan, E. (2018) 'A Survey on Feasibility and Suitability of Blockchain Techniques for the E-Voting Systems', *International Journal of Advanced Research in Computer and Communication Engineering*, 7 3), pp. 124-134. doi:10.17148/IJARCCE.2018.7324

51. Casino, F., Dasaklis, T. K. and Patsakis C. (2019) *Telematics and informatics*. Elsevier

52. Catalini, C., and Joshua S.G. (2016) 'Some Simple Economics of the Blockchain. Technical Report', *National Bureau of Economic Research*.

53. Carter, L. and Ubacht, J. (2018) 'Blockchain applications in government', in *Proceedings of the 19th Annual International Conference on Digital Government Research: Governance in the Data Age*, pp. 1-2.

54. Chatfield, A. T., and AlAnazi, J. (2015) 'Collaborative governance matters to e-government interoperability: An analysis of citizen-centric integrated interoperable e-government implementation in Saudi Arabia', *International Journal of Public Administration in the Digital Age* (IJPADA), 2 (3), pp. 24-44. doi:10.4018/ijpada.2015070102

55. Chen, Y., Dawes, S. S., and Chen, S. (2017) 'E-government Support for Administrative Reform in China', *Proceedings of the 18th Annual International Conference on Digital Government Research*, June 07 - 09, 2017, Staten Island, NY, USA (pp. 329-335). ACM. doi:10.1145/3085228.3085269

56. Chen, S., and Xie, Z. (2015) 'Is China's e-governance sustainable? Testing Solow IT productivity paradox in China's context', *Technological Forecasting and Social Change*, 96, pp. 51-61. doi:10.1016/j.techfore.2014.10.014

57. Chen, Y.N., Chen, H., Huang, W., and Ching, R.K. (2006) 'E-government strategies in developed and developing countries: An implementation framework and case study', *Journal of Global Information Management* (JGIM), 14 (1), pp. 23-46. doi:10.4018/jgim.2006010102

58. Cheng, S., Zeng, B., and Huang, Y. Z. (2017) 'Corrigendum: Research on application model of Blockchain', *IOP Conf. Series: Earth and Environmental Science*, 93.

59. Choejey, P., Fung, C. C., Wong, K. W., Murray, D., and Xie, H. (2015) 'Cybersecurity practices for e-Government: an assessment in Bhutan' In *The 10th International Conference on e-Business, Bangkok, Thailand*.

60. Ciborra, C., and Navarra, D. D. (2005) 'Good governance, development theory, and aid policy: Risks and challenges of e-government in Jordan', *Information technology for development*, 11 (2), pp. 141-159. doi:10.1002/itdj.20008

61. da Conceição, A. F., da Silva, F. S., Rocha, V., Locoro, A., and Barguil, J. M. (2018) Electronic 'Health Records using Blockchain Technology', *arXiv*, 1804 (v1), p. 10078. Available at: https://arxiv.org/pdf/1804.10078.pdf

62. Cryptomathic. (2015) 'A key component for e-government security' Available at: https://www.cryptomathic.com/news-events/blog/keyfor-egovernment-security-central-signing-authentication/.

63. Curity. (2015) ‘On public and private Blockchains’ [Online] *V. Buterin*, 1 (1), pp. 36-63 Available: https://blog.ethereum.org/2015/08/07/ on-public-and-private-Blockchains/

64. Dada, D. (2006) ‘The failure of e-government in developing countries: a literature review’, *The Electronic Journal of Information Systems in Developing Countries*, 26 (1), pp. 1-10. doi:10.1002/j.1681-4835.2006.tb00176.x

65. David T., Giuseppe G., Luca S., Aspyn C.P., and Zixuan Z. (2019) ‘Blockchain interoperability’, *US Patent* 10,298,585.

66. Dawes, S. S. (2009) ‘Governance in the Digital Age: a Research and Action Framework for an Uncertain Future’, *Government Information Quarter*ly, 26 (2), pp. 257–264.

67. G. DeCandia et al. (2007) ‘Dynamo: Amazon’s highly available key-value store’, *SIGOPS Oper. Syst. Rev.,* 41 (6), pp. 205–220.

68. Deng. (2008) ‘Towards objective benchmarking of electronic government: an inter-country analysis, Transform. Govern’, *People Process Policy*, 2 (3), p. 162.

69. Deshpande, A., Stewart, K., Lepetit, L., and Gunashekar, S. (2017) *Overview Report: Distributed Ledger Technologies/Blockchain: Challenges, Opportunities and the Prospects for Standards.* British Standards Institution (BSI).

70. Diallo, N., Shi, W., Xu, L., Gao, L., Chen, L., Lu, Y., and Shah, N.E. (2018) ‘eGov-DAO: A better government using Blockchain based decentralized autonomous organization’, *2018 International Conference on eDemocracy and eGovernment* (ICEDEG), 4-6 April 2018, Ambato, Ecuador (pp. 166-171). IEEE. doi:10.1109/ICEDEG.2018.8372356

71. Dorri, A., Kanhere, S. S., Jurdak, R., and Gauravaram, P. (2017) ‘Blockchain for iot security and privacy: The case study of a smart home’, In *2017 IEEE international conference on pervasive computing and communications workshops* (PerCom workshops) (pp. 618–623).

72. Dorri, A., Kanhere, S., and Jurdak, R. (2017) 'MOF-BC: A memory optimized and flexible Blockchain for large scale networks', *Future Gener. Comput. Syst*, 92, pp. 357–373. [CrossRef]

73. Du, P., Yu, S., and Yang, D. (2018) 'Development process: Chinese e-governance from exploration to comprehensive promotion', In *The Development of E-governance in China: Improving Cybersecurity and Promoting Informatization as Means for Modernizing State Governance* (Vol. Research Series on the Chinese Dream and China's Development Path, pp. 1-12). Springer. Available at: https://books.google.co.in/books?id=euFmDwAAQBAJ&printsec=frontcover#v=onepage&q&f=false

74. Dwivedi, P., and Sahu, G. P. (2008) 'Challenges of E-government Implementation in India. Computer Society of India (CSI)', *Special Interest Group on e-Governance* (SIGeGov), SIGeGov Publications. Available at: https://www.researchgate.net/profile/G_Sahu/publication/260320339_Challenges_of_E-government_Implementation_in_India/links/542dec4f0cf29bbc126eff58.pdf

75. e-Government. (2015) Available at: http://www.worldbank.org/en/topic/ict/brief/egovernment (Accessed 14 April 2017)

76. eGov4dev. (2008) 'eGovernment for Development: Resources', *eGovernment for development organization*. Available at: http://www.egov4dev.org/websites/resources/examples.html

77. Ekblaw, A., Azaria, J. D., Halamka, A., and Lippman. (2016) 'A Case Study for Blockchain in Healthcare: "MedRec" prototype for electronic health records and medical research data', In *Proceedings of IEEE open & big data conference*, pp. 13, 2016.

78. E-Estonia. (2017) https://e-estonia.com ; Omri Barzilay, "3 Ways Blockchain Is Revolutionizing Cybersecurity," Forbes, August 21, 2017, https://www.forbes.com/sites/omribarzilay/2017/08/21/3-ways-Blockchain-isrevolutionizing-cybersecurity/ ; and "Estonian eHealth and the Blockchain," The Review, Gemalto, June 21, 2017, https://www.gemalto.com/review/Pages/Estonian-eHealth-and-the-Blockchain.aspx

79. Elisa, N. (2017) 'Usability, accessibility, and web security assessment of e-government websites in tanzania', *International Journalof Computer Applications,* 164 (5), pp. 42-48.

80. Elisa, N., Yang, L., Chao, F., and Cao, Y. (2018) 'A framework of Blockchain-based secure and privacy-preserving E-government system', *Wireless Networks* (pp. 1-11). Springer.

81. El-sofany, H.F., Al-Tourki, T., Al-Howimel, H., and Al-Sadoon, A. (2012) 'E-Government in Saudi Arabia: Barriers, challenges and its role of development', *International Journal of Computer Applications*, 48 (5), pp. 16-22. Available at: https://pdfs.semanticscholar.org/3357/014aaff15c56ad3badd99b7538b56b3a7b35.pdf

82. European Commission. eGovernment Benchmark Framework 2012–2019: Method Paper for the Benchmarking Exercises (Comprehensive Rules from 2012 to 2019); Publications Office of the EU: Luxembourg, 2019; pp. 1–72. [CrossRef]

83. Eyal, I. I and Sirer, E. G. (2014) 'Majority is not enough: Bitcoin mining is vulnerable', in *Proceedings of International Conference on Financial Cryptography and Data Security,* Berlin, Heidelberg, pp. 436– 454.

84. Fan, Q. (2011) 'An evaluation analysis of e-government development by local authorities in Australia', *International Journal of Public Administration*, 34 (14), pp. 926-934. doi:10.1080/01900692.2011.615550

85. Fan, Q. (2018) A longitudinal evaluation of e-government at the local level in Greater Western Sydney (Gws) Australia', *International Journal of Public Administration,* 41 (1), pp. 13-21. doi:10.1080/01900692.2016.1242621

86. Feng, Q., He, D., Zeadally, S., Khan, M. K., and Kumar, N. (2019) 'A survey on privacy protection in Blockchain system', *J. Netw. Comput. Appl.,* 126, pp.45–58.

87. Forman, M. (2002) 'E-Government Strategy. EXECUTIVE OFFICE OF THE PRESIDENT OFFICE OF MANAGEMENT AND BUDGET' Available at: http://unpan1.un.org/intradoc/groups/public/documents/unpan/unpan025640.pdf

88. Fountain, J. E. (2009) 'Bureaucratic Reform and E-Government in the United States: An Institutional Perspective', in *Routledge Handbook of Internet Politics, Routledge, New York*, NY, pp. 99–113.

89. Fusco, F., Lunesu, M. I., Pani, F., Ippo, E., and Pinna, A. (2018) 'Crypto-voting, a Blockchain based e-Voting System' [online] *KMIS*, pp. 221-225. Available at: https://www.researchgate.net/profile/Andrea_Pinna4/publication/327907758_Crypto-voting_a_Blockchain_based_e-Voting_System/links/5cb8de2da6fdcc1d499ef07a/Crypto-voting-a-Blockchain-based-e-Voting-System.pdf

90. Gabriel, B. (2018) 'E-Governance and Cybersecurity: User Perceptions of Data Integrity and Protection in Ghana,' *5th Biennial Social Science Conference of the University of Education*, Winneba.

91. Garg, P., Gupta, B., Chauhan, A. K., Sivarajah, U., Gupta, S., and Modgil, S. (2020) 'Measuring the perceived benefits of implementing Blockchain technology in the banking sector', *Technological Forecasting and Social Change*, Article No. 120407.
92. Gao, J., Asamoah, K. O., Sifah, E. B., Smahi, A., Xia, Q., Xia, H. (2018) 'GridMonitoring: Secured sovereign Blockchain based monitoring on smart grid', *IEEE Access: Practical Innovations, Open Solutions*, 6, pp. 9917–9925. https://doi.org/10.1109/ ACCESS.2018.2806303.

93. Gertrude Chavez-Dreyfuss. (2018) 'Coca-Cola, U.S. State Dept to Use Blockchain to Combat Forced Labor', *Reuters*. Available at: https://www.reuters.com/article/us-Blockchain-coca-cola-labor/coca-cola-u-sstate-dept-to-use-Blockchain-to-combat-forced-labor-idUSKCN1GS2PY.

94. Ghayur, A. (2006) 'Towards good governance: developing an e-government', *The Pakistan Development Review,* 45 (4), pp. 1011–1025. Available at: http://www.pide.org.pk/pdf/PDR/206/Volume4/1011-1025.pdf

95. Gilmore, A., and D'Souza, C. (2006) 'Service excellence in e-governance issues: An Indian case study', *JOAAG*, 1 (1), pp. 1-14. Available at: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.550.389&rep=rep1&type=pdf

96. GKToday. (2016) 'E-governance- applications, models, successes, limitations, and potential' [online] *GK Today*. Available at: https://www.gktoday.in/gk/e-governance-applications-models-successes-limitations-and-potential/

97. Gray, R. M. (2011) *Entropy and Information Theory*. Springer Science & Business Media.

98. Grewal, D., Motyka, S., and Levy, M. (2018) 'The evolution and future of retailing and retailing education', *Journal of Marketing Education*, 40 (1), pp. 85–93.

99. Goede, M. (2019) *Archives of Business Research*. Available at: academia.edu

100. Gordon, W. J. and Catalini, C. (2018) 'Blockchain Technology for Healthcare: Facilitating the Transition to Patient-Driven Interoperability', *Comput. Struct. Biotechnol. J.*, 16, pp. 224–230.

101. Gov.UK. (2019) 'Government Digital Services Corporate report: Who we are and what we do' [online] *Gov.UK*. Available at: https://www.gov.uk/government/publications/the-government-digital-service-who-we-are-and-what-we-do/who-we-are-and-what-we-do

102. Guanghua, L. U. (2009) 'E-government, People and Social Change: A Case Study in China', *The Electronic Journal of Information Systems in Developing Countries*, 38 (1), pp. 1-23. doi:10.1002/j.1681-4835.2009.tb00266.x

103. Haran, M. H. (2016) ' Framework Based Approach for the Mitigation of Insider Threats in Egovernance IT Infrastructure', *International Journal of Science and Research,* 3 (4), pp. 5- 10.

104. Hao, Y., Piao, C., Zhao, Y., and Jiang, X. (2019) 'Privacy preserving government data sharing based on hyperledger Blockchain' In *International Conference on e-Business Engineering* (pp. 373-388). Springer, Cham.

105. Hammer, M. and Shipman, D. (1980) 'Reliability mechanisms for SDD-1: A system for distributed databases,' *ACM Trans. Database Syst*., 5 (4), pp. 431–466.

106. Harris, B. (2000) 'e-Governance'. Available at: http://www.iadb.org

107. Haque, A. K. (2019) 'Need for Critical Cyber Defence, Security Strategy and Privacy Policy in Bangladesh–Hype or Reality?' *International Journal of Managing Information Technology* (IJMIT), 11 (1), pp. 37-50. doi:10.5121/ijmit.2019.11103

108. Heng, H. (2017) 'The Application of Blockchain Technology in E-government in China,' *School of Information Management,* SunYat-sen University.

109. Hjalmarsson, F. P., Hreioarsson, G. K., Hamdaqa, M. and Hjalmtysson, G. (2018) 'Blockchain-Based E-Voting System' In *Proceedings of the IEEE 11th International Conference on Cloud Computing* (CLOUD), San Francisco, CA, USA, 2–7, pp. 983–986. [CrossRef]

110. Hsieh, Y. Y., Vergne, J. P. J., and Wang, S. (2017) 'The internal and external governance of Blockchain-based organizations: Evidence from cryptocurrencies' In *Bitcoin and beyond* (pp. 48-68). Routledge.

111. Nessus, (2005) 'F5 BIG-IP Cookie Remote Information Discolsure'. Available at: https://www.tenable.com/plugins/nessus/20089

112. Nessus, (2015) 'Web Application Potentially Vulnerable to Clickjacking'. Available at: https://www.tenable.com/plugins/nessus/85582

113. Rapid7, (2007) 'X.509 Certificate Subject CN'. Available at: https://www.rapid7.com/db/vulnerabilities/certificate-common-name-mismatch/

114. ZAP, 'Absence of Anti-CSRF Tokens'. Available at: https://www.zaproxy.org/docs/alerts/10202/

115. ZAP, 'Content Security Policy (CSP) Header Not Set'. Available at: https://www.zaproxy.org/docs/alerts/10038/

116. ZAP, 'Cookie No HttpOnly Flag'. Available at: https://www.zaproxy.org/docs/alerts/10010/

117. ZAP, 'Cookie Without Secure Flag'. Available at: https://www.zaproxy.org/docs/alerts/10011/

118. ZAP, 'Cookie without SameSite Attribute'. Available at: https://www.zaproxy.org/docs/alerts/10054/

119. ZAP, 'Cross-Domain JavaScript Source File Inclusion'. Available at: https://www.zaproxy.org/docs/alerts/10017/

120. ZAP, 'Timestamp Disclosure'. Available at: https://www.zaproxy.org/docs/alerts/10096/

121. ZAP, 'X-Content-Type-Options Header Missing'. Available at: https://www.zaproxy.org/docs/alerts/10021/

122. ZAP, 'Timestamp Disclosure'. Available at: https://www.zaproxy.org/docs/alerts/10096/

123. ZAP, 'X-Content-Type-Options Header Missing'. Available at: https://www.zaproxy.org/docs/alerts/10021/

124. Hou, H. (2017) 'The application of Blockchain technology in E-government in China. In Computer Communication and Networks (ICCCN),' *2017 26th International Conference on* (pp. 1-4). IEEE.

125. Huang W, Meoli M, and Vismara, S. (2020) 'The geography of initial coin offerings', *Small Business Economics*, 55 (1), pp. 77–102.

126. Hudson, L. (2001) 'e-Governance: one country's strategy' [online] *OECD Observer*. Available at: http://oecdobserver.org/news/archivestory.php/aid/481/e-Governance:_one_country_92s_strategy.html

127. Huh, S., Cho, S., and Kim, S. (2017) 'Managing iot devices using Blockchain platform' In *2017 19th international conference on advanced communication technology* (ICACT) (pp. 464–467).

128. Huumo, J., Ko, D., Choi, S., Park, S., and Smolander, K. (2016) 'Where Is Current Research on Blockchain Technology?—A Systematic Review', *PLoS ONE*, 11 (10)

129. Iansiti, M., and Lakhani, K. R. (2017) 'The truth about Blockchain', *Harvard Business Review*, 95 (1), pp. 118–127.

130. Irfan, M. I. (2017) 'The Role of E-Governance in Administrative Efficiency and Combating Corruption: Case of Sri Lanka', *Global Journal of Management and Business Research*, 17 (2), 38-50. Available at: https://www.journalofbusiness.org/index.php/GJMBR/article/view/2309

131. Jakobsson, M. and Juels, A. (1999) 'Proofs of work and bread pudding protocols (extended abstract)' in *Secure Information Networks*. Boston, MA, USA: Springer, pp. 258–272.

132. Jamal, A., Helmi, R. A., Syahirah, A. S., and Fatima, M.-A. (2019) 'Blockchain-Based Identity Verification System' *IEEE 9th International Conference on System Engineering and Technology* (ICSET), 7-7 Oct.2019, Shah Alam, Malaysia (pp. 253-257). IEEE. doi: 10.1109/ICSEngT.2019.8906403

133. Janssen, M., and Estevez, E. (2013) 'Lean government and platform-based governance—Doing more with less', *Government Information Quarterly*, 30 (Supplement 1), pp. S1-S8. doi:10.1016/j.giq.2012.11.003

134. Javaid U., Siang, A. K, and Aman M. N, et al. (2018) 'Mitigating IoT device based DDoS attacks using Blockchain', *CryBlock'18*, Munich, Germany.

135. Jo, H. J. and Choi, W. (2019) 'BPRF: Blockchain-based privacy-preserving reputation framework for participatory sensing systems', *PLoS ONE*, 14, p. e0225688.

136. Juan, M. D., Andrés, R. P., Rafael, P. M., Gustavo, R. E., and Manuel, P. C. (2018) 'A Model for National Electronic Identity Document and Authentication Mechanism Based on Blockchain', *International Journal of Modeling and Optimization,* 8 (3), pp. 160-165. doi:10.7763/IJMO.2018.V8.642

137. Jun, M. (2018) 'Blockchain government - a next form of infrastructure for the twenty-first century', *Journal of Open Innovation: Technology, Market, and Complexity*, 4 (7).

138. Jun, L., and Hui, Z. (2010) 'Mobile communication, public participation, and e-governance in China: a case study of Xiamen anti-PX demonstration', *Proceedings of the 4th International Conference on Theory and Practice of Electronic Governance*, October 25 - 28, 2010, Beijing, China (pp. 327-332). ACM. doi:10.1145/1930321.1930388

139. Kalakota, R., and Whinston, A. B. (1997) 'Electronic Commerce. Reading'. *MA: Addison-Wesley*.

140. Källner, C. (2019) 'Blockchain Technology in Disaster Risk Management: Transforming the Delivery of Emergency Relief.', *Sweden: Division of Risk Management and Societal Safety*, Lund University.

141. Karame, G. (2016) 'On the Security and Scalability of Bitcoin's Blockchain', *In Proceedings of The 2016 ACM SIGSAC Conference on Computer and Communications Security*, pp. 1861-1862.
142. Karokola, G. R. (2012) 'A framework for securing e-government services: The case of Tanzania.' Ph.D. thesis, Department of Computer and Systems Sciences, Stockholm University.

143. Kataoka K., Gangwar S., and Podili P. (2018). 'Trust list: internet-wide and distributed IoT traffic management using Blockchain and SDN.' Paper presented at: Proceedings of IEEE 4th World Forum on Internet of Things (WF-IoT), pp. 296–301.

144. Kazmi, S.N. (2010) 'Factors influencing e-Governance implementation: Issues and challenges in Pakistan', *Fifth International Conference on Digital Information Management* (ICDIM), 5-8 July 2010, Thunder Bay, ON, Canada (pp. 326-331). IEEE. doi:10.1109/ICDIM.2010.5664643

145. Kim, K., and Kang, T. (2017) 'Does Technology Against Corruption Always Lead to Benefit? The Potential Risks and Challenges of Blockchain Technology', *OECD's Anti-Corruption and Integrity Forum* (p. 22 pp). OECD. Available at: http://www.oecd.org/cleangovbiz/Integrity-Forum-2017-Kim-Kang-Blockchain-technology.pdf

146. King, S. and Nadal, S. M. (2012) 'PPCoin: Peer-to-peer crypto-currency with proof-of-stake' [online]. Available at: https://pdfs.semanticscholar. org/0db3/8d32069f3341d34c35085dc009a85ba13c13.pdf?_ga=2. 189270443.1680383901.1589560842-407403572.1523881355

147. Kirkman, S., and Newman, R. (2018) 'A cloud data movement policy architecture based on smart contracts and the Ethereum Blockchain,' Paper Presented at the Proceedings - *2018 IEEE International Conference on Cloud Engineering* (pp. 371–377). . https://doi. org/10.1109/IC2E.2018.00071.

148. Kiviant, T. (2015) 'Beyond Bitcoin: Issues in Regulating Blockchain Transactions', 65 (569), pp. 569-608.

149. Khan, H. U., Alsahli, A., and Alsabri, H. (2013) 'E-Government in Saudi Arabia: Analysis on present and future', *Journal of Electronics and Communication Engineering Research,* 1 (3), pp. 1-13.

150. Khan, A., Krishnan, S., and Dhir, A. (2021) 'Electronic Government and Corruption: Systematic Literature Review, Framework, and Agenda for Future Research', *Technological Forecasting and Social Change*, 167 (120737).
151. Kothe, D. B., Mjolsness, R. C. and Torrey, M .D. (1991) 'RIPPLE: a computer program for incompressible flows with free surfaces,' *Los Alamos National Lab*. LA-10612-MS, Los Alamos, NM.

152. Konashevych, O., and Poblet, M. (2019) 'Blockchain Anchoring of Public Registries: Options and Challenges', *Proceedings of the 12th International Conference on Theory and Practice of Electronic Governance*.

153. Kshetri, N. (2017) 'Blockchain's roles in strengthening cybersecurity and protecting privacy', *Telecommunications Policy*. Available at: DOI:https://doi.org/10.1016/j.telpol.2017.09.003.

154. Kshetri, N., and Voas, J. (2018) 'Blockchain-Enabled E-Voting', *IEEE Software*, 35 (4), pp. 95-99.

155. Kumar, P., Kumar, D., and Kumar, N. (2014) 'E-governance in India: Definitions, challenges and solutions', *International Journal of Computer Applications*, 101 (16), pp. 6-8. Available at: https://arxiv.org/ftp/arxiv/papers/1411/1411.1876.pdf

156. Lacity, M. C. (2018) 'Addressing key challenges to making enterprise Blockchain applications a reality', *MIS Quarterly Executive*, 17 (3).

157. Lakshman, A. and Malik, P. (2010) 'Cassandra: A decentralized structured storage system', *SIGOPS Oper. Syst. Rev*., 44 (2), pp. 35–40.

158. Larsen, J. W., Smith, A., Maurer, G., Johnson, K., Amiotes, D. and Wolf, D. E., INTHETELLING. COM, INC. (2014) 'Digital asset management, authoring, and presentation techniques.' *U.S. Patent Application*, 14/316,765.

159. Larios-Herna´ndez, G. J. (2017) 'Blockchain entrepreneurship opportunity in the practices of the unbanked', *Business Horizons*, 60 (6), pp. 865–74.

160. Lamport, L., Shostak, R. and Pease, M. (1982) 'The Byzantine generals problem,' *ACM Trans. Program. Lang. Syst.,* 4 (3), pp. 382–401.

161. Lapointe, C., and Fishbane, L. (2019) 'The Blockchain Ethical Design Framework', *Innovations: Technology, Governance, Globalization*, 12 (3-4), pp. 50-71.

162. Lemuria, C. and Jolien, U. (2018) 'Blockchain applications in government', Conference Paper. DOI:10.1145/3209281.3209329.

163. Leonard, M. (2018) 'When it comes to e-gov, the U.S. is now No. 11.' [online] *GCN*. Available at: https://gcn.com/articles/2018/07/31/un-egov-rankings.aspx

164. Lin, C., He, D., Huang, X., Raymond, C. K., and Vasilakos, A.V. (2018) 'BSeIn: A Blockchain-based secure mutual authentication with fine-grained access control system for industry 4.0', *J. Netw. Comput. Appl.,* 116, pp. 42–52.

165. Lin, Y. (2018) 'A comparison of selected Western and Chinese smart governance: The application of ICT in governmental management, participation and collaboration', *Telecommunications policy*, 42 (10), pp. 800-809. doi:10.1016/j.telpol.2018.07.003

166. Lin, I. C. and Liao, T. C. (2017) 'A Survey of Blockchain Security Issues and Challenges', *IJ Network Security*, 19 (5), pp. 653-659.

167. Longzhi, Y., Noe, E., and Neil, E. (2018) 'Privacy and Security Aspects of E-government in Smart Cities.' Department of Computer and Information Sciences, Northumbria University, Newcastle Upon Tyne, NE1 8ST UK.

168. Loo, B.P., and Wang, B. (2017) 'Progress of e-development in China since 1998', *Telecommunications Policy*, 41 (9), pp. 731-742. doi:10.1016/j.telpol.2017.03.001

169. Lu, Y. (2018) 'Blockchain: A survey on functions, applications and open issues', J*ournal of Industrial Integration and Management*, 30 (4), p. 1850015. Melbourne, VIC, Australia — April 03 - 05, 2019 ,doi:10.1142/S242486221850015X

170. Lu, Z., Liu, W., Wang, Q., Qu, G., and Liu, Z. (2018) 'A Privacy-Preserving Trust Model Based on Blockchain for VANETs', *IEEE Access*, 6, pp. 45655–45664.

171. Malik, P., Dhillon, P., and Verma, P. (2014) 'Challenges and future prospects for E-governance in India', *International Journal of Science, Engineering and Technology Research* (IJSETR), 3 (7), pp. 1964-1972. Available at: https://pdfs.semanticscholar.org/dd55/f2877dca75d5276597a7c1a3c7a301227407.pdf

172. Marr, B. (2018) 'The 5 Big Problems With Blockchain Everyone Should Be Aware Of' [online] *Forbes*. Available at: https://www.forbes.com/sites/bernardmarr/2018/02/19/the-5-big-problems-with-Blockchain-everyone-should-be-aware-of/#5a6d20501670

173. Marc, H. and Aroon M. (2009) 'E-Governance and Quality of Life: Associating Municipal E-Governance with Quality of Life Worldwide', *Handbook of Research on Strategies for Local E-Government Adoption and Implementation: Comparative Studies*, p. 11.

174. Marchionini, G., Samet, H., and Brandt, L. (2003) 'Digital government', *Communications of the ACM*, 46 (1), pp. 25-27.

175. Martinovic, I., Kello, L. and Sluganovic I. (2017) Centre for Technology and Global Affairs, University of Oxford. Available at: ctga.ox.ac.uk

176. Meijer, D., and Ubacht, J. (2018) 'The governance of Blockchain systems from an institutional perspective, a matter of trust or control? In *Proceedings of the 19th annual international conference on digital government research: Governance in the data age* (pp. 1-9).

177. Millar, L. (2004) 'Networking government: e-government in New Zealand', *Public Sector*, 27 (4), pp. 1-10. Available at: http://unpan1.un.org/intradoc/groups/public/documents/apcity/unpan021670.pdf

178. Millard, J. (017) *Government 3.0 – Next Generation Government Technology Infrastructure and Services*. Springer

179. Mingus, M. S., and Zhu, J. (2018) 'Increasing Citizen Access and Local Government Responsiveness in Yichang, China', *International Public Management Journal*, 21 (3), pp. 369-391. doi:10.1080/10967494.2017.1399945

180. Mohamed, R. and Rajandran, K. (2017) 'A Study on Cyber Security in E-Governance With Reference to Areas of ThanjavurDistrict-Tamil Nadu,' *Asia Pacific Journal of Research*.

181. Mohanta, B. K., Jena, D., Panda, S. S., and Sobhanayak, S. (2019) 'Blockchain Technology: A Survey on Applications and Security Privacy Challenges', *Internet of Things*, 8, p. 100107. doi:10.1016/j.iot.2019.100107

182. Mosa, A., El-Bakry, H. M., El-Razek, S. A., and Hasan, S. Q. (2016) 'A proposed E-government framework based on cloud service architecture', *International Journal of Electronics and Information Engineering*, 5 (2), pp. 93-104. doi:10.6636/IJEIE.201612.5(2).05

183. Mukhoryanova, O. A., Novikova, I. V., Rudich, S. B., and Bogushevich, E.V. (2016) 'E-Government in the Western European Countries', *Indian Journal of Science and Technology*, 9 (16), pp. 1-13. doi:10.17485/ijst/2016/v9i16/90757

184. Murah, M. Z., and Ali, A. A. (2018) 'Web Assessment of Libyan Government e-Government Services', *Assessment,* 9 (12), pp. 583-590.

185. Nakamoto, S. (2008) 'Bitcoin: A peer-to-peer electronic cash system', *Decentralized Business Review*, 21260.

186. New Zealand Government. (2019) 'NZ's digital transformation' [online] *New Zealand Government.* Available at: https://www.digital.govt.nz/digital-government/digital-transformation/nz-digital-transformation/

187. Niforos, M., Ramachandran, V. and Rehermann, T. (2017) 'Block Chain: Opportunities for Private Enterprises in Emerging Market', *International Finance Corporation*. World Bank Group.

188. Niranjanamurthy, M., Nithya, B. N., and Jagannatha, S. (2018) 'Analysis of Blockchain technology: pros, cons and SWOT', *Cluster Computing*, 22 (6), pp. 14743–14757. doi:10.1007/s10586-018-2387-5

189. Nkwe, N. (2012) 'E-government: challenges and opportunities in Botswana', I*nternational journal of humanities and social science*, 2 (17), pp. 39-48. Available at: https://pdfs.semanticscholar.org/e863/32923fc092fdca4067ec941b1434f4774e76.pdf

190. Noe, E. (2017) 'Usability, accessibility and web security assessment of e-government websites in tanzania', *International Journal of Computer Applications*, 164 (5), pp. 42–48.

191. O'Neill, R.R. (2009) 'E-government transformation of public governance in New Zealand?' [online] *Victoria University of Wellington*. Available at: http://researcharchive.vuw.ac.nz/bitstream/handle/10063/929/thesis.pdf?sequence=1

192. O'Toole, K. (2007) 'E-governance in Australian Local government: Spinning a Web around Community', *International Journal of Electronic Government Research* (IJEGR), 3 (4), pp. 58-83. doi:10.4018/jegr.2007100104

193. Oakley, K. (2002) 'What is e-governance?' [online] *Local Futures Group, London. Council of Europe.* Available at: https://www.coe.int/t/dgap/democracy/Activities/GGIS/E-governance/Work_of_egovernance_Committee/Kate_Oakley_eGovernance_en.asp

194. Ojo, A. and Adebayo, S. (2017) *Government 3.0–Next Generation Government Technology Infrastructure and Services: Roadmaps, Enabling Technologies & Challenges 2017*. Springer.

195. Ojo, A., Janowski, T., and Estevez, E. (2005) 'Determining Progress Towards e-Government: What are the core indicators?' *5th European Conference on e-Government (ECEG2005)* (pp. 313-322). Academic Conferences Limited. Available at: https://pdfs.semanticscholar.org/4a21/53c4f8f8a0dacb52068c2dda4027c7d3d6e2.pdf

196. Okot-Uma, R. W. (2004) 'The Roadmap to e Governance Implementation: Selected Perspectives.' [online] *Okot-Uma, Rogers W'O*. Available at: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.466.5098&rep=rep1&type=pdf

197. Ølnes, S. and Jansen, A. (2017) 'Blockchain Technology as Support Infrastructure In E-Government' in *International Conference on Electronic Government, Springer*, *Cham*, pp. 215–227.

198. Ølnes, S., Ubacht, J., and Janssen, M. (2017) 'Blockchain in government: Benefits and implications of distributed ledger technology for information sharing', *Government Information Quarterly*, 34 (3), pp. 355-364

199. Ølnes, S. and Jansen, A. (2018) 'Blockchain technology as infrastructure in public sector: An analytical framework', *Proceedings of the 19th Annual International Conference on Digital Government Research: Governance in the Data Age*, Delft, The Netherlands — May 30 - June 01, 2018 (p. 77). ACM. doi:10.1145/3209281.32092

200. Osman, I. H., Anouze, A. L., Irani, Z., Al-Ayoubi, B., Lee, H., Balcı, A., .,.,Weerakkody,

V. (2014) 'COBRA framework to evaluate e-government services: A citizen-centric perspective', *Government information quarterly,* 31 (2), pp. 243-256.

201. Ott, A., Hanson, F., and Krenjova, J. (2018) 'Introducing integrated e-government in Australia.' [online] *Australian Strategic Policy Institute*. Available at: https://www.acs.org.au/content/dam/acs/acs-publications/E-Gov%20Report.pdf

202. Paech, P. (2017) 'The governance of Blockchain financial networks', *The Modern Law Review*, 80 (6), pp. 1073-1110.

203. Pardo, T. A. and Styrin, E. (2010) 'Digital Government Implementation: A Comparative Study in USA and Russia', *Americas Conference on Information Systems, AMCIS 2010* (p. 330). AMCIS. Available at: https://pdfs.semanticscholar.org/fd72/814fce6edcce563e136520fed4fa631ae842.pdf

204. Palvia, S. C., and Sharma, S. S. (2007) 'E-government and e-governance: definitions/domain framework and status around the world', *International Conference on E-governance*, 5, pp. 1-12. Available at: https://www.csi-sigegov.org/1/1_369.pdf

205. Pandya, D. C., and Patel, N. J. (2017). 'Study and analysis of E-Governance Information Security (InfoSec) in Indian Context', *Journal of Computer Engineering (IOSR-JCE),* 19 (1), pp. 4-7. doi:10.9790/0661-1901040407

206. Pankowska, M. (2008) 'National frameworks' survey on standardization of e-Government documents and processes for interoperability', *Journal of Theoretical and Applied Electronic Commerce Research*, 3 (3), pp. 64-82. doi:10.4067/S0718-18762008000200006

207. Paramashivaiah, P., and Suresh, B. K. (2016) 'E-governance: Issues and challenges in India', *OIDA International Journal of Sustainable Development*, 9 (8), pp. 11-16.
208. Paskaleva, K. A. (2009). 'Enabling the smart city: the progress of city e-governance in Europe', *International Journal of Innovation and Regional Development*, 1 (4), pp. 405-422. doi:10.1504/IJIRD.2009.02273

209. Pathak, R. D., Sharma, V., Husain, Z., Gupta, N., and Smith, R. F. (2016) 'E-governance for poverty alleviation: Indian cases and prospects for poverty alleviation in Uttar Pradesh', *Chinese Public Administration Review*, 3 (3/4), pp. 51-61. doi:10.22140/cpar.v3i3/4.62

210. Pawlak, M., Guziur, J., and Poniszewska-Marańda, A. (2018) 'Voting process with Blockchain technology: auditable Blockchain voting system' In *International*

Conference on Intelligent Networking and Collaborative Systems (pp. 233-244). Springer, Cham.

211. Pau, L. F. (2010) 'Business and social evaluation of denial of service attacks of communications networks in view of scaling economic counter-measures' In 2010 IEEE/IFIP network operations and management symposium workshops (NOMS Wksps) (pp. 126–133).

212. Paul, A., and Paul, V. (2011) 'The Implementation Issues of e-Governance in India', *Proceedings of the UGC Sponsored National Seminar on Modern Trends in Electronic Communication and Signal Processing*, 3-4 February 2011, Piravom, Kerala (pp. 43-48). Excel India Publishers. Retrieved July 13, 2019, from Haitham

213. Peck, M. E. (2017) 'Blockchains: How They Work and Why They'll Change the World - IEEE Spectrum', *IEEE Spectrum*.

214. Peters, G., Panayi, E., and Chapelle, A. (2015) 'Trends in cryptocurrencies and Blockchain technologies: a monetary theory and regulation perspective'.

215. Pilkington, M. (2016) '11 Blockchain technology: Principles and applications', *Research handbook on digital transformations*, 225.

216. Pilkington, M., Crudu, R., and Grant, L. G. (2017) 'Blockchain and bitcoin as a way to lift a country out of poverty-tourism 2.0 and e-governance in the Republic of Moldova', *International Journal of Internet Technology and Secured Transactions*, 7 (2), pp. 115-143.

217. Prakash, G., and Singh, A. (2016) 'A New Public Management Perspective in Indian E-Governance Initiatives', *Public Management,* pp. 71-80. Available at: http://unpan1.un.org/intradoc/groups/public/documents/UN-DPADM/UNPAN040636.pdf

218. Purser, S. (004). *A practical guide to managing information security*. Artech House.

219. Rao, V. R. (2011) 'Collaborative government to employee (G2E): Issues and challenges to e-government', *Journal of e-Governance*, 34 (4), pp. 214-229. Available at: https://dl.acm.org/citation.cfm?id=2336312

220. Ramadoss, B., and Palanisamy, R. (2012) 'Issues and challenges in electronic governance planning.' [online] *St Francis Xavier University, Canada*. Available at: https://www.researchgate.net/profile/Ram_Palanisamy/publication/220082762_Issues_and_challenges_in_e-governance_planning/links/5564b42508aec4b0f4859055/Issues-and-challenges-in-e-governance-planning.pdf

221. Ramli, R. M. (2017) 'E-Government Implementation Challenges in Malaysia and South Korea: A Comparative Study', *Electronics Journal of Information System for Developing Countries*, 80 (1), pp. 1–26.

222. Rashid, M. A., and Pajooh, H. H. (2019) 'A Security Framework for IoT Authentication and Authorization Based on Blockchain Technology', *18th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/13th IEEE International Conference On Big Data Science And Engineering* (TrustCom/BigDataSE), 5-8 Aug. 2019, Rotorua, New Zealand (pp. 264-271). IEEE. doi:10.1109/TrustCom/BigDataSE.2019.00043

223. Rauchs, M. et al. (n.d) 'Distributed ledger technology systems: A conceptual framework', *SSRN Electron. J.,* to be published, doi: 10.2139/ssrn.3230013.

224. Razzaq, A., Khan, M. M, Talib, R., Butt, A. D., Hanif, N. and Afzal, S. researchgate.net

225. Rehman, M., Esichaikul, V., and Kamal, M. (2012) 'Factors influencing e-government adoption in Pakistan', *Transforming Government: People, Process and Policy,* 6 (3), pp. 258-282.

226. Reyna, A., Martín, C., Chen, J., Soler, E., and Díaz, M. (2018) 'On Blockchain and its integration with IoT. Challenges and opportunities', *Future Gener. Comput. Syst*., 88, pp. 173–190

227. Rényi, A. (1961) 'On measures of entropy and information' in *Proceedings of the Fourth Berkeley Symposium on Mathematical Statistics and Probability*, Volume 1: Contributions To the Theory of Statistics, University of California Press, pp. 547–561.

228. Riad, A., El-Bakry, H. M., and El-Adl, G. H. (2011) 'E-government frameworks survey', *International Journal of Computer Science Issues*, 8 (3, 2), pp. 319-344.

229. Risius, M., and Spohrer, K. (2017) 'A Blockchain research framework', *Business and Information Systems Engineering*, 59 (6), pp. 385-409. doi:10.1007/s12599-017-0506-0

230. Rodrigues B, Bocek T, Lareida A, Hausheer D, Rafati S, and Stiller B. A. (2017) Blockchain-based architecture for collaborative DDoS mitigation with smart contracts', *IFIP International Conference Autonomous Infrastructure Management Security*, 10356, pp. 16- 29.

231. Rodrigues, G., Sarabdeen, J., and Balasubramanian, S. (2016) 'Factors that influence consumer adoption of e-government services in the UAE: A UTAUT model perspective', *JIC,* 15 (1), pp. 18-39.

232. Rot, A., and Blaicke, B. (2019) *2019 9th International Conference on Advanced Computer Information Technologies (ACIT).* Available at: ieeexplore.ieee.org

233. Roy, J. (2003) 'Introduction of e-government', *Social Science Computer Review*, 21 (1), pp. 3-5.

234. Samra, H., Li, A., Soh, B., and Al Zain, M. (2019) 'Utilisation of hospital information systems for medical research in Saudi Arabia: A mixed-method exploration of the views of healthcare and IT professionals involved in hospital database management systems', *Health Information Management Journal,* p. 1833358319847120.

235. Santos, R., Bennett, K. and Lee, E. (2021) 'Blockchain: Understanding Its Uses and Implications', *The Linux Foundation*.

236. Scott, J. K. (2006) 'Do US municipal government web sites support public involvement?', *Public administration review*, 66 (3), pp. 341-353. doi:10.1111/j.1540-6210.2006.00593.x

237. SEC, S. (2000). '2: Recommended elliptic curve domain parameters. Mississauga: Standards for efficient cryptography group'. Certicom Corp.

238. Seifert, J. W., and Chung, J. (2009) 'Using e-government to reinforce government—citizen relationships: comparing government reform in the United States and China', *Social Science Computer Review*, 27 (1), pp. 3-23. doi:10.1177/0894439308316404

239. Seltsikas, P., and O'keefe, R. M. (2010) 'Expectations and outcomes in electronic identity management: The role of trust and public value', *European Journal of Information Systems*, 19 (1), pp. 93–103.

240. Shah, M. (2007) 'E-governance in India: Dream or reality', *International Journal of Education and Development using ICT*, 3 (2), pp. 125-137. Available at: https://www.learntechlib.org/p/188043/

241. Shaikh, A. Z., Shah, U. L., and Wijekuruppu, C. (2016) 'Public service delivery and e-governance: The case of Pakistan', *International Journal for Infonomics*, 9 (2), pp. 1161-1170. Available at: https://infonomics-society.org/wp-content/uploads/iji/published-papers/volume-9-2016/Public-Service-Delivery-and-e-Governance-The-Case-of-Pakistan.pdf

242. Shafaq, N.K, Mohammed, S., and Majdalawieh, M. (2019). 'Blockchain Technology as a Support Infrastructure in EGovernment Evolution at Dubai Economic Department,' *Proceedings of the 2019 International Electronics Communication Conference on* - IECC '19.

243. Sharma, S. K. (2006) 'An E-Government Services Framework, Encyclopaedia of Commerce, E-Government and Mobile Commerce', *Mehdi Khosrow-Pour, Information Resources Management Association*, Idea Group Reference, USA, pp. 373-378.

244. Sheer, H. F., Gioulis, A., Naeem, A. R., and Markantonakis, K. (2018) 'E-voting with Blockchain: an e-voting protocol with decentralisation and voter privacy', *arXiv e-prints*, arXiv-1805.

245. Sigdel, S. (2007) 'E-Government for Good Governance' [online] *Weekly English Spotlight*, Available at: http://egovernancenepal.blogspot.com/2007/04/e-governance

246. Signore, O., Chesi, F., and Pallotti, M. (2005) 'E-government: challenges and opportunities', *CMG Italy-XIX annual conference*, 7-9 June 2005, Florence, Italy (pp. 7-9). CMG. Available at: https://www.comune.pisa.it/doc/cmg2005Italy.pdf

247. Singh, S., and Karaulia, D. S. (2011) 'E-Governance: Information Security Issues', *International Conference on Computer Science and Information Technology* (ICCSIT'2011) Pattaya Dec. 2011 (pp. 120-124). IEEE.

248. Singh, R., Tanwar, S., and Sharma, T. P. (2020) 'Utilization of Blockchain for mitigating the distributed denial of service attacks', *Security and privacy*.

249. Srivastava, S. C., and Teo, T. S. (2008) 'The Relationship Between E-Government and National Competitiveness: The Moderating Influence of Environmental Factors', *Communications of the association for information systems*, 23 (1), pp. 73-94.
250. Svein, Ø. and Arild, J. (2017) Blockchain Technology as s Support Infrastructure in e-Government. *Western NorwayResearch Institute*: Sogndal, Norway.

251. Swan, M. (2015) *Blockchain: Blueprint for a new economy*. Newton: O'Reilly Media, Inc.

252. Target News Service Washington. (2018) 'Addressing Challenges in Blockchain' Available at: ProQuest: Proquest website

253. Technology, M. O. (2019). '*S*audi e-Government Portal provides 2500 e-services for citizens and residents'. [online] Saudi Minsitry of Communications and Information Technology. Available at: https//www.mcit.gov.sa/en/media-center/news/89560

254. Teicher, J., and Dow, N. (2002) 'E-government in Australia: Promise and progress', *Information Polity*, 7 (4), pp. 231-246. doi:10.3233/IP-2002-0020

255. Terzi, S., Votis, K., Tzovaras, D., Stamelos, I., and Cooper, K. (2019) 'Blockchain 3.0 Smart Contracts in E-Government 3.0 Applications', *arXiv*, 06092. Available at: https://arxiv.org/ftp/arxiv/papers/1910/1910.06092.pdf

256. Theodorou, S. and Sklavos N. (2019) *Smart Cities Cybersecurity and Privacy*. Elsevier

257. Topprcom. (2019) 'E-Governance'. *Topper.com*. Available at: https://www.toppr.com/guides/business-law-cs/elements-of-company-law-ii/e-governance/

258. Twizeyimana, J. D., Larsson, H., and Grönlund, Å. (2018) 'E-government in Rwanda: Implementation, Challenges and Reflections', *Electronic Journal of e-Government*, 16 (1), pp. 19-31. Available at: https://oru.diva-portal.org/smash/get/diva2:1262879/FULLTEXT01.pdf

259. UN. (2018) 'United Nations e-government survey 2018: Gearing E-Government to support transformation towards sustainable and resilient societies', *United Nations*. Available at: https://publicadministration.un.org/egovkb/Portals/egovkb/Documents/un/2018-Survey/E-Government%20Survey%202018_FINAL%20for%20web.pdf

260. UN. (2020) 'UN E-Government Survey 2020'. Available at: UN E-Government Survey 2020

261. UN, P.A. (2016) 'Chapter 1: Mobilizing e-government to build resilient societies: preconditions and enabling environment', *UNO*. Available at: https://publicadministration.un.org/egovkb/Portals/egovkb/Documents/un/2018-Survey/E-Government%20Survey%202018_Chapter%201.pdf

262. UN. (2018) 'United Nations e-government survey 2018: Gearing E-Government to support transformation towards sustainable and resilient societies', *United Nations*. Available at: https://publicadministration.un.org/egovkb/Portals/egovkb/Documents/un/2018-Survey/E-Government%20Survey%202018_FINAL%20for%20web.pdf

263. Underwood, S. (2016) 'Blockchain beyond bitcoin', *Communications of the ACM*, 59 (11), pp. 15–17.

264. Vásquez, A., Bernal, J. F., and Tarazona, T. M. (2019) *International Conference on knowledge Management in Organisations*. Springer

265. Waller, L., and Genius, A. (2015) 'Barriers to transforming government in Jamaica: challenges to implementing initiatives to enhance the efficiency, effectiveness and service delivery of government through ICTs (e-Government)', *Transforming Government: People, Process and Policy,* 9 (4), pp. 480-497. doi:10.1108/TG-12-2014-0067

266. Wang, B., Sun, J., He, Y., Pang, D., and Lu, N. (2018) 'Large-scale Election Based On Blockchain', *Procedia Comput. Sci*., 129, pp. 234–237

267. Wang, Y., and Kogan, A. (2018) 'Designing confidentiality-preserving Blockchain-based transaction processing systems', *International Journal of Accounting Information Systems*, 30, pp. 1–18.

268. Wang, Y., Ren, J., Lim, C., and Swee-Won L. (2019). 'A Review of fast-growing Blockchain Hubs in Asia', *School of Business, Singapore University of Social Sciences*. https://doi.org/10.31585/jbba-2-2-(5)2019

269. Weerakkody, V., Irani, Z., Lee, H., Hindi, N., and Osman, I. (2016) 'Are UK citizens satisfied with e-government services? Identifying and testing antecedents of satisfaction', *Information Systems Management*, 33 (4), pp.331-343. doi:10.1080/10580530.2016.1220216

270. Wehrl, A. (1978) 'General properties of entropy', *Rev. Modern Phys*, 50 (2), p. 221.

271. Weidong, S., Lei, X., Zhimin, G., and Lin, C. (2018) 'eGov-DAO: a Better Government using Blockchain based-Decentralized Autonomous Organization Conference. Available at https://www.researchgate.net/publication/325632774

272. West, D.M. (2004) 'E-Government and The Transformation of Service Delivery and Citizen Attitude', *Public Administration Review*, 64 (1), pp. 15-26.
273. Wilson, T. (2016) 'Expert Shortage Hampers Japanese Financials in Blockchain Race'. [Online]. Available at: https://www.reuters.com/article/us-japan-fintechBlockchain-idUSKCN10S2GN. (Accessed Oct. 2, 2018)

274. World Bank Group. (2018) '*Cryptocurrencies and Blockchain*.' Available at: http://documents.worldbank.org/curated/en/293821525702130886/pdf/Cryptocurrencies-and-Blockchain.pdf.

275. World Bank (2004a) "E-Government", (Online). Accessed from: www.worldbank.org/egov.

276. World Bank. (2004b) 'Building Blocks of e-Governments: Lessons from Developing Countries', *Development Economics Vice Presidency and Poverty Reduction and Economic Management Network* (PREM Notes for Public Sector), No. 91.
277. Wu, J.G. (2015) 'Measuring E-government performance of provincial government website in China with slacks-based efficiency measurement', *Technological forecasting and social change*, 96, pp. 25-31. doi:10.1016/j.techfore.2015.01.007

278. Wu, K., Peng, B., Xie, H. and Huang, Z. (2019) 'An information entropy method to quantify the degrees of decentralization for Blockchain systems' In *2019 IEEE 9th International Conference on Electronics Information and Emergency Communication*, ICEIEC, IEEE pp. 1–6.

279. Wu, Y., and Bauer, J.M. (2010) 'E-government in China: deployment and driving forces of provincial government portals', *Chinese Journal of Communication*, 3 (3), pp. 290-310. doi:10.1080/17544750.2010.499633

280. Wu, Y., Tang, S., Zhao, B., and Peng, Z. (2019) 'BPTM: Blockchain-Based Privacy-Preserving Task Matching in Crowdsourcing', *IEEE Access*, 7, pp. 45605–45617.

281. Wüst, K., and Gervais, A. (2018) 'Do you need a Blockchain?' In *Crypto Valley Conference on Blockchain Technology (CVCBT)*, IEEE, 2018, pp. 45–54.

282. Wutongshu. (n.d) 'The first project of Blockchain-based government services in China locates in Chancheng'. Available at: http://91otc.baijia.baidu.com/article/ 55623 9. (Accessed 20 February 2017)

283. Xiong, Y., and Du, J. (2019) 'Electronic evidence preservation model based on Blockchain', *Proceedings of the 3rd International Conference on Cryptography, Security and Privacy*, Kuala Lumpur, Malaysia —January 19 - 21, 2019 (pp. 1-5). ACM. doi:10.1145/3309074.3309075

284. Xu, C., Liu, H., Li, P., and Wang, P. (2018) 'A Remote Attestation Security Model Based on Privacy-Preserving Blockchain for V2X', *IEEE Access*, 6, pp. 67809–67818.

285. Xu, L., Chen, L., Gao, Z., Chang, Y., Iakovou, E., and Shi, W. (2018) 'Binding the physical and cyber worlds: A Blockchain approach for cargo supply chain security enhancement', Paper presented at the *IEEE International Symposium on Technologies for Homeland Security* (HST).

286. Yamin, M., and Mattar, R. (2016) 'E-Government in Saudi Arabia-An Empirical Study', *BVICAM's International Journal of Information Technology*, 8 (1), pp. 944-949. Available at: https://pdfs.semanticscholar.org/f381/2bdfa1d96fb5b88d1e4cdfd9db95e12decce.pdf

287. Yang, L., Elisa, N., and Eliot, N. (2018) *Privacy and security aspects of E-government in smart cities*. New York: Elsevier Press.

288. Yang, L., Elisa, N., and Eliot, N. (2019) 'Privacy and security aspects of E-government in smart cities', *Smart Cities Cybersecurity and Privacy*, pp. 89-102. doi:10.1016/B978-0-12-815032-0.00007-X

289. Yang, J., Lu, Z., and Wu, J. (2018) 'Smart-toy-edge-computing-oriented data exchange based on Blockchain', *J. Syst. Archit*., 87, pp. 36–48

290. Yavuz, E., Koc, A. K., Çabuk, U. C., and Dalkılıç, G. (2018) 'Towards secure e-voting using Ethereum Blockchain', *6th International Symposium on Digital Forensic and Security (ISDFS),* 22-25 March 2018, Antalya, Turkey (pp. 1-7). IEEE. doi:10.1109/ISDFS.2018.8355340

291. Yesser E-government Program. (2019) [Online] Available at: http://www.yesser.gov.sa/EN/mediacenter/Annual_Reports/Anual%20Report%20foe%20web.pdf.

292. Yildiz, M. (2007) 'E-government research: Reviewing the literature, limitations, and ways forward', *Government Information Quarterly*, 24 (3), pp. 646–665.

293. Zhang, P., White, J., Schmidt, D. C., Lenz, G., and Rosenbloom., S. T. (2018) 'FHIRChain: applying Blockchain to securely and scalably share clinical data', *Computational and structural biotechnology journal*, 16, pp. 267-278. doi:10.1016/j.csbj.2018.07.004

294. Zhang, R., Xue, R., and Liu, L. (2019) 'Security and Privacy on Blockchain', *ACM Comput. Surv.,* 52, pp. 1–34

295. Zhang, Y.-H., and Liu, X. F. (2021) 'Traffic Redundancy in Blockchain Systems: The Impact of Logical and Physical Network Structures', *2021 IEEE International Symposium on Circuits and Systems* (ISCAS). doi:10.1109/iscas51556.2021.94013

296. Zhao, F., Scavarda, A.J., and Waxin, M.F. (2012) 'Key issues and challenges in e-government development: An integrative case study of the number one eCity in the Arab world', *Information Technology & People*, 25 (4), pp.395-422. doi:10.1108/09593841211278794

297. Zhao, J. J., and Zhao, S. Y. (2010) 'Opportunities and threats: A security assessment of state e-government websites', *GovernmentInformation Quarterly,* 27 (1), pp. 49-56.

298. W. Zhao, "PBoC filings reveal big picture for planned digital currency", coindesk, Jul. 2018. Accessed on: Sep. 29, 2018. [Online]. Available at: https://www.coindesk.com/pboc-filings-reveal-bigpicture-for-planned-digital-currency/.

299. Zhang, N., Zhong, S., and Tian, L. (2017) ‘Using Blockchain to Protect Personal Privacy in the Scenario of Online Taxi-hailing’, *International Journal of Computers Communication and Control*, 12 (6), pp. 886-902.

300. Zheng, X., Mukkamala, R. R., Ravi, V., and Joaqun, O. M. (2018) ‘Blockchain-based personal health data sharing system using cloud storage’ In *Proceedings of the 2018 International Conference on E-Health Networking, Application, and Services (HealthCom’18).* IEEE, Los Alamitos, CA, pp. 1–6.

301. Zheng, Z., Xie, S., Dai, H., Chen, X., and Wang, H. (2017) ‘An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends’, *2017 IEEE International Congress on Big Data (BigData Congress).* doi:10.1109/bigdatacongress.2017.

302. Zhonghua, Z., Xifei, S., Lei, L., Jie, Y., Wang, Y., and Dapeng L. (2021) ‘Recent Advances in Blockchain and Artificial Intelligence Integration: Feasibility Analysis, Research Issues, Applications, Challenges, and Future Work’, *Hindawi Security and Communication Networks*, 2021. https://doi.org/10.1155/2021/9991535.

303. Ziemba, E., Papaj, T., and Descours, D. (2014) ‘Assessing the quality of e-government portals – the Polish experience.’ In: *2014 Federated Conference on Computer Science and Information Systems*, 2, pp. 1259–1267. https://doi.org/10.15439/2014F121.