University of Technology Sydney
Faculty of Engineering and Information Technology
School of Electrical and Data Engineering

Identifying Security and Privacy Issues in the End-user Systems

Nazar Waheed

A Thesis Submitted
in Fulfillment of the
Requirements for the Degree

Doctor of Philosophy

under the supervision of

Dr. Priyadarsi Nanda
Dr. Muhammad Ikram
Dr. Wenjing Jia

Sydney, Australia

October 2023

CERTIFICATE OF ORIGINAL AUTHORSHIP

I, NAZAR WAHEED declare that this thesis, is submitted in fulfilment of the requirements for the award of DOCTOR OF PHILOSOPHY, in the Faculty of Engineering and Information Technology at the University of Technology Sydney.

This thesis is wholly my own work unless otherwise referenced or acknowledged. In addition, I certify that all information sources 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.

Student Name: Nazar Waheed

Student Signature:

Date: March 28, 2024

ABSTRACT

Security and privacy issues in End-user systems, for example, Internet of Things (IoT), websites, and mobile platforms, have received significant attention from industry and academia. Compared to classical network systems, IoT systems have significant privacy and security concerns because of their resource-constrained and heterogeneous nature, such as unauthorised data access, weak authentication protocols, and difficulty applying traditional security measures due to device heterogeneity and resource constraints. Recent machine learning and blockchain advances hold significant promises for solving these issues. This thesis aims to comprehensively analyse the security and privacy issues in IoT and propose solutions by combining machine learning algorithms and blockchain technologies. The practical applications of these solutions range from enhancing smart home security to securing IoT-enabled healthcare, thus significantly contributing to the trustworthiness and resilience of these rapidly evolving technologies.

Secondly, We propose Privacy-Enhanced Living - a differential privacy-based framework to ensure comprehensive security for data generated by smart homes. We employ a randomised response technique for the data and utilise Local Differential Privacy to achieve data privacy. The data is then transmitted to an aggregator, where an obfuscation method is applied to ensure individual anonymity. Furthermore, we implement the Hidden Markov Model technique at the aggregator level and apply differential privacy to the private data from smart homes.

Next, We propose FedBlockHealth - a novel hybrid approach combining federated learning and blockchain technology to provide a secure and privacy-preserved solution for IoT-enabled healthcare applications. Our approach leverages a public-key cryptosystem that provides semantic security for local model updates, while blockchain technology ensures the integrity of these updates and enforces access control and accountability. The federated learning process enables a secure model aggregation without sharing sensitive patient data. We implement and evaluate our proposed framework using Extended Modified NIST datasets, demonstrating its effectiveness in preserving data privacy and security while maintaining computational efficiency.

Finally, Web-based chatbots provide website owners with the benefits of increased sales, immediate response to their customers, and insight into customer behaviour. While Web-based chatbots are getting popular, they have received little scrutiny from security researchers. The benefits to owners come at the cost of users' privacy and security. Vulnerabilities, such as tracking cookies and third-party domains, can be hidden in the chatbot's iFrame script. This thesis aims to analyse these threats and highlight them to the End-users so that they can be more careful when using web-based chatbots.

Acknowledgements

First, Alhamdulillah, for all the blessings and guidance, especially during tough times.

Thank you to UTS for the PhD scholarship. Big thanks to my supervisors: Dr. Priyadarsi Nanda for always guiding and encouraging me; Dr. Muhammad Ikram for helping when I was stuck; and Dr. Xiangjian He for his patience and always being positive.

I'm forever grateful to my parents, and sisters. Their dreams and prayers have always pushed me forward.

To my wife, Kiran, and our kids, Muhammad, Ahmad, and Taha: Your love and support mean everything. I'm sorry for the times I was away, but you've made this journey possible.

Thanks to my friend, Dr. Abdullah Waris, for showing me this path. Also, Dr. Waleed and Dr. Salman, for believing in me from the start.

Lastly, during the toughest times, friends like Adnan Mir, Mian Ahmad Jan, Saqib Nawaz, Imran Makhdoom, Muhammad Saqib, Usman Naseem, and Wafa Soomro have been my rock. Thank you for being there.

Contents

List of Publications

Journal Papers

J-1. **N. Waheed**, X. He, M. Ikram, , M. Usman, S.S. Hashmi, and M. Usman, "Security and Privacy in IoT Using Machine Learning and Blockchain: Threats and Countermeasures," *ACM Computing Surveys*, vol. 53, no. 6, pp. 1-37, Nov. 2021. (*Corresponding to Chapter 2 and Chapter 3*)

Conference Papers

C-1. **N. Waheed**, A.U. Rehman, A.Z. Almalmaie, and P. Nanda, "FedBlockHealth: A Synergistic Approach to Privacy and Security in IoT-Enabled Healthcare through Federated Learning and Blockchain," *GlobeCom 2023*, Malaysia, 8-11 Oct 2023. (*Corresponding to Chapter 4*)

C-2. **N. Waheed**, F. Khan, M.A. Jan, A. Z. Almalmaie, and P. Nanda, "Privacy-Enhanced Living: A Local Differential Privacy Approach to Secure Smart Home Data," *IEEE COINS 2023*, Germany, 1-3 Sep 2023. (*Corresponding to Chapter 3*)

C-3. **N. Waheed**, M. Ikram, S.S. Hashmi, X. He, and P. Nanda, "An Empirical Assessment of Security and Privacy Risks of Web-based Chatbots," *WISE 2022*, France, 8-11 Oct 2022. (*Corresponding to Chapter 5*)

List of Figures

Chapter 1

Introduction

In today's digital era, End-user systems, particularly the Internet of Things (IoT) and web technology, have become essential components of our daily lives. A staggering 70% of IoT devices currently in use are vulnerable to cyber-attacks, underscoring the critical need for enhanced security measures [1]. Additionally, this report also revealed that 98% of all IoT device traffic is unencrypted, leaving personal and confidential data exposed on the network. Alongside the vulnerabilities of IoT devices, security concerns extend to chatbots, which play a pivotal role in customer service and data handling. Recent insights reveal that chatbots are susceptible to threats like data breaches, social engineering attacks, and interception of data transmission due to inadequate security measures. Moreover, the AI models that power these chatbots could be prone to adversarial and injection attacks, compromising user privacy and data integrity. To combat these threats, best practices such as robust authentication processes, regular security audits, data encryption, and adherence to data protection regulations are critical for safeguarding against unauthorized access and ensuring the confidentiality of sensitive user data [2–4]. With the increasing reliance on ubiquitous and digital technologies, user-centric systems are essential to offer various functionalities to fulfil individuals' needs and preferences through seamless access to information, services, and entertainment. An End-user system is a combination of hardware and software components specifically designed to facilitate the interaction between individuals and technology. Web technology encompasses many tools, techniques, and standards that designers, developers, and content providers use to deliver content across the World Wide Web (WWW) [5,6].

IoT is a network of interconnected embedded devices configured with sensors and software that enable such physical devices to collect and exchange meaningful data. Such information can be shared and communicated without human intervention, facilitating various services through Information Communication Technology (ICT) [7, 8]. IoT improves the efficiency as well as decision-making capabilities of the system and provides new services and experiences. IoT devices are thus widely used in many and diverse applications of different industries, e.g., transportation, healthcare, agriculture, manufacturing, and smart cities [9, 10].

End-user systems' ubiquity and multifaceted functionalities empower and make an integral and essential component of our digital ecosystem. IoT devices are primarily weak in configuration and do not have adequate security resistance against sophisticated cyber-attacks and future security threats. Such systems come with inherent security and privacy vulnerabilities, which are unique to each type of system. Thus, malicious actors aim for such systems to damage their functionality and services, affecting technology-based businesses exceedingly due to the interruption of services, data breaches/proliferation, and user privacy concerns. Therefore, such technology-enabled systems can only provide their functionalities with complete competence with adequate security level [11, 12]. Hence, this thesis explores comprehensive security and privacy issues in End-user systems, focusing on IoT devices and websites through a rigorous investigation of their roots, implications, and potential mitigations.

1.1 Background

This section presents the background of IoT and End-user devices to get an overview of such systems. Furthermore, we discuss crucial security and privacy issues by focusing on IoT systems and Web-based chatbots.

1.1.1 Overview on IoT and End-user devices

The recent rapid increment in modern technologies offers notable advancements in the domain of connected devices. IoT has emerged as a transformative theory, and End-user devices persist in evolving and catering to the needs of individuals. This background illustrates a comprehensive outline and comparison between IoT devices and End-user devices, emphasizing their corresponding characteristics, functionalities, and effects on different aspects of our lives [13].

IoT devices are embedded components configured with software, sensors, and network proficiencies to automatically gather and transmit consequential information over the Internet with heterogeneous systems for effective results. They can independently execute activities based on pre-defined instructions and contribute to intelligent and automated decision-making processes. Such devices include simple objects (e.g., wearable devices and smart home/office appliances) to complex systems (e.g., Programmable Logic Controllers (PLCs) and autonomous vehicles) [14].

Developers mainly design and develop End-user devices for individual users to connect directly with systems/networks, enhancing their user experience in everyday activities. Such devices are usually operated and controlled by individuals straightaway to browse Internet content, communicate with other persons, access applications, and execute relevant other tasks. Examples of End-user devices are smartphones, computers, smartwatches, and tablets [15]. The availability of competent processors, modern software, and high-resolution displays have impressively improved the abilities of End-user devices for performing complex tasks, computing large amounts of data, and providing immersive experiences [16]

Both (IoT and End-user devices) contribute to the digital ecosystem. However, there are various important aspects in which both have differences, and are presented below:

- *Intelligence and Autonomy*: IoT devices can be operated independently with varied degrees of autonomy while the user controls End-user devices.
- *Scope of functionality:* IoT devices are developed for specific applications and operations, while End-user devices provide a more comprehensive range of functionalities, individuals' needs, and personalization.
- *Scale and deployment:* IoT devices are mainly deployed on a large scale for data collection, analytics, and meaningful insights. End-user devices are primarily used to satisfy individual needs being deployed at a small scale.
- *Connectivity and Communication*: IoT devices are designed to be interconnected with various other devices, while End-user devices are developed to connect with the Internet for online services.
- *Security and privacy challenges*: IoT and End-user devices have concerns regarding security and privacy, but IoT devices have more challenges as such devices are continuously interconnected and involved in crucial tasks.

1.1.2 Security and Privacy Challenges in IoT devices

The proliferation of IoT in recent years needs massive IoT components to fulfil the market requirements, which motivates IoT manufacturers to deliver less protected devices in the IoT market. However, connectivity, limited computational resources, and diverse deployment scenarios in IoT devices create various opportunities for attackers to perform destructive actions through physical and remote attacks over such components [7, 17]. The risks associated with data privacy have also been underlined in IoT devices, as data collection, processing, and transmitting are huge. There are various possibilities for exposing sensitive information, data leakage, and privacy breaches [18, 19]. Key security and privacy challenges associated with IoT devices are analyzed in different aspects, which are as follows.

IoT devices are resource-constrained in nature as they are configured with fixed computing, storage, communication protocols, and battery capabilities. Thus, it isn't easy to implement robust security mechanisms in IoT devices [20]. Such devices mostly perform various operations within complex networks, and their protection against security threats depends on the aggregated security of the network infrastructure. Network protection implementations with limited security features can also expose IoT systems to threats of authentication, confidentiality, integrity, access control, availability, and privacy [21, 22]. Firmware and software are vital components in IoT devices for executing different tasks effectively. However, attackers can exploit IoT systems through potential vulnerabilities (that are present in such components), resulting in illegal control of devices, attack execution, and unauthorized access. One of the critical security issues in IoT devices is providing a robust authentication and authorization mechanism. It is essential to confirm the authenticity of an IoT device through multiple security measures to prevent unauthorized access [23].

IoT's inherent heterogeneity poses a significant challenge in developing comprehensive security solutions, i.e., diverse characteristics, software systems and configurations, varied standards, and implementation techniques in such devices. The need for standardized security mechanisms and frameworks in IoT devices presents remarkable challenges as there are issues in policy enforcement and updating the system [24].

Due to the capability to identify patterns and learn from data, Machine Learning (ML) algorithms have emerged as favourable tools for improving security in IoT networks. Some recent works, such as [25], have leveraged such algorithms to detect and predict security threats through network traffic patterns and device behaviour. Despite these promising efforts, the application of ML in IoT security still needs to be competitive as malicious actors also continue to work on advanced security threats to damage IoT systems. Therefore, it is required to analyze various attack identification and prediction comprehensively approaches for the latest findings [26]. Blockchain technology is known for its decentralization, transparency, and immutability, and this technology can help address different IoT security and privacy challenges [27]. However, integrating blockchain technology into IoT systems often introduces efficiency, scalability, and interoperability challenges, which should be thoroughly analyzed [28].

Considering the above-discussed concerns, it is necessary to provide a more comprehensive literature that combines meaningful features of ML and blockchain technologies to address IoT security and privacy issues. For instance, ML could help predict and mitigate threats in an IoT network, while blockchain technology could provide a secure and transparent platform for managing and deploying ML models. Researchers have explored these technologies separately but still have to investigate for detailed analysis [29, 30].

Addressing these gaps, this thesis aims to provide a comprehensive investigation into the potential of ML and blockchain technologies for enhancing IoT security and privacy. It proposes novel methodologies for integrating these technologies into IoT systems, evaluates their performance in real-world scenarios, and explores the potential challenges and trade-offs. This work aims to contribute to the existing body of knowledge and advance the understanding of IoT security in the context of these emerging technologies.

1.1.3 Security and Privacy Challenges in Web-based Chatbots

Web-based chatbots are virtual assistants developed using Artificial Intelligence (AI) to connect with users through web-based platforms to provide appropriate answers or responses automatically based on the given queries by users. They are used in different web and application-based platforms, i.e., social media, websites, and messaging applications, to offer immediate support and enrich the user experience anytime [31, 32]. Chatbots are already in use in various applications. However, they have recently become more knowledgeable and effective in providing better results due to the development and integration of advanced AI-based techniques. Thus, Web-based chatbots are cost-effective, scalable, multi-tasking, anytime availability, and enhanced user experience; thereby, their usage has increased exponentially [33–35]. Though Web-based chatbots have various benefits and features, there are decisive security and privacy concerns [36, 37], as discussed below:

- *Data Privacy*: Chatbots collect and store data (e.g., private information, usage patterns, preferences, demographic information, chat history, etc.) for better efficiency and correctness through the learning process. Therefore, it is important to safeguard the collected/stored user data properly by implementing adequate data encryption algorithms and access control mechanisms over the entire system. Otherwise, it can lead to privacy infringement and unauthorized access issues [38, 39].

- *Security Integration*: Chatbots regularly communicate with various and multiple systems, applications, and third-party services. Integrating security over the system is crucial to resist the exposure of decisive data, illegitimate access, modification of data, and recovery plan from the damage(s). Hence, it is required to appropriately consider security integration while designing, developing, and deploying Web-based chatbots [34, 40, 41].

- *Authentication and Authorization*: Chatbots are integrated into applications and websites to perform various tasks without human intervention; thereby, it is necessary to verify (through robust user authentication methods) the users who request answers to their queries. Otherwise, there are possibilities that unauthorized access can be provided to illegal users, directing to impersonation attacks [36,42].

- *Vulnerabilities*: Chatbots are associated with different internal and external applications, software systems, and third-party services that may introduce vulnerabilities in chatbots to learn the chatbot system (for launching attacks later) by gaining access through malware, Ransomware, or their variants. Such incidents can happen in the case of inadequate implementation of security measures over the chatbot system [43].

- *Data mismanagement*: Chatbots collect and store user data to improve future answers. However, misusing such data may lead to negative consequences, such as losing trust among users and potential customers. However, such incidents can happen if rigorous data protection measures and proper data handling practices are not implemented [36,44].

To mitigate the above-mentioned risks, it is essential to implement robust security measures (i.e., standardized security protocols and frameworks), providing transparency in data management and usage practices and relevant guidelines compliance for preventing the exposure of user data. Additionally, regular security audits and testing should be performed to identify and address advanced and potential vulnerabilities in the chatbot system. Moreover, appropriate training for human operators to manage crucial and private should be implemented to avoid human errors.

1.2 Research Objectives

This PhD thesis aims to meticulously investigate and analyze specific security and privacy challenges that emerge from End-user systems, particularly focusing on IoT devices and websites. The study will focus on the following main objectives:

- *Comprehensive Review*: To carry out an in-depth survey of existing security and privacy issues in IoT devices and explore potential countermeasures using ML and blockchain technologies.
- *Privacy-Enhanced Living System*: To design and propose a differential privacy-based system, Privacy-Enhanced Living (PEL), to ensure comprehensive privacy for data generated by IoT devices in smart homes.
- *Framework Development*: To design and implement an innovative framework that enhances the security and privacy of IoT devices using ML algorithms with blockchain technologies.
- *Dataset Creation*: To prepare a novel public dataset of selected Web-based chatbots extracted from the Alexa top 1-million popular websites, providing a valuable resource for future research and development activities.
- *Empirical Assessment*: To empirically assess security and privacy risks associated with Web-based chatbots, contributing to understanding potential vulnerabilities in such systems that can be used to develop intrusion/defensive solutions.

This research aims to provide valuable insights into security and privacy threats present in End-user systems and propose practical solutions to tackle some of the above-discussed challenges. The findings of this study are expected to significantly contribute to advancing the field of security and privacy and provide meaningful guidance for developing secure and privacy-preserving End-user systems.

1.2.1 Research Questions

We present research questions based on the objectives mentioned above in order to fulfil the purpose of this thesis work:

1. What are advanced security and privacy challenges for End-user systems that are essential to address in the near future?

2. How can secure data collection and advanced privacy measures be combined within a comprehensive framework in intelligent environments? How can the effectiveness of such a framework be assessed in real-world applications?

3. How can ML and blockchain technologies be integrated to offer a robust defence mechanism against the latest security and privacy threats in IoT devices?

4. What are the latest security and privacy concerns that are crucial and associated with Web-based chatbots? How can such risks be empirically evaluated through a novel public dataset?

1.3 Contributions

The research conducted for this PhD thesis, aligned with its above-defined objectives, has resulted in the following significant contributions:

1. We perform a comprehensive study of potential security and privacy challenges in IoT devices and their countermeasures using ML and blockchain technologies together. (RQ1)

2. We propose a differential privacy-based system, named *Privacy-Enhanced Living (PEL)*, to confirm privacy for data generated by smart homes. (RQ2)

3. We develop an innovative framework, named *FedBlockHealth*, for enhancing IoT devices' security and privacy level by involving ML algorithms with blockchain technologies for the healthcare industry. (RQ3)

4. We prepare a novel public dataset of selected Web-based chatbots extracted from well-known Alexa's top 1-million popular websites. (RQ4)

5. We perform an experimental evaluation of the security and privacy risks involved in Web-based chatbots. (RQ4)

1.4 Research Methodoloy

The primary objective of this research is to systematically enrich the security and privacy of End-user data collected, processed, stored, and transferred among IoT devices and websites during their regular operations. This work's research methodology is categorized into three parts: (i) *Literature Review*, (ii) *Security and Privacy for IoT Devices*, and (iii) *Security and Privacy for Websites*. Furthermore, it is displayed in Figure 1.1 for better representation. The first stage of this research focuses on surveying various potential threats over the End-user systems and identifying open research challenges. Taking the first stage into account, the second stage is to analyze the integration of ML and blockchain technologies (for smart home and healthcare industries) to address the identified security and privacy challenges. The third stage focuses on the experimental evaluation of associated security and privacy risks in Web-based chatbots deployed over websites.

1.5 Thesis Organization

The rest of this thesis is structured as follows:

Chapter 2 discusses End-user systems, focusing on IoT devices and Web-based chatbots. Section 2.1 explains End-user systems as well as the security and privacy potential challenges in End-user systems. In particular, Section 2.2 provides a comprehensive review of potential security and privacy challenges in IoT devices, while in Section 2.3, security and privacy challenges in Web-based chatbots are explained. Moreover, related works are analyzed in Section 2.4 to understand the status of the discussed challenges in IoT and Web-based chatbots.

Chapter 3 presents our comprehensive survey of mitigating IoT Threats in Sec-

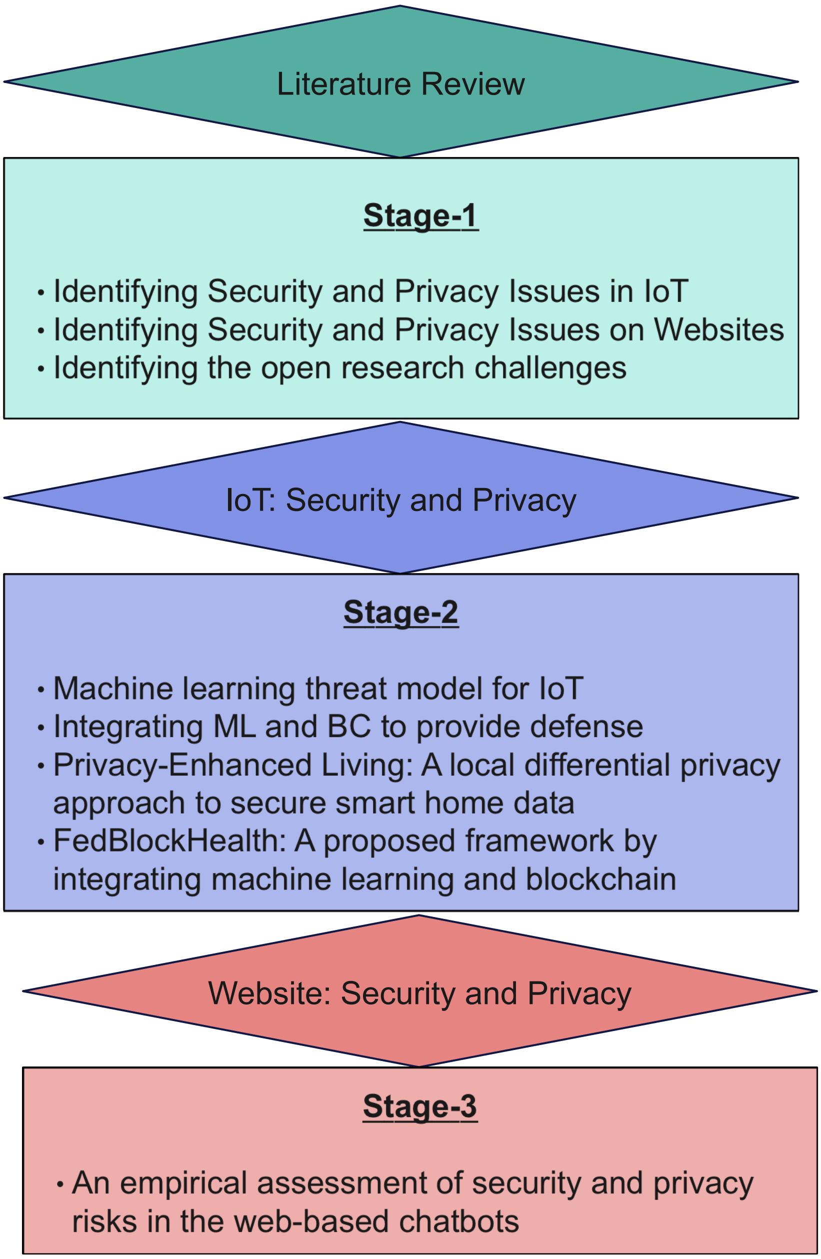

Literature Review
Stage-1
• Identifying Security and Privacy Issues in IoT
• Identifying Security and Privacy Issues on Websites
• Identifying the open research challenges
IoT: Security and Privacy
Stage-2
• Machine learning threat model for IoT
• Integrating ML and BC to provide defense
• Privacy-Enhanced Living: A local differential privacy approach to secure smart home data
• FedBlockHealth: A proposed framework by integrating machine learning and blockchain
Website: Security and Privacy
Stage-3
• An empirical assessment of security and privacy risks in the web-based chatbots

Figure 1.1 : Research methodology.

tion 3.1 by combining Machine Learning and Blockchain technologies. Section 3.2 proposes a privacy-preserving secure framework that can be applied to real-time IoT applications in a smart home environment.

In Chapter 4, we present *FedBlockHealth*, an innovative approach that merges Federated Learning with blockchain technology to create a secure and privacy-preserving solution for IoT-enabled healthcare applications. This chapter explores the utilization of a public-key cryptosystem to semantically secure local model updates while employing blockchain technology to ensure the integrity of these updates and enforce access control and accountability.

In Chapter 5, we embark on a comprehensive investigation into the security and privacy issues in Web-based chatbots on Alexa's top 1-million popular websites. This chapter offers valuable insights into the current Web-based chatbot security and privacy landscape, highlighting vulnerabilities and suggesting potential directions for future research.

Finally, Chapter 6 outlines the conclusion and future research direction of this thesis.

Chapter 2

Literature Review

This chapter provides a comprehensive overview of End-user devices (Section 2.1), IoT devices (Section 2.2), and Websites (Section 2.3). These technologies form the backbone of our digital world, and understanding their security and privacy challenges is paramount. Following this, we analyse the security and privacy challenges of IoT devices and Websites, aiming to identify potential issues and threats within our thesis domains. We discuss related work in Section 2.4, enabling readers to understand relevant concepts and methods and identify gaps in the existing research. This chapter also analyses relevant articles on these domains to understand the current status of security and privacy challenges and their solutions.

2.1 End-User Systems

The End-user system architecture is the design and structure of hardware and software components that offer an interaction between End-users and a particular system/application while leveraging the desired functionality of various technologies. Figure 2.1 displays a typical layered End-user system architecture. It consists of the following elements.

- *User Interface*: This is a graphical representation of different functions by taking accessibility, ease of usage, responsiveness, and quickness into account for better user experiences.
- *Client Applications*: This includes three types of applications (desktop, web, and mobile) to efficiently and directly access the system's functionalities and

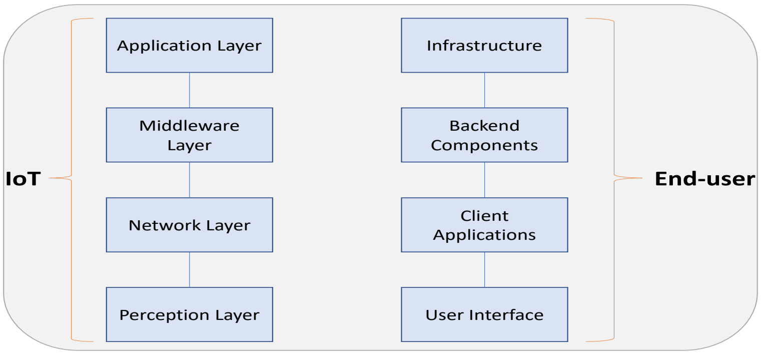


Figure 2.1 : The Architecture Outline of IoT and End-user Systems

features.

- *Backend Components*: It consists of the fundamental logic and computing abilities to implement various algorithms, policies, testing, and workflows by performing data storage, retrieval, manipulation, and communication (internal and external) operations.

- *Infrastructure*: This represents physical or virtual networking components in order to support the infrastructure (e.g., servers, networks, and cloud services) through processing, communication protocols, and storage resources [45, 46].

Having discussed the architecture of End-user systems, we now turn to the security challenges these systems face.

2.1.1 Security Challenges in End-User Systems

End-user devices are used by individuals for rich user experience in their regular activities [7]. Such End-user systems are easy targets for malicious actors as cyber threats are exponentially growing due to weak or inadequate implementation of security and privacy measures in those devices, and attackers also perform sophisticated attacks for the successful execution of adverse actions [8]. We discuss potential aspects of security challenges as follows:

- *Malware*: Software/firmware update files should be installed in End-user devices regularly to keep the device up-to-date with various features and functionalities. It is necessary that only authorised parties must install such files, and they should install only legitimate files. It is also required to check often regarding any malicious activities, e.g., access of root users, disruption in device operations, illegal changes in applications, stealing data in an unauthorised manner, sending vulnerable files (i.e., viruses, worms, trojans, ransomware, and spyware), and enabling remote control illicitly [47, 48].
- *Weak User Credentials and Authentication*: Users have multiple devices for different purposes, and keeping diverse user credentials (i.e., identity and password) for each device/account is difficult. Therefore, users typically select similar user credentials for all accounts/devices. To easily remember user credentials, users often choose weak or straightforward passwords that allow attackers to perform malicious actions over End-user devices. Some low-cost End-user devices are not configured with multi-factor authentication methods to confirm the authenticity of a user through multiple credentials; thereby, it becomes easier to penetrate such devices. It is also essential to design robust authentication mechanisms to avoid the risk of unauthorised access to End-user devices. End-user devices are the prime target for data breaches when malicious actors get unauthorised access to private and crucial data [49, 50].
- *Limited Knowledge and Training*: People mostly use various End-user devices for varied intentions, and such devices are enabled with many features and functionalities. However, very few users know all device operations and features. Adversaries have good knowledge of various End-user devices and know potential loopholes that can help them with unintentional actions (executed

by End-users). End-users are unfamiliar with potential threats and safe operation practices (e.g., web browsing, password storage and security, social media), leading to various security incidents. Without proper training and education on password security, phishing awareness, and secure web browsing, End-users are likelier to fall victim to attacks. As a result, unknown entities may gain unauthorised access to confidential information or essential system components [51–53].

- *Insecure Wireless Connectivity*: When users travel from one place to another (e.g., outside home, state, or country), End-user devices should have Internet connectivity to enable various features and provide up-to-time information in different functionalities. In such a scenario, users need a mobile or public network to enable the Internet. Establishing a connection with compromised or insecure networks can direct the exposure of End-user devices that may include the implementation of different attacks, e.g., man-in-the-middle, modification, session disclosure, impersonation, and eavesdropping attacks [54–56].

- *Vulnerable Software/Hardware*: Attackers develop new skills by learning novel techniques and methods for successively launching attacks as defensive solutions implement various security measures to protect against threats. Thus, it is necessary to keep the operating system of End-user devices updated by installing the latest security patches and updates. Failure to install and update the newest security patches can open an opportunity for adversaries to expose End-user devices by executing known vulnerabilities. Furthermore, faulty hardware components should also be replaced with better components to prevent the risk of attacks at the embedded level [57–59].

2.1.2 Privacy Challenges in End-User Systems

End-users are directly connected with multiple End-user devices for different purposes, and their data is associated with such devices for storage, computation, and communication. It is, therefore, important to consider the privacy concerns of End-users who connect and interact with diverse systems and networks by using heterogeneous technologies [60, 61]. Privacy concerns include the data leakage risk while pairing the device with the system/network through discovery protocols, exchanging personal information over communication protocols, sharing resources without implementing adequate security measures, and exposing devices to known vulnerabilities. This opens the door for an adversary to disrupt the system to deliver unexpected and abnormal outcomes remotely. We discuss potential aspects of security challenges as follows:

- *Data Collection/Storage/Computation*: Applications/Systems available on End-user devices gather various kinds of data about users' location, movements, activities, and preferences for data analytics. Such collected information is mostly shared with third-party entities for recommendations, personalised experiences, and advertisement purposes without the knowledge of End-users. The disclosure of such data may lead to privacy concerns as the data owner is unaware of such activities. End-user devices are configured with limited security protection due to the cost and feasibility of diverse applications. In such a scenario, there are possibilities that the requirement of secure computation and storage may not be satisfied properly, revealing the private data of End-users [61, 62].

- *Device Tracking*: Most End-user devices are configured with the Global Positioning System (GPS) for navigation and location-based services. When the GPS service is enabled, it allows tracing the user's location through a satellitebased radio navigation system. Such applications and services are helpful for End-users in their daily activities. However, it also raises privacy concerns for End-users when geo-location data is stored without user consent. Many applications also share such information with other systems, which may allow attackers to get private data if those systems are weak in privacy configurations [27, 63, 64].

- *Data Leakage*: Data is exchanged/processed/stored in End-user systems to perform different functionalities. Unauthorised or fortuitous disclosure of personal information (while data-in-rest, data-in-transit, or data-in-process) is considered data leakage. Such activities can be carried out intentionally or accidentally due to malware, unreliable wireless connection, untrusted application/platform, or device loss/theft. As a result, such user privacy issues may also lead to financial loss, identity theft, or damage to the user/organisation's reputation. Therefore, it is required to implement appropriate authentication and encrypted techniques to avoid the exposure of private data [65–67].

2.2 IoT Devices

The rapidly evolving domain of the Internet of Things (IoT) comprises an intricate, interconnected system of various devices, sensors, networks, and applications. This intricate, interconnected system, called the IoT architecture, is established to facilitate seamless data collection, transfer, processing, and delivery to the End-user. The architecture involves several components, layers, and communication protocols that support connectivity and interaction among different elements within the system. At the core of this architecture resides the *Perception Layer*, composed of IoT devices such as actuators, sensors, wearables, and other associated physical components. These devices are instrumental in collecting meaningful environmental data, including metrics like humidity, movement, and temperature. The *Network Layer*, comprising varied communication protocols like Bluetooth, Long-Term Evolution (LTE), Wireless Fidelity (Wi-Fi), Infrared, and Zigbee, functions as the second layer. It ensures efficient data transfer among gateways and devices, enabling subsequent processing. The third layer, known as *Middleware*, serves as a cloud or platform to extract data from gateways and to process it for storage, analytics, and complex operations. Lastly, the *Application Layer* focuses on delivering the processed data to the End-user using effective visual representations such as graphs, dashboards, or charts over web or mobile-based applications [68, 69]. Nonetheless, incorporating these devices into the IoT framework is full of complications. Specifically, security and privacy-related challenges have emerged as significant concerns within the IoT domain. In the ensuing sections, we will delve into these challenges, explore their implications for IoT devices, and discuss potential strategies to tackle them. Figure 2.1 illustrates a typical layered IoT system architecture.

In summary, IoT devices form the backbone of the IoT architecture, playing a crucial role in data collection, transfer, and processing. However, their integration into the IoT system presents several challenges, particularly in terms of security and privacy.

2.2.1 Security Challenges in IoT Devices

IoT devices, which integrate sensors, networks, embedded components, and software capabilities, measure and exchange pertinent information autonomously. On the other hand, End-user devices, used directly by individuals, enrich the user experience in their regular activities [7, 8]. We analyze various security challenges in IoT systems as follows:

- *Insecure Communication Channel*: In IoT systems, various communication protocols/networks such as Bluetooth, LTE, Wi-Fi, Infrared, or Zigbee transmit data. When such communication protocols are not secured adequately, malicious actors can perform adverse activities to disrupt (i.e., eavesdropping, malicious data injection, user impersonation) the functionalities of IoT systems [70].

- *Weak Authentication*: Manufacturers often pre-configure many IoT devices with default passwords, which makes these credentials readily discoverable. This ease of access enables attackers to exploit IoT devices with weak or unchanged default passwords, gaining unauthorized entry into these embedded components. In addition, due to their low-cost nature, IoT devices often lack robust authentication mechanisms to protect them against various security threats. This lack of protection can potentially allow unauthorized entities to gain control over embedded components and carry out harmful activities [71, 72].

- *Vulnerable Firmware*: Most IoT devices run firmware to update their systems with the latest security patches and prevent various security threats. However, vulnerabilities in such firmware may expose IoT devices to get unauthorized access to manage the whole IoT network/system. Certain IoT components do not undergo regular firmware updates, exposing them to known vulnerabilities. Consequently, one should verify the accuracy and authenticity of firmware before installing it on IoT devices [73, 74].

- *Malware*: Malicious software presents significant threats to IoT devices, exploiting them in numerous potential ways. For instance, attackers can hijack compromised devices to execute Distributed Denial of Service (DDoS) attacks. IoT devices can even distribute malware programs due to their connectivity to other systems/networks. Furthermore, adversaries can design malware to siphon off critical personal information from these IoT devices. If manufacturers embed malware into the devices during production, it can instigate supply chain attacks [75].

- *Lack of Adequate Encryption*: Information in IoT systems is exchanged in a public network, and thus, it is required to implement appropriate encryption mechanisms for IoT systems while sharing crucial and private information. Otherwise, the disclosure/changes of such information can lead to confidentiality and integrity attacks. Thus, the failure to protect data can result in unexpected active and passive challenges during the system operations [76,77].

Table 2.1 : Summary of Security Threats in IoT with Their Relationship in Different Attributes

Threat	**Impact**	**Attack**	**Type**	**Layer of Impact**	**Solution**
Security	Availability	DoS	Flooding	Physical, MAC	Multiple
			DDoS	Physical, MAC	Multiple
			Botnet	Physical, MAC	Multiple
		Physical	Damage	Physical	Physical Security
			Environmental	Physical	Shielding
			Power Loss	Physical	uninterrupted power
			Hardware Failure	Physical	Backup
			Tampering	Physical	Physical Security
	Integrity	MiTM	Sybil Attack	Physical, MAC, Network	code attestation, radio resources testing, key pool
			Spoofing	Network	anti-spoofing software
			message tamper		
		Malware	Injection	Application	
			Virus	Application	
			Worms	Application	

In conclusion, while offering numerous benefits, IoT devices also present significant security challenges. These challenges span from insecure communication channels and weak authentication to vulnerable firmware, malware threats, and inadequate encryption. Addressing these challenges is not just a necessity but a crucial step towards ensuring IoT systems' safe and effective operation. Table 2.1 gives an outline of security threats in IoT, making it easier for the readers to understand potential impacts and relations over different attributes.

However, the challenges continue beyond security. As we delve deeper into IoT devices, we encounter another set of equally critical issues - privacy concerns. These concerns, intertwined with security, present a complex landscape that needs careful navigation. In the following section, we will explore these privacy challenges in detail, shedding light on their implications and discussing potential strategies to address them.

2.2.2 Privacy Challenges in IoT Devices

IoT devices are used in various home-based and industrial applications for different purposes by individuals and automated systems. Various risks may be encountered in such devices, such as software vulnerabilities, hardware faults, and data disclosure, which may raise privacy concerns while using IoT devices. Privacy challenges are associated with potential security concerns for IoT devices. IoT devices store most of the credentials in their memory storage for better functionalities and quick execution of relevant operations. However, such practices may lead to privacy breaches resulting from illegal data access/sharing, tracking, or surveillance. Besides, IoT devices are interconnected with other networks/systems for various services, and third-party applications often request extensive permissions, which can inadvertently or deliberately collect various data from IoT devices. Such collected information is shared with unauthorized entities without the data owner's knowledge. This raises significant concerns about data privacy, consent, and the potential misuse of personal information [46, 60]. We discuss potential aspects of privacy challenges that can damage the resistance of IoT devices against various threats.

- *Data Transmission*: IoT devices are connected with other components and networks to perform subsequent tasks that can be input for the next processing task or can deliver the final outcomes. During this process, crucial and private information is transferred to the next level, and there can be a scenario in which a specific task may reveal some sensitive data (of IoT device users and their actions). Thus, it is indispensable to protect personal data from privacy exposures [62].

- *Weak Device Configuration*: Most IoT devices are enabled with low-cost sensors to meet the lightweight and cost-effective requirements of the IoT architecture. Such sensors, for example, cameras, GPS, and microphones, have limited privacy protection features in their functionalities. Due to limited services, IoT devices may not have robust mechanisms to withstand privacy attacks. Accordingly, private data can be collected and shared unknowingly, which may pose significant privacy concerns while using IoT devices in various applications [78, 79].

- *User Data*: To provide better services and functionalities according to the user's needs, service providers in the IoT domain collect the usage data of IoT devices. However, it is not entirely secure as there is an opportunity for service providers to share such collected information with other organizations, and they might not have adequate security policies that can protect private data. In such a scenario, data privacy concerns arise over IoT devices [80].

In conclusion, privacy is a significant concern in IoT devices. Challenges such as data transmission, weak device configuration, and user data collection and use pose severe threats to the privacy of individuals and organizations. Addressing these

Table 2.2 : Summary of Privacy Threats in IoT with Their Relationship in Different Attributes

Threat	Impact	Attack	Type	Layer of Impact	Solution
Privacy	Confidentiality	MiTM	Eavesdropping	Network	Encryption
			Impersonation	Network	Encryption
			Sniffing	Network	Encryption
			Authorization	Application	Access Control
		Data Privacy	Data Leakage	Multiple	
			Re-identification	Multiple	data suppression, generalization, noise addition
			Data tampering	Multiple	anonymization
			Identity Theft	Multiple	anonymization
		Others	Poodle	Transport	Use TLSv1.2
			Heartbleed	Transport	
			Freak	Transport	Turnoff export cipher suite options in browser

challenges is critical to maintaining trust in IoT systems and ensuring widespread adoption. Table 2.2 summarises privacy threats, which helps understand their importance in different attributes.

2.2.3 Threats to IoT Devices

IoT consists of many heterogeneous sensing devices that communicate with each other over the wired or wireless network. Since manufacturers use low-cost components to configure IoT devices, the threats these devices encounter within IoT networks deviate substantially from those in conventional networks. Additionally, these IoT devices come equipped with fixed memory and processing power. Implementing very high-cost and strict security measures over IoT devices is a challenge. Implementing such measures on IoT devices can significantly impact their performance and often lead to the unavailability of their services. Besides, it is also a challenging task to implement a variety of communication protocols over a vast number of devices [81–83]

Considering the above-discussed points, attackers may have more opportunities to execute various adverse activities over the IoT network. Since the IoT network is a vast paradigm, and having an intermediate entity to verify in the automation systems is always tricky, security challenges over communication may arise regularly. There is another scenario of software and firmware updates in which installing malicious binary files on IoT devices may grant remote access to adversaries, providing complete control to unknown entities in the interconnected system. As a result, an attacker can perform impersonation, Denial of Service (DoS), man-in-the-middle, session hijack, and modification attacks [84–86]. Accordingly, threats based on battery drainage, lack of standardization, computing/storage capabilities, and unavailability of trust are specific to IoT devices. In contrast, IoT network-based threats are shared across the IoT architecture [87, 88].

- *Denial of Service*: This attack is mainly launched to absorb the network and processing capabilities with invalid or modified requests with bogus information, and this results in the weakening of computational and network resources, such as processing power and bandwidth consumption. As a result, legitimate users may not have access to the services, and they become victims of a DoS attack. There is a possibility of another attack scenario in which multiple attackers aim at a specific user to overwhelm its resources by sending counterfeit requests from many devices, and this approach is known as a Distributed DoS attack [89, 90].

- *Impersonation*: In the IoT environment, different types of devices are connected over the network to share meaningful information with others, offering better results. In this, if an attacker is successful in posing as a legitimate entity and gains illegal entry to the IoT ecosystem, then it is known as the execution of an impersonation attack. Adversaries can also pose challenging risks to humans, devices, organizations, and infrastructures. Attackers exploit security deficiencies (such as poor mechanisms for authentication and authorization, outdated software/firmware, or default login credentials) of IoT devices and networks to deceive approaches into considering that they are authorized users. After gaining access, they can execute various malicious activities, i.e., such as disrupting functionalities, modifying the information, penetrating the network, getting private information, or manipulating data over the IoT ecosystem. This allows an attacker to expose IoT devices against authentication, integrity, and confidentiality issues. Consequently, implementing an impersonation attack can lead to devastating impacts on the system. In conclusion, impersonation attacks can cause substantial damage to the interconnected system of IoT devices. To protect the system against an impersonation attack, it is necessary to implement strict security measures with advanced technologies and regularly update the system with the latest firmware. Collective action is needed by end-users, network/system administrators, and manufacturers to make such systems more resilient and safe from impersonation threats [70, 91, 92].

- *Man-in-the-middle*: The quick expansion of IoT devices has changed the lives of humans, but it also involves a variety of cybersecurity risks that can disclose confidential data, such as personal information and private conversations. Adversaries intercept data transmissions (that happen between communicating IoT devices) to understand and extract meaningful information from such packets. Moreover, the extracted information can be used to launch other security attacks to fail authentication and integrity in the IoT ecosystem. An attacker discreetly plays the role of an intermediary to collect sensitive information. Executing this malicious activity is called a man-in-the-middle (MITM) attack. Malicious actors can penetrate IoT networks to get illicit access to personal information while connected devices share data over the network. This attack can reveal confidential information about the system, exceptionallyexceptionally damaging businesses, individuals, and industries. MITM attacks can potentially compromise sensitive data that may lead to untrustworthiness. To avoid the risks of this attack, it is required to enforce adequate security measures in the IoT system by encrypting relevant data while exchanging packets. This can avert the exposure of the information [93–96].

In summary, the unique characteristics of IoT devices, such as their use of low-cost components and fixed memory and processing power, present a unique set of threats. These include software and firmware updates, battery drainage, lack of standardization, computing/storage capabilities, and unavailability of trust. Addressing these threats is crucial to ensuring the security and reliability of IoT systems.

2.3 Websites

The widespread availability and affordability of computing devices have led to a surge in Internet-based services. This increased website traffic, mainly e-commerce and e-banking platforms, has also attracted malicious actors, necessitating robust security mechanisms. However, these mechanisms must be user-friendly to prevent restricting legitimate users from accessing websites or causing them to malfunction. Failure to do so can lead to hostile user experiences [97]. This section discusses the potential security and privacy challenges and threats websites face.

2.3.1 Security Challenges in Websites

This subsection delves into websites' significant security challenges, including Cross-Site Scripting (XSS), Poor Authentication, Data Breaches, and Lack of Security Awareness. Security is a significant requirement for websites, especially as the usage of online platforms for various transactions and services in the private and government sectors has exponentially increased. Security challenges can compromise the integrity of website content and put user data at risk. New web applications consist of various components such as architectures, software, libraries, third-party associations, frameworks, and diverse systems. If not correctly configured, these components can introduce security flaws and vulnerabilities. Therefore, it is essential to regularly update and assess web applications for any new or unknown vulnerabilities. Failure to do so can expose the entire web system to significant risks [98, 99].

- *Cross-Site Scripting (XSS)*: It is a significant vulnerability in web applications that can allow malicious actors to hijack user sessions, modify or steal sensitive and crucial data, or gain control of the whole web system. To perform such malicious activities, attackers prepare malicious scripts that can be executed in the web browser of the user computing machines to compromise their communications and data over the network system. Such attacks can be launched through web links, cookies, or input fields [100, 101].

- *Poor Authentication*: Authenticating users is necessary to access different web content. For this, suitable authentication mechanisms should be designed and implemented effectively to avoid concerns of unauthorized user access. Poor or simple authentication approaches can raise security challenges due to weak password policies or inadequate key management. Besides, implementing inadequate, misconfigurations or expired Transport Layer Security (TLS) protocols can compromise the security of user data that is transferred from a user's browser to the web server and vice versa [102, 103].

- *Data Breaches*: Websites typically store the private data of users, i.e., personal information, conversations, and financial details. The execution of varied cyber attacks (i.e., injection of malware, weak system designs, outdated software, or hacking of websites) can lead to data breaches. Once attackers get an entry, they can steal private details, such as personal information, login credentials, health data, and financial records. Impair security implementations can expose confidential data that may significantly destroy individuals' private details and cause reputational damage to the website owners [104–106].

- *Lack of Security Awareness*: It refers to a scenario where End-users, owners, and technical developers of websites do not have adequate knowledge and comprehension of various cybersecurity risks (that may arise through potential cyber threats) and best practices (to avert from different cybersecurity risks). The lack of such awareness can make websites vulnerable and potential targets for attackers to perform a variety of attacks [107, 108]

When robust security measures are implemented for websites, the risk of data leakage and illegal user access can be reduced. This helps in satisfying user privacy successfully. However, the lack of security practices can raise data privacy issues in which private information can be accessed illegitimately. Security and privacy are eventually interdependent parts in the implementation of a website that can offer its services continuously and effectively. Accordingly, we now discuss potential privacy challenges in websites in the next section.

2.3.2 Privacy Challenges in Websites

This subsection explores the critical privacy challenges in websites, such as Data Collection, Unauthorized Data Sharing, and Third-Party Services. Web applications regularly obtain and store a large amount of personal data (that includes names, birth dates, locations, contact details, and other relevant information), confidential data (e.g., bank details and financial information), and sensitive data (e.g., health records). Ensuring the security of stored data is challenging, as disclosing such data can put the lives of humans at risk. Therefore, a robust mechanism is required to provide adequate encryption, proper data retrieval, and access while preserving security and privacy properties [109, 110].

- *Data Collection*: When End-users access various websites for their requirements, web applications collect browsing preferences, network location, and cookies through advanced technologies, which poses privacy concerns as users may access various accounts from different devices. Ensuring appropriate data collection and computation consent is difficult by implementing data protection policies such as the General Data Protection Regulation (GDPR [111]). Hence, it is essential to implement robust mechanisms for data collection over web applications [112, 113].

- *Unauthorized Data Sharing*: Most web application service providers share user data with third parties without the consent of data owners. In such scenarios, there is a high chance that privacy violations may happen due to misuse of such data rather than the primary intention of data collection, stealing data of users without their knowledge. Further, such activities also direct user profiling by gathering relevant information from various sources that help malicious actors gain individuals' behaviours and preferences. Besides, this may also impact trust between the End-users and unreliable websites [114, 115].

- *Third-Party Services*: Many web platforms are associated with third-party services for different functionalities, and it is an important procedure in the fast-growing technological world. Since third-party services are one of the attackers' targets for disrupting the system operations, exposing any data (exchanging from the main website server to the third-party server and vice versa) can create significant issues for users and websites. Moreover, data may be transferred and processed worldwide for third-party services, and they have different jurisdictions, making it more challenging to provide adequate data protection [116,117].

When security and privacy challenges are not solved properly, they can lead to threats, as these challenges are closely associated with threats. Thus, it is indispensable to understand potential threats to reduce the risks in websites. In the following section, a discussion is given on possible threats to websites.

2.3.3 Threats to Websites

This subsection discusses the most common website threats, including Phishing, SQL Injection, and Social Engineering. Websites are used to access online content and submit information. Since such activities can be done over the web from any place, there is a possibility to execute various security and privacy threats. Some of the critical threats over websites are discussed as follows:

- *Phishing*: It is a threat based on designing and developing a bogus web portal that looks very similar to an original website (of any target organization). The development of such fake websites is to access user accounts by knowing their correct login credentials. Common techniques of Phishing attacks are generally executed by using social engineering approaches (e.g., emails or messages) to motivate users to access such fake websites easily. There are various defensive mechanisms to protect against phishing threats. However, attackers regularly learn and develop new methods for launching attacks. It is vital to protect websites from such threats through regular checks and updates [118, 119].

- *SQL Injection*: Attackers use a malevolent method to exploit potential vulnerabilities in web applications based on SQL databases. In this, an adversary injects malicious instructions into the application's input fields. As a result, the application may execute unintended data queries, gain control over the whole database server, reveal sensitive information, manipulate the content in the database, remove specific data from the database, or bypass authentication [120].
- *Social Engineering*: These threats aim to motivate users by displaying relevant information of interest. As a result, users may access spurious websites due to suggestions from various social media platforms (which provide bogus or incorrect information). Thus, there is the risk of impersonation, modification, data disclosure, access restriction, and manipulation. Since such adverse activities can reveal sensitive information and the trust of users for varied technology-based services, it is difficult to avert such threats over websites. It may compromise websites and users' security [43, 121–123].

In conclusion, the above-discussed security and privacy challenges help us understand the possibility of making IoT devices and websites vulnerable from different perspectives. Nevertheless, the continuous emergence of offensive and defensive strategies presents potential risks to IoT devices and websites while offering solutions to myriad security and privacy challenges. Consequently, the subsequent section delves into recent advancements in these areas.

2.4 Related Works

While we have previously explored the concept and associated security and privacy issues of End-user devices, which comprise various devices, the primary research focus of this thesis is specifically on IoT devices and Websites. Therefore, moving forward, our discussions will be exclusively centered around IoT devices and Websites, excluding other types of End-user systems.

A discussion on the current status of the existing work is an essential aspect of the thesis as it describes the basis for the research, supports understanding of the existing and proposed research design and techniques, and helps researchers to obtain background knowledge in the specific domain.

2.4.1 IoT Devices

Sharmeen et al. [124] proposed an ML mechanism that could be trained through static, dynamic, and hybrid features to detect malicious programs in industrial IoT networks while using application program interfaces. There are various techniques, such as Support Vector Machine (SVM), Random Forest (RF), k-Nearest Neighbors (kNN), and Naive Bayes (NB), that could be applied in identifying malware. However, the hybrid approach is more effective in intrusion detection. Existing attacks are relatively easy to launch at a significant level as the structure of IoT architecture is dynamic regarding hardware and software due to varied IoT components and limited resource availability. Moreover, complex attacks (e.g., remotely through a wireless channel) can be successful over IoT devices and systems. Thus, it is suggested in [87] to implement another research design (i.e., continuously learning from the current scenario, integrating new methods automatically, and defending against different types of attacks) to secure IoT systems efficiently. In this work, various ML and Software Defined Networking (SDN) approaches are analyzed to realize their features and limitations for an IoT network, and they discussed a variety of IoT security and privacy challenges over such approaches.

In 2019, Da et al. [125] prepared a survey on ML-based Intrusion Detection System (IDS) mechanisms for IoT systems/devices as there was no or very limited literature that discusses applications of ML in the area of IoT to detect up-to-date abnormalities. Furthermore, they provided a study on the most commonly applied IDS approaches and used datasets for IoT security experiments. However, this work [125] mainly covers IDS solutions proposed before 2019. Thereby, it may not provide the latest IoT security or privacy threats.

During the same year, another survey work [126] was prepared by considering IoT network IDS using ML as such learning-based methods have significant positive consequences in addressing security and privacy challenges. This survey discusses a detailed review and comparison of various NIDSs deployed/proposed by involving different ML techniques to detect threats and identify challenges in IoT systems/devices. Furthermore, Chaabouni et al. [126] analyzed these ML-based NIDS mechanisms to understand the performance and noticed that such approaches are proposed to protect IoT systems from specific types of threats (common attacks and identified/considered from some generalized security attack datasets). Therefore, it is required to consider real-world security and privacy datasets (to understand the performance of various NIDSs in IoT effectively) that are focused on IoT systems and devices, and such datasets can be used to benchmark results for the purpose of training, evaluation, and verification for ML-based approaches.

Solutions developed using ML and Deep Learning (DL) techniques can be leveraged to offer intelligence operations in IoT systems and devices to tackle a variety of security and privacy concerns. In [83], a survey is prepared by focusing on the applications of ML to provide different solutions for complex security and privacy challenges in IoT systems/devices. Further, a systematic evaluation is done for the already proposed relevant security solutions and discussed potential research directions using ML and DL to address security issues in the IoT network. This survey article analyzes various attack paths and security requirements while reviewing current solutions for IoT security problems. However, the efforts on security and privacy issues are limited to discussing attacks and including ML and DL approaches.

In 2020, Mohanta et al. [30] presented a survey to identify various security and privacy issues in IoT applications and analyze the possibility of new solutions to address such challenges (in IoT devices and systems) by exploring advanced technologies. In this work, the IoT architecture is explained to understand the background of it. After that, security challenges are identified by focusing on each layer of the IoT architecture, providing a better explanation of such problems. Besides, a detailed survey on ML, Blockchain, and Artificial Intelligence (AI) technologies is elucidated to clarify how such technologies can be useful in addressing security and privacy challenges in IoT systems/devices. Federated Learning (FL) emerges as a significant addition to the discourse on ML in IoT. FL enables distributed model training across numerous devices while keeping the training data localized, thereby enhancing data privacy. This approach is instrumental in addressing the security and privacy challenges identified earlier, making it a fitting complement to the technologies discussed by Mohanta et al. [30]. It is within this context that we introduce our proposed FedBlockHealth framework, which integrates FL with Blockchain to fortify privacy and security in IoT health applications. Detailed discussions of FedBlockHealth's implementation, its approach to addressing IoT's unique security and privacy challenges, and its practical applications within the healthcare domain are expounded upon in Chapter 4.

ML techniques yield more effective outcomes in IoT applications and services. Meanwhile, Blockchain methods offer significant advantages in tackling security and privacy challenges, primarily because executed transactions in Blockchain systems are nearly immutable. Therefore, Blockchain and ML are essential technologies that can be useful in solving various security and privacy challenges in IoT systems and devices. Since existing studies on these technologies are focused either on ML or Blockchain while considering mainly security concerns. As a part of this thesis, we provided an extensive research study on recent security and privacy threats [127]. Furthermore, a survey is given by analyzing existing ML and Blockchain-based solutions (that are proposed to solve security and privacy problems in IoT). Since ML and Blockchain methods are not fully leveraged to overcome various security and privacy issues, potential challenges are identified in implementing such technologies in the IoT domain, and directions to address such challenges are also discussed for better development of IoT systems.

IoT devices and systems have limited resources in various aspects and are configured with less or no security policies. However, such components are widely used in many applications in our daily life. Therefore, it is required to analyze security challenges in detail while integrating new technologies in the IoT architecture for more effective consequences. In [128], investigations are done to understand potential challenges and suggest low-cost solutions to solve hardware security problems while integrating emerging technologies in this domain. A review is prepared for IoT security threats by focusing on software, hardware, and communication aspects. A device and network protection discussion is also presented to avoid the risk of different attacks.

ML and DL technologies offer effective results in various IoT applications and services. However, such technologies can also be applied in different adversarial activities, creating security and privacy challenges while offering beneficial use cases in IoT systems. Blockchain technology can be leveraged to solve security concerns but may expose the collected information, leading to data leakage challenges. Therefore, it is essential to understand in detail and explicitly how developing such technologies can be more meaningful in avoiding security and privacy risks. Wu et al. [129] discussed and analyzed various ML and Blockchain applications by concentrating on consensus mechanisms, communication, and storage. Further, security and privacy risks are investigated over these three components while considering Blockchain and ML. This is useful to researchers in understanding potential challenges that can be viewed in designing security solutions for IoT. Moreover, open problems are discussed in this domain that should be solved while developing solutions for IoT systems.

ML-based solutions facilitate improving the results in multiple IoT applications and services, but privacy concerns may arise due to information leakage. Federated Learning (FL) is an ML technique that helps satisfy privacy and trains an algorithm in a distributed manner. Due to advancements in varied technologies, attackers can also perform malicious activities on FL algorithms. Unal et al. [130] suggested to use Blockchain technology to protect FL algorithms (while integrating with IoT systems and devices) from different integrity attacks. Then, a Blockchain-based integration approach is presented for FL to mitigate privacy problems and protect data analytics services from security attacks. Using fuzzy hashing to identify abnormalities and deviations in FL-trained models, a detection mechanism is also proposed.

ML and DL algorithms are extensively applied in different IoT systems to collect relevant data from the surrounding environment and intelligently make real-time decisions without involving humans continuously. Since computing and storage facilities have significantly relied on the centralized system in IoT applications and services, such arrangements can increase security and privacy risks as well as scalability in the growing number of IoT components. FL can support reducing privacy risks specifically. However, there are still various challenges (i.e., single point of failure, information leakage, distributed denial of service attacks, and scalability) that may help attackers to perform malicious activities without detection. The combination of FL and Blockchain can be leveraged to address such concerns. A survey on

Blockchain-based FL approaches is recently presented in [131] to comprehensively protect IoT systems. This study discusses the current research status on Blockchain, its applications and literature in FL methods, Blockchain and FL integration problems in IoT, present security challenges in the IoT domain, and possible solutions to mitigate such security and privacy issues using advanced technologies.

The number of IoT components is exponentially increasing in varied smart applications and services for our daily needs, offering more comfort and improving the quality of life of users. Thus, the usage of IoT devices in various applications and services has been raised. It is correspondingly necessary to identify and explore security, privacy, operational, and system challenges from different perspectives. Accordingly, recent studies [30, 83, 87, 124–126, 128–131] are analyzed in this domain, and the summary of these surveys is given in Table 2.3 by considering their scope in each survey work.

Table 2.3 : Summary of Relevant ML and Blockchain-based Studies and Their Key Contributions in IoT

Survey Study	**Applications of IoT**	**IoT Security and Privacy**	**Applications of ML**	**ML Security and Privacy**	**Applications of Blockchain**	**Blockchain Security and Privacy**	**Blockchain and ML-based Solutions**
[30]	✓	◐	×	◐	×	◐	✓
[83]	✓	◑	✓	×	×	×	✓
[87]	✓	◐	✓	◐	✓	◐	✓
[124]	✓	◐	✓	×	×	×	✓
[125]	✓	◐	✓	×	×	×	✓
[126]	✓	✓	✓	◐	×	×	✓
[128]	✓	◐	✓	◐	✓	◐	×
[129]	✓	◐	✓	◐	✓	◐	×
[130]	✓	×	✓	✓	✓	✓	✓
[131]	✓	✓	✓	✓	✓	×	✓

✓: Discussed on the specific area in that research study; ×: Not included the specific area in that research study;

◐: Only discussed about security; ◑: Only discussed about privacy;

IoT devices are constrained by the inherent limitations of processing power, memory, storage, energy capacity, and size. Designing robust, cost-effective security solutions for these limited resources is a complex endeavor. Overcoming these challenges necessitates moving beyond conventional methodologies and investigating cutting-edge technologies. Machine Learning (ML) and Blockchain are instrumental in transforming various IoT-based systems, addressing diverse security and privacy concerns in our rapidly progressing digital landscape. Nevertheless, these advancements fortify the system and network architectures but also introduce numerous potential vulnerabilities. Hence, identifying and scrutinizing various security and privacy risks, which could undermine IoT systems and devices through different attack vectors, is paramount. Our previous study, [127], establishes a crucial groundwork for this thesis. It provides a comprehensive survey of existing literature, identifies contemporary security and privacy threats facing IoT as detailed in Section 2.2, and discusses how Blockchain and ML technologies could potentially counteract these threats, as further explored in Section 3.1.

In addition, we delve into the challenges that arise when integrating ML and Blockchain technologies to address threats to IoT systems and devices. This examination, presented in [132], aims to inform and guide researchers in their quest to design and develop practical solutions. The details of this investigation will be discussed in Chapter 4. Given the limitations of IoT devices in implementing comprehensive security measures, the burgeoning proliferation of such devices warrants heightened attention toward user and system security and privacy. Without this focus, the advantages offered by IoT could inadvertently result in detrimental personal and financial repercussions. It is, therefore, crucial to enforce strategies based on differential privacy to protect against security and privacy threats adequately, a subject we further elaborate on in [133] and detail in Chapter 3.

IoT devices and websites are interdependent as websites can be considered as the central hub to manage the IoT architecture, and IoT devices can execute different tasks from a remote place. In conclusion, the combination of both can create an interconnected ecosystem that can offer better user experiences and mutual benefits. Therefore, it is also important to understand the latest work on security and privacy challenges in websites.

2.4.2 Websites

Web-based application and service developers should explicitly declare all required permissions regarding data privacy that are needed to execute different tasks. However, only some websites reveal such policies openly and clearly. Besides, they may collect the personal data of users while accessing websites. Such activities can reveal Personally Identifiable Information (PII) through advertisements, recommendation algorithms, and third-party scripts [134–136], infringing the data privacy regulations [137]. Users' data can likewise be disclosed unintentionally while using web-based chatbots, which may raise security and privacy risks [138].

Online services are primarily enabled with chatbot facilities to have conversations between the software system and users automatically, which helps in addressing different types of user queries quickly. Chatbots are nowadays used in e-commerce, banking and financial services, education, healthcare, travel, entertainment, and other similar services. However, there are different security and privacy challenges (i.e., data modification, user impersonation, information availability, legitimate user/data access, data privacy, replaying transactions, and disclosure of information) that are needed to consider thoroughly while using web-based services in crucial applications and services. Bhuiyan et al. [139] proposed a Blockchain-empowered chatbot that can be useful in financial assistance to overcome potential security issues in such chatbots. This mechanism can be used with one banking organization effectively. However, privacy concerns may arise when such systems are integrated with multiple banking institutions.

Health data is sensitive and crucial. Thus, it is most important to preserve the privacy of patient data while using chatbot services for conversations. Otherwise, the consequences may significantly harm users regarding health and finance. Biswas et al. [140] proposed two mechanisms for chatbots. The first technique performs filtering and transformation of entities by considering user privacy. The second method is focused on the Searchable Encryption (SE) concept to satisfy user privacy in chatbot conversations, and an understanding of the chatbot design is optional in this technique. In the first approach, knowing the chatbot design on the user side is necessary for effective results. However, such requirements may disclose the design structure and system architecture, which might allow attackers to explore possible vulnerabilities in the system.

Advanced chatbots rely on state machines to perform various tasks, such as collecting information, identifying appropriate answer for the query, providing the result to a specific user, and learning based on conversations (which may help in improving services for future queries). However, there is a possibility for privacy management concerns due to multimodal dialogues. To deal with such issues, an agent-based framework in [141] facilitates configuring and deploying personalized chatbots in multimodel environments. In this framework, users are authorized to store and share their data, allowing them to remove data from their memory.

Chatbots learn from the dataset (that includes the shared data) to answer the query requested by the user. Since training DL models with the dataset can infringe on user privacy, privacy concerns may arise in chatbots. Various works in this domain address user privacy by implementing secure multi-party computation and differential privacy. However, such approaches require access to user data, thereby knowing private data. FL can help protect user data privacy through distributed learning techniques. Ait et al. [142] presented a chatbot using FL to preserve data privacy while offering customer support at a large scale level. While integrating such a method with real-world datasets, the effectiveness is still needed to measure for efficient outcomes.

Table 2.4 : Overview of Recent Surveys on Web-based Chatbots

Study	**Applications**	**Security**	**Privacy**	**Evaluation**
[138]	Chatbots	×	✓	Privacy concerns
[139]	Chatbots	✓	✓	Security concerns
[140]	Chatbots	×	✓	No
[141]	Chatbots	×	✓	Privacy concerns
[142]	Chatbots	×	✓	Privacy concerns

✓**:** Topic discussed in the respective research study.

×**:** Topic not covered in the study.

Web-based chatbot services are widely used in multiple applications. Recent surveys [138–142] are explored to understand the status of privacy challenges in chatbots, and its overview is presented in Table 2.4 by focusing on the scope of their studies. However, adequate attention to security and privacy evaluations has not been given to chatbots, which help attackers to collect users' data through cookies and third-party vulnerabilities. Moreover, it is yet required to evaluate the security and privacy risks in detail for Web-based chatbot services. Therefore, we present an empirical analysis of web-based chatbots among the top 1 million Alexa-ranking websites. A detailed examination of the security and privacy risks of Web-based chatbots is discussed more in Chapter 5.

2.5 Summary

This chapter presented an overview of End-user devices, IoT devices, and websites to get background knowledge. After that, various security and privacy issues are analyzed that can intercept/interrupt the functionalities and operations of such devices and technologies. Furthermore, various threats are discussed to know how to create potential issues in these architectures. Finally, related work is discussed that helps understand the current status of challenges and solutions to address them.

Chapter 3

Machine Learning and Blockchain based Countermeasures for IoT Threats

After discussing security and privacy challenges in End-user systems (focused on IoT and websites) in Chapter 2, Section 3.1 of this chapter is to investigate Machine Learning (ML) and Blockchain technologies to address security and privacy challenges in IoT. Section 3.2 discusses privacy-preserving framework for smart home-based IoT applications. A taxonomy of ML and Blockchain technologies solutions is presented that can be applied to protect from the latest security and privacy threats. The research gaps in the current ML and Blockchain-based approaches are identified and described those are useful in strengthening security and privacy in the IoT environment. Based on this systematic research analysis, it is identified that a convergence of these two technologies is more meaningful in protecting IoT devices and systems from sophisticated security and privacy attacks. This research work [127] has been published as a part of a review paper in *ACM Computing Surveys journal*. This is the first work that presents a review of security and privacy exposures in the IoT environment, a convergence of ML and Blockchain technologies, security and privacy challenges in integrating both technologies over IoT systems, and their potential countermeasures to address such challenges. This contribution is extensively described in Section 3.1.

Besides, a privacy-preserving secure framework has been proposed that can be applied to real-time IoT applications in a smart home environment to preserve data privacy through Local Differential Privacy (LDP) and randomized response approaches. Furthermore, the Hidden Markov Model (HMM) method aggregates the received data from deployed IoT devices in a home. This proposed framework [133] has been presented and published in the proceedings of the *IEEE COINS 2023*. A detailed explanation of this privacy-preserving secure framework contribution is given in Section 3.2.

3.1 Mitigating IoT Threats

The first computer worm is *Creeper* which was written in 1971 for adversarial experiments [143]. From that time, there are many incidents of attack scenarios in the IoT environment [144–147]. Many solutions have been proposed to address various security and privacy challenges that have significant impacts on IoT devices and systems. Since the IoT architecture is different in characteristics rather than other Information Technology (IT) systems, it is necessary to address varied challenges exclusively. ML and Blockchain technologies offer productive results in solving various security and privacy issues in IoT. Accordingly, these two technologies are widely involved in recent secure and privacy-preserving solutions for the IoT domain [30, 127, 129, 130, 148]. Therefore, a discussion on ML and Blockchain solutions is presented in Section 3.1.1 and Section 3.1.2, respectively.

3.1.1 ML Algorithms and Application to Mitigate IoT Threats

ML is used as a data analysis and decision-making technique. For example, data traffic entering a network can be analyzed through an ML model to make an informed decision. Since adversaries also learn new technologies regularly to develop advanced attacking approaches that can be implemented over the system/network [149, 150], it is more important to understand different attack vectors. In this, attackers may target the specific stage (i.e., input, processing, or output) to perform destructive activities. Figure 3.1 displays the main components of the ML threat model and gives an overview of target stages. Here, adversaries may launch data modification, poisoning, or injection attacks that directly affect the consequences [151]. Therefore, it is required to have a secure extensively to protect from a variety of attacks.

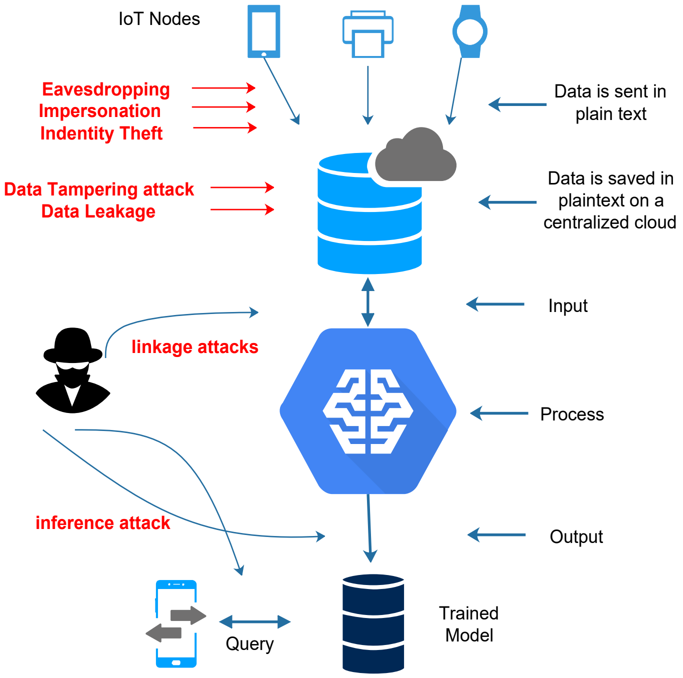


Figure 3.1 : An illustration of the ML threat model for IoT at different stages: (i) *input*, (ii) *process*, or (iii) *output*.

3.1.1.1 Security efforts using Machine Learning

Several security solutions have been proposed using ML algorithms as a tool, as shown in Table 3.1. To deal with the flooding attacks, Diro et al. [152] argued that fog-computing reduced the risk of eavesdropping and Man-in-The-Middle (MiTM) attacks by restricting the communication to the proximity of IoT devices. Capitalizing on this idea, they used the Long Short Term Memory (LSTM) algorithm in their model as it can remember the older data. For binary classification, they compared their results with logistic regression using ISCX2012 dataset, which had 440,991 normal traffic instances and 71,617 DoS attack instances. The Deep Learning (DL) model LSTM took considerably more time to train than LR, but its accuracy was

9% better. The second dataset used was AWID from [153], and consists of normal traffic instances (1,633,190 training and 530,785 tests), injection attack instances (65,379 training and 16,682 tests), flooding attack instances (94848 training and 8097 testings) and impersonation attack instances (48,522 training and 20,079 testings). After comparing LSTM against softmax for multi-class classification, the resultant accuracy obtained was 14% improved.

In a similar study, Abeshu and Chilamkurti highlighted that the resource constraints of an IoT device made it a potential threat to DoS attacks [154]. Classic ML algorithms are less accurate and less scalable for cyber-attack detection in a massively distributed network such as IoT. Such a massive amount of data produced by billions of IoT devices enable the DL models to learn better than the shallow algorithms. The authors in [154] argued that most of the employed DL architectures had used pre-training for feature extraction, which could detect anomalies and thus reduced the workload of a network administrator. However, their work was focused on distributed DL through parameters and model exchange for the applications of fog computing. Fog computing reduced the load of computing power and storage space from the IoT devices. It is, therefore, the ideal spot where an intrusion can be detected. The existing Stochastic Gradient Descent (SGD) for fog-to-things computing needs parallel computing. Thus, the centralized SGD will choke due to the massive amount of data in IoT. Therefore the study proposed a distributed DL-driven Intrusion Detection Systems (IDS) using NSL-KDD dataset, where the stacked auto-encoder (SAE) was used for feature extraction, and soft-max regression (SMR) was used for the classification. Their study proved that the SAE as a DL worked better than traditional shallow models in terms of accuracy (99.27%), FAR and DR. Both Diro et al. [152] and Abeshu et al. [154] proved that the DL algorithms performed better than shallow ML models.

As a first attempt to DoS detection, Tan et al. [155] used triangle-area-based

Table 3.1 : Existing IoT security solutions using Machine Learning algorithms.

*Notations used- I: ISCX2012, A: AWID, N: NSL-KDD, K: KDDCUP99, U: UNSW-NB15, NB: NIMS botnet, P: Private, AWI: Aegan WiFi Intrusion, Ab: AbdroZoo, D: Drebin, C: CTU-13, Ky: Kyoto 2006+

Ref.	Threat	Type of Threat	IoT Use case	Algo used	Feature Extraction	Feature Selection	Dataset	Accuracy
Diro et al. [152]	DoS	Flooding	Fog	LSTM	-	-	I, A	I (99.91), A (98.22)
Abeshu et al. [154]	DoS	Flooding	Fog	Softmax	SAE	-	N	99.2
Tan et al. [155]	DoS	Flooding	NIDS	TAB	MCA	Norm.	K	normalized 99.95
Tan et al. [156]	DoS	Flooding	CV	EMD	MCA	PCA	K, I	K (99.95), I(90.12)
Moustafa et al. [157]	Botnet	Flooding	IoT	Adaboost	CC	-	U, NB	U(99.54)
Ahmad et al. [158]	MiTM	Impersonation	Healthcare	LSTM RNN	NG	-	P	-
Aminanto et al. [159]	MiTM	Impersonation	WiFi	ANN	D-FES	-	AWI	99.92
Chatterjee et al. [160]	MiTM	Impersonation	RF Comm	ANN	-	-	P	99.9
Azmoodeh et al. [161]	Malware	Code Ijnection	IoBT	DCN	OpCodes	IG	P	98.37
Aonzo et al. [162]	Malware	Malware	Android	-	Static Analysis Technique	Manual	P	98.9
Wei et al. [163]	Malware	Malware	Android	NB, C4.5, kNN	Dynamic Analysis technique	NA	P	-
Feng et al. [164]	Malware	Malware	Android	ensemble + LR	Manual	Chi-Square	Ab, D	98.18
Wang et al. [165]	Malware	Malware	Android	ensemble	String + structural	ensemble	Multi-sources	98.4
Maimo et al. [166]	Anomaly	Anamoly	5G	LSTM	Weighted Loss	ASD (DBN+SAE)	C	-
Niyaz et al. [167]	Anomaly	Anamoly	NIDS	Softmax	SAE using Backpropogation	-	Ky	2- 88.39, 5- 79.10
Ambusaidi et al. [168]	Anomaly	Anomaly	NIDS	LSSVM	MMIFS	FMIS	K, N, Ky	K 99.95,I 90.12
Zhou et al. [169]	Dataset	Multiple	IoT	DFEL	-	-	N, U	>98.5
Prabavathy et al. [170]	Dataset	Multiple	Fog	OS-ELM	-	-	N	97.36

technique to speed up the feature extraction in Multivariate Correlation Analysis (MCA). Features were generated to reduce the overhead, using the data that entered the destination network. Along with this, the "triangle area map" module was applied to extract the geometrical correlations from a pair of two distinct features to increase the accuracy of zero-day attack detection. In an attempt to improve their results from [155], Tan et al. [156] used Earth Mover's Distance (EMD) to find the dissimilarities between observed traffic and a pre-built normal profile. The network traffic was interpreted into images by feature extraction using MCA and analyzed to detect anomalies using KDDCup99 and ISCX datasets. Using the sample-wise correlation, the accuracy of their results obtained was 99.95% (KDD) and 90.12% (ISCX). However, the study neither revealed the data size nor the effects of varying sample sizes. Moreover, MCA assumed the change to be linear, which was not a realistic approach. Another form of DoS attack in IoT is called a botnet attack. To prevent botnet attacks against HTTP, MQTT (Message Queuing Telemetry Transport), and DNS, the authors of [157] developed an IDS, which is an ensemble of Decision Tree (DT), NB, and Artificial Neural Network (ANN). Since the correntropy values of benign and malicious vectors were too close, it was decided to use DT, NB, and ANN as they could classify such vectors efficiently. The performance metrics were detection-rate and false-positive rate, for which their proposed ensemble was better than every individual algorithm in that ensemble. For the datasets of UNSW and NIMS, the accuracies achieved were 99.54% and 98.29%, respectively.

Similar to DoS attacks, the MiTM attacks are one of the most frequently occurring attacks in an IoT network. In regard to this, a lot of technical solutions have been proposed for several applications. The authors [158] have used LSTM RNN to prevent the impersonation attacks in a smart healthcare scenario, since traditional feedforward neural networks cannot capture the sequence and time-series data, due to their causal property. Moreover, the researchers solved the vanishing gradient issue of RNN algorithm and improved accuracy. At first, the predicted value was calculated based on the dataset log of three months (for a patient who is taking insulin injections). If the predicted and calculated values differed for more than a certain threshold, then by using the combination of DL and gesture recognition, the correct dosage was ensured. However, model details and analysis procedure were missing in their work.

Similarly in another scenario to prevent the impersonation attacks, the authors of [160] utilized Physical Unclonable Function (PUF), which is an inherent characteristic of silicon chips that is unique and can be used as a basis of authentication in RF communication. During the manufacturing phase, every transmitter inherits some unique features called *offset* from an ideal value. The authors have used these offsets as their features to recognize the device, train their system on it, and then detect the accuracy. Using ANN MATLAB toolbox, the performance metrics were calculated. With the help of ML, the simulation results could detect 4,800 nodes transmitters with an accuracy of 99.9% and 10,000 nodes under varying channel conditions, with an accuracy of 99%. The proposed scheme can be used as a standalone security feature, or as a part of traditional multi-factor authentication. PUF is inherent and inexpensive and can significantly benefit IoT, wherein each wireless sensor's physical values can be stored in a secure server replacing traditional key-based authentication. However, the authors in their approach have assumed the server storing the PUF values is safe. Aminanto et al. used an unsupervised ensemble of ML algorithms using SVM, ANN, and C4.5 for feature extraction and ANN as the classifier [159]. In their process of deep-feature extraction and selection (D-FES), first, they used SAE to extract the features, then SVM, ANN, and C4.5 were used for feature selection, and finally, ANN was used to classify. The study achieved an accuracy of 99.92% by using AWID dataset, on which an earlier study by Kolias et al. [153] had the worst accuracy for impersonation attack.

According to *Statista* [171], mobile phone users would reach close to three billion by 2020. This increase in usage made mobile phones vulnerable to the malware attack [161–165,172]. Azmoodeh et al. [161] believed that OpCodes could be used to differentiate benign-ware and malware. Class-wise Information Gain (CIG) is used for feature selection because the global feature selection causes imperfections, and even reduces system efficiency especially when the dataset is imbalanced. They also claimed that this combination of OpCode and DL for IoT had never been explored. Using Eigenspace and deep convolutional networks algorithms, 99.68% accuracy was achieved, with precision and recall rates of 98.59% and 98.37%, respectively. Similarly, to mitigate malware, Wei et al. [163] extracted the features using the dynamic analysis technique. They used application functional classification to train the classifier for clean and malicious data, while, in the testing phase, kNN was used to divide data into known categories. J48 decision tree and NB were used to perform 10-fold cross-validation. Depending on the performance metric, the study claimed 90% accuracy.

Contrary to dynamic analysis [163], the authors of [162] used static analysis techniques for feature extraction considering all the Application Platform Interfaces (API) that were not studied previously. Feature selection was made manually based on the most-used features by the previous researchers. They claimed the accuracy of 98.9% with the second biggest malware testbed dataset ever used. As the intrusion techniques were getting sophisticated, the static analysis became invalid, and it was therefore required to use a dynamic scheme [164]. With the static analysis techniques, the attackers adopted deformation technologies, which could bypass the detection while dynamic analysis methods were promising due to its resistance to code transformation techniques. The authors of [164] proposed a new framework, called EnDroid, based on these issues. The proposed model used "Chi-Square" for feature extraction, five different algorithms (decision tree, linear SVM, extremely randomized trees, random forest & boosted trees) as an ensemble for base-classification, while LR was used as meta-classifier. For the dataset, a combination of “AbdroZoo” and “Drebin” datasets was utilized so that an accuracy of 98.2% was achieved. Wang et al. argued that most of the existing literature on malware detection was based on static string features, such as permissions and API usage extracted from the apps [165]. However, since malware had become sophisticated, using a single type of static feature might result in a false-negative. In their proposed model - DriodEnsemble, a fusion of string and structural features was utilized to detect Android malware. Using an ensemble of SVM, kNN, and RF, the model was evaluated against 1,386 benign apps and 1,296 malapps. The study proved to have attained an accuracy of 98.4%, which was better than detection accuracy (95.8%) using only string features, while the accuracy obtained with only structural features was 90.68%.

Anomaly detection is a generic technique where any irregular traffic is flagged as a threat. Several studies [166–168] have attempted to provide secure IDS using ML algorithms. In this regard, an unsupervised DL technique called STL was used by Niyaz et al. [167], and it was based on SAE and SMR. By using NSL-KDD dataset, the comparison was made using 2-class, 5-class, and 23-class classification, and proved 2-class classification to be better than SMR. A multi-class ML-based classification using Mutual Information (MI) was proposed by Ambusaidi et al. [168]. For the linearly dependent variable, Mutual Information Feature Selection (MIFS) with Linear Correlation Coefficient (LLC) was used. For the non-linear dependent variable, the authors used FMIS+MI, made changes to the already existing MIFS algorithm [173] and showed their novelty. For the Linear model (Flexible Linear Correlation Coefficient based Feature Selection [FLCFS]), the study modified the existing LLC [173] and proposed a new model. An MI can cope with linear as well as non-linear dependents. However, its algorithm can cause redundancy to the classification. Ambusaidi et al. [168] chose *estimator*, which relied on estimating the entropies of the given data using average densities from each datum to its k-nearest neighbors. Another reason for this study was that the previous studies had not provided any steps as to how they chose β. The performance was compared using three different datasets of KDDCUP99, NSL-KDD, and Kyoto 2006+, while the metric performance indicators were Accuracy, DR, FPR, and F-measure. Maimo et al. [166] focused on 5G application for anomaly detection based on LSTM. Features extraction was made from network flows using weighted loss function, while feature reduction was made by using DBN and SAE models because of similar structure (where the prediction can be computed using matrix operations followed by the activation function) [166]. After implementing their model using CTU-13 botnet dataset, the authors claimed to have obtained a precision of up to 0.95.

Several studies using ML algorithms as a tool have claimed to reduce cyber-attacks effectively. However, Zhou et al. [169] based their proposal *Deep Feature Embedding Learning* (DFEL) on DL because traditional ML algorithms took extra time to train data. The comparison of their proposal using the datasets of NSL-KDD and UNSW-NB15 confirmed the improvement in recall level of gaussian Naive Bayes (NB) classifier from 80.74% to 98.79%, apart from the running time of SVM significantly reduced from 67.26 seconds to 6.3 seconds. In another similar study [170], the authors claimed that the existing ML algorithms were inefficient for IoT applications and therefore a much faster Extreme-Learning-Machine (ELM) could be used instead [170]. Furthermore, they found that the existing security approaches for IoT were centralized and cloud-based, and they, in turn, inherited latency and high power consumption. The proposed IDS for IoT used fog computing for implementation in a distributed fashion in two steps. In the first step, attack detection at fog nodes used an online sequential extreme learning machine (OS-ELM) to identify the attacks in the incoming traffic from the IoT virtual clusters. In the second step, these detected threats were summarized and analyzed at a cloud server. The results of the new algorithm showed better Accuracy, False Positive Rate (FPR), and True Positive Rate (TPR) after comparison with the existing NB, ANN, and standard ELM. Furthermore, the experimental results using the Azure cloud also confirmed that the fog-computing-based attack detection was faster than the cloud-computing based attack detection. However, the study did not compare the results with any existing ML/DL based algorithm used for fog-computing.

3.1.1.2 Privacy efforts using Machine Learning

Several privacy-preserving ML algorithms have been proposed, as shown in Table 3.2. Similar to security, privacy is also compromised by a MiTM attack. In this regard, several studies have used ML algorithms to counter different types of MiTM attacks. For example, the study by Xiao et al. [174] used game theory–a kind of reinforcement learning, which compared the channel states of the data packets to detect spoofing attacks. The authentication process was formulated as a zero-sum authentication game consisting of the spoofers and the receivers. The threshold was determined by using Nash Equilibrium (NE), implemented over Universal Software Radio Peripherals (USPRs), and the performance was then verified via field tests in typical indoor environments.

As an improvement to their work, Xiao et al. [175] applied logistic regression to evaluate the channel model information collected from multiple access points to detect spoofing more accurately. A comparison was made using distributed Frank-Wolfe (dFW)-based and incremental aggregated gradient (IAG)-based authentication to reduce overall communication overhead. IAG-based PHY-layer authentication reduced communication overhead and increased detection accuracy. In addition to authentication issues, Aksu et al. [176] raised an argument concerning the wearable device, for which the previous schemes only focused on user authentication.

However, the device being used should also be authenticated. Such devices could act as MiTMs, which might have similar user authentication details. However, in the background, it might leak all the information to the attacker. Wearables could only connect to the more powerful base device via Bluetooth with authentication and encryption. Since the device name and encryption keys could be compromised easily, it was therefore much secure to use hardware-based fingerprinting [176]. The proposed framework in [176] utilized an inter-packet timing-based timing analysis method based on the Bluetooth classic protocol packets. There were four steps in this framework. Initially, Bluetooth classic packets were captured. This was followed by feature extraction. In the subsequent phase, fingerprints were generated using probability distributions. Finally, these stored fingerprints were matched against incoming data from wearable devices to identify any unfamiliar devices. By selecting the best algorithm out of twenty from the training results, the study claimed to achieve an accuracy of 98.5%.

Data plays a crucial role in training an ML model. For example, we can use patients' historical data to make a predictive decision for any new patient. However, patients are reluctant to share their data due to obvious privacy concerns. The studies, as shown in [177–179], have worked towards solving these issues. In [177], the researchers proposed a new framework called eDiag, which used non-linear kernel SVM to successfully classify medical information, while preserving user data and service provider's model privacy. Previous studies had used Homomorphic Encryption (HE) techniques, which, according to the study, were not appropriate for online medical prediagnosis. Using their framework, Zhu et al. [177] claimed to have achieved a classification accuracy of 94% without compromising privacy. Similarly, the authors in [178] classified the privacy issues as *learning-privacy problem* and *model-privacy problem* to protect users' sensitive information and model results, respectively.

Jia et al. [178] argued that the previous work used either gradient-values instead of real-data, or they assumed that the learning model was private, but the learned model was publicly known, or they used complicated encryption procedures. In comparison to all of these studies, Jia et al. [178] proposed a uniform Oblivious Evaluation of Multivariate Polynomial (OMPE) model, which did not contain complicated encryption procedures. Their results proved that the classification data and learned models were protected from several privacy attacks. The research in [178] focused on model-privacy issues. However, the learning-privacy problem was not discussed. This issue was solved by Ma et al. [179], who argued that encrypting any user-data by the public key was a widely used privacy-preserving technique but at the cost of key management. To preserve the data privacy, Ma et al. [179] proposed a cloud-based DL model that worked with multiple keys to attaining privacy of the user data called Privacy-preserving DL Multiple-keys (PDLM). In their proposed model, a service provider (SP) sent encrypted user data to the cloud which performs training of the data without knowing the real data. Their evaluation of the PDLM showed that PDLM had successfully preserved privacy with lower efficiency as compared to the conventional non-private schemes.

To improve ML algorithms privacy, Sun et al. [180] proposed an improved version of fully HE that reduced the size and noise of the multiplicative cyphertext by using the re-linearization technique. In their scheme, private hyperplane decision-based classification, private NB classification, and private decision tree's comparison were also implemented. In a similar paper, the same authors successfully reduced the user-server iterations to half, without compromising privacy.

Social media platforms like Twitter and Facebook have enriched people's lives at the cost of privacy issues. Several companies used blacklisting techniques to filter benign traffic. However, a survey showed that 90% of the people would fall prey to these attacks before they were blacklisted. To prevent these attacks efficiently, ML algorithms were used. However, these algorithms were inefficient in real-time due to their slower learning rate. In a study, Feng et al. [181] proposed a multistage detection framework using DL, where an initial detection occurred at a mobile terminal whose results were then forwarded to the cloud server for further calculation. By using Convolutional Neural Network (CNN) as a classification algorithm, the authors claimed to achieve approximately 91% utilizing the Sino Weibo dataset. Similarly, the lack of privacy protection mechanisms in a Vehicular Ad hoc Network (VANET) environment was raised by Zhang et al. [182]. In VANET, Vehicle nodes tend to learn collaboratively, raising privacy concerns, where a malicious node can obtain sensitive data by inferring from the observed data. A single node has limited computational and memory resources. The solution was presented by using collaborative IDS with distributed ML algorithms and resolving the privacy issues by proposing the concepts of dynamic differential privacy to protect the privacy of a training dataset.

Table 3.2 : Existing IoT privacy solutions using machine learning algorithms.

Ref.	Threat	Attack	Use Case	Algorithm	Dataset	Accuracy
Xiao et al. [174]	MiTM	Spoof detection	WSN	QL, DQ	Private	-
Xiao et al. [175]	MiTM	Spoof detection	MiTMO Landmark	Softmax	Private	-
Aksu et al. [176]	MiTM	Authentication	Wearable devices	best of 20	Private	(Precision) 98.5%
Ma et al. [179]	Data Privacy	Data Leakage	Cloud	SGD	-	95%
Zhang et al. [182]	Data Privacy	Inference attack	VANET	LR	NSL-KDD	-
Jia et al. [178]	Data Privacy	Multiple	Distributed Systems	OMPE	realworld	-
Zhu et al. [177]	Data Privacy	Multiple	Healthcare	SVM	realworld	94%
Sun et al. [180]	Data Privacy	Multiple	General	HBD, NB, DT	-	-
Feng et al. [181]	Anomaly	Spam	MSN	CNN	Sino Weibo	91.34%

3.1.2 Blockchain techniques and Application to Mitigate IoT Threats

Blockchain (BC) is a secure mesh network [183], that is fault-tolerant, transparent, verifiable, and audit-able [184]. The frequently used keywords to describe

BC benefits are *decentralized, P2P, transparent, trust-less, immutable.* These attributes make a BC more reliable than an untrusted central client-server model. The smart contract is a computer protocol on BC which guarantees the execution of a planned event [185]. According to Restuccia et al. [87], the blockchain guarantees data integrity and validity, making it a suitable solution for protection against data tampering in IoT devices.

3.1.2.1 Security efforts using Blockchain

Several BC-based solutions for supply-chain, identity management, access management, and IoT were proposed [186]. However, the existing solutions either do not respect the time delay, and cannot be applied to the resource-constrained IoT devices [187]. In contrast to that some studies, like [188] were only focused on the improvement of time response of an IoT device, rather than their security and privacy. Machado et al. [187] offered data integrity for Cyber-Physical Systems (CPS) by splitting their BC architecture into three levels: IoT, Fog, and Cloud. At the first level, the IoT devices in the same domain created trust in each other using Trustful Space-Time Protocol (TSTP), which is based on Proof-of-Trust (PoT). At the Fog level, Proof-of-Luck (PoL) was used to create fault-tolerant IoT data which produces a cryptographic digest for a data audit. The data generated from the first level was hashed using SHA-256 and saved temporarily. After the acknowledgment and consensus were reached, the data was permanently stored at the third level of cloud, which is a public ledger. Other than data integrity, the study also offered key management using time synchronization and the location of the node. HECOPS was used to estimate the node's location via multi-lateration, and TSTP provided clock synchronization. The paper proposed to use multiple consensuses, such as PoT and PoL, but it did not cater to any user privacy issue. Another paper [189] provided data integrity with the idea of securing data collected from the drone using public BC. DroneChain presented had four modules; *drones*, *control system*, *cloud server*, and *a BC network*. Drones were controlled by the control system, and the data was encrypted and stored using the cloud server on a decentralized BC. The resultant system was trusted and accountable, offered instant data integrity, and had a resilient backend. However, the study used Proof-of-Work (PoW), which was not the best choice for a real-time IoT application like drones. In addition, the work did not offer data provenance and user/data security.

DoS attacks are one of the frequently executing attacks due to their comparatively straightforward implementation and the ever-growing number of insecure digital devices. Due to cheap IoT technologies, hackers can easily control multiple IoT devices to launch an attack. According to [190], the Software-Defined Network (SDN) top layer is prone to brute force attacks. Since SDN is controlled by software, it can be targeted by injecting malicious applications, and also gives rise to the DoS/DDoS attacks. The earlier methods to prevent DDoS are not compatible with a light-weight multi-standard IoT environment. Other than that, SDN can suffer flooding attacks, saturation attacks, and MiTM attacks due to lack of authentication in the plain-text Transport Control Protocol (TCP) channel. Tselios et al. [190] argued that BC offered a better solution to protect IoT devices from security attacks and enforced trust between multi-vendor devices, as it was decentralized, fault-tolerant, and tamper-proof. These valuable BC properties make it resistant to data tampering and flooding attacks. However, all of the solutions mentioned above were theoretical ideas as no practical implementation was done. In another paper, Sharma et al. [191] improved the security vulnerability in SDN by proposing a distributed SDN architecture for IoT using BC called DistBlockNet. The BC was used to verify, validate, and download the latest flow rule table for the IoT forwarding devices. The proposed DistBlockNet model was compared with the existing solutions, and the results were better in terms of real-time security threat detection and overhead usage.

In another study, the researchers highlighted a MiTM security gap in a smart-grid, where any malicious actor could modify user data sent over the Internet [192]. Secondly, the customers could not audit their costly utility bills, because the current smart-grid was unpredictable, and it did not provide any early warnings to the customer indicating higher energy usage. To avoid the above issues, this study proposed to use cryptographic data transmission using public and private keys for the user ID as well as the smart contract, which was placed on a BC. This technique ensured an immutable, secure, and transparent smart-grid system. However, PoW could be extremely expensive and resource exhausting.

The study in [193] argued that the existing logistics systems were neither transparent nor credible to trace. The existing systems were centralized, relied on multiple TTPs, and focused on a single transporter. Hasan et al. [193] proposed a proof of delivery system using BC technique. In their transporter system, the nodes were *seller*, *buyer*, *courier services*, *arbitrator* and *Smart Contract Attestation Authority* (SCAA). The initial agreement was a smart contract that was placed on Inter-Planary File System (IPFS) and was executed once all the parties agreed. The item was transported between several transporters as per the smart contract (maximum three in this paper), which was created every time for the next transporter. Finally, once the buyer has verified and collected the item, the payment is released to the seller. In the case of any rejection (i.e., transaction failure), the *arbitrator* takes over, settles the dispute and redistributes the amount based on the negotiated agreement. This proposed physical-asset-delivery system has inherent BC security against MiTM and DoS attacks. However, the authors have not paid any particular attention to user ID management and data privacy. The study by Gupta et al. [194] used OMENT++ on one application scenario where the authors claimed to have tackled Sybil attacks and replay attacks in an IoT network. First, they introduced a new layered architecture with two more layers in the underlying IoT architecture. They explained their algorithm, idea, and work by comparison in terms of metrics of *Transactions added to the BC per second (Ftx)*, *Blocks added to the BC per second (Fblk)*, and *Memory space utilized (Mmempool)*.

IDS is one of the widely used monitoring devices to detect anomaly traffic behavior. In a study by Golomb et al. [195], the authors argued that the current anomaly IDS were not efficient since the training phase considered only benign traffic. An adversary could exploit this vulnerability by injecting malicious data, which might be regarded as benign. Secondly, the trained model might not be as efficient, since it might be missing some IoT device traffic, which was only event-driven by, for example, a fire alarm. Both of the issues were solved by using a Collaborative IoT Anomaly (CIoTA) Detection using BC technique, where all IoT devices of the same type were trained simultaneously. Since a large number of IoT devices were being trained based on their local data traffic, the chances of an adversarial attack were minimum. Each device would generate a locally trained model which would be collaboratively merged into a globally trained model by using BC technique. The study successfully implemented CIoTA and proved its benefits for eliminating the adversarial attacks. However, the separate block generated for each IoT model would increase the amount of data.

Along with the research on frequently researched security threats such as Data integrity, MiTM, and DoS, several studies have focused on providing solutions to multiple attacks. Sharma et al. in [196] presented an affordable, secure, and always accessible BC technique for distributed cloud architecture. The combination of SDN and BC implemented the security of the fog nodes. The study brought the resource extensive tasks closer to the edge of an IoT network, which not only ensured better security but also improved end-to-end transmission delay. The authors further claimed that the model was adaptive based on the encountered threats and attacks, and reduced administrative workload. The main focus of this paper was to provide an architecture based on BC-cloud in fog computing, which was scalable, secure, resilient, and fast. The comparison was made in terms of throughput, response time, and false alarm rate. However, there was no consideration to the data privacy, user ID management, or the key management. Similarly, Sharma et al. in [197] claimed that the existing Distributed Mobile Management (DMM) lacked robustness against the security threats due to its centralized architecture. Their proposed scheme based on the BC showed improved latency, delay, and energy consumption, without affecting the existing network layout. However, the study used PoW consensus, which is energy-hungry and offered no user privacy.

All of the above solutions are mentioned in Table 3.3, where most of the researchers have focused on using PoW as a consensus algorithm, which is not suitable for a real-time IoT application. Moreover, most of them have not considered user anonymity and data integrity.

Table 3.3 : Taxonomy of existing IoT security solutions using blockchain techniques. Here, U, D, and K mean *User security*, *Data security*, and *Key management*, respectively.

Ref.	**Threat**	**Use Case**	**BC used**	**BC type**	**Consensus**	**Security**	**Weakness**
Machado et al. [187]	Data Integrity	Cyber Physical System	Ethereum	Public	PoT + PoL	D/K	Did not address *U*
Liang et al. [189]	Data Integrity	Drone	-	Public	PoW	D/K	(i) PoW is inefficient for real-time applications (ii) Public BC is insecure
Tselios et al. [190]	DoS	SDN	NG	Public	-	None	*U*/*D*/*K* not addressed
Sharma et al. [191]	DoS	SDN	Bitcoin	Public	PoW	None	Lack of data integrity & *U*
Gao et al. [192]	MiTM	SmartGrid	-	Private	PoW	U/D/K	Encryption techniques are complex and slower
Hasan et al. [193]	MiTM	logistics	Ethereum	Private	PoW	K	Did not address *U* & *D*. Overall less secure
Gupta et al. [194]	MiTM	IoT	Bitcoin	Public	Private	K	Only simulation is done for basic security
Golomg et al. [195]	Anomaly	Network	Private	Public	Private	D/K	Block per IoT model will increase the data.
Sharma et al. [196]	Multiple	Fog-SDN	Ethereum	Public	Proof-of-Service	None	No *U* or *D* is offered
Sharma et al. [197]	Multiple	5G	Multiple	Both	Multiple	None	PoW is costly, plus *U*/*D*/*K* not addressed

3.1.2.2 Privacy efforts using Blockchain

Privacy is a complicated issue in a BC that can be accomplished, but at the cost of throughput and speed [184]. A hacker can identify the patterns of a permissionless

BC since all of the transactions happen in public and make an informed decision about the source. BC-based privacy-preserving was proposed by several researchers to solve this issue [198–206].

Wang et al. proposed a BC-based model, tackling the MiTM attack issues in a crowdsensing application [198]. The user privacy was implemented by using node cooperation method, in which the server released the sensing task as well as its price, which was pre-paid on the BC. The users would perform the sensing task and upload the sensing data, and finally, the user was paid as per their achievements. To achieve user-data privacy, the authors proposed k-anonymity, in which the sensing task was not given to an individual, but a group and the sensed data gathered was also in the form of a group, which preserved privacy of a single-user. The announcement VANET is something in which the users (nodes) shared some information that might benefit other users in the network. According to the researchers of CreditCoin [199], the current VANET system had a lack of privacy as well as motivation for the users to share any data. CreditCoin was proposed that offered decentralization, trust, and motivation by paying the user their incentives. The shared information was immutable, so the source did not fake any news either, benefiting the whole VANET community from it. For example, the information might be "a traffic accident on ABC road going towards XYZ". Another VANET application was proposed by Lu et al. in [200], where the authors added privacy to the users in the existing bitcoin platform using the lexicographic Merkle tree. Furthermore, the forgery was controlled by adding a reputation weight to every vehicle in the network. However, the study used PoW as their consensus protocol, which is very costly and can create traffic bottlenecks in a resource constraint VANET application.

First, of its nature, Zhou et al. [201] claimed to design the BC-based IoT system where the servers helped users to process encrypted data without learning from the data. HE was used to secure the data in a private BC using Practical Byzantine

Fault Tolerance (pBFT) consensus. The authors in [202] argued that although the BCs were immutable and tamper-proof, once a block was executed, they did not cater confidentiality and privacy of the data as anyone could see the plain-text. When such a BC was integrated with IoT, it was more vulnerable due to a massive influx of data. Rahulamathavan et al. focused on these issues by proposing a privacy-preserving BC architecture for IoT applications based on the Attribute-based Encryption (ABE) [202].

The previous studies offered the solution by using symmetric encryption like Advanced Encryption Standard (AES), which meant that the key must be shared with the data to enable the miners of the BC to verify the content and update the BC. However, such a technique could not guarantee privacy. ABE used single encryption to keep data private and safe. In a scenario of a hospital, the main server could encrypt data before transmitting the attributes, such as DOCTOR or NURSE, which could only be read by the concerned node by using the same attributes and decrypting them. The BC architecture could secure data manipulation since multiple nodes verified a single transaction. After the approval, the data was stored and could not be tampered. Lastly, there was no central control, making all of the transactions transparent and fair. However, the cluster head could read the data, which might be exploited by an attack.

Fan et al. working in the 5G network application argued that the work on access control of an encrypted data still needed to be explored [203]. Despite several advantages of ABE, if a user wanted to change his policy, the attribute revocation and re-encryption took much time. Additionally, the owners did not control their public data, and the trust was delegated to the third parties. Centralized systems were fault-prone, and could cause traffic choking. Fan et al. used BC to solve these issues, by using encrypted cloud storage for the provision of privacy-preserving and data-sharing systems, which was tamper-resistant, fully controlled by the user, and always accessible to anyone on request [203]. However, their proposal had several drawbacks; for example, the miners could share the information without user consent. Moreover, the BC proposed is public, which means anyone could access it.

Aitzhan et al. [204] addressed the issues of transaction security and privacy by using multi-signatures. Since the traditional systems were insecure, unreliable, and publicly accessible, the messages were sent in an encrypted form that offered privacy and security in communication. User anonymity was ensured by using the public key and private key. Similarly, another concept of multi-signatures was mentioned by Guo et al. [205]. The authors found that the current Electronic Health Record (EHR) system was centralized with no user privacy or control over it. Health records are critical documents as they have a personal medical history. The user should be in control of them, but they should be unforgeable as well. In previous studies, Attribute-Based Signatures (ABS) enabled trust between the two parties; however, it was unreliable and restricted to a single signature. Encashing the ABS advantages, Guo et al. presented an ABS with multiple access (MA-ABS), which guaranteed privacy with access control to the user, and confidence of real information to the verifier [205]. Moreover, using BC for maintenance of data reinforced immutation, unforgeability, and decentralization. Privacy-preserving was achieved by using MA-ABS and collusion attacks were avoided by using pseudorandom function seed. The study also proposed Key management by using KeyGen.

In a similar attempt, [206] offered a new consortium BC called PETCON, that was based on the bitcoin platform using PoW for the PHEV to trade the surplus electricity between them. The existing P2P was a single point of failure, and it was expensive and untrustworthy. Kang et al. [207] improved upon the privacy of a vehicular data in the existing P2P data sharing networks. Due to the resource constraints in a vehicular system, the data was forwarded to the edge computers for powerful computation. The data shared was vulnerable, due to which, the researchers in this study used consortium BC, where only the selected nodes could perform the audit and verification. They also introduced the use of smart-contracts, which ensured user-authenticity and secure data-sharing, and improved data-credibility. The consortium model reserved the energy as it selected a lesser number of nodes for data maintenance. Vehicle-ID authentication was done by digital signatures using public/private keys, while *Elliptic curve digital signature algorithm* provided key-management. The authors also touched upon data privacy management by storing the raw data using the proof-of-storage.

Table 3.4 : Overview of existing IoT privacy solutions using blockchain techniques.

Here U, D, and K mean *User security*, *Data security*, and *Key management*, respectively.

Ref.	**Threat**	**Use Case**	**BC used**	**BC type**	**Consensus**	**Privacy**	**Weakness**
Wang et al. [198]	MiTM	Crowdsensing	Bitcoin	Private	PoW	U/D	Prone to collusion attacks.
Li et al. [199]	MiTM	Vanet	Private	Private	Private	U/D/K	Poor key management
Lu et al. [200]	Data Privacy	VANET	Bitcoin	Private	PoW	U/D/K	PoW is slow & not ideal for real-time scenario.
Zhou et al. [201]	Data Privacy	IoT	Ehtereum	Private	pBFT	U/D	Block time not suitable for real-time IoT
Rahulamathavan et al. [202]	Data Privacy	IoT	Bitcoin	Public	PoW	D/K	Unsuitable for real-time IoT as block time is 10 m.
Fan et al. [203]	Data Privacy	5G	Private	Public	DPos	U/D/K	Miners can share data & store data, BC is public.
Aitzhan et al. [204]	Data Privacy	Smartgrid	PriWatt	Public	PoC	U	Did not address *D* and *K*
Guo et al. [205]	Data Privacy	Healthcare	Private	Public	-	U/D/K	No BC model or consensus technique mentioned.
Kang et al. [206]	Data Privacy	PHEV	PETCON	Consortium	PoW	K	Did not address *U* or *D*

3.1.3 Integrating ML and BC to mitigate IoT Threats

In this Section, we look at the existing security and privacy solutions for IoT with the integration of ML algorithms and BC techniques.

3.1.3.1 Security Solutions Using ML and BC

Agrawal et al. claimed to eliminate spoofing attacks with the combination of ML algorithms and BC techniques [208]. By securing the user-device communication, the user in a valid IoT-zone is continuously monitored, and the communication logs are saved on the BC. The records are immutable and can be verified for any suspicious activities. The existing user authentication techniques include one-time-password (OTP) or security questions, which are limited to single authentication. By using Hyperledger as a BC platform, the authors resolved this issue by considering continuous security using IoT-zone identification, IoT-token generation, and token validation. However, the study considered IoT-hub as a center of communication, which voided the concept of decentralization. There was no user or data privacy in concern, and the dataset was too small for a DL model.

The open nature of Android poses new security challenges and attacks. Gu et al. [209] illuminated that Android-based systems were highly targeted by malware, trojans, and ransomware with evolving nature when studied overtime [210]. The existing schemes, which can be classified as either static-based analysis or dynamic-based analysis, had certain drawbacks such as high computation time costs and types of code obfuscations such as variable encoding and encryption [211]. Gu et al. proposed a new Multi-Feature detection Model (MFM) of Android-based devices, where they utilized a fact-base of malicious codes by using Consortium BC for Malware Detection and Evidence Extraction (CB-MDEE) in mobile devices. Compared with the previous algorithms, CD-MDEE achieved higher accuracy with lower processing time.

Using the Exonum BC platform and Deep Neural Network (DNN) ML algorithms, the proposed architecture leverage upon BC's properties to send and sell their data *as and when* required giving optimum access control to their health data [212]. As the data in the storage would be encrypted, the compromise of the storage would not lead to data leakage. The proposed scheme utilizes hash functions and public-key signatures for encrypting user data to guarantee authorization and validity. The paper, however, lacks the in-depth comparison with other schemes, other than being just a theoretical framework.

Table 3.5 : Overview of existing IoT security solutions using machine learning algorithms and blockchain techniques. Here, K stands for *Key management*.

Ref.	Attacks	Use Case	Algo	Dataset	Metric	BC used	BC type	Consensus	Privacy
Agrawal et al. [208]	MiTM	IoT	VMM+ LST	Private	Accuracy	Hyperledger	Private	pBFT	K
Gu et al. [209]	Malware	Android	MFM	Drebin	FPR, DR, Acc	Private	Consortium	-	none
Mamoshina et al. [212]	Access Control	Healthcare	DNN	-	-	Exonum	Private	BFT	U/D/K

Table 3.6 : Summary of existing IoT privacy solutions using Machine Learning algorithms and blockchain techniques. Here, U, D, and K mean *User security*, *Data security*, and *Key management*, respectively.

Ref.	Attacks	Use Case	Algo	Dataset	Metric	BC used	BC type	Consensus	Privacy
Mendis et al. [213]	Data Leakage	General IoT	CNN	Private	Accuracy	Ethereum	Private	PoS	D
Mendis et al. [214]	Data Leakage	SDN	CNN	MNIST	Accuracy	Ethereum	Private	PoS	U/D/K
Weng et al. [215]	Data Privacy	General	CNN	MNIST	Accuracy	Corda	Private	BAP*	U/D/K
Shen et al. [216]	Data Privacy	Smart Cities	SVM	BCWD+HDD	Accuracy	NG	NG	PoW	U/D/K
Goel et al. [217]	Data Tampering	Computer Vision	DNN	MNIST/CIFAR-10	Accuracy	Private	Public	-	U/D/K
Fadaeddini et al. [218]	Data Privacy	Self-driving Cars	-	-	-	Stellar	Public	SCP†	U/D/K

3.1.3.2 Privacy Solutions Using ML and BC

Many companies rely on big datasets to optimize their target audience and enhance their profits, but such data contain sensitive personal information, such as political preferences, which can be exploited by interested entities. It is, therefore, crucial to preserve the privacy of such users, and if required, compensate them for their contributions. Moreover, certain domains have an abundance of data, which can be beneficial for research and development, but the data cannot be shared with third parties. Furthermore, the same data can be manipulated and raise doubts on its integrity. To improve upon the above architecture, several studies have been proposed [214, 216, 218–220].

Mendis et al. [213] proposed fully autonomous individual contributors working

*Byzantine agreement protocol

†Stellar Consensus Protocol

in a decentralized fashion without disturbing the functionality and overall efficiency, which they later on improved in their work in [214]. Their comparison against federated learning using the MNIST dataset for CNN model generated more than 94% accuracy in each scenario. The smart contracts incentivizing the computing contributors executed the peer-to-peer transactions. However, in their study [214], the execution time with encryption increased 100%. Moreover, the architecture was based on the ethereum BC having a block-time of 12 seconds, and hence it might not feasible for a real-time IoT application, for example, video streaming.

DeepChain proposed BC based value-driven, incentives mechanism to solve security issues [215]. DeepChain guarantees data privacy and audit-ability for the model training process. Confidentiality is employed using the Threshold Paillier algorithm that provides an additive homomorphic property. Using CNN algorithms and MNIST dataset, DeepChain proved that the more parties participated in collaborative training, the higher the training accuracy was.

ML classifiers require datasets to train. These datasets are collected from different entities who are usually reluctant to share their data due to several privacy concerns such as data leakage, data integrity, and ownership. The users do not know how and when their data may be used. To preserve these privacy issues, Shen et al. [216] proposed a fusion of ML with blockchain. A privacy-preserving SVM based classifier was used to train the encrypted data collected from IoT users, while the BC platform provided data sharing among multiple data providers. However, the solution used encryption techniques to preserve privacy, which is not suitable for a resource constraint IoT device. The use of the BC platform is also not explained in detail.

In yet another study, an attempt to create tamper-proof DNN models is done with the help of BC [217]. Using the BC properties like *transitive hash*, *cryptographic* *encryption*, and *decentralized nature*, an architecture named *DeepRing* is proposed. A shared common ledger stored the state of the model. Ouroboros block stored all blocks' hashes, which was used to track the compromised block in case of any tampering attack. Since the querent encrypted the query with its public key, and the output was only encrypted using the public key of the querent, no one else could access the model results. Focusing on the adversarial attacks on network parameters, the authors compared DNN architecture with DeepRing architecture. The DNN architecture without BC using CIFAR-10, MNIST and Tiny ImageNet datasets dropped by their accuracy by 20.71%, 47%, and 34%, respectively. However, the DNN with BC suffered 0% accuracy loss.

Similar work is done in the latest research by Fadaeddini et al. [218], who proposed a framework where the privacy of data-owners was preserved by training the shared model on their data locally. After the learning is completed, the data-owners only shared the learned parameters of the model. The study demonstrated *self-driving cars* application scenario, which used the Stellar BC platform for the decentralized deep learning infrastructure. The contributors are paid for their work as they helped in improving the accuracy of self-driving cars. The learned model is saved on a distributed file system known as IPFS (Inter-Planary File System), which is resistant to DDoS attacks. The framework also controls the authenticity of computing partners to avoid any malicious activities. Although the work is novel and ticks all the privacy issues (i.e., user privacy, data privacy, and key management), however, there is a lack of comparative analysis which can prove that their work is better than the traditional framework.

3.1.4 Research Challenges

3.1.4.1 Challenge to Machine Learning Algorithms in IoT

ML algorithms are utilized for analysis after being trained on a large number of datasets to adapt to the desired output dynamically. These models may be used, for example, in navigating a robot or for speech recognition, where human expertise either does not exist or cannot be used. ML algorithms have also been utilized very efficiently to analyze threats against several cybersecurity domains. Although ML algorithms perform well in many areas, they have some limitations in the IoT environment:

- **Scalability and Complexity**: In recent studies, several ML algorithms have effectively reduced the cyber attacks. However, ML algorithms are not an ideal pick for IoT applications due to its limitations. Diro et al. claimed that the traditional ML algorithms were limited in scalability, feature extraction, and accuracy [152]. Whereas, Moustafa et al. [157] argued that ML algorithms could not solve many problems, primarily when it was implemented in a complex resource-constrained IoT environment. Another work done by Abeshu et al. [154] proved that the traditional ML algorithms were less scalable and less accurate in a vast distributed network such as IoT. After comparing classical ML algorithms with DL methods, several studies learned that most DL techniques used pre-training for feature extraction. DL not only saved administrative time but also reduced feature dimensionality by reducing redundancy [167, 221–224].

- **Latency**: As a solution to the above issues, some authors, for example, Xiao et al. [175] proposed to use ensemble ML algorithms. The ensemble algorithm proved to be performing better than each ML algorithm individually, but it was computationally expensive. As an alternative to classical ML, most of the studies pointed out that DL is a better choice for IoT. In another study, the authors proposed *Deep Feature Embedding Learning* (DFEL) [169]. They utilized the DL-based model because the traditional ML algorithms increased training time in Big Data scenarios. Using the datasets of NSL-KDD and UNSW-NB15, they claimed to have improved in the recall of gaussian NB classifier from 80.74% to 98.79%. Moreover, their method significantly reduced the running time of SVM from 67.26 seconds to 6.3 seconds. The improvement in recall-rate and running time perfectly suit an IoT application.

- **Compatibility**: Although the above solutions have performed better, we believe that these DL-based techniques are application-specific. In such cases, a model trained for solving one problem may not be able to perform well for another problem in the similar domain [83].

- **Vulnerability**: One of the critical challenges to the ML/DL techniques in IoT is to secure themselves from any security or privacy attacks. Adversarial attacks against ML models may degrade system performance, as such attacks significantly reduce the output accuracy [225]. The attack severity is proportional to the amount of information available to an adversary about the system [226], which is very difficult to counter. As depicted in Figure 3.1 an adversary can attack ML models at different levels, for example, tampering the input parameters. Goel et al. [217] highlighted that much work is done to counter input level attacks [227–231], however, the research focus on adversarial attacks on network parameters is very less. Some of these attacks can be proven deadly, for example, in a healthcare application where an ML algorithm is used to analyze the amount of insulin provided by a patient. If an adversary can inject malicious code and alter the ML algorithm's input, the amount of insulin may be increased and cause death to the patient.

Regarding the above issues, we believe that the ML algorithms for IoT need to be optimised for scalability, speed, compatibility, and security & privacy. We think that privacy-preserving ML algorithms, such as differential privacy and light-weight HE, should be explored to overcome the discussed challenges.

3.1.4.2 Challenges to Blockchain in IoT

- **Latency and speed**: Although the BC technology was introduced a decade ago, its real benefits were realized only recently. In recent studies, many efforts have been made to utilize BC in several applications, such as logistics, food, smart grid, VANET, 5G, healthcare, and crowdsensing. However, the existing solutions do not respect the latency issues of BC, and cannot be applied to the resource-constrained IoT devices [187, 232]. The most widely used BC consensus is PoW, as depicted in Table 3.4. PoW is a slow (limited to seven transactions per second compared to an average of two thousand transactions per second for the visa credit network) and requires a lot of energy [184, 185, 233]

- **Computation, processing, and data storage**: There is a substantial cost of computation, power, and memory involved in maintaining a BC across a vast network of peers [233, 234]. According to the Song et al., in May 2018, the bitcoin ledger size had surpassed 196 GB. These limitations suggest poor scaling and transaction speed for an IoT device. Although an alternative was to offload their computation tasks onto a central server - cloud, or a semi-decentralized server - fog, this, however, adds network latencies [234, 235].

- **Compatibility and Standardization**: Like any emerging technology, one of the BC challenges is its standardization for which the laws need to be reformed [236]. Cybersecurity is a difficult challenge, and it would be naive to think that we all will see a security and privacy standard that can eliminate all risks of cyber-attack against IoT devices anytime soon. Even so, a security standard can ensure that devices meet "reasonable" standards for security and privacy. There are a number of fundamental security and privacy capabilities that should be included in any IoT device.

- **Vulnerability**: Although the BC is non-repudiable, trustless, decentralized, and tamper-proof, a blockchain-based system is only as secure as the system's access point. In a public BC-based system, anyone can access and view the data contents. While the private blockchain is one of the solutions to the above problem, it raises other issues such as trusted third party, centralized-control, and access-control legislation. In general, the blockchain-enabled IoT solutions must meet the security and privacy requirements such as (i) the data must be stored securely by satisfying the confidentiality and integrity requirements; (ii) data must be securely transmitted; (iii) data must be shared transparently, securely and in an accountable fashion; (iv) the properties of authenticity and non-reputation must be preserved; (v) the selective disclosure property must be satisfied by the data-sharing platform, and (vi) the explicit consent of data sharing must be taken by the involved parties [237].

3.1.4.3 Challenges to ML & BC in IoT

We believe that a single technology or a tool, like BC or ML, will not suffice in providing optimum security and privacy for IoT networks. Therefore, it is a dire need of time for the research community to explore the provision of IoT security and privacy with the merger of BC and ML, that has the following challenges:

- **Storage**: As discussed in Section 3.1, ML algorithms perform better with larger datasets [152, 154]. However, the increase of data in BC platforms will degrade its performance [234]. It is an open research issue to find a balance, which would be ideal for IoT applications.

- **Latency:** Depending upon the scenario, an IoT network may generate a considerable amount of data requiring more time for training and computation, which may potentially increase the overall performance (i.e., latency) of traditional ML models [187, 232].
- **Scalability:** ML and BC have scalability challenges, in terms of both the processing and communication costs. Many ML algorithms impose additional processing and communication costs with the increase of data that is imminent for most IoT networks. Similarly, the BC performs poorly as the number of users and networking nodes increases [238, 239]. On average, an Ethereum BC performs 12 transactions per second, which is unacceptable in traditional IoT applications, where millions of transactions are happening every second [240].
- **Vulnerability:** Although the combination of ML and BC can tremendously increase security and privacy, there are a few challenges as well. The increasing number of threats, including malware and malicious code, increases the challenge of identifying, detecting, and preventing them in real-time IoT networks. The training phase of ML takes longer, and while it is possible to detect malicious traffic, this is only possible with a trained model [225]. Blockchain, on the other side, can guarantee data immutability and can identify their transformations. However, the issue is with the data that is corrupted before entering the blockchain. Additionally, the malfunctioning of sensors and actuators from the start cannot be detected until that particular device has been tested [235]. Besides the above issues, public BC is prone to privacy evasion techniques as the stored data is publicly accessible and available to all readers. Using private BC is one of the solutions to these challenges; however, this would limit access to a large amount of data required for ML to perform efficiently [240].

The IoT devices can generate a massive amount of data, which should be typically processed in real-time. Since the demand for IoT-based BC is different, there is much research going on to bring a new BC that is compatible with IoT. However, the most important limitations on BC are ledger storage and transaction per second (TPS). Although in the latest BCs, such as Hyperledger Fabric, TPS is down to milliseconds, a lot still needs to be done for a BC to work smoothly in the IoT environment. Similarly, in the context of the secure BC model of IoT, the security needs to be built-in, with validity checks, authentication, and data verification, and all the data needs to be privacy-preserved at all levels. We need a secure, safe, and privacy-preserved IoT framework.

3.1.5 Summary

In Section 3.1, we have reviewed the latest existing literature survey on IoT security and privacy using ML algorithms as well as BC technologies and highlighted their gaps. This study has presented the current solutions to IoT security and privacy by utilizing ML algorithms, BC techniques, and the integration of both. To better understand the security and privacy issues in an ML, we have also attempted to present an ML threat model for IoT based on the previous studies. Finally, We discuss a few research challenges to ML algorithms in IoT, BC techniques in IoT , and the challenges to the combination of ML and BC in IoT.

The generation, storage, analysis, and communication of data are fundamental to the IoT ecosystem. A holistic approach is in demand, where a vulnerability-free system needs to be built, through measures such as adherence to best practices and continual testing. The system should be able to learn and adapt to the latest trends in threats (zero-day attacks) since malicious activities are dynamic. In this regard, ML/DL can be extremely beneficial in analyzing the traffic. At the same time, the BC can serve as a basis to keep a ledger of logs and communication in an IoT environment. Since this data is immutable, it can be used confidently in the court of law as a piece of evidence.

Among the studies conducted on IoT security and privacy, most of them focused on providing security or privacy. We believe that for a system to be secure, both security and privacy are equally important. Moreover, data privacy is the most critical factor, which can only be valid when considered end-to-end. The current systems lack the integrity of datasets that are used to train a model. Any adversary can tamper these datasets to obtain their desired results.

Currently, the integration of ML algorithms with BC techniques to achieve IoT security and privacy is a relatively new area, which requires further exploration. However, some of the research questions are: (i) Can we use BC to eliminate DDoS attacks in an IoT network by integrating it with ML algorithms? (ii) Can the resource-constrained IoT device leverage upon BC's inherited encryption to perform in real-time? (iii) Can BC introduce trust in traditional collaborative ML-based IoT Intrusion Detection Systems? Moreover, several organizations, both public and private, rely on the data generated by IoT devices. How can we trust the data, whether *in motion*, or *at rest*? This question becomes more difficult to answer in a centralized cloud-based IoT architecture. We can extract meaningful data from privacy-preserving ML algorithms, whereas BC can offer security and trust. In the next Section 3.2, we aim to design and develop a privacy-preserving IoT framework, which will offer privacy-preserving data sharing and privacy-preserving data analysis.

3.2 Securing Smart Home User Data Using LDP

The rapid expansion of Internet of Things (IoT) devices in smart homes has significantly improved the quality of life, offering enhanced convenience, automation, and energy efficiency. However, this proliferation of connected devices raises critical concerns regarding security and privacy of the user data. In this section, we propose a differential privacy-based system to ensure comprehensive security for data generated by smart homes. We employ the randomized response technique for the data and utilize Local Differential Privacy (LDP) to achieve data privacy. The data is then transmitted to an aggregator, where an obfuscation method is applied to ensure individual anonymity. Furthermore, we implement the Hidden Markov Model (HMM) technique at the aggregator level and apply differential privacy to the private data received from smart homes. Consequently, our approach achieves a dual layer of privacy protection, addressing the security concerns associated with IoT devices in smart cities.

3.2.1 Smart Homes and Data Privacy

Advancements in software and hardware have driven the expansion of information and communication technologies (ICT), playing a crucial role in smart city development. By incorporating ICT into urban operations, cities become more efficient and adaptable, leading to the prevalent term ”smart city.” These urban environments leverage ICT and other strategies to enhance residents' quality of life, catering to the needs of present and future generations across social, environmental, and economic dimensions.

The Internet of Things (IoT) is an essential component in the development of smart cities, acting as their backbone. Smart cities are made feasible through the use of IoT, which includes smart sensors, smartphones, radio-frequency identification (RFID), and smart meters as central elements of the IoT framework. The IoT framework comprises various modules, such as electronics, firmware, networks, sensors, and software. Wireless devices, including sensors, displays, actuators, and home appliances, are connected through IoT, enabling a large amount of data to be generated and exchanged among devices and the Internet to achieve ubiquitous interconnectivity. IoT devices have propelled a data explosion, transferring vast amounts of data to the cloud for real-time processing in applications such as electronic healthcare systems, vehicular ad hoc networks (VANETs), and smart homes [241]. In IoT networks, sensor data is collected from various applications, and different sensor device data is analyzed using deep learning approaches [242]. Sundaravadivel et al. [243] proposed a system based on IoT called smart-Log, which identifies nutritious food items for children using deep learning. IoT has numerous applications, such as VANET and smart homes [244], and electronic healthcare systems used for real-time data processing.

Smart Home is a vital IoT application that uses connected devices to make our lives more efficient and convenient. Smart homes provide security to homeowners and can be controlled remotely, offering comfort and security [244]. Sensor-collected data can be used for home activity prediction within smart homes [245], smart healthcare for patient treatment [246], disorder assessment, and smart city pedestrian monitoring [247]. In smart cities, data is exchanged among smart homes. To participate in smart cities, people must feel secure and protected. Security and privacy protections are essential, especially when data is transferred from one area to another with multiple parties having access to it. Various techniques in the literature are used for data privacy, such as k-anonymity, l-diversity, t-closeness, and differential privacy, respectively.

This section aims to explore differential privacy techniques for ensuring the data privacy of Smart homes. In 2006, Dwork proposed the use of differential privacy to prevent adversaries from accessing data. Differential privacy is a crucial technique for data privacy. This paper focuses on securing smart home data using local differential privacy (LDP). In smart homes, people do not want their data to be accessible to outsiders. Centralized Differential Privacy (CDP) is based on the assumption that the aggregator node will be honest, which is difficult to guarantee in real life. To preserve privacy, LDP is suggested with strong privacy guarantees [248, 249], which is an extension of differential privacy. LDP can resist adversaries with background knowledge and uses distributed randomized processes to prevent data leakage. LDP has various industrial applications, such as Google's LDP structure called "RAPPOR" [250], which is used in Chrome to collect user behavior data. Apple announced the use of LDP for user privacy preservation at WWDC 2016 [251].

In this section, we propose a method for sending home data to the aggregator while considering that aggregator nodes might be malicious. Therefore, LDP is applied to the real-time data of homes. The data is privatized before being sent to the aggregator. In our proposed model, an obfuscation method is applied at the aggregator side to ensure that the aggregator cannot recognize the homeowner, achieving anonymity. Our model also incorporates the hidden Markov model (HMM) concept, a widely used approach for time series data modeling with applications in various areas such as bioinformatics, speech recognition, and Internet traffic modeling. Once the model is trained, it can be used to detect anomalies by scanning for unlikely series of observations. The aggregator also employs CDP on privatized home data. Our research aims to achieve double privacy.

The contributions of this section are as follows:

- We design a secure smart home data collection framework.
- We calculate the privacy risk using a probabilistic technique based on the hidden Markov model (HMM), which computes the probabilities of smart home data.
- We apply an obfuscation method to obfuscate high-risk data to achieve anonymity.
- We utilize the differential privacy concept at the aggregator side to achieve double privacy.

The rest of this section is organized as follows: Section 3.2.2 provides the related work. Section 3.2.3 presents the problem along with a background introduction on DP, LDP, HMM theory, and Randomized Response. Section 3.2.4 describes the proposed scheme. In Section 3.2.5, the evaluation of the proposed scheme is presented followed by its limitations in Section **??**. Finally, the paper is concluded and future research directions are provided in Section 3.2.6.

3.2.2 Differential Privacy in Smart City Data Protection

The development of information and communication technology has facilitated more convenient lives for residents in smart cities. However, the transmitted data may contain sensitive information necessitating privacy protection. Various privacy techniques, including differential privacy, have been proposed by researchers to ensure data privacy. This paper specifically focuses on securing smart home data using local differential privacy.

Dwork introduced differential privacy in 2006 to prevent unauthorized access to data [250]. Subsequent research has expanded on differential privacy in various contexts, such as battery load balancing [251], cost reduction in smart meters [252], and edge filtering for reducing calculation and communication overhead [253]. Privacy-preserving structures for smart homes have also been proposed, including LDP-based schemes for reducing energy consumption and preserving privacy [254] and the Differential Privacy-based Real-time Load Monitoring (DPLM) approach for concealing load values [255].

In a study by Wang et al. [256], the LDP concept was employed to privatize hospital data, but it did not protect individual privacy. Our proposed system addresses this limitation by utilizing an obfuscation method to achieve individual privacy. Additionally, we apply centralized differential privacy at the aggregator level to provide dual-layer privacy protection.

3.2.3 Foundations of Differential Privacy

3.2.3.1 Central Differential Privacy

Differential Privacy, also known as Centralized Differential Privacy (CDP), is a privacy model in which data is entrusted to a third party, often a database owner. This entity receives queries and provides responses with the addition of a specific level of noise to the data to ensure privacy. Formally, differential privacy is predicated on the concept of neighboring datasets, denoted as q and q', which differ by only a single data point.

Definition 1 (Neighboring Datasets): A randomized algorithmic function G satisfies the condition of ε-differential privacy if, for any possible outcome $h \in$ Range(G) and any two adjacent datasets q and q', the following inequality holds:

$$P[G(q) \in h] \leq \exp(\varepsilon) \times P[G(q') \in h] \tag{3.1}$$

In Equation 3.1, ε is the privacy parameter, which controls the privacy level of the proposed mechanism and the resulting output function G. Range(G) denotes the range of the function. A smaller value of ε is desired for achieving higher privacy, and vice versa.

3.2.3.2 Local Differential Privacy

Local Differential Privacy (LDP) is a more recent model for privacy, which relies heavily on local variants. The aim is to reduce trust in third-party data aggregators, collectors, or other entities by adopting a zero-trust approach. In this scenario, individuals generate locally differential private results by adding noise to their data before transmitting the scrambled information for aggregation. However, the noise in LDP is typically larger than in Centralized Differential Privacy (CDP).

LDP is used when there is no desire to trust a centralized aggregator. By applying a randomized response, the data is obscured by the data holder at the local level.

The data holder then sends the concealed data to a potentially untrusted data aggregator. To formally define LDP, let D be the complete dataset, and consider a randomized algorithm T that takes two data tuples a and b as input and produces output a^*. ε-local differential privacy (or ε-LDP) is defined on T and $\varepsilon > 0$, which is the privacy parameter, as follows:

Definition 2 (ε-local differential privacy): A randomized algorithm T satisfies ε-local differential privacy if and only if for output a^* and two input tuples $a, b \in D$, the following inequality is satisfied:

$$P[T(a) = a^*] \leq e^{\varepsilon} \times P[T(b) = a^*] \tag{3.2}$$

In simple terms, LDP implies that the data aggregator cannot confidently determine whether the input record is a or b by observing the output a^*. LDP differs from CDP, which is defined on two neighboring databases. The two databases differ by only one record.

3.2.3.3 Randomized Response in LDP

The Randomized Response (RR) method was proposed by H. Warner et al. in 1965 [250]. It is commonly used in Local Differential Privacy (LDP) approaches, such as RAPPOR [257]. In RR, an end user is asked a question with a binary answer, either "yes" or "no." A coin is flipped with a probability of p for showing heads. To protect the end user's privacy, RR allows the end user to respond with the opposite answer when heads are shown. As a result, the data aggregator cannot confidently determine the accurate answer for a particular end user.

Definition 3: The RR mechanism is a mapping with $A = B$ that satisfies the following equality:

$$Q(a|b) = \begin{cases} \frac{e^{\varepsilon}}{|B|-1+e^{\varepsilon}}, & \text{if } a = b, \\ \\ \frac{1}{|B|-1+e^{\varepsilon}}, & \text{if } a \neq b. \end{cases} \tag{3.3}$$

Here, $Q(a|b)$ is the conditional probability, B is the true dataset, A is the privatized dataset, $b \in B$, $a \in A$, $|B|$ is the size of set B, and ε is the privacy parameter.

3.2.3.4 Hidden Markov Model in Data Analysis

A Hidden Markov Model (HMM) is a sequence of random variables with the Markov property. HMM is effective in identifying network anomalies and is used in various applications. By utilizing HMM, it is possible to estimate the likelihood of an observed sequence within the home data.

The Learning Problem in HMM The learning problem involves estimating model parameters $w = A, B, \pi$ from a set of observations. The set of hidden states and set of observation symbols V can also be estimated.

The Evaluation Problem in HMM In the evaluation problem, the set of observation sequence O and a model $P(O/w)$ are considered. The probability $P(O/w)$ represents how well the model matches the observations.

Our research focuses on a distributed approach for solving HMM inference problems, where each household's data is kept confidential. We propose a solution that computes the HMM without compromising individual data privacy.

3.2.4 Differential Privacy Framework for Smart Home Data Protection

Our research paper proposes a differential privacy-based system to protect the privacy of data collected from smart homes by adding noise using the LDP approach.

The RR algorithm is used at the client end to achieve privacy, followed by an obfuscation method applied at the aggregator end to ensure individual privacy. The proposed system provides double privacy protection for the client and the aggregator, respectively. To ensure home data privacy, we use the LDP approach, where the data from smart homes is sent to the aggregator, which could be potentially malicious. The HMM model is used at the aggregator node to allow secure distributed computation without leaking data. In addition, an obfuscation method is used to achieve anonymity and prevent the aggregator from recognizing the homeowner. Our primary objective is to achieve double privacy by applying LDP and CDP methods. The proposed system addresses the concerns of smart home individuals unwilling to have their private data leaked. Using LDP and HMM models in our system ensures that computation can be performed using private data without revealing it to unauthorized third parties as shown in Fig. 3.2.

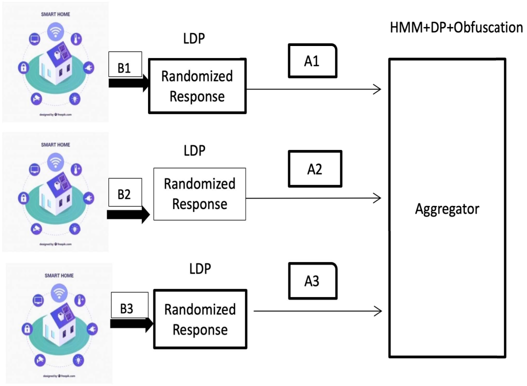


Figure 3.2 : Securing Smart Homes using LDP.

3.2.4.1 Local Differential Privacy (LDP) Implementation

The aggregator node can potentially leak the home data, so we apply the LDP concept to the data as the first line of defense. We apply the LDP algorithm, which is provided below, to ensure the privacy of the home data being sent to the aggregator node.

Algorithm 3.1 LDP Algorithm

```
  Input: $b$ = real data, $B$ = real dataset, $n$ = the size of $B$
  $R$ = random number between 0 and 1
  $\epsilon$ = The private budget
  Output: The privatized data $A$
if $R < \frac{e^{\epsilon}}{|B|-1+e^{\epsilon}}$ then return b
else $index = R - \frac{e^{\epsilon}}{|B|-1+e^{\epsilon}} mod \frac{1}{\frac{e^{\epsilon}}{|B|-1+e^{\epsilon}}}$
    for $bi$ in $B$ do
        if $i = index$ and $bi \neq b$ then return $bi$
        end if
        if $i = index$ and $bi = b$ then return $bi$+1
        end if
    end for
end if
```

HMM at Aggregator node The data is forwarded to the aggregator, where the HMM is applied. Inspired from [258] as shown in Fig. 3.3, $S_1, S_2, \ldots, S_N$ are the hidden states that are used to represent $Home1, Home2, \ldots, HomeN$, respectively. Time is divided into T slots, i.e., t=$\{1, 2, 3, ...T\}$. At time t=1, the state is called q_1; at t=2, the state is called q_2; and at t=T, the state is called q_T, respectively. Meanwhile, $Z_1, Z_2, \ldots, Z_N$ are called the visible states.

Consider an HMM with parameters A, B, π as mentioned in the previous section. Observations are carried out at time intervals 0 and T. Every home's data is observed in the system. The sequence of T observations in which home data is observed is represented as $O_j = O_{j1}, O_{j2}, \ldots, O_{jT}$.

By including a null state, the HMM can be easily extended with v to denote no observation. We assume that the observations of different homes are independent.

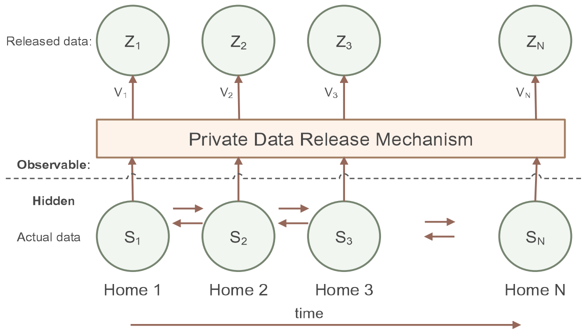


Figure 3.3 : Overview of the HMM.

Furthermore, we assume in our paper that the probability of observation for different homes' data is similar and denoted by b_{jk}. So,

$$P\left(\frac{O}{q_t}\right) = S_i = b_{jk} \tag{3.4}$$

3.2.4.2 Using HMM for the Evaluation Problem

We use two different HMM procedures to solve the evaluation problem: a forward procedure and a backward procedure. In the forward procedure, we need to calculate $P\left(\frac{O}{w}\right)$, which is the likelihood of observation given the parameters $w = (\pi, A, B)$. The forward variable can be defined as: $\alpha_t(i) = P(O_1, O_2, \ldots, O_t, q_t = s_i|w)$

Here, $\alpha_t(i)$ is the partial observation probability from 1 to t, and at this time, the state is s_i, given the model parameter w.

The complete procedure for forward HMM is shown in Algorithm 2.

3.2.4.3 Training HMM

The Backward HMM Algorithm 3.3 plays a crucial role in computing the probability of an observation sequence given a Hidden Markov Model (HMM) in computational linguistics and ML applications. It is used to calculate the backward

Algorithm 3.2 Forward HMM Algorithm

```
Initialize: $t \leftarrow 1$, $a_{ij}$, $b_{jk}$, $O_T$, $\alpha_{jt}$
for Each iteration $t = 1 : T$ do
    $\alpha_{j(t)} = b_{jk} v_t \sum_{i=1}^{N} \alpha_{i(t-1)} a_{ij}$;
    loop until $t = T$
end for
return $P\left(\frac{O}{w}\right) \leftarrow \alpha_{j(T)}$ for Final state
```

variable $\beta_i(t)$, which represents the probability of being in state s_i at time t and generating the observation sequence from $t+1$ to T, given the model parameters $w = (\pi, A, B)$ and the observation sequence $O = (O_1, O_2, ..., O_T)$. The algorithm iteratively computes the backward variable in reverse order from time T to time 1. The output of the algorithm is the probability of the observation sequence given the model, which is a critical parameter for various HMM applications, such as speech recognition, natural language processing, and bio-informatics.

Algorithm 3.3 Backward HMM Algorithm

```
Initialize: $t = T$, $b_jT$, $a_{iJ}$, $b_{jk}$, $O^T$
for Each iteration $t = T - 1$ to 1 in reverse order do
    $\beta_i(t) = \Sigma_{j=1}^{N} a_{ij} b_{jk} O_{t+1} \beta_j(t+1)$
end forreturn $P\left(\frac{O}{w}\right) \leftarrow \beta_i(1)$ for the known initial state
```

3.2.4.4 The Baum-Welch Algorithm

To effectively select the parameter w, there is no known method to directly maximize the observed sequence probability. We also require the following variable $\gamma_{ij}(t)$, which is the probability of being in a state s_i at time $t-1$ and state s_j at time t given the observations:

$$\gamma_{ij}(t) = P(q_{t-1} = s_i, q_t = s_j | O, w) \tag{3.5}$$

The $\gamma_{ij}(t)$ can be calculated from the forward and backward variables $\alpha_i(t-1)$ and $\beta_j(t)$ as:

$$\gamma_{ij}(t) = \frac{\alpha_i(t-1) a_{ij} b_{jk} \beta_j(t)}{P\left(\frac{O}{w}\right)} \tag{3.6}$$

Expected number of transitions from s_i to s_j For a sequence O at any time, it will be simply $\sum_{t=1}^{T-1} \gamma_{ij}(t)$ transitions. Thus, it gives the expected number of transitions from state s_i to state s_j. The total number of expected transitions from s_i to any state is: $\sum_{t=1}^{T-1} \sum_{j=1}^{N} \gamma_{ij}(t)$. Thus, when these two quantities are known, then we can update the transition probability a_{ij} as:

$$a_{ij} = \frac{\sum_{t=1}^{T-1} \gamma_{ij}(t)}{\sum_{t=1}^{T-1} \sum_{j=1}^{N} \gamma_{ij}(t)} \tag{3.7}$$

Similarly, we can update the emission probability b_{jk} as:

$$b_{jk} = \frac{\sum_{t=1}^{T} \xi_{jt}(t)}{\sum_{t=1}^{T} \sum_{k=1}^{M} \xi_{jt}(t)} \tag{3.8}$$

where, $v_t = v_k$ and $\xi_{jt}(t) = \gamma_{jt}(t)$ if $O_t = v_k$, otherwise $\xi_{jt}(t) = 0$.

The algorithm starts with arbitrary values for a_{ij} and b_{jk}. Then, we estimate $\alpha_i(t)$ and $\beta_j(t)$ using those values. After that, we calculate $\gamma_{ij}(t)$ and update the values of a_{ij} and b_{jk}. This process is repeated until the algorithm converges. At that point, the updated values of a_{ij} and b_{jk} are used to evaluate the model w for any given observation sequence $O(t)$. This is how the HMM is trained.

3.2.4.5 Obfuscation at Aggregator

The privacy risk for home data is assessed based on the predicted privacy probability. To mitigate high privacy risks at the expense of utility loss, high-risk data is replaced with alternative data from various paths in the HMM. This process transforms the high-risk data into low-risk data. Alongside the HMM model, a list of alternative data suggestions is generated, each with their respective privacy risk and computed utility loss. The system selects a single substitute data point from this list to control the privacy risk.

3.2.4.6 Adversarial Machine Learning

Our obfuscation technique is vulnerable to privacy attacks since both the trained dataset and adversaries have access to the learned probabilities of the HMM. This vulnerability could allow adversaries to estimate the data by computing or guessing privacy risk values using the learned HMM probabilities and potentially compromise the privacy. The adversary may employ various methods within the HMM with high risks to deduce the data. To address this issue, we propose to incorporate the adversarial ML techniques into our HMM model by adding noise. This noise addition is determined by the privacy parameter ϵ and query function sensitivity S, and is introduced in terms of count/probabilities. Therefore, the degree of noise addition depends on both ϵ and S, respectively.

3.2.5 Performance Evaluation and Insights

In this section, we elaborate on the tasks designed to evaluate and validate the effectiveness of our privacy-preserving approaches within smart home environments. Our evaluation strategy encompasses a series of experiments aimed at assessing the resilience and efficiency of our proposed methods against various privacy risks and adversarial attacks.

3.2.5.1 Dataset Generation Methodology

To conduct the evaluation of our privacy-preserving approaches within smart home environments, we generated a synthetic dataset that simulates real-world scenarios. This dataset was inspired by publicly available data characteristics found in health-related datasets, such as the diabetes dataset on Kaggle [259], and tailored to reflect the specific needs of our research while upholding the highest ethical standards.

The synthetic dataset comprises 1000 entries, each representing a hypothetical home resident's search query related to diabetes management and related health concerns. The dataset includes the following attributes for each entry:

- **QueryID**: A unique identifier for the search query, ranging from Q1 to Q1000.
- **Timestamp**: The date and time of the query, generated to reflect a distribution over the past year, ensuring a realistic temporal spread.
- **SearchQuery**: The content of the search query, selected from a predefined list of diabetes-related topics, including "diabetes symptoms," "diabetes diet," "blood sugar levels," "type 2 diabetes," and "managing diabetes." These queries were chosen to represent common concerns and information needs among individuals interested in diabetes.
- **AgeGroup**: The age group of the individual making the query, categorized into five groups: "18-25," "26-35," "36-45," "46-55," and "56+." This categorization aims to reflect a diverse demographic interest in the topic.
- **InterestLevel**: An indicator of the query's implied level of concern or urgency regarding the topic, with possible values of "Low," "Medium," and "High."

Table 3.7 presents various diseases among residents of different homes, who seek

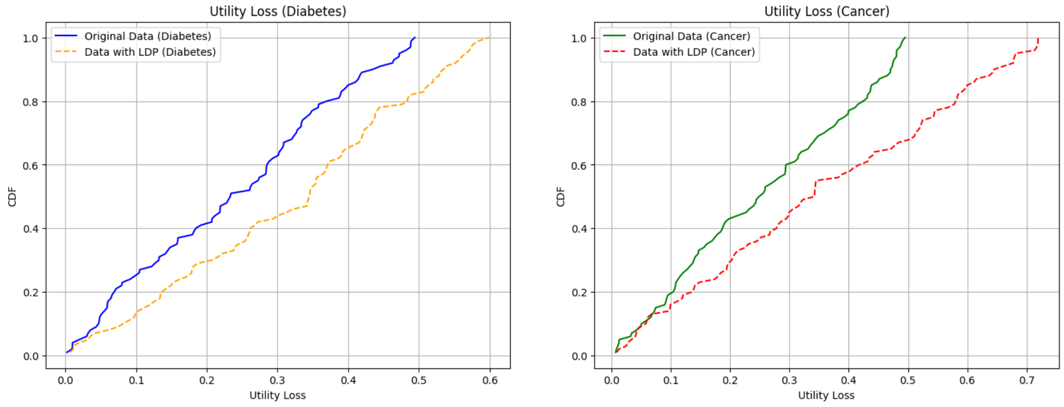
Table 3.7 : Datasets used

	Search queries data related to diseases	**Data usage of energy Appliances**
Number of entries (E)	2000	45 (Total Appliances)
Number of Users (U)	45	30 (Used Appliances)
Number of Applications	10	-
	E¿100	E ¿= 15 and E ¡= 20
Sample data	1200 (E), 30(U)	22 energy appliances used in homes

to collect information on these diseases. However, residents are unwilling to share or reveal any health information to outsiders, as this information is sensitive and poses a high risk. Unauthorized individuals accessing or modifying the queries in the data of some homes could potentially discover a specific resident's disease status.

Ethical Considerations and Data Privacy Given the sensitive nature of health-related data, we opted to generate a synthetic dataset to avoid any privacy concerns associated with using real user data. The dataset was designed to mimic realistic search patterns and demographics without correlating to any identifiable individuals or actual search queries. This approach allowed us to conduct our research with a high degree of ethical integrity, ensuring that our findings are applicable to real-world scenarios without compromising individual privacy.

Data Generation Tools The dataset was created using Python, leveraging libraries such as Pandas for data manipulation, NumPy for numerical operations, and Faker for generating realistic timestamps. This programmatic approach allowed for the controlled creation of data, ensuring consistency and reproducibility in our research methodology.



(a) (b)

Figure 3.4 : (a) Utility Loss in Diabetes Data (b) Utility Loss in Cancer Data

3.2.5.2 Evaluation methodology

This synthetic dataset served as the foundation for evaluating the effectiveness and efficiency of our proposed privacy-preserving methods against various privacy risks and adversarial attacks. By simulating realistic scenarios, we were able to derive valuable insights into the practical application of Local Differential Privacy (LDP) and obfuscation techniques, contributing significantly to the field of smart home data privacy.

Experimental Design and Outcomes Our experiments were structured to measure the effectiveness of the Local Differential Privacy (LDP) technique in obfuscating sensitive information contained within the datasets. The key metrics for evaluation included utility loss and privacy risk, with the aim of achieving a minimal impact on data utility while maximizing privacy protection.

We applied an adversarial-resistant obfuscation method to the datasets, comparing the utility and privacy risk of the actual versus obfuscated data. Our analysis revealed that while some obfuscated data instances achieved zero privacy risk with minimal utility loss, others resulted in significant deviations from the original data's

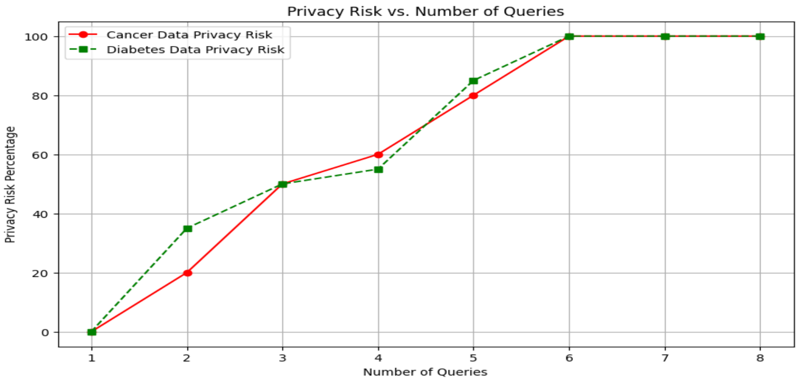


Figure 3.5 : Average Privacy Risk with increasing number of queries

meaning.

Figure 3.4a presents a comparison between the distribution of utility loss in diabetes data with and without the application of Local Differential Privacy (LDP). The utility loss for the original dataset is calculated, sorted, and then plotted to create a cumulative distribution function (CDF), which shows the likelihood of utility loss at various levels within the dataset.

The LDP dataset, in comparison, displays a broader spread of utility loss. This is due to the introduction of noise, which is necessary for enhancing data privacy but results in an increased loss of data utility. The corresponding CDF for the LDP dataset is thus shifted to indicate higher utility loss across the data points. The graph shows that after applying LDP, the utility loss is, on average, 20% greater than in the original dataset.

Similarly, Figure 3.4b assesses utility loss in cancer data. The CDF for the original cancer data set shows the probability of utility loss before privacy measures are applied. After applying LDP, the cancer data exhibits a greater increase in utility loss compared to the diabetes data post-LDP application, which is reflected in the CDF's sharper rise. This signifies a higher sensitivity to LDP's noise addition in cancer data, which necessitates a stronger approach to privacy protection.

The CDFs in both figures allow us to see how utility loss is distributed across the datasets and reveal the impact of LDP on the data. They show that while LDP can successfully increase privacy, it also has the potential to significantly reduce the clarity or usefulness of the original data.

Home residents add data to examine about certain diseases on internet. Then after searching six or more queries, the home residents notice that the privacy risk percentage gets high to 100% as shown in Figure 3.5. It shows that by adding different number of queries, the privacy risk gets high and it reaches to 100% after adding five or more queries.

The experiments conducted offer valuable insights into the practical application of LDP and obfuscation techniques for smart home data privacy. Our findings underscore the importance of carefully balancing privacy protection with data utility, suggesting that effective privacy-enhancing methods can significantly reduce privacy risks with minimal impact on the usefulness of the data.

Limitations and Future Directions While the synthetic datasets employed in our study provide a basis for evaluating our proposed methods, future research may explore the application of these techniques to real-world data collected from actual smart home environments. This would further validate the efficacy and applicability of our approaches in practical settings.

3.2.6 Summary

In Section 3.2, we employ the Local Differential Privacy (LDP) technique and propose a framework for securing data collection in smart homes based on the k-Anonymity Randomized Response (k-RR) algorithm. Although the literature contains numerous studies on obfuscation methods addressing the privacy risks associated with internet data entries, these approaches tend to be specific to particular data types and do not universally apply. Additionally, they often neglect obfuscating high-risk data using semantically similar information. Moreover, adversarial machine-learning techniques have yet to be thoroughly explored in the context of home data obfuscation. To address the limitations of existing methodologies, we propose a privacy-aware data obfuscation approach in our study. Through experiments utilizing home data, our results demonstrate the effectiveness of the proposed method in evaluating the privacy risk of obfuscated and original high-risk home data. In future research, we aim to expand the applicability of our proposed scheme to additional home datasets, such as smart meter data, for monitoring residential electricity consumption. Furthermore, we envision adapting our obfuscation method into a user-centric application, potentially a browser plug-in, to enhance individual privacy protections.

Chapter 4

FedBlockHealth: A Synergistic Approach to Privacy and Security in IoT-Enabled Healthcare through Federated Learning and Blockchain

This chapter introduces **FedBlockHealth**, a novel hybrid approach by combining federated learning and blockchain technology to provide a secured and privacy-preserved solution for IoT-enabled healthcare applications. Our approach leverages a public-key cryptosystem that provides semantic security for local model updates, while blockchain technology ensures the integrity of these updates and enforces access control and accountability. The federated learning process enables a secure model aggregation without sharing sensitive patient data. We implement and evaluate our proposed framework using EMNIST datasets, demonstrating its effectiveness in preserving data privacy and security while maintaining computational efficiency. The results suggest that our hybrid approach can significantly enhance the development of secure and privacy-preserved IoT-enabled healthcare applications, offering a promising direction for future research in this field. This work part of our work published in the *IEEE Globecomm 2023* [132].

4.1 Federated Learning and Blockchain Integration for Secure IoT-Enabled Healthcare

In healthcare, Internet of Things (IoT) devices like wearables, sensors, and medical equipment have transformed applications and services, enabling remote monitoring, diagnostics, and personalized treatments [260]. For effective healthcare, IoT devices must be reliable and accurate, as inaccuracies could result in misdiagnosis or improper treatment. The sensitive patient data collected by IoT devices is vulnerable to various cyber attacks. Thus, robust security measures are essential to protect patient privacy and ensure safety. Regulatory requirements, such as HIPAA and GDPR, further emphasize the need for robust solutions [261].

Traditional centralized machine learning approaches have various drawbacks, including higher communication costs, battery consumption, and potential security risks [262]. Federated Learning (FL), a distributed machine learning approach, has emerged as an alternative that enhances user privacy by training models over remote devices or data centers without sharing the raw data [263]. However, FL is vulnerable to poisoning attacks, and attackers can recover data from gradients [127,264]. Integrating FL with blockchain has been explored in healthcare [265,266], but these studies lack comprehensive solutions addressing privacy and security while maintaining computational efficiency.

FL faces security vulnerabilities, model inconsistency and inaccuracy, limited network bandwidth, and data imbalances between clients [267]. We propose FedBlockHealth, a novel hybrid approach combining FL and blockchain (BC) technology for secure and privacy-preserved IoT-enabled healthcare applications to address these vulnerabilities. Our approach leverages a public-key cryptosystem for local model update semantic security and BC for decentralized data storage, management, and access control. FL ensures secure model aggregation without sharing sensitive patient data, maintaining privacy, security, and computational efficiency.

Research has addressed FL challenges, such as non-IID data distributions [268], global model convergence [269], and the client device and data heterogeneity [270]. Differential privacy has been introduced [271], and applied to FL [272]. Blockchain has been used to secure patient data [273] but with centralized machine learning for disease detection.

Our FedBlockHealth framework offers vital contributions to privacy-preserving IoT-enabled healthcare. These contributions include

- **Hybrid Approach:** An Algorithm is proposed to combine FL and BC technology to address privacy and security challenges in IoT-enabled healthcare scenarios. Smart contracts are designed for all clients to data on BC. This hybrid approach ensures the integrity and privacy of patient data while maintaining computational efficiency.

- **Semantic Security:** To secure the communication between clients and server, the Elgamal public-key cryptosystem is employed in our framework to provide semantic security for local model updates and ensures that sensitive patient information remains private during the FL process.

- **Performance Evaluation:** Our proposed CNN framework for FL is evaluated using the EMNIST dataset. The approach maintains privacy and security while ensuring computational efficiency. Results demonstrate its effectiveness compared to traditional ANN and CNN models by achieving 99.9% accuracy and a loss of 0.01%. This is the result of reducing the number of layers and adding a batch Normalization layer, which alternatively decreased complexity and the use of Feedforward and Backpropagation approach.

- **Scalability and Applicability:** Our framework FedBlockHleath is designed to be scalable and applicable to a wide range of healthcare scenarios, paving the way for future research and development in secure and privacy-preserving IoT-enabled healthcare applications.

In this chapter, we discuss the problem statement and system architecture in Section 4.2, followed by the methodology in Section 4.3. Experimental results and analysis are presented in Section 4.4, and finally, we conclude the study and suggest future research in Section‘4.5.

4.2 FedBlockHealth: A Blockchain-Integrated Federated Learning System

To circumvent the problem of data privacy and security, in this paper, we proposed the FedBlockHealth model illustrated in Fig. 4.1, in which patient data is received through IoT devices and stored in the hospital database represented by the client. Each client has a locally trained CNN model shared by the global server. Each client trains independently, and the updated weights, encrypted through the EL-Gammal approach, are shared with the global server for aggregation. On the other hand, each client sends model updates to the BC for data storage. Note that a smart contract is designed for each client before the transaction in model updates are forwarded to the transaction pool for validation. After completing the validation process, the system stores the transaction in blocks, and authorized users from the BC network can only access the data.

4.2.1 Detailed System Architecture

The proposed system architecture, FedBlockHealth, comprises a Key Generation Centre (KGC), a server, and multiple participants.

4.2.1.1 Key Generation Centre

The KGC is a trusted entity responsible for system setup, public parameter generation, and private key distribution to each participant and the server. The KGC is fully trusted and does not collide with any other entities.

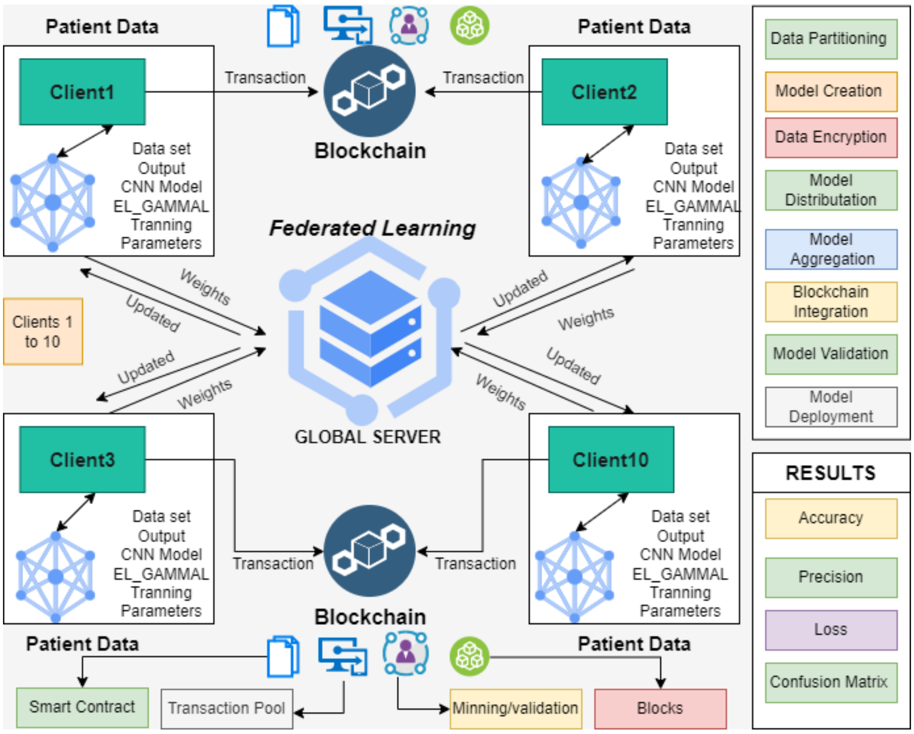


Figure 4.1 : The proposed FedBlockHealth model, where clients data are stored in blockchain and local model weights are shared with global server.

4.2.1.2 Server

The server is a shared location for securely aggregating encrypted local gradients from all participating clients and distributing updated global parameters. In encrypted computing techniques, an adversarial setting is often assumed, where all entities, except the KGC, follow the protocol precisely while attempting to infer sensitive data from the training data.

4.2.1.3 Clients

Each client represents a hospital that possesses a health-related dataset and a copy of the trained model shared by the global server. During learning, clients train their local models on their private datasets and share local gradients/weights with the server. Malicious clients may attempt to communicate with the server for nefarious purposes, necessitating measures to prevent such activities and protect the data privacy of legitimate clients. Hence, the EL-Gammal encryption approach is used to secure communication between clients and the global server. On the other hand, smart contracts are created for each client to communicate with the BC network. Figure 4.1 illustrates the proposed system architecture.

4.2.1.4 Federated Learning Process

Federated learning is a distributed machine learning technique allowing multiple parties to train a model collaboratively without sharing their raw data. In our system model, we assume that multiple healthcare providers (clients) are participating in the FL process to improve the accuracy of the Convolutional Neural Network (CNN) model. Each healthcare provider maintains their datasets of medical images and trains a local CNN model using FL. The local model weights are encrypted using an ElGamal cryptosystem before being sent to the central server. The central server aggregates the encrypted model weights and updates the global CNN model. The updated global model weights are then sent back to the clients for further training. The process continues iteratively until the model converges to a satisfactory accuracy level as reflected in Algorithm 4.4. FL allows stakeholders to improve their models by leveraging the network's collective intelligence without sharing their personal data.

4.2.1.5 Blockchain Network Integration

The proposed system uses BC technology to manage access control and provide an immutable record of the training process in FL in healthcare. The system initially designs smart contracts for each client and then transfers the model updates to a smart contract for conversion to hash as shown in Algorithm 4.1. Afterward, the system forwards the hash to the transaction pool, and the miners pick it for mining. Once the miners have picked the hash, they create blocks. The authorized clients can retrieve the data stored in blocks through their smart contract, as depicted in Algorithm 4.3. This approach enables the system to manage access to the distributed CNN model transparently and securely while ensuring the integrity of the training process.

4.2.2 Integration of Federated Learning with Blockchain

We can transform healthcare data management, analysis, and use by integrating BC technology and FL. Using BC technology, we can manage patient data securely and transparently while employing FL to develop predictive models for disease diagnosis or personalized treatment plans. We can achieve the integration of BC technology and FL in healthcare through the following steps:

1. Data partitioning: The healthcare data is partitioned among multiple hospitals or healthcare institutions to ensure data privacy and security. Each hospital holds its data locally.

2. Model creation: A central server creates a CNN model, which trains the data from all the participating hospitals through the federated averaging algorithm presented in Algorithm 4.4.

3. Data encryption: The hospital data is encrypted using a cryptographic algorithm ElGamal discussed in the following subsection, adding an extra layer of security and privacy.

4. Model distribution: The central server receives the encrypted data and distributes the CNN model to all participating hospitals.

5. Local model training: Each hospital trains the CNN model on their local encrypted data using FL, which involves multiple rounds of model training and aggregation of model updates.

6. Model aggregation: The hospitals send their encrypted model updates to the central server, which aggregates the updates to create a global model as presented in Algorithm 4.4.

7. Blockchain integration: The updated models of clients are stored on a BC, ensuring the model updates' transparency and immutability.

8. Model validation: A third-party auditor validates the global model to confirm that it meets the necessary accuracy and security standards.

9. Model deployment: The validated global model is then deployed back to the participating hospitals for local inference on new data.

Algorithm 4.1 Smart Contract

```
INPUT Client Registration
if Registration == successful then
    Check data from the Global server
else
    Register client as a New Client
    U ← Client
    Store Data on Blockchain
    Encrypt data Using Sha256 Algo
    OUTPUT generate Application Binary Interface of Contract
    generate Byte code of Contract
    Decrypt data Using Sha256 Algorithm
end if
```

4.2.3 Feedforward and Backpropagation in Distributed Learning

Clients discretize their model updates, add discrete Gaussian noise, and submit them for modular secure summation. This comprehensive end-to-end system

Algorithm 4.2 Operation of Blockchain

```
INPUT Client Data
Client Data
Data added to Smart Contract
Data Converted using SHA256 Hashing Algorithm
Data transfer to transaction Pool
Minners minne the transaction
Transaction are converted into blocks
OUPUT Client data    ▷ Only Authorized person access the data
```

employs the ElGamal encryption scheme. To perform a forward pass through the network, we use the following iterative formula to compute each neuron in the subsequent layer [274]:

$$a^l = \sigma \times (W \times a^{(l-1)} + b) \tag{4.1}$$

Backpropagation efficiently computes gradients, and the optimizer uses these gradients to train the neural network:

$$w^{t+1} = w^t - n \times \nabla_w \times L(D^t, w^t) \tag{4.2}$$

The equation represents the Feedforward function $f(x, w) = y$, where w is the parameter vector, and the training dataset is $D = \{(x_i, y_i); i \in L\}$. L represents the loss function, and backpropagation is defined as:

$$\frac{1}{|D|} \sum_{(x_i, y_i) \in D} \ell(y_i, f(x_i, w)) \tag{4.3}$$

Training continues until the loss function reaches an optimal minimum value. Following this approach, the proposed system architecture effectively addresses distributed learning challenges, ensuring data privacy and successfully training a high-quality centralized model.

Algorithm 4.3 Blockchain Integration with Federated Learning

```
Input: Training dataset, Test dataset, EMNIST images
Output: Trained and secured data
Initialization:
Initialize the blockchain network.
Create a smart contract for the FL Server and Clients.
Client-Side Operations:
for each client $U$ in the pool do
    Connect to the blockchain network.
    Register $U$ with the smart contract.
    Load the pre-trained CNN model weights.
    Execute the Federated Learning Algorithm on $U$'s data.
end for
Server-Side Operations:
Connect to the blockchain network.
Register as the FL server with the smart contract.
Collect local gradients from all clients.
Aggregate the gradients using the Federated Learning Algorithm.
Blockchain Operations:
Record each client's model update transactions on the blockchain.
Ensure all transactions are tamper-proof.
Guarantee transparency and accountability in the Federated Learning process.
```

4.3 Methodology

In order to enhance data privacy, this study investigates the performance of FL on the Extended Modified National Institute of Standards and Technology (EMNIST) datasets by utilizing a Convolutional Neural Network (CNN). FL on EMNIST datasets using a CNN can address the challenge by training the model on local data held on different healthcare devices while keeping the data decentralized and preserving the privacy of individual patients. The architecture of the employed CNN comprises four convolutional layers, each succeeded by a max-pooling layer and an additional two fully connected layers within the hidden layer structure. Given the flexibility of the convolutional layer, the subsequent section presents the proposed CNN model tailored explicitly for FL applications. Only retrain the pre-trained model and the fully connected layers after using previously trained convolutional layers. We examined the performance of FL on the EMNIST datasets using a CNN.

In order to improve the accuracy of our model, we have introduced two additional hidden layers, which enable the extraction of more complex features from the input data. We have utilized the stochastic gradient descent (SGD) optimizer to optimize the model's performance further. The SGD optimizer iteratively refines the model's parameters to minimize the discrepancy between the predicted and actual outputs. This is accomplished by computing the gradient of the loss function with respect to the parameters and updating them in the opposite direction of the gradient, ultimately determining the optimal parameters for the model. As a result, the model can more accurately predict the output. Furthermore, securing the communication between clients and the global server is vitally important; therefore, we use the El-Gamal Multiplicative Cryptosystem approach. El-Gamal Multiplicative Cryptosystem is preferred over other techniques because it provides both confidentiality and data integrity during transmission. Unlike other techniques, it simultaneously

Algorithm 4.4 Federated Learning for CNN

```
Initialize: Training dataset ($D_T$, $D'_T$), libraries
Input: EMNIST images
Output: Trained and secured data
Initialize blockchain, import necessary libraries
Upload $D_T$, $D'_T$ as CSV
Create CNN Model
for each client $u$ do
    Generate key pair for $u$, store public key on Blockchain
end for
Import federated learning model ($tff$)
for iteration $n = 1 : N$ do
    for image-training step $l = 1 : L$ do
        for pixel iteration $k = 1 : K$ do
            Update pixel using Sigmoid
        end for
        Update visited pixels using Relu
    end for
    for client $u$ do
        Compute client contribution
    end for
    Distribute updates among clients
end for
Accuracy Check:
for epoch do
Parameters: $n = 70$, batch= 10, clients= 10, buffer= 100, prefetch= 10
end for
```

encrypts plaintext and signature generation, ensuring that the data remains secure and unaltered during transmission. Additionally, ElGamal encryption relies on mathematical problems that are computationally difficult to solve, making it a more secure approach to encryption [275].

4.3.1 El-Gamal Multiplicative Cryptosystem

ElGamal encryption is a public-key cryptography algorithm that is based on the Diffie-Hellman key exchange [274]. In the context of federated learning, it can be used to encrypt the model parameters before they are sent from the client devices to the central server for aggregation. This helps to ensure that the model parameters remain secure and confidential during the transmission.

The ElGamal encryption algorithm comprises three parts:

- **Key generation**: In this step, a user generates a public-private key pair. The public key encrypts, while the private key decrypts.
- **Encryption:** To encrypt the model parameters, the client device selects a random value known as the session key. The client uses the session key to encrypt the model parameters with ElGamal encryption. Then, the encrypted session key and model parameters are sent to the central server for aggregation.
- **Decryption**: The central server uses its private key to decrypt the encrypted session key and the encrypted model parameters. The decrypted session key decrypts the encrypted model parameters.

The security of the ElGamal encryption algorithm relies on the difficulty of the Discrete Logarithm Problem (DLP), which involves finding the exponent x in the equation $g^x \bmod p = h$. This problem is computationally complex, making ElGamal encryption secure against attacks from hackers. In summary, using the ElGamal cryptosystem in federated learning with the CNN model adds a security layer to the model parameters during transmission. This ensures the privacy and confidentiality of the model parameters, even when transmitted over a public network. The El-Gamal Multiplicative Cryptosystem Algorithm is presented in 4.5, while its mathematical proof will appear in the extended version of this model.

Algorithm 4.5 Pseudo-code of the ElGamal technique

```
**Input:** Exponential ElGamal
**Output:** Messages are encoded by exponentiation
Give Value $v_1 = 4, v_2 = 5$
$v_1 \leftarrow$ generator.selfApply(4)
$v_2 \leftarrow$ generator.selfApply(5)
$c_1 \leftarrow$ ElGamal.encrypt(Public Key, $v_1$)
$c_2 \leftarrow$ ElGamal.encrypt(Public Key, $v_2$)
Combine $\leftarrow c_1$.apply($c_2$)
Results $\leftarrow$ ElGamal.decrypt(Private Key, Combine)
Calculate $v = v_1 \cdot v_2$ in message space:
          generator.selfApply($v = v_1 \cdot v_2$)
Print results
End
```

4.4 Performance Evaluation and Simulation

This section aims to evaluate the performance of the proposed FL system using the EMNIST datasets with a Convolutional Neural Network (CNN). We compare the privacy-enhanced system to the non-private baseline and discuss the trade-offs between privacy, model complexity, and accuracy.

Table 4.1 : Model details and performance comparison

	CNN(base)	CNN(proposed)	ANN(proposed)
Training data set	60,000	71,039	71,039
Testing dataset	10,000	14,799	14,799
Validation dataset	-	17,760	17,760
Model	CNN	CNN	ANN
Accuracy Level	99.03%	99.99%	68.91%
Epoch	150	40	70

4.4.1 Dataset and Model Architecture

We use the EMNIST dataset, which consists of 28x28 gray-scale images of handwritten digits. We divide the dataset into 71,039 training samples, 14,799 testing samples, and 17,760 validation samples. We further partition the data among ten clients for distributed training.

The CNN model used for evaluation consists of four convolutional layers, max-pooling layers, two fully connected layers and a batch normalization layer. The convolutional layers extract essential features from the input images, while the deeper layers identify more complex patterns. Similarly, we use flattened and dense layers to convert the output of the convolutional layer into a single-dimensional vector and perform classification, respectively.

4.4.2 Training and Evaluation

During the training phase, the clients train their local models on their respective datasets and share the local gradients with the central server. The server aggregates the gradients, updates the global model, and broadcasts it back to the clients. This process repeats until the loss function converges to an optimal value. Figures 4.2 and

4.3 show the accuracy and loss graphs of the CNN model applied to the EMNIST dataset. After 70 epochs, we achieved an accuracy of 95.57% and a loss value of 1.4.

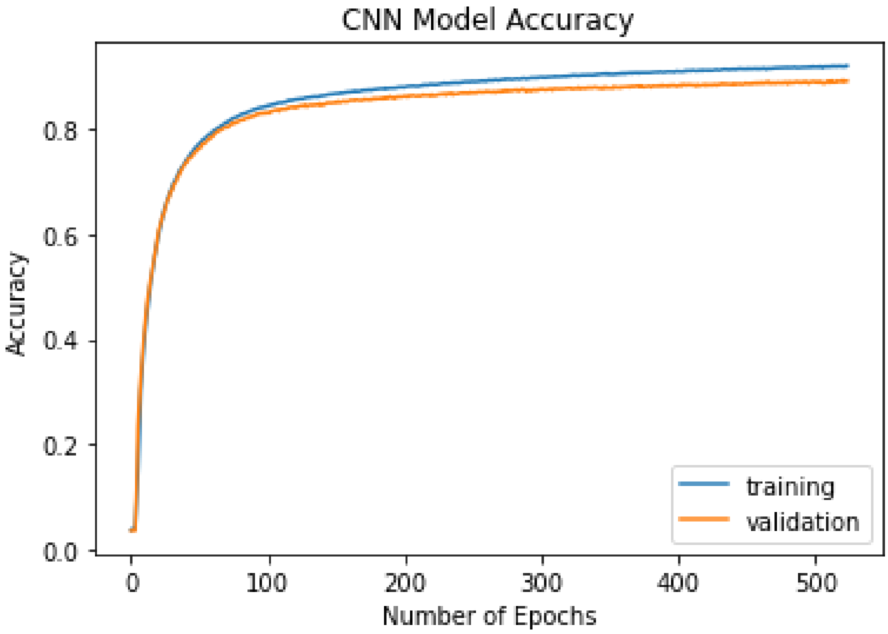


Figure 4.2 : Accuracy of FedBlockHealth based CNN Model.

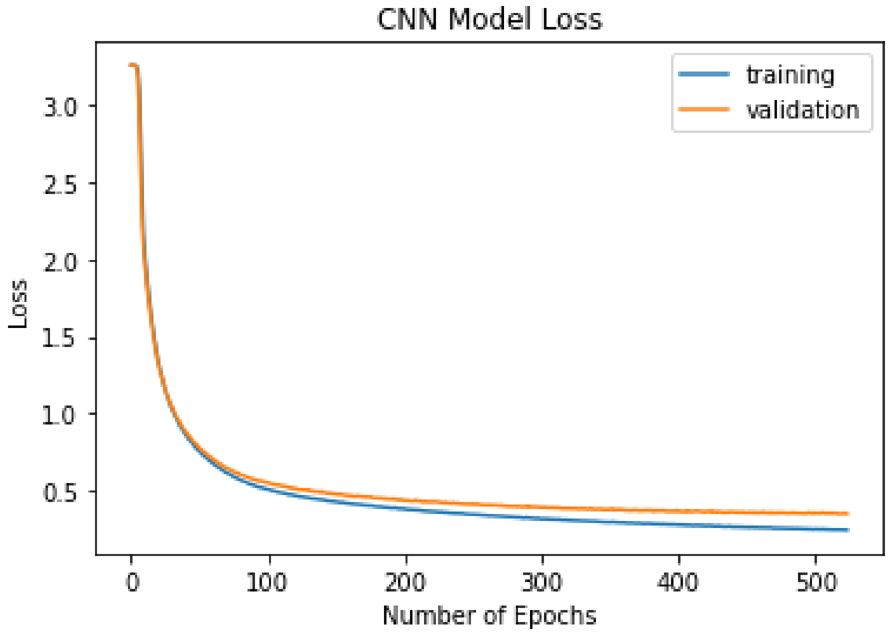


Figure 4.3 : Loss of FedBlockHealth based CNN Model.

4.4.3 Comparison with Baseline and Alternative Models

We compare the performance of our proposed system with the non-private baseline model and an alternative Artificial Neural Network (ANN) model. The baseline CNN model achieved an accuracy of 99.03% after 150 epochs, while our privacy-enhanced CNN model reached an accuracy of 99.99% after 40 epochs. The ANN model, on the other hand, achieved an accuracy of 68.91% after 70 epochs. This is due to the reduced complexity of the model by limiting the hidden layers, using the batch norm layer for faster training, and using the Feedforward and Backpropagation approach. The performance is reflected in Table 4.1 summarizes the model details and performance comparisons.

The results indicate that the proposed privacy-enhanced FL system with a CNN model achieves competitive performance compared to the non-private baseline. Although the accuracy is slightly lower, the model ensures privacy preservation and employs a less complex encryption technique. In contrast, the ANN model performs significantly worse, demonstrating the importance of using appropriate model architectures for the specific problem domain.

4.5 Summary

This study presented a privacy-enhanced federated learning (FL) system, incorporating blockchain and smart contracts, using a convolutional neural network (CNN) for distributed training on the EMNIST dataset. The system effectively balances data privacy preservation and model performance, making it a suitable solution for sensitive data tasks in IoT-enabled healthcare applications. Our evaluation demonstrates that the privacy-enhanced CNN model achieves 99.99% accuracy. We employed ElGamal encryption to maintain anonymity while enabling computation in the ciphertext space. This method ensures privacy preservation and utilizes a less complex encryption technique. Additionally, integrating blockchain technology and smart contracts enhance the integrity and security of the system. Future work will involve using high-dimensional datasets and exploring more complex neural network models to enhance accuracy and efficiency in privacy-preserving IoT-enabled healthcare applications.

Chapter 5

Web-based Chatbots as End-user Systems: Security and Privacy Issues

Websites are among the most common and widely used platforms among the various types of end-user systems. They are the digital storefronts for businesses, the portals for government services, and the hubs for social interaction. As such, they are rich with user data and interactions, making them attractive targets for cyber threats.

Within the ecosystem of a website, web-based chatbots have emerged as a crucial component. These chatbots, often embedded as an iFrame within the website, provide services from customer support to sales and marketing. They have become increasingly popular due to their ability to provide immediate responses, increase sales, and offer insight into customer behaviour.

However, despite their benefits, web-based chatbots have yet to be extensively scrutinized from a security and privacy perspective. This lack of focused research is concerning, given that these chatbots, like any other component of a website, have the potential to be exploited for malicious purposes. Specifically, issues such as the use of insecure protocols for data transfer, and the heavy reliance on tracking cookies for advertisement purposes, pose significant threats to user privacy and security. Therefore, this chapter aims to delve into these and other security and privacy issues of web-based chatbots, shedding light on this under-researched area and contributing to the broader discourse on end-user system security.

5.1 Introduction

Web-based chatbots provide website owners with the benefits of increased sales, immediate response to their customers, and insight into customer behaviour. While Web-based chatbots are getting popular, they have not received much scrutiny from security researchers. The benefits to owners come at the cost of users' privacy and security. Vulnerabilities, such as tracking cookies and third-party domains, can be hidden in the chatbot's iFrame script. This chapter presents a large-scale analysis of five Web-based chatbots among the top 1-million Alexa websites. Through our crawler tool, we identify the presence of chatbots in these 1-million websites. We discover that 13,392 out of the top 1- million Alexa websites (1.58%) use one of the five analysed chatbots. Our analysis reveals that the top 300k Alexa ranking websites are dominated by `Intercom` chatbots that embed the least number of third-party domains. `LiveChat` chatbots dominate the remaining websites and embed the highest samples of third-party domains. We also find that 721 (5.38%) web-based chatbots use insecure protocols to transfer users' chats in plain text. Furthermore, some chatbots heavily rely on cookies for tracking and advertisement purposes. More than two-thirds (68.92%) of the identified cookies in chatbot iFrames are used for ads and tracking users. Our results show that, despite the promises for privacy, security, and anonymity given by most websites, millions of users may unknowingly be subject to poor security guarantees by chatbot service providers.

A Web-based chatbot (or bot) is a computer program interacting with users via a conversational user interface that simulates a conversation with a human user via textual methods [276]. Web-based chatbots offer improved customer services and efficiently manage human resources [277, 278]. For example, a website owner performs customer acquisition tasks (such as new customer queries or after-sales services) through customer service (or sales and marketing) personnel. As the business gets bigger and busier, the traditional way of interacting with online customers gets choked up, resulting in an increased waiting queue. Besides, the customer service representative may not be available around the clock. Web-based chatbot provides a website owner with the benefits of increased sales, immediate response to their customers' queries and insights into customers' behaviours. While Web-based chatbots are getting popular, they have not received much scrutiny from security researchers. The benefits of chatbots can come at the cost of privacy and security threats. Third-party domains and cookies inherit these threats, which might be built into the script. These domains and cookies can be used to track users and provide personalised advertisements. There has been a plethora of work done based on the security and privacy issues of a complete website [220, 279, 280]. However, to our knowledge, no research study focuses explicitly on Web-based chatbots' privacy and security issues.

While Web-based chatbots are getting popular and come with several benefits, as mentioned above, their advantages inherit several disadvantages. *Firstly*, consumers are concerned about their privacy and security [277]. Despite the remarkable improvements in Web-based chatbots being able to mimic a human conversation, they are vulnerable to the Reconnaissance, and Man-in-the-Middle attacks [281]. *Secondly*, since the chatbot is a computer program, it does not have its own identity or emotions like an actual human. Customers often tend to make connections during conversations, which is lacking when engaging with chatbots. The lack of personality in chatbots and their inability to make an emotional connection is a concern for some customers. *Finally*, a Web-based chatbot is still in its infancy since natural language processing is not the core competency in chatbot applications and is still in the development phase [277]. Web-based chatbots are prone to common communication errors; therefore, companies and organisations are cautious in using them to avoid brand damage.

Although several studies have taken place to study chatbots in general, none of them covers their security and privacy comprehensively. There has been extensive research on the security and privacy issues of websites. However, to the best of our knowledge, we did not find any study that focuses on the iFrame component of the Web-based chatbot for the same issues. Despite the assurances for privacy, security, and anonymity given by the websites and privacy policies, users are victims of personally identifiable information (PII) leakages [282]. Similarly, by using chatbot services, users may inadvertently be exposed to privacy and security risks [220].

In summary this chapter investigates following research aspects:

1. We present the first large-scale study of security and privacy issues in chatbots on Alexa top 1-million popular websites [283]. We detect 13,392 (1.58%) websites leveraging web chatbots for customers' interaction. We release our data and scripts for future research.

2. We analyse the 13,392 (1.58%) websites for the type of chatbots and analyse the coverage of the detected chatbots. We find that 21.78% of the chatbot websites belong to the non-IT business category, while the percentage of Information Technology (IT) chatbot websites is 16.16%, and shopping with 5.89% is the third most dominant category. We also analyse the security and privacy issues of our dataset chatbot websites. We explore the chatbot websites and find that 5.38% of them are still using the insecure HTTP protocol, where an alarming 12.9% of the websites ranking ¿500k still transfer their visitors' data in plaint-text. This result shows that non-IT business, IT and shopping websites are more vulnerable among the most popular websites than other categories.

3. Our analysis illuminates that chatbots have a disproportionate use of cookies for tracking and *essential* or *useful* functionalities. We discover 5,396 cookies

in 2,110 websites leveraging `Drift` chatbot. 5,113 (94.62%) and 283 (5.24%) of the cookies are used for Tracking and essential functionalities, respectively. On the other hand, 2,185 websites rely on `Hubspot` for the provision of chat services via a total number of 15,829 unique cookies with 79.35% (12561) for tracking, while the rest are essential cookies.

4. We identify the top 10 third-party domains embedded in the iFrames of each web-based chatbot. The most common third-parties are well-known operators, for example, googleapis, cloudflare, w3, and facebook. These operators are imported by 39.67% (5361), 15.43% (2085), 6.1% (822), and 3.35% (453) web-based chatbots, respectively.

In this chapter, we extensively employ various general terms in the context of our research. To ensure a comprehensive understanding, we initially present an introduction to the general concepts and terms that are utilized throughout the chapter.

Advertising and tracking domain: The *advertising and tracking* domain (or tracker) is the URL of an entity embedded in a web page. The purpose of a tracker is to re-identify a user's visit on the web page again for loading custom themes or analytics (*first-party* tracking) or to re-identify a given user across different websites for building the user's browsing profile or providing personalised advertisements (*third-party* tracking).

iFrame: An iFrame or inline Frame is an HTML document embedded within an HTML web page. The purpose of an iFrame is to display embedded HTML contents from a different web page into the current web page. The contents of iFrames can be videos, maps, advertisements, chatbot services, and tracking components like cookies and JavaScript codes. Hence, besides providing utilities and services, iFrames can also be used for third-party tracking.

Cookie: A cookie (or HTTP cookie) is a text file stored on the user's device by the web browser. The content of a cookie is in plain text format. A cookie is generated by the web server (of a web page) and is sent back from the user's device to the web server at each subsequent visit by the user. A cookie can store shopping carts, theme preferences of the user, or the user's authentication status. Cookies generated by third-parties via iFrames can be used for third-party tracking. Section 5.3.2 discuss different types of cookies in detail.

The rest of this chapter is organised as follows: In Section 5.2, We present our methodology (Figure 5.1) for web-based chatbot detection and data collection. In Section 5.3, we analyse our chatbots in the top 1-million Alexa websites and present our findings, such as the presence of chatbots on websites, tracking cookies, and third-party domains. Section 5.4 presents the related work while we conclude our work by presenting the gaps with some future directions in Section 5.5.

5.2 Chatbot Detection Methodology and Dataset

We begin by presenting our methodology, over-viewed in Figure 5.1 for detecting chatbots employed in the top 1-million Alexa websites. We then characterise our dataset.

5.2.1 Discovering Chatbots

Using Selenium Web Driver, we develop an automated web crawler to automate analysed websites' visiting and rendering process. We implement a crawler framework to increase our chatbot coverage and maximise the number of detected chatbots. We begin by discovering web-based chatbot services on the Alexa top 1-million websites. To this end, we find the difference between a normal website and the website with a chatbot service. We manually inspect the first Alexa top 100 websites for *potential* web chatbot services. Typically, websites implement chatbot

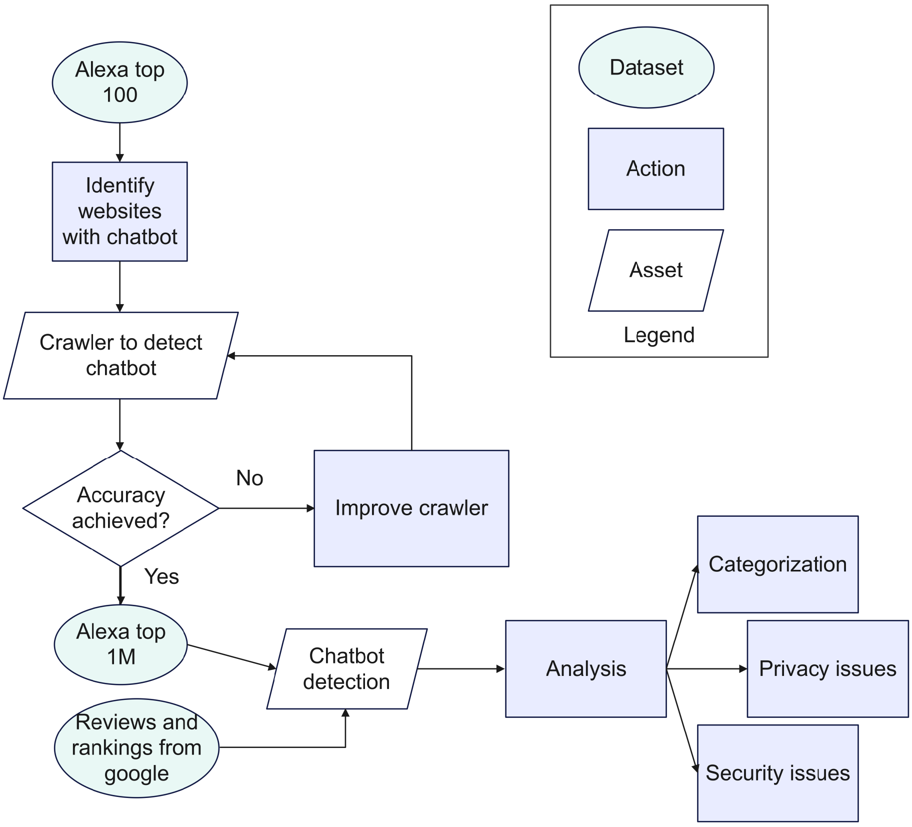


Figure 5.1 : Overview of our crawling and analysis methodology: We manually inspect the top 100 Alexa websites for chatbots to identify chatbot services and to construct keywords list for automatic detection of chatbots in the top 1-million Alexa websites. We then perform an analysis to categorise websites and analyse security and privacy issues.

services in iFrames; therefore, we explicitly focused on the iFrame of the chatbot on these 100 websites. The keywords include: ‘*chat widget*’, *let’s chat*, *drift-widget*, ‘*chat now*’, and ‘*chatbot*’. While we acknowledge that our keywords list is not exhaustive to include chatbots on non-English language websites, we do consider our method for chatbots as a *lower-limit* on the number of chatbots on the top 1-million Alexa websites.

Next, we crawl through the chatbot websites and extract their chatbot iFrame cookies only instead of the whole website since we are specifically interested in the security and privacy issues of the web-based chatbots. We then analyse the embedded third-party domains in each of those chatbots. To extract the third-party domains, we only check the contents of the iFrame of a chatbot instead of the complete website's DOM. Overall, we find 13,392 (1.58%) chatbot websites.

Issues and Limitations. For chatbot websites, once a website renders ultimately, the chatbot icon is found at the bottom right corner of the screen. Sometimes, the chatbot is not visible on the respective website mainly due to one of the following reasons: (*i*) the chatbot is only available during specific office hours, and (*ii*) the chatbot is offline/hidden as the developers may be working on it.

5.2.2 Categorising Chatbot Websites

Next, to analyse the coverage of chatbots on various websites, we aim to categorise the Alexa top websites. There are several databases and tools available and website categories stored. However, due to its popular utility among researchers, we use crawling techniques on *Fortiguard* website classification tool [284] to gather this information. The websites that return errors while rendering in the first phase are manually labelled. This way, we label the category of each chatbot website in our dataset (13,392 websites). The top 10 categories by frequency of occurrence are depicted in Figure 5.2. These ten categories comprise 74.9% (10,028 websites) of our dataset. We find that most of the chatbot websites are used by *non-IT Business* and *IT* category websites. Although all five chatbots are prevalent, `Intercom` chatbot is the preferred choice for these two categories. We also observe that chatbots are not a popular choice among *Games*, and *Government & Legal Organizations* related website owners.

5.2.3 Dataset

We present a comprehensive analysis by breaking the dataset into parts, with each part having 10,000 websites to get an in-depth measurement of our study. Based

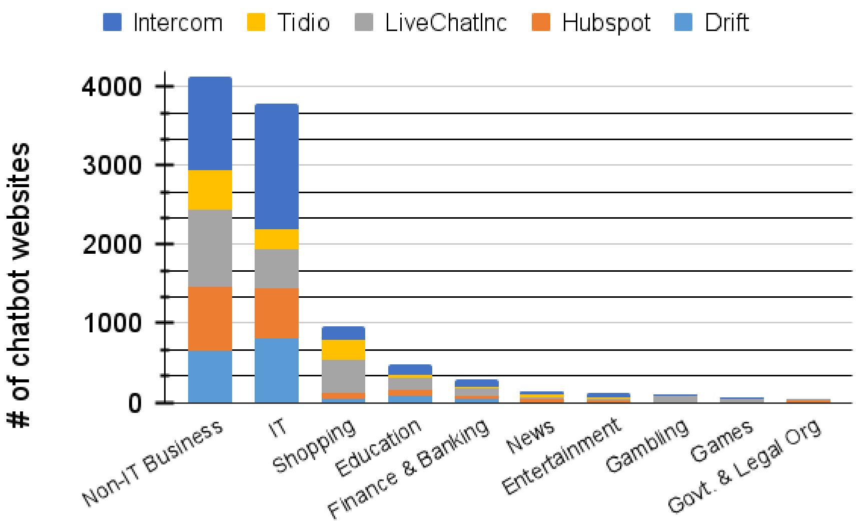


Figure 5.2 : Categories of chatbot websites in the top 1-million Alexa websites.

upon the keywords (cf. § 5.2), we run our crawler that detects chatbots on 3.5% of the analysed websites. To check the accuracy of our crawler, we manually label the first hundred Alexa ranking websites and perform manual testing on them. We learn that our model is 61% accurate. The reason is that there are several possible ways to write a website script, and using the keywords alone is not an optimum solution.

Finding a common script, or tag among all of them is not possible. However, we find some unique keywords/tags/elements. Figure 5.3 shows the iFrame of a chatbot website www.synology.com. It has a tag *id='chat-widget-container'*, which can be used to filter the `LiveChat` chatbot websites. Similarly, we select five chatbots: `LiveChat`, `Drift`, `Intercom`, `Tidio` and `Hubspot` based on their frequencies of occurrence in the top 10k Alexa ranking websites. Overall, our crawler identifies 13,392 chatbot websites from Alexa top 1-million websites.

Table 5.1 summarises our findings. We observe that the `Intercom` chatbot is the preferred choice for the most popular set of websites (top 300k) followed by `LiveChat` for the next tier of Alexa ranking websites. Overall, `Intercom` chatbot

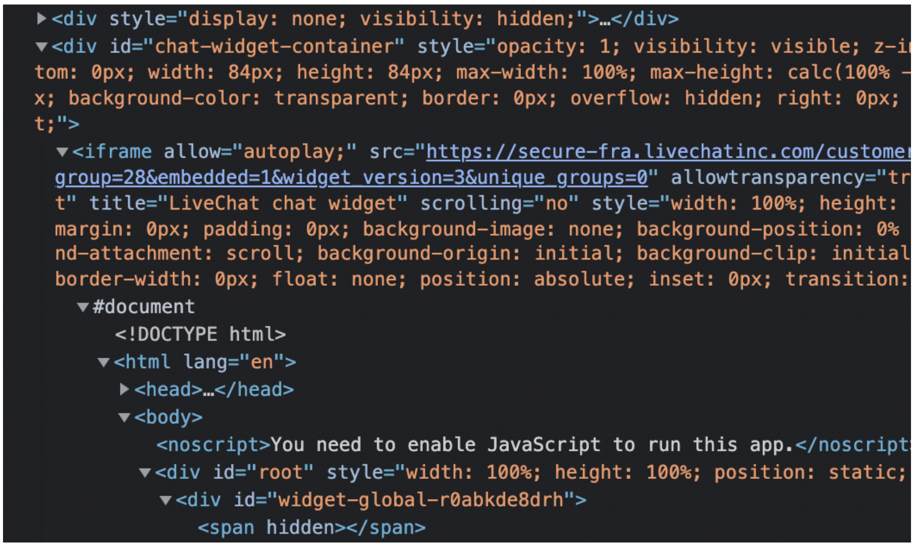
Table 5.1 : Frequency (and percentage) of chatbot services amongst the Alexa top 1-million websites. Highlighted trends show `Intercom` chatbot is the preferred choice for the most popular set of websites followed by `LiveChat` which is also the preferred choice for the next tier of popular websites.

	Chatbots					# Total (%)
Alexa Rank	**Drift**	**LiveChat**	**Hubspot**	**Tidio**	**Intercom**	
1-100K	613 (0.61%)	433 (0.43%)	205 (0.21%)	81 (0.81%)	933 (0.93%)	2,265 (2.27%)
100K-200K	451 (0.45%)	611 (0.61%)	364 (0.36%)	185 (0.19%)	749 (0.75%)	2,360 (2.36%)
200K-300K	407 (0.41%)	586 (0.59%)	388 (0.39%)	342 (0.34%)	676 (0.68%)	2,399 (2.40%)
300K-400K	295 (0.30%)	573 (0.57%)	409 (0.41%)	364 (0.36%)	527 (0.53%)	2,168 (2.17%)
400K-500K	149 (0.15%)	433 (0.43%)	303 (0.30%)	286 (0.29%)	424 (0.42%)	1,595 (1.60%)
500K-600K	65 (0.07%)	347 (0.35%)	158 (0.16%)	218 (0.29%)	272 (0.27%)	1,060 (1.04%)
600K-700K	51 (0.05%)	337 (0.34%)	138 (0.14%)	125 (0.13%)	180 (0.18%)	831 (0.83%)
700K-800K	45 (0.05%)	142 (0.14%)	70 (0.07%)	4 (0.004%)	149 (0.15%)	410 (0.41%)
$\geq$ 800K	26 (0.05%)	69 (0.15%)	67 (0.14%)	50 (0.11%)	93 (0.20%)	304 (0.64%)
Overall (1-million)	2,102 (0.25%)	3,531 (0.42%)	2,102 (0.25%)	1,655 (0.20%)	4,002 (0.47%)	**13,392 (1.58%)**

is found on 29.88% of them, `LiveChat` on 26.37%, `Drift` as well as `Hubspot` on 15.70%, and `Tidio` on 12.36% only.

Based on the above findings, in the first round, we crawl the top 10k websites and render their DOMs. After optimising our crawler, we can filter all chatbots with 100% accuracy.

We also search for the top Web-based chatbots by using different keywords over the google search. We find chatbot rankings and reviews on the websites in [285–291] (accessed in Feb 2022). We choose the top three chatbots. After selecting *MobileMonkey*, *Aivo*, and *Pandorabots* from the blogs and reviews, we run our automated scraper for the top 200k websites and find only two chatbots belonging to *MobileMonkey*, four chatbots to *Botsify*, and zero for both *Aivo* and *Pandorabots*. Therefore, due to their insignificant presence, we do not consider them in our analysis



```
▶<div style="display: none; visibility: hidden;">…</div>
▼<div id="chat-widget-container" style="opacity: 1; visibility: visible; z-i
tom: 0px; width: 84px; height: 84px; max-width: 100%; max-height: calc(100% -
x; background-color: transparent; border: 0px; overflow: hidden; right: 0px;
t;">
  ▼<iframe allow="autoplay;" src="https://secure-fra.livechatinc.com/customer
  group=28&embedded=1&widget_version=3&unique_groups=0" allowtransparency="tr
  t" title="LiveChat chat widget" scrolling="no" style="width: 100%; height:
  margin: 0px; padding: 0px; background-image: none; background-position: 0%
  nd-attachment: scroll; background-origin: initial; background-clip: initial
  border-width: 0px; float: none; position: absolute; inset: 0px; transition:
    ▼#document
       <!DOCTYPE html>
      ▼<html lang="en">
        ▶<head>…</head>
        ▼<body>
           <noscript>You need to enable JavaScript to run this app.</noscript
          ▼<div id="root" style="width: 100%; height: 100%; position: static;
            ▼<div id="widget-global-r0abkde8drh">
               <span hidden></span>
```

Figure 5.3 : An example of an iFrame enabling a typical chatbot service on a website.

further.

As a second attempt, we manually re-analyse the top 100 websites and find two relevant chatbots (*SF-chat* and *SnatchBot*) and search for them over the top 10k websites using an automated script. For *Salesforce* chatbot, we only find it to be on their own websites, for example, *cloudforce* and *exactforce*. On all other top 10k websites, we do not find any other websites having either of these chatbots. Seven hundred twenty-nine (729) websites do not render in the first phase, and they are analysed again in the second attempt (we learn that rendering chatbot websites take longer than our previous timeout). We also manually analyse the 100 chatbots from 100,000 to 100,100 range and find three chatbots only, i.e., (i) `Drift`, (ii) `Intercom`, and (iii) `eLum`[*] . `Drift` is already included in our study, `Intercom` is found on numerous websites (after initial automated crawler verification), and `eLum` is not found anywhere else since it is a private custom chatbot. Moreover, please note that social-media related chatbots like Facebook messenger are not valid since they require human interaction and are not automated. Therefore, we do not include

[*] https://eluminoustechnologies.com

them in our analysis. For the rest of the study, we use only five chatbots, which are `Drift`, `Hubspot`, `LiveChat`, `Tidio`, and `Intercom`.

5.3 Exploring Web Chatbots

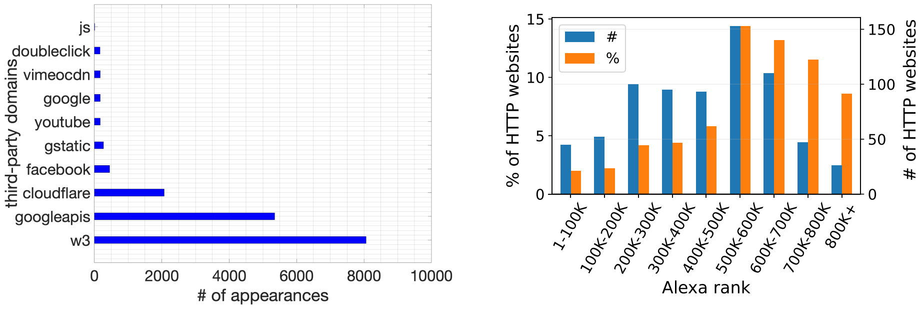
5.3.1 Analysis of HTTP Chatbot Websites

To check whether a website uses HTTP, our crawler defaults to communicating with the site over HTTP by simply concatenating the `"http://"` or `"http://www."` string with the hostname provided in the Alexa data. Once the crawler receives a final response and does not redirect the client requests from HTTP to HTTPs, it is marked as HTTP. We also check the websites that have errors by manually inspecting each one and discover that such websites are very few. The main reason for the errors is that they do not exist anymore (something that Alexa should take care of as it is not updated). The trend in the Figure 5.4b shows that less popular websites are less secure. The percentage of websites that use HTTP version increases for websites ranked 500K. The percentage is calculated from the number of HTTP chatbot websites (Figure 5.4b) and the total number of chatbot websites in each of the 100K category (Table 5.1). Overall, We find that 721 (5.38%) out of 13,392 chatbot websites still use the insecure HTTP version.

5.3.2 Analysis of Cookies

The online ecosystem is composed of a large number of organizations engaging in tracking user behaviour across the web [292]. This is accomplished by various techniques, including tracking cookies, pixel tags, beacons, and other sophisticated mechanisms. Below, we provide an overview of the most common cookies.

Identification Cookies These cookies can track visitors' conversations and interactions with a website. The customer service representative uses such information to



(a) (b)

Figure 5.4 : (a) Breakdown of third-parties found in web-based chatbots. (b) Number (and percentage) of web-based chatbots using insecure HTTP websites in top Alexa websites.

offer better service. It is challenging to learn about any old chat with the customer without these cookies.

Tracking Cookies These are the most common cookies used now to track user behaviour, user information and visits to a website.

Performance and Functionality Cookies These cookies are used to enhance the performance and functionality of a website but are non-essential to their use. However, certain functionalities like videos may become unavailable, or the login details are required every time a user visits the website.

Conditional Cookies These cookies may be written onto a website since they depend on using a specific feature of a website.

Marketing Cookies These are account-based marketing cookies used to identify prospects and personalise sales and marketing interactions.

Analytics and Customization Cookies These cookies are used to determine the effectiveness of marketing campaigns. Website owners use them to collect limited data from end-user browsers to enable them to understand the use of their websites.

Advertising Cookies These cookies collect information over time about users' online activity on the websites and other online services to customise online advertisements.

The details about all cookies used on every chatbot can be read on their website [293–297].

5.3.2.1 Drift

According to `Drift`, the primary reason it uses cookies is to track user interactions with the visited website. It also uses cookies to customise products to the need of a customer. `Drift` claims that the data is never sold or sent to third-parties. Instead, it is used in their platform to allow for more personalised and specific messaging [293].

5.3.2.2 Hubspot

According to `Hubspot`, it uses cookies to track users who visit a `Hubspot` chatbot website. These cookies keep track of visit counts and information about the sessions (such as session start timestamp). When the `Hubspot` software is run on a website, it leaves behind these cookies to help `Hubpost` identify the users on future visits [295].

5.3.2.3 LiveChat

We search for `LiveChat` cookies manually by inspecting several websites. We do not find any tracking cookie in our manual search. To confirm, we inquire from the `LiveChat` support team to ensure that none of the cookies is used for tracking purposes. The support team confirmed the same. The `LiveChat` chatbots automatically save and store two essential cookies on the user's device when a user visits a website with `LiveChat` widget [296]. The two essential cookies are as follows:

__lc_cid (customerID) This is a functional cookie that `LiveChat` account service uses. The purpose of this cookie is to verify the identity of a customer created.

__lc_cst (customerSecureToken) This is also a functional cookie that `LiveChat` account service uses to identify a user, for example, *name*, *IP address*, and *geolocation.*

5.3.2.4 Tidio

According to `Tidio`, it uses cookies to maintain, improve and customise the user experience. Additionally, the cookies are used to remember the visitor's choice, such as language preference. `Tidio` claims to collect information, including PII, and assures that it will be used by them only. We cannot find any evidence of `Tidio` cookies on any of the websites using their chatbots, nor can we find any information about what cookies are used on their website [297].

5.3.2.5 Intercom

According to `Intercom`, its chatbot writes "first-party" cookies only and assures that its cookies are strictly private and confidential. The purpose of these cookies is to identify users and keep track of sessions. Intercom states that it uses two cookies only [294]; however, this claim is contradictory to our findings discussed below

5.3.2.6 Findings/Discussion

To distinguish between a first-party and a third-party cookie, we consider any cookie with the same name as the respected chatbot as a first-party. We also consider

Table 5.2 : Distribution of cookies across Web-based chatbots.

	Categories of Cookies			
Chatbots	**Essential**	**Tracking & Analytics**	**Ads & Marketing**	**Total**
Drift	283 (5.38%)	5,113 (94.62%)	-	5,396
Hubspot	3,268 (20.65%)	12,561 (79.35%)	-	15,829
Intercom	8,942 (47.08%)	6,620 (34.85%)	3,433 (18.07%)	18,995
Total	12,493 (31.06%)	24,294 (60.4%)	3,433 (8.54%)	40,220

the cookies that chatbot service providers have mentioned on their websites as first-party. We declare any other cookie as a third-party. We find a total number of 2,110 websites using `Drift`. From these, a total of 5,396 cookies are discovered. 5,113 (94.62%) of them are used for Tracking, and 283 (5.24%) are essential cookies. Hubspot is used on 2,185 websites, which have 15,829 cookies. 12,561 (79.35%) are tracking, while the rest are *essential* cookies. `Intercom` chatbot websites are 4,037, generating 18,995 cookies, out of which 52.92% are either tracking, advertisement or marketing cookies, while 47.08% are essential cookies for functionality. No cookies are found on either `LiveChat` or `Tidio` chatbots. More than two-thirds of the discovered cookies are used for tracking or advertisement purposes.

5.3.3 Analysis of Third-party Domains

We parse the URLs from the chatbot iFrames, extract the second-level domains using *tldextract*[†], and compare them with the respective website. If they match, it is declared a first-party domain; otherwise, it is stated as a third-party domain. For instance, we extract `googleapis.com` and `drift.com` domains from the

[†] https://pypi.org/project/tldextract/

Table 5.3 : Distribution of top ten third-parties embedded in the iFrames of Web-based chatbots.

Third-party Domain	**Drift**	**LiveChat**	**Intercom**	**Tidio**	**Hubspot**	**Total**
w3.org	742	5	0	6,501	813	8,061
googleapis.com	28	3,502	0	1,537	282	5,349
cloudflare.com	2,063	1	0	0	10	2,074
facebook.com	0	0	0	0	453	453
gstatic.com	0	0	0	0	268	268
youtube.com	0	0	0	0	174	174
google.com	0	0	0	0	172	172
vimeocdn.com	0	0	0	0	171	171
doubleclick.net	0	0	0	0	166	166
rlets.com	0	0	5	0	0	5
other domains	0	19	0	7	3,872	3,989
Total	2,833	3,527	5	8,045	2,053	**20,791**

iFrame of `Drift` chatbot embedded in the landing page of https://www.drift.com. Given that `googleapis.com` does not match with `drift.com`, our method labelled `googleapis.com` as third-party whilst `drift.com` as first-party.

Figure 5.4a depicts, and Table 5.3 lists the top 10 third-party domains embedded in the iFrames of chatbots. We observe that all chatbots rely on third-party services such as W3, Google APIs, and Cloudflare for iFrame templates, fonts, and hosting and storing content, respectively. We observe that only one third-party domain (`rlets.com`) is found on the `Intercom` websites. Since `Intercom` dominates the top 300k Alexa websites (52% of total web-based chatbot websites), suggesting that the top websites do not rely much on advertising and analytical services revenues funnelled from chatbots. On the other hand, less popular websites generate 99.9% of the top ten third-party domains. Hubspot based websites have the most variety[‡] of third-party domains, making it the most vulnerable. One hundred forty-five different third-party domains are present in Hubspot websites.

5.4 Comparative Analysis

To the best of our knowledge, no prior work has been done to address the privacy and security risks of cookies or third-party scripts embedded in web-based chatbots. Previous work has analysed PII leaks via advertisements and third-party scripts on various domains such as Facebook [298–301], mobile eco-system [302–304], and web forms [305].

There are security and privacy risks associated with chatbots [306, 307]. In *financial* chatbots, Bhuiyan et al. proposed a chatbot leveraging a private blockchain platform to conduct secure and confidential financial transactions [308]. Chatbots have also been developed to remove sensitive information from the conversation before passing it to its NLP engine [309]. Meanwhile, threats on the chatbot's client-side (such as unintended activation attacks and access control attacks) and network-side (such as MITM attacks and DDoS attacks) have been studied in the literature [310]. Bozic et al. conducted a preliminary security study on an open-source chatbot to identify XSS and SQLi vulnerabilities [311]. Their work did not find any XSS and SQLi vulnerabilities and was limited to analysing only one chatbot. No prior work has been done to study the iFrames of Web-based chatbots and to determine the types of cookies embedded. In this chapter, to fill the gap, we study the prevalence of five chatbots in Alexa top 1-million websites and analyse the chatbot cookies and third-party domains embedded in the iFrames of chatbots.

[‡] Drift=3, Livechat=10, Hubspot=145, Tidio=4, Intercom=1

While prior research has extensively explored privacy and security risks in website as a whole, the specific area of web-based chatbots, particularly concerning confidentiality, cookies and third-party scripts has not been sufficiently addressed. This thesis fills this critical gap by focusing on the unique vulnerabilities associated with chatbots, a subject that has yet to be comprehensively explored in the literature. Moreover, to the best of our knowledge there is no analytical or empirical study done on web-based chatbots and on the intricacies of chatbot iFrames and the types of cookies and third-party domains embedded within them. Our research provides a pioneering analysis of these aspects, offering insights into the prevalence and implications of chatbot integration in the top-ranking websites.

5.5 Summary

In this chapter, *firstly*, we have presented the difference between websites with and without chatbots. We have found the keywords to detect chatbots on the analysed websites. We have also manually inspected the top 1,000 websites to validate chatbot detection. *Secondly*, we have designed and implemented a crawler tool that systematically explores and collects DOMs from the top 1-million Alexa websites. We have discovered that a subset of 13,392 (1.58%) of these websites use our five selected chatbots. We have found the frequencies of these chatbots in ten different categories and discovered that non-IT business websites had used 21.78% of them. Our analysis has revealed that the top 300k Alexa ranking websites are dominated by `Intercom`, while `LiveChat` dominates the remaining chatbot websites. We have also found that 5.38% of the chatbot use insecure protocols to transfer users' chats in plain-text. Our results show that, despite the promises for privacy, security, and anonymity given by the majority of the websites, millions of users may be unknowingly subject to poor security guarantees by chatbot service providers on the same websites.

In our future work, we aim to extend these findings to the distribution of third-party domains and trackers in categories of web-based chatbots websites. This will help analyse and identify the dependence of chatbot websites on advertising and analytical services. Another area to explore is whether any chatbot websites render content that it does not directly load. Informed by the study by Ikram et al. [312], this work can be extended to analyse the dependency web-resources chains of the chatbots. Finally, our work analysed chatbots implemented in iFrames. Chatbots might also be served via new web frameworks such as React [313] and Angular [314], and in such cases, our data collection methodology needs update to capture chatbots implemented via such frameworks.

Chapter 6

Conclusions and Future Work

This chapter summarises the research conducted in this thesis. The primary focus was to address the security and privacy challenges in End-user systems, specifically in IoT devices and Websites. The research commenced with comprehensively analysing the current threats and vulnerabilities inherent to IoT and Websites. From this foundational analysis, several vital contributions emerged. In response to the security and privacy challenges identified in IoT devices, an extensive study was conducted, underscoring the potential of ML and blockchain as viable countermeasures. This insight led us to propose a novel Privacy-Enhanced Living (PEL) framework designed to strengthen data privacy in smart homes. Building on this integration of technologies (ML and BC), the FedBlockHealth framework was introduced, aiming to enhance security measures in IoT devices, particularly within the healthcare context. As the research delved into Websites, the research identified significant gaps towards the security and privacy issues in the Web-based chatbots. There needed to be more comprehensive research done focusing on Web-based chatbots. To address this huge gap, we empirically analysed Web-based chatbots' security and privacy issues on Alexa's top 1-million websites. In response, a unique public dataset of these chatbots was established, illuminating their security and privacy implications. The dataset revealed insights such as the dominance of certain chatbot platforms in specific Alexa rankings and the concerning use of insecure protocols by a subset of these chatbots. An empirical assessment followed, highlighting potential vulnerabilities, such as the disproportionate use of cookies for tracking, and providing valuable insights to develop future protective strategies.

6.1 Summary of the Thesis

6.1.1 Chapter 2

Chapter 2 addressed research question 1, by thoroughly reviewing advanced security and privacy challenges in End-user systems, specifically focusing on IoT devices and Websites. The chapter detailed the current threats to IoT devices, categorised them into security and privacy domains, and discussed potential countermeasures using ML and blockchain technologies. Subsequently, the chapter explored the security and privacy challenges unique to Websites.

6.1.2 Chapter 3

To answer research question 2, Chapter 3 began with a detailed analysis of the current threats facing IoT devices, focusing on their security and privacy aspects. This analysis led to the identification of various types of attacks and their effects. While potential solutions were briefly discussed, the chapter emphasised the role of Machine Learning (ML) algorithms and Blockchain (BC) technologies. Recognising gaps in current research, the chapter highlighted the importance of combining ML and BC to improve IoT security and privacy. This Section 3.1 concluded by presenting an ML-based threat model for IoT, drawing from previous studies, and discussing the challenges associated with using ML and BC in the IoT context.

Shifting from the general IoT landscape, the second Section 3.2 of this chapter focused on the specific area of smart homes, where privacy risks are exceptionally high. To address these concerns, the Local Differential Privacy (LDP) technique was used, leading to the proposal of a new framework based on the k-Anonymity Randomised Response (k-RR) algorithm. Unlike many existing studies that focus on obfuscation for specific data types, our approach aimed for broader applicability, addressing the need for obfuscation of high-risk data. Noting the limited research on adversarial machine-learning techniques in home data obfuscation, we introduced a method that considers data privacy. This method goes beyond just hiding data, offering a strong solution tailored to the specific needs and vulnerabilities of home data. Tests using real-world home data showed the effectiveness of the proposed method, confirming its ability to assess the privacy risks of both hidden and original high-risk home data. The findings from this chapter emphasise the need for advanced, context-specific privacy solutions and suggest directions for future research. This could include combining the proposed method with other privacy-enhancing technologies or applying it to other sensitive areas.

6.1.3 Chapter 4

We addressed research question 3 in Chapter 4. This chapter introduces a privacy-enhanced federated learning (FL) system that integrates blockchain and smart contracts, utilising a convolutional neural network (CNN) for distributed training on the EMNIST dataset. The system is designed to balance data privacy preservation with model performance, making it an apt solution for handling sensitive data in IoT-enabled healthcare applications. Our evaluation reveals that the privacy-enhanced CNN model achieves an impressive 99.99% accuracy. We employed ElGamal encryption, a less complex yet effective method, to maintain anonymity and enable computation in the cipher-text space. The integration of blockchain technology and smart contracts further fortifies the integrity and security of the system. This chapter underscores the potential of our approach to enhancing privacy and efficiency in distributed learning tasks, particularly in healthcare applications.

6.1.4 Chapter 5

To answer research question 4, in Chapter 5, we have synthesised our comprehensive investigation into the landscape of Web-based chatbots on Alexa top 1-million popular websites. *Firstly*, we delineated the differences between websites with and without chatbots, identifying keywords for chatbot detection and manually validating the top 1,000 websites. *Secondly*, we designed a crawler tool to explore and collect DOMs, discovering 13,392 websites (1.58%) utilising our selected chatbots. Our analysis revealed a dominance of `Intercom` in the top 300k Alexa ranking websites, while `LiveChat` prevailed in the rest. We also uncovered that 5.38% of chatbots use insecure protocols, transferring users' chats in plain text. Despite promises of privacy and security, our results indicate potential vulnerabilities, including the disproportionate use of cookies, with 94.62% used for tracking in 2,110 websites leveraging the `Drift` chatbot. Additionally, we identified the top 10 third-party domains in web-based chatbots. This chapter encapsulates our large-scale study, highlighting key insights and underscoring the need for enhanced security measures in the rapidly evolving field of chatbots.

6.2 Future Works

Using Machine Learning (ML) with Blockchain (BC) to improve IoT security and privacy is a growing research area. This thesis raises several open research issues as below:

(a) Design and develop end-to-end trusted, secure and privacy-preserving mechanisms for resource constraint End-user systems.

(b) Expand the applicability of the proposed frameworks in this thesis to other home datasets, notably smart meter data for monitoring residential electricity consumption.

(c) Adapt the obfuscation method into a user-centric tool, possibly a browser plug-in, to bolster individual privacy protections.

Regarding Web-based chatbots, potential avenues for future research include:

(a) Investigate the distribution of third-party domains and trackers across various chatbot websites to understand their dependence on advertising and data analysis services.

(b) Examine whether chatbot websites display content they do not directly load, potentially using the findings from Ikram et al. [312] as a foundation.

(c) Analyze the dependency chains of chatbots in terms of web resources.

(d) Extend the study to chatbots implemented using newer web frameworks, such as React [313] and Angular [314], which would necessitate modifications to the data collection methodology.

6.2.1 Enhancing IoT Security through Real-World Application

In addressing the evolving security and privacy challenges inherent to IoT devices and Web-based systems, this thesis has underscored the potential of integrating Machine Learning (ML) and Blockchain (BC) technologies as countermeasures. Building upon these foundations, the proposed Privacy-Enhanced Living (PEL) framework and FedBlockHealth framework represent significant strides towards bolstering data privacy and enhancing security measures within the IoT domain, particularly within smart homes and healthcare contexts, respectively.

While these contributions mark a pivotal advancement in theoretical and simulation-based research, the transition towards real-world applicability presents a critical next step. The feedback received highlights the imperative for further real-world testing and the continuous adaptation of these solutions to meet practical, operational demands.

6.2.2 Collaborative Pilot Studies and Industry Engagement

Recognizing the need for empirical validation and scalability assessment, a plan for collaborative pilot studies with industry and academic partners is crucial. These pilot studies aim to rigorously test the practical viability of the PEL and FedBlock-Health frameworks within live IoT ecosystems. Such collaborations will not only provide a platform for real-world application but also offer insights into the operational challenges and scalability potential of these solutions.

Industry partnerships, in particular, will serve as a conduit for integrating theoretical models into existing and forthcoming IoT infrastructures. Through these synergies, the proposed solutions can be refined and optimized, ensuring their resilience against evolving security threats and their adaptability to the technological advancements and user needs characteristic of the IoT landscape.

The insights gleaned from these engagements will be instrumental in transitioning from a primarily theoretical exploration to actionable, scalable security solutions for IoT devices and systems. It will validate the applicability of the proposed frameworks in real-world settings and inform ongoing research and development efforts aimed at addressing the dynamic security and privacy challenges facing the IoT domain.

Bibliography

[1] U. 42, “2020 unit 42 iot threat report,” 2020. [Online]. Available: https://unit42.paloaltonetworks.com/iot-threat-report-2020/

[2] SiteLock. (2023) Chatbot security risks & best practices to know. Accessed: 2023-03-13. [Online]. Available: https://www.sitelock.com/blog/chatbot-security-risks-best-practices

[3] Verloop.io. (2023) Conversational chatbot security: Threats, measures, best practices. Accessed: 2023-03-13. [Online]. Available: https://www.verloop.io/conversational-chatbot-security-threats-measures-best-practices/

[4] LayerX Security. (2023) Chatbot security explained: A comprehensive guide. Accessed: 2023-03-13. [Online]. Available: https://layerxsecurity.com/chatbot-security-explained/

[5] L. Atzori, A. Iera, and G. Morabito, “The internet of things: A survey,” *Computer Networks*, vol. 54, no. 15, pp. 2787–2805, 2010.

[6] L. Da Xu, W. He, and S. Li, “Internet of things in industries: A survey,” *IEEE Transactions on industrial informatics*, vol. 10, no. 4, pp. 2233–2243, 2014.

[7] F. A. Alaba, M. Othman, I. A. T. Hashem, and F. Alotaibi, “Internet of things security: A survey,” *Journal of Network and Computer Applications*, vol. 88, pp. 10–28, 2017.

[8] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao, “A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications,” *IEEE Internet of Things journal*, vol. 4, no. 5, pp. 1125–1142, 2017.

[9] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, “Internet of things (iot): A vision, architectural elements, and future directions,” *Future Generation Computer Systems*, vol. 29, no. 7, pp. 1645–1660, 2013.

[10] S. Chen, H. Xu, D. Liu, B. Hu, and H. Wang, “A vision of iot: Applications, challenges, and opportunities with china perspective,” *IEEE Internet of Things journal*, vol. 1, no. 4, pp. 349–359, 2014.

[11] M. Antonakakis, T. April, M. Bailey, M. Bernhard, E. Bursztein, J. Cochran, Z. Durumeric, J. A. Halderman, L. Invernizzi, M. Kallitsis *et al.*, "Understanding the mirai botnet," in *26th USENIX security symposium (USENIX Security 17)*, 2017, pp. 1093–1110.

[12] M. Stoyanova, Y. Nikoloudakis, S. Panagiotakis, E. Pallis, and E. K. Markakis, "A survey on the internet of things (iot) forensics: challenges, approaches, and open issues," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 2, pp. 1191–1221, 2020.

[13] Z. Yang, Y. Yue, Y. Yang, Y. Peng, X. Wang, and W. Liu, "Study and application on the architecture and key technologies for iot," in *2011 International Conference on Multimedia Technology.* IEEE, 2011, pp. 747–751.

[14] G. Kortuem, F. Kawsar, V. Sundramoorthy, and D. Fitton, "Smart objects as building blocks for the internet of things," *IEEE Internet Computing*, vol. 14, no. 1, pp. 44–51, 2009.

[15] M. Chiang and T. Zhang, "Fog and iot: An overview of research opportunities," *IEEE Internet of Things journal*, vol. 3, no. 6, pp. 854–864, 2016.

[16] S. Zhang, J. Liu, H. Guo, M. Qi, and N. Kato, "Envisioning device-to-device communications in 6g," *IEEE Network*, vol. 34, no. 3, pp. 86–91, 2020.

[17] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, "Security, privacy and trust in internet of things: The road ahead," *Computer Networks*, vol. 76, pp. 146–164, 2015.

[18] R. Roman, J. Zhou, and J. Lopez, "On the features and challenges of security and privacy in distributed internet of things," *Computer Networks*, vol. 57, no. 10, pp. 2266–2279, 2013.

[19] L. Tawalbeh, F. Muheidat, M. Tawalbeh, and M. Quwaider, "Iot privacy and security: Challenges and solutions," *Applied Sciences*, vol. 10, no. 12, p. 4102, 2020.

[20] N. Neshenko, E. Bou-Harb, J. Crichigno, G. Kaddoum, and N. Ghani, "Demystifying iot security: an exhaustive survey on iot vulnerabilities and a first empirical look on internet-scale iot exploitations," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 3, pp. 2702–2733, 2019.

[21] J. H. Ziegeldorf, O. G. Morchon, and K. Wehrle, "Privacy in the internet of things: threats and challenges," *Security and Communication Networks*, vol. 7, no. 12, pp. 2728–2742, 2014.

[22] M. Ammar, G. Russello, and B. Crispo, "Internet of things: A survey on the security of iot frameworks," *Journal of Information Security and Applications*, vol. 38, pp. 8–27, 2018.

[23] H. Kim and E. A. Lee, "Authentication and authorization for the internet of things," *IT Professional*, vol. 19, no. 5, pp. 27–33, 2017.

[24] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of things: A survey on enabling technologies, protocols, and applications," *IEEE communications surveys & tutorials*, vol. 17, no. 4, pp. 2347–2376, 2015.

[25] A. L. Buczak and E. Guven, "A survey of data mining and machine learning methods for cyber security intrusion detection," *IEEE Communications surveys & tutorials*, vol. 18, no. 2, pp. 1153–1176, 2015.

[26] P. McDaniel, N. Papernot, and Z. B. Celik, "Machine learning in adversarial settings," *IEEE Security & Privacy*, vol. 14, no. 3, pp. 68–72, 2016.

[27] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, "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).* IEEE, 2017, pp. 618–623.

[28] D. E. Kouicem, A. Bouabdallah, and H. Lakhlef, "Internet of things security: A top-down survey," *Computer Networks*, vol. 141, pp. 199–221, 2018.

[29] Y. Qian, Y. Jiang, J. Chen, Y. Zhang, J. Song, M. Zhou, and M. Pustišek, "Towards decentralized iot security enhancement: A blockchain approach," *Computers & Electrical Engineering*, vol. 72, pp. 266–273, 2018.

[30] B. K. Mohanta, D. Jena, U. Satapathy, and S. Patnaik, "Survey on iot security: Challenges and solution using machine learning, artificial intelligence and blockchain technology," *Internet of Things*, vol. 11, p. 100227, 2020.

[31] G. Cameron, D. Cameron, G. Megaw, R. Bond, M. Mulvenna, S. O'Neill, C. Armour, and M. McTear, "Towards a chatbot for digital counselling," in *Proceedings of the 31st International BCS Human Computer Interaction Conference (HCI 2017) 31*, 2017, pp. 1–7.

[32] Z. Lin, P. Xu, G. I. Winata, F. B. Siddique, Z. Liu, J. Shin, and P. Fung, "Caire: An end-to-end empathetic chatbot," in *Proceedings of the AAAI conference on artificial intelligence*, vol. 34, no. 09, 2020, pp. 13 622–13 623.

[33] M. Nuruzzaman and O. K. Hussain, "A survey on chatbot implementation in customer service industry through deep neural networks," in *2018 IEEE 15th International Conference on e-Business Engineering (ICEBE).* IEEE, 2018, pp. 54–61.

[34] A. Androutsopoulou, N. Karacapilidis, E. Loukis, and Y. Charalabidis, “Transforming the communication between citizens and government through ai-guided chatbots,” *Government information quarterly*, vol. 36, no. 2, pp. 358–367, 2019.

[35] S. Paliwal, V. Bharti, and A. K. Mishra, “Ai chatbots: Transforming the digital world,” *Recent Trends and Advances in Artificial Intelligence and Internet of Things*, pp. 455–482, 2020.

[36] M. Hasal, J. Nowaková, K. Ahmed Saghair, H. Abdulla, V. Snášel, and L. Ogiela, “Chatbots: Security, privacy, data protection, and social aspects,” *Concurrency and Computation: Practice and Experience*, vol. 33, no. 19, p. e6426, 2021.

[37] J. Edu, C. Mulligan, F. Pierazzi, J. Polakis, G. Suarez-Tangil, and J. Such, “Exploring the security and privacy risks of chatbots in messaging services,” in *Proceedings of the 22nd ACM Internet Measurement Conference*, 2022, pp. 581–588.

[38] R. Belen Saglam, J. R. Nurse, and D. Hodges, “Privacy concerns in chatbot interactions: When to trust and when to worry,” in *HCI International 2021-Posters: 23rd HCI International Conference, HCII 2021, Virtual Event, July 24–29, 2021, Proceedings, Part II 23.* Springer, 2021, pp. 391–399.

[39] L. Jenneboer, C. Herrando, and E. Constantinides, “The impact of chatbots on customer loyalty: A systematic literature review,” *Journal of theoretical and applied electronic commerce research*, vol. 17, no. 1, pp. 212–229, 2022.

[40] E. Adamopoulou and L. Moussiades, “Chatbots: History, technology, and applications,” *Machine Learning with Applications*, vol. 2, p. 100006, 2020.

[41] G. Murtarelli, A. Gregory, and S. Romenti, “A conversation-based perspective for shaping ethical human–machine interactions: The particular challenge of chatbots,” *Journal of Business Research*, vol. 129, pp. 927–935, 2021.

[42] M. Yan, P. Castro, P. Cheng, and V. Ishakian, “Building a chatbot with serverless computing,” in *Proceedings of the 1st International Workshop on Mashups of Things and APIs*, 2016, pp. 1–4.

[43] F. Salahdine and N. Kaabouch, “Social engineering attacks: A survey,” *Future Internet*, vol. 11, no. 4, p. 89, 2019.

[44] M. Shumanov and L. Johnson, “Making conversations with chatbots more personalized,” *Computers in Human Behavior*, vol. 117, p. 106627, 2021.

[45] S. M. Furnell, A. Jusoh, and D. Katsabas, “The challenges of understanding and using security: A survey of end-users,” *Computers & Security*, vol. 25, no. 1, pp. 27–35, 2006.

[46] S. Das, L. Dabbish, and J. Hong, “A typology of perceived triggers for end-user security and privacy behaviors,” in *Fifteenth Symposium on Usable Privacy and Security ({SOUPS} 2019)*, 2019.

[47] H. Oz, A. Aris, A. Levi, and A. S. Uluagac, “A survey on ransomware: Evolution, taxonomy, and defense solutions,” *ACM Computing Surveys (CSUR)*, vol. 54, no. 11s, pp. 1–37, 2022.

[48] R. Feng, S. Chen, X. Xie, G. Meng, S.-W. Lin, and Y. Liu, “A performance-sensitive malware detection system using deep learning on mobile devices,” *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 1563–1578, 2020.

[49] J. Bonneau, C. Herley, P. C. Van Oorschot, and F. Stajano, “The quest to replace passwords: A framework for comparative evaluation of web authentication schemes,” in *2012 IEEE symposium on security and privacy*. IEEE, 2012, pp. 553–567.

[50] K. Thomas, J. Pullman, K. Yeo, A. Raghunathan, P. G. Kelley, L. Invernizzi, B. Benko, T. Pietraszek, S. Patel, D. Boneh *et al.*, “Protecting accounts from credential stuffing with password breach alerting,” in *28th USENIX Security Symposium (USENIX Security 19)*, 2019, pp. 1556–1571.

[51] N. A. G. Arachchilage and S. Love, “Security awareness of computer users: A phishing threat avoidance perspective,” *Computers in human behavior*, vol. 38, pp. 304–312, 2014.

[52] H. Aldawood and G. Skinner, “Reviewing cyber security social engineering training and awareness programs—pitfalls and ongoing issues,” *Future Internet*, vol. 11, no. 3, p. 73, 2019.

[53] M. Zwilling, G. Klien, D. Lesjak, Ł. Wiechetek, F. Cetin, and H. N. Basim, “Cyber security awareness, knowledge and behavior: A comparative study,” *Journal of Computer Information Systems*, vol. 62, no. 1, pp. 82–97, 2022.

[54] K. Yang, K. Zhang, J. Ren, and X. Shen, “Security and privacy in mobile crowdsourcing networks: challenges and opportunities,” *IEEE communications magazine*, vol. 53, no. 8, pp. 75–81, 2015.

[55] K. Krombholz, K. Busse, K. Pfeffer, M. Smith, and E. Von Zezschwitz, “If https were secure, i would’nt need 2fa end user and administrator mental models of https,” in *2019 IEEE Symposium on Security and Privacy (SP)*, 2019, pp. 246–263.

[56] J. Hiller, J. Pennekamp, M. Dahlmanns, M. Henze, A. Panchenko, and K. Wehrle, "Tailoring onion routing to the internet of things: Security and privacy in untrusted environments," in *2019 IEEE 27th International Conference on Network Protocols (ICNP)*. IEEE, 2019, pp. 1–12.

[57] S. Ray, E. Peeters, M. M. Tehranipoor, and S. Bhunia, "System-on-chip platform security assurance: Architecture and validation," *Proceedings of the IEEE*, vol. 106, no. 1, pp. 21–37, 2017.

[58] F. Alsubaei, A. Abuhussein, and S. Shiva, "Security and privacy in the internet of medical things: taxonomy and risk assessment," in *2017 IEEE 42nd conference on local computer networks workshops (LCN workshops)*. IEEE, 2017, pp. 112–120.

[59] I. Sarrigiannis, E. Kartsakli, K. Ramantas, A. Antonopoulos, and C. Verikoukis, "Application and network vnf migration in a mec-enabled 5g architecture," in *2018 IEEE 23rd International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD)*. IEEE, 2018, pp. 1–6.

[60] E. Zeng, S. Mare, and F. Roesner, "End user security and privacy concerns with smart homes," in *Symposium on Usable Privacy and Security (SOUPS)*, vol. 220, 2017.

[61] M. Tabassum, T. Kosinski, and H. R. Lipford, "I don't own the data: End user perceptions of smart home device data practices and risks," in *Fifteenth symposium on usable privacy and security (SOUPS 2019)*, 2019, pp. 435–450.

[62] K. Martin and K. Shilton, "Putting mobile application privacy in context: An empirical study of user privacy expectations for mobile devices," *The Information Society*, vol. 32, no. 3, pp. 200–216, 2016.

[63] L. Barkhuus and A. K. Dey, "Location-based services for mobile telephony: a study of users' privacy concerns." in *Interact*, vol. 3. Citeseer, 2003, pp. 702–712.

[64] P. Krebs and D. T. Duncan, "Health app use among us mobile phone owners: a national survey," *JMIR mHealth and uHealth*, vol. 3, no. 4, p. e4924, 2015.

[65] L. Li, A. Bartel, T. F. Bissyandé, J. Klein, Y. Le Traon, S. Arzt, S. Rasthofer, E. Bodden, D. Octeau, and P. McDaniel, "Iccta: Detecting inter-component privacy leaks in android apps," in *2015 IEEE/ACM 37th IEEE International Conference on Software Engineering*, vol. 1. IEEE, 2015, pp. 280–291.

[66] S. Alneyadi, E. Sithirasenan, and V. Muthukkumarasamy, “A survey on data leakage prevention systems,” *Journal of Network and Computer Applications*, vol. 62, pp. 137–152, 2016.

[67] J. Kang, Z. Xiong, D. Niyato, Y. Zou, Y. Zhang, and M. Guizani, “Reliable federated learning for mobile networks,” *IEEE Wireless Communications*, vol. 27, no. 2, pp. 72–80, 2020.

[68] P. Datta and B. Sharma, “A survey on iot architectures, protocols, security and smart city based applications,” in *2017 8th international conference on computing, communication and networking technologies (ICCCNT).* IEEE, 2017, pp. 1–5.

[69] M. Burhan, R. A. Rehman, B. Khan, and B.-S. Kim, “Iot elements, layered architectures and security issues: A comprehensive survey,” *Sensors*, vol. 18, no. 9, p. 2796, 2018.

[70] W. H. Hassan *et al.*, “Current research on internet of things (iot) security: A survey,” *Computer Networks*, vol. 148, pp. 283–294, 2019.

[71] J. Ahamed and A. V. Rajan, “Internet of things (iot): Application systems and security vulnerabilities,” in *2016 5th International conference on electronic devices, systems and applications (ICEDSA).* IEEE, 2016, pp. 1–5.

[72] Y. Meng, W. Zhang, H. Zhu, and X. S. Shen, “Securing consumer iot in the smart home: Architecture, challenges, and countermeasures,” *IEEE Wireless Communications*, vol. 25, no. 6, pp. 53–59, 2018.

[73] Y. Zheng, A. Davanian, H. Yin, C. Song, H. Zhu, and L. Sun, “{FIRM-AFL}:{High-Throughput} greybox fuzzing of {IoT} firmware via augmented process emulation,” in *28th USENIX Security Symposium (USENIX Security 19)*, 2019, pp. 1099–1114.

[74] P. Sun, L. Garcia, G. Salles-Loustau, and S. Zonouz, “Hybrid firmware analysis for known mobile and iot security vulnerabilities,” in *2020 50th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN).* IEEE, 2020, pp. 373–384.

[75] E. Bertino and N. Islam, “Botnets and internet of things security,” *Computer*, vol. 50, no. 2, pp. 76–79, 2017.

[76] S. Vashi, J. Ram, J. Modi, S. Verma, and C. Prakash, “Internet of things (iot): A vision, architectural elements, and security issues,” in *2017 international conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC).* IEEE, 2017, pp. 492–496.

[77] A. Manzoor, M. Liyanage, A. Braeke, S. S. Kanhere, and M. Ylianttila, "Blockchain based proxy re-encryption scheme for secure iot data sharing," in *2019 IEEE international conference on blockchain and cryptocurrency (ICBC)*. IEEE, 2019, pp. 99–103.

[78] H. Sato, A. Kanai, S. Tanimoto, and T. Kobayashi, "Establishing trust in the emerging era of iot," in *2016 IEEE Symposium on Service-Oriented System Engineering (SOSE)*. IEEE, 2016, pp. 398–406.

[79] X. Jiang, M. Lora, and S. Chattopadhyay, "An experimental analysis of security vulnerabilities in industrial iot devices," *ACM Transactions on Internet Technology (TOIT)*, vol. 20, no. 2, pp. 1–24, 2020.

[80] Z.-K. Zhang, M. C. Y. Cho, C.-W. Wang, C.-W. Hsu, C.-K. Chen, and S. Shieh, "Iot security: ongoing challenges and research opportunities," in *2014 IEEE 7th international conference on service-oriented computing and applications*. IEEE, 2014, pp. 230–234.

[81] Q. Jing, A. V. Vasilakos, J. Wan, J. Lu, and D. Qiu, "Security of the internet of things: perspectives and challenges," *Wireless Networks*, vol. 20, pp. 2481–2501, 2014.

[82] I. Makhdoom, M. Abolhasan, J. Lipman, R. P. Liu, and W. Ni, "Anatomy of threats to the internet of things," *IEEE communications surveys & tutorials*, vol. 21, no. 2, pp. 1636–1675, 2018.

[83] F. Hussain, S. A. Hassan, R. Hussain, and E. Hossain, "Machine learning for resource management in cellular and iot networks: Potentials, current solutions, and open challenges," *IEEE communications surveys & tutorials*, vol. 22, no. 2, pp. 1251–1275, 2020.

[84] B. Lee and J.-H. Lee, "Blockchain-based secure firmware update for embedded devices in an internet of things environment," *The Journal of Supercomputing*, vol. 73, pp. 1152–1167, 2017.

[85] F. Meneghello, M. Calore, D. Zucchetto, M. Polese, and A. Zanella, "Iot: Internet of threats? a survey of practical security vulnerabilities in real iot devices," *IEEE Internet of Things journal*, vol. 6, no. 5, pp. 8182–8201, 2019.

[86] T. Alladi, V. Chamola, B. Sikdar, and K.-K. R. Choo, "Consumer iot: Security vulnerability case studies and solutions," *IEEE Consumer Electronics Magazine*, vol. 9, no. 2, pp. 17–25, 2020.

[87] F. Restuccia, S. D'Oro, and T. Melodia, "Securing the internet of things in the age of machine learning and software-defined networking," *IEEE Internet of Things journal*, vol. 5, no. 6, pp. 4829–4842, 2018.

[88] I. Butun, P. Österberg, and H. Song, "Security of the internet of things: Vulnerabilities, attacks, and countermeasures," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 1, pp. 616–644, 2019.

[89] Z. Tan, A. Jamdagni, X. He, P. Nanda, and R. P. Liu, "A system for denial-of-service attack detection based on multivariate correlation analysis," *IEEE transactions on parallel and distributed systems*, vol. 25, no. 2, pp. 447–456, 2013.

[90] Z. Tan, A. Jamdagni, X. He, P. Nanda, R. P. Liu, and J. Hu, "Detection of denial-of-service attacks based on computer vision techniques," *IEEE transactions on computers*, vol. 64, no. 9, pp. 2519–2533, 2014.

[91] T. Limbasiya and N. Doshi, "An analytical study of biometric based remote user authentication schemes using smart cards," *Computers & Electrical Engineering*, vol. 59, pp. 305–321, 2017.

[92] A. E. Omolara, A. Alabdulatif, O. I. Abiodun, M. Alawida, A. Alabdulatif, and H. Arshad, "The internet of things security: A survey encompassing unexplored areas and new insights," *Computers & Security*, vol. 112, p. 102494, 2022.

[93] C. Kolias, G. Kambourakis, A. Stavrou, and S. Gritzalis, "Intrusion detection in 802.11 networks: Empirical evaluation of threats and a public dataset," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 1, pp. 184–208, 2015.

[94] R. Mitev, M. Miettinen, and A.-R. Sadeghi, "Alexa lied to me: Skill-based man-in-the-middle attacks on virtual assistants," in *Proceedings of the 2019 ACM Asia Conference on Computer and Communications Security*, 2019, pp. 465–478.

[95] J. Singh, Y. Bello, A. R. Hussein, A. Erbad, and A. Mohamed, "Hierarchical security paradigm for iot multiaccess edge computing," *IEEE Internet of Things journal*, vol. 8, no. 7, pp. 5794–5805, 2020.

[96] O. Salem, K. Alsubhi, A. Shaafi, M. Gheryani, A. Mehaoua, and R. Boutaba, "Man-in-the-middle attack mitigation in internet of medical things," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 3, pp. 2053–2062, 2021.

[97] S. Calzavara, R. Focardi, M. Squarcina, and M. Tempesta, "Surviving the web: A journey into web session security," *ACM Computing Surveys (CSUR)*, vol. 50, no. 1, pp. 1–34, 2017.

[98] B. A. Azad, P. Laperdrix, and N. Nikiforakis, "Less is more: quantifying the security benefits of debloating web applications," in *28th USENIX Security Symposium (USENIX Security 19)*, 2019, pp. 1697–1714.

[99] A. Gkortzis, D. Feitosa, and D. Spinellis, "Software reuse cuts both ways: An empirical analysis of its relationship with security vulnerabilities," *Journal of Systems and Software*, vol. 172, p. 110653, 2021.

[100] G. E. Rodríguez, J. G. Torres, P. Flores, and D. E. Benavides, "Cross-site scripting (xss) attacks and mitigation: A survey," *Computer Networks*, vol. 166, p. 106960, 2020.

[101] F. Caturano, G. Perrone, and S. P. Romano, "Discovering reflected cross-site scripting vulnerabilities using a multiobjective reinforcement learning environment," *Computers & Security*, vol. 103, p. 102204, 2021.

[102] R. H. Steinegger, D. Deckers, P. Giessler, and S. Abeck, "Risk-based authenticator for web applications," in *Proceedings of the 21st European Conference on Pattern Languages of Programs*, 2016, pp. 1–11.

[103] R. F. Olanrewaju, B. U. I. Khan, M. A. Morshidi, F. Anwar, and M. L. B. M. Kiah, "A frictionless and secure user authentication in web-based premium applications," *IEEE Access*, vol. 9, pp. 129 240–129 255, 2021.

[104] R. Chakraborty, J. Lee, S. Bagchi-Sen, S. Upadhyaya, and H. R. Rao, "Online shopping intention in the context of data breach in online retail stores: An examination of older and younger adults," *Decision Support Systems*, vol. 83, pp. 47–56, 2016.

[105] Y. Zou and F. Schaub, "Beyond mandatory: Making data breach notifications useful for consumers," *IEEE Security & Privacy*, vol. 17, no. 2, pp. 67–72, 2019.

[106] Z. Fang, M. Xu, S. Xu, and T. Hu, "A framework for predicting data breach risk: Leveraging dependence to cope with sparsity," *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 2186–2201, 2021.

[107] M. Bada, A. M. Sasse, and J. R. Nurse, "Cyber security awareness campaigns: Why do they fail to change behaviour?" *arXiv preprint arXiv:1901.02672*, 2019.

[108] P. Emami-Naeini, H. Dixon, Y. Agarwal, and L. F. Cranor, "Exploring how privacy and security factor into iot device purchase behavior," in *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, 2019, pp. 1–12.

[109] J. Reardon, Á. Feal, P. Wijesekera, A. E. B. On, N. Vallina-Rodriguez, and S. Egelman, "50 ways to leak your data: An exploration of apps' circumvention of the android permissions system," in *28th USENIX security symposium (USENIX security 19)*, 2019, pp. 603–620.

[110] A. R. Smink, S. Frowijn, E. A. van Reijmersdal, G. van Noort, and P. C. Neijens, "Try online before you buy: How does shopping with augmented reality affect brand responses and personal data disclosure," *Electronic Commerce Research and Applications*, vol. 35, p. 100854, 2019.

[111] T. Linden, R. Khandelwal, H. Harkous, and K. Fawaz, "The privacy policy landscape after the gdpr," *arXiv preprint arXiv:1809.08396*, 2018.

[112] I. Sanchez-Rola, M. Dell'Amico, P. Kotzias, D. Balzarotti, L. Bilge, P.-A. Vervier, and I. Santos, "Can i opt out yet? gdpr and the global illusion of cookie control," in *Proceedings of the 2019 ACM Asia conference on computer and communications security*, 2019, pp. 340–351.

[113] C. Matte, N. Bielova, and C. Santos, "Do cookie banners respect my choice?: Measuring legal compliance of banners from iab europe's transparency and consent framework," in *2020 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2020, pp. 791–809.

[114] O. Alrawi, C. Zuo, R. Duan, R. P. Kasturi, Z. Lin, and B. Saltaformaggio, "The betrayal at cloud city: An empirical analysis of {Cloud-Based} mobile backends," in *28th USENIX Security Symposium (USENIX Security 19)*, 2019, pp. 551–566.

[115] B. Amin Azad, O. Starov, P. Laperdrix, and N. Nikiforakis, "Web runner 2049: Evaluating third-party anti-bot services," in *Detection of Intrusions and Malware, and Vulnerability Assessment: 17th International Conference, DIMVA 2020, Lisbon, Portugal, June 24–26, 2020, Proceedings 17*. Springer, 2020, pp. 135–159.

[116] J. Sørensen and S. Kosta, "Before and after gdpr: The changes in third party presence at public and private european websites," in *The World Wide Web Conference*, 2019, pp. 1590–1600.

[117] V. Bannihatti Kumar, R. Iyengar, N. Nisal, Y. Feng, H. Habib, P. Story, S. Cherivirala, M. Hagan, L. Cranor, S. Wilson *et al.*, "Finding a choice in a haystack: Automatic extraction

of opt-out statements from privacy policy text," in *Proceedings of The Web Conference 2020*, 2020, pp. 1943–1954.

[118] R. M. Mohammad, F. Thabtah, and L. McCluskey, "Predicting phishing websites based on self-structuring neural network," *Neural Computing and Applications*, vol. 25, pp. 443–458, 2014.

[119] N. Abdelhamid, A. Ayesh, and F. Thabtah, "Phishing detection based associative classification data mining," *Expert Systems with Applications*, vol. 41, no. 13, pp. 5948–5959, 2014.

[120] D. Kaur and P. Kaur, "Empirical analysis of web attacks," *Procedia Computer Science*, vol. 78, pp. 298–306, 2016.

[121] R. Heartfield and G. Loukas, "A taxonomy of attacks and a survey of defence mechanisms for semantic social engineering attacks," *ACM Computing Surveys (CSUR)*, vol. 48, no. 3, pp. 1–39, 2015.

[122] I. A. M. Abass, "Social engineering threat and defense: a literature survey," *Journal of Information Security*, vol. 9, no. 04, p. 257, 2018.

[123] M. Hijji and G. Alam, "A multivocal literature review on growing social engineering based cyber-attacks/threats during the covid-19 pandemic: challenges and prospective solutions," *Ieee Access*, vol. 9, pp. 7152–7169, 2021.

[124] S. Sharmeen, S. Huda, J. H. Abawajy, W. N. Ismail, and M. M. Hassan, "Malware threats and detection for industrial mobile-iot networks," *IEEE access*, vol. 6, pp. 15 941–15 957, 2018.

[125] K. A. Da Costa, J. P. Papa, C. O. Lisboa, R. Munoz, and V. H. C. de Albuquerque, "Internet of things: A survey on machine learning-based intrusion detection approaches," *Computer Networks*, vol. 151, pp. 147–157, 2019.

[126] N. Chaabouni, M. Mosbah, A. Zemmari, C. Sauvignac, and P. Faruki, "Network intrusion detection for iot security based on learning techniques," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 3, pp. 2671–2701, 2019.

[127] N. Waheed, X. He, M. Ikram, M. Usman, S. S. Hashmi, and M. Usman, "Security and privacy in iot using machine learning and blockchain: Threats and countermeasures," *ACM Computing Surveys (CSUR)*, vol. 53, no. 6, pp. 1–37, 2020.

[128] P. Williams, I. K. Dutta, H. Daoud, and M. Bayoumi, "A survey on security in internet of things with a focus on the impact of emerging technologies," *Internet of Things*, vol. 19, p. 100564, 2022.

[129] Y. Wu, Z. Wang, Y. Ma, and V. C. Leung, "Deep reinforcement learning for blockchain in industrial iot: A survey," *Computer Networks*, vol. 191, p. 108004, 2021.

[130] D. Unal, M. Hammoudeh, M. A. Khan, A. Abuarqoub, G. Epiphaniou, and R. Hamila, "Integration of federated machine learning and blockchain for the provision of secure big data analytics for internet of things," *Computers & Security*, vol. 109, p. 102393, 2021.

[131] W. Issa, N. Moustafa, B. Turnbull, N. Sohrabi, and Z. Tari, "Blockchain-based federated learning for securing internet of things: A comprehensive survey," *ACM Computing Surveys*, vol. 55, no. 9, pp. 1–43, 2023.

[132] N. Waheed, A. U. Rehman, A. Nehra, M. Farooq, N. Tariq, M. A. Jan, F. Khan, A. Z. Alalmaie, and P. Nanda, "Fedblockhealth: A synergistic approach to privacy and security in iot-enabled healthcare through federated learning and blockchain," *arXiv preprint arXiv:2304.07668*, 2023.

[133] N. Waheed, F. Khan, S. Mastorakis, M. A. Jan, A. Z. Alalmaie, and P. Nanda, "Privacy-enhanced living: A local differential privacy approach to secure smart home data," in *2023 IEEE International Conference on Omni-layer Intelligent Systems (COINS)*. IEEE, 2023, pp. 1–6.

[134] O. Starov, P. Gill, and N. Nikiforakis, "Are you sure you want to contact us? quantifying the leakage of pii via website contact forms." *Proc. Priv. Enhancing Technol.*, vol. 2016, no. 1, pp. 20–33, 2016.

[135] M. Ikram, H. J. Asghar, M. A. Kaafar, B. Krishnamurthy, and A. Mahanti, "Towards seamless tracking-free web: Improved detection of trackers via one-class learning," *arXiv preprint arXiv:1603.06289*, 2016.

[136] H. Yun, G. Lee, and D. J. Kim, "A chronological review of empirical research on personal information privacy concerns: An analysis of contexts and research constructs," *Information & Management*, vol. 56, no. 4, pp. 570–601, 2019.

[137] T. Libert, "An automated approach to auditing disclosure of third-party data collection in website privacy policies," in *Proceedings of the 2018 World Wide Web Conference*, 2018, pp. 207–216.

[138] C. Ischen, T. Araujo, H. Voorveld, G. van Noort, and E. Smit, "Privacy concerns in chatbot interactions," in *Chatbot Research and Design: Third International Workshop, CONVERSATIONS 2019, Amsterdam, The Netherlands, November 19–20, 2019, Revised Selected Papers 3*. Springer, 2020, pp. 34–48.

[139] M. S. I. Bhuiyan, A. Razzak, M. S. Ferdous, M. J. M. Chowdhury, M. A. Hoque, and S. Tarkoma, "Bonik: A blockchain empowered chatbot for financial transactions," in *2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*. IEEE, 2020, pp. 1079–1088.

[140] D. Biswas, "Privacy preserving chatbot conversations," in *2020 IEEE Third International Conference on Artificial Intelligence and Knowledge Engineering (AIKE)*. IEEE, 2020, pp. 179–182.

[141] D. Calvaresi, J.-P. Calbimonte, E. Siboni, S. Eggenschwiler, G. Manzo, R. Hilfiker, and M. Schumacher, "Erebots: Privacy-compliant agent-based platform for multi-scenario personalized health-assistant chatbots," *Electronics*, vol. 10, no. 6, p. 666, 2021.

[142] A. Ait-Mlouk, S. Alawadi, S. Toor, and A. Hellander, "Fedbot: Enhancing privacy in chatbots with federated learning," *arXiv preprint arXiv:2304.03228*, 2023.

[143] I. C. Society, I. of Electrical, and E. Engineers, *IEEE Annals of the History of Computing*. IEEE Computer Society, 2005, no. v. 27-28. [Online]. Available: https://books.google.com.au/books?id=xv9UAAAAMAAJ

[144] M. Hogan, B. Piccarreta, I. I. C. S. W. Group *et al.*, "Interagency report on status of international cybersecurity standardization for the internet of things (iot)," National Institute of Standards and Technology, Tech. Rep., 2018.

[145] C. Policy, "WhatsApp hack: Is any app or computer truly secure?" *BBC News*, pp. 1–7, 2019. [Online]. Available: https://www.bbc.com/news/technology-48282092

[146] C. Wheelus and X. Zhu, "Iot network security: Threats, risks, and a data-driven defense framework," *IoT*, vol. 1, no. 2, pp. 259–285, 2020.

[147] S. A. A. Abir, S. N. Islam, A. Anwar, A. N. Mahmood, and A. M. T. Oo, "Building resilience against covid-19 pandemic using artificial intelligence, machine learning, and iot: A survey of recent progress," *IoT*, vol. 1, no. 2, pp. 506–528, 2020.

[148] S. K. Singh, S. Rathore, and J. H. Park, “Blockiotintelligence: A blockchain-enabled intelligent iot architecture with artificial intelligence,” *Future Generation Computer Systems*, vol. 110, pp. 721–743, 2020.

[149] A. Creswell, T. White, V. Dumoulin, K. Arulkumaran, B. Sengupta, and A. A. Bharath, “Generative adversarial networks: An overview,” *IEEE signal processing magazine*, vol. 35, no. 1, pp. 53–65, 2018.

[150] I. Goodfellow, J. Pouget-Abadie, M. Mirza, B. Xu, D. Warde-Farley, S. Ozair, A. Courville, and Y. Bengio, “Generative adversarial networks,” *Communications of the ACM*, vol. 63, no. 11, pp. 139–144, 2020.

[151] Q. Liu, P. A. N. Li, W. Zhao, and W. E. I. Cai, “A Survey on Security Threats and Defensive Techniques of Machine Learning : A Data Driven View,” *IEEE Access*, vol. 6, pp. 12 103–12 117, 2018.

[152] A. Diro and N. Chilamkurti, “Leveraging LSTM Networks for Attack Detection in Fog-to-Things Communications,” *IEEE Communications Magazine*, vol. 56, no. 9, 2018.

[153] C. Kolias, G. Kambourakis, A. Stavrou, and S. Gritzalis, “Intrusion detection in 802.11 networks: Empirical evaluation of threats and a public dataset,” *IEEE Communications Surveys & Tutorials*, vol. 18, no. 1, pp. 184–208, 2015.

[154] A. Abeshu and N. Chilamkurti, “Deep Learning: The Frontier for Distributed Attack Detection in Fog-To-Things Computing,” *IEEE Communications Magazine*, vol. 56, no. 2, pp. 169–175, 2018.

[155] Z. Tan, A. Jamdagni, X. He, P. Nanda, and R. P. Liu, “A system for denial-of-service attack detection based on multivariate correlation analysis,” *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 2, pp. 447–456, Feb 2014.

[156] Z. Tan, A. Jamdagni, X. He, P. Nanda, R. P. Liu, and J. Hu, “Detection of denial-of-service attacks based on computer vision techniques,” *IEEE Transactions on Computers*, vol. 64, no. 9, pp. 2519–2533, Sep. 2015.

[157] N. Moustafa, B. Turnbull, and K. R. Choo, “An ensemble intrusion detection technique based on proposed statistical flow features for protecting network traffic of internet of things,” *IEEE Internet of Things journal*, vol. 6, no. 3, June 2019.

[158] U. Ahmad, H. Song, A. Bilal, S. Saleem, and A. Ullah, "Securing Insulin Pump System Using Deep Learning and Gesture Recognition," *Proceedings - 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications and 12th IEEE International Conference on Big Data Science and Engineering, Trustcom/BigDataSE 2018*, 2018.

[159] M. E. Aminanto, R. Choi, H. C. Tanuwidjaja, P. D. Yoo, and K. Kim, "Deep abstraction and weighted feature selection for Wi-Fi impersonation detection," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 3, pp. 621–636, 2017.

[160] B. Chatterjee, D. Das, and S. Sen, "RF-PUF: IoT security enhancement through authentication of wireless nodes using in-situ machine learning," *Proceedings of the 2018 IEEE International Symposium on Hardware Oriented Security and Trust, HOST 2018*, vol. PP, no. c, pp. 205–208, 2018.

[161] A. Azmoodeh, A. Dehghantanha, and K.-K. R. Choo, "Robust malware detection for internet of (battlefield) things devices using deep eigenspace learning," *IEEE transactions on sustainable computing*, vol. 4, no. 1, pp. 88–95, 2018.

[162] S. Aonzo, A. Merlo, M. Migliardi, L. Oneto, and F. Palmieri, "Low-Resource Footprint, Data-Driven Malware Detection on Android," *IEEE Transactions on Sustainable Computing*, vol. 3782, 2017.

[163] L. Wei, W. Luo, J. Weng, Y. Zhong, X. Zhang, and Z. Yan, "Machine learning-based malicious application detection of android," *IEEE Access*, vol. 5, pp. 25 591–25 601, 2017.

[164] P. Feng, J. Ma, C. Sun, X. Xu, and Y. Ma, "A novel dynamic android malware detection system with ensemble learning," *IEEE Access*, vol. 6, pp. 30 996–31 011, 2018.

[165] W. Wang, Z. Gao, M. Zhao, Y. Li, J. Liu, and X. Zhang, "DroidEnsemble: Detecting Android Malicious Applications with Ensemble of String and Structural Static Features," *IEEE Access*, vol. 6, pp. 31 798–31 807, 2018.

[166] L. F. Maimó, Á. Luis, P. Gómez, F. J. G. Clemente, M. G. I. L. Pérez, and G. M. Pérez, "A Self-Adaptive Deep Learning-Based System for Anomaly Detection in 5G Networks," *IEEE Access*, vol. 6, 2018.

[167] A. Javaid, Q. Niyaz, W. Sun, and M. Alam, "A deep learning approach for network intrusion detection system," *EAI Endorsed Transactions on Security and Safety*, vol. 3, no. 9, 5 2016.

[168] M. A. Ambusaidi, X. He, P. Nanda, and Z. Tan, "Building an intrusion detection system using a filter-based feature selection algorithm," *IEEE Transactions on Computers*, vol. 65, no. 10, pp. 2986–2998, Oct 2016.

[169] Y. Zhou, M. Han, L. Liu, J. S. He, and Y. Wang, "Deep learning approach for cyberattack detection," *INFOCOM 2018 - IEEE Conference on Computer Communications Workshops*, 2018.

[170] S. Prabavathy, K. Sundarakantham, and S. M. Shalinie, "Design of Cognitive Fog Computing for Intrusion Detection in Internet of Things," *Journal of Communications and Networks*, vol. 20, no. 3, pp. 291–298, 2018.

[171] EMarketer, "Number of smartphone users worldwide from 2014 to 2020 (in billions)," 2016. [Online]. Available: https://www.statista.com/statistics/330695/number-of-smartphone-users-worldwide/

[172] S. Sharmeen, S. Huda, J. H. Abawajy, W. N. Ismail, and M. M. Hassan, "Malware Threats and Detection for Industrial Mobile-IoT Networks," *IEEE Access*, vol. 6, pp. 15 941–15 957, 2018.

[173] W. H. Press, S. A. Teukolsky, W. T. Vetterling, and B. P. Flannery, *Numerical Recipes in C (2Nd Ed.): The Art of Scientific Computing*. New York, NY, USA: Cambridge University Press, 1992.

[174] L. Xiao, , Y. Li, and G. Han, "PHY-Layer Spoofing Detection With Reinforcement Learning in Wireless Networks," *IEEE Transactions on Vehicular Technology*, vol. 65, no. 12, pp. 10 037–10 047, 2016.

[175] L. Xiao, X. Wan, X. Lu, Y. Zhang, and D. Wu, "IoT Security Techniques Based on Machine Learning: How Do IoT Devices Use AI to Enhance Security?" *IEEE Signal Processing Magazine*, vol. 35, no. 5, 2018.

[176] H. Aksu, A. S. Uluagac, and E. Bentley, "Identification of Wearable Devices with Bluetooth," *IEEE Transactions on Sustainable Computing*, pp. 1–1, 2018.

[177] H. Zhu, X. Liu, R. Lu, and H. Li, "Efficient and Privacy-Preserving Online Medical Prediagnosis Framework Using Nonlinear SVM," *IEEE Jounral of Biomedical and Health Informatics*, vol. 21, no. 3, pp. 838–850, 2017.

[178] Q. Jia, L. Guo, Z. Jin, and Y. Fang, "Preserving model privacy for machine learning in distributed systems," *IEEE Transactions on Parallel and Distributed Systems*, vol. 29, no. 8, pp. 1808–1822, 2018.

[179] X. Ma, J. Ma, H. Li, Q. Jiang, and S. Gao, "PDLM: Privacy-Preserving Deep Learning Model on Cloud with Multiple Keys," *IEEE Transactions on Services Computing*, pp. 1–13, 2018.

[180] X. Sun, P. Zhang, J. K. Liu, J. Yu, and W. Xie, "Private machine learning classification based on fully homomorphic encryption," *IEEE Transactions on Emerging Topics in Computing*, vol. 6750, no. c, 2018.

[181] B. Feng, Q. Fu, M. Dong, D. Guo, and Q. Li, "Multistage and Elastic Spam Detection in Mobile Social Networks through Deep Learning," *IEEE Network*, vol. 32, no. 4, pp. 15–21, 2018.

[182] T. Zhang and Q. Zhu, "Distributed Privacy-Preserving Collaborative Intrusion Detection Systems for VANETs," *IEEE Transactions on Signal and Information Processing over Networks*, vol. 4, no. 1, pp. 148–161, 2018.

[183] R. Baxter, N. Hastings, A. Law, and E. Glass, "Future uses of blockchain. vol. 39," 5.

[184] K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the internet of things," *Ieee Access*, vol. 4, pp. 2292–2303, 2016.

[185] G. Chapron, "The environment needs cryptogovernance," *Nature*, vol. 545, no. 7655, pp. 403–405, 2017.

[186] N. Kshetri, "Blockchain's roles in strengthening cybersecurity and protecting privacy," *Telecommunications Policy*, vol. 41, no. 10, 2017. [Online]. Available: https://@doi.org/10.1016/j.telpol.2017.09.003

[187] C. Machado and A. A. Frohlich, "IoT data integrity verification for cyber-physical systems using blockchain," *Proceedings - 2018 IEEE 21st International Symposium on Real-Time Computing, ISORC 2018*, 2018.

[188] N. Tapas, G. Merlino, and F. Longo, "Blockchain-based iot-cloud authorization and delegation," in *2018 IEEE International Conference on Smart Computing (SMARTCOMP)*, 2018, pp. 411–416.

[189] X. Liang, J. Zhao, S. Shetty, and D. Li, "Towards data assurance and resilience in iot using blockchain," in *MILCOM 2017 - 2017 IEEE Military Communications Conference (MILCOM)*, Oct 2017, pp. 261–266.

[190] C. Tselios, I. Politis, and S. Kotsopoulos, "Enhancing SDN security for iot-related deployments through blockchain," *2017 IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN)*, vol. 2017-Janua, 2017.

[191] P. K. Sharma, S. Singh, Y. S. Jeong, and J. H. Park, "DistBlockNet: A Distributed Blockchains-Based Secure SDN Architecture for IoT Networks," *IEEE Communications Magazine*, vol. 55, no. 9, 2017.

[192] J. Gao, K. O. Asamoah, E. B. Sifah, A. Smahi, Q. Xia, H. Xia, X. Zhang, and G. Dong, "Gridmonitoring: Secured sovereign blockchain based monitoring on smart grid," *IEEE access*, vol. 6, pp. 9917–9925, 2018.

[193] H. R. Hasan and K. Salah, "Blockchain-Based Proof of Delivery of Physical Assets with Single and Multiple Transporters," *IEEE Access*, vol. 6, 2018.

[194] Y. Gupta, R. Shorey, D. Kulkarni, and J. Tew, "The applicability of blockchain in the Internet of Things," *2018 10th International Conference on Communication Systems and Networks, COMSNETS 2018*, vol. 2018-Janua, 2018.

[195] T. Golomb, Y. Mirsky, and Y. Elovici, "Ciota: Collaborative iot anomaly detection via blockchain," *CoRR*, vol. abs/1803.03807, 2018. [Online]. Available: http://arxiv.org/abs/1803.03807

[196] P. K. Sharma, M. Y. Chen, and J. H. Park, "A Software Defined Fog Node Based Distributed Blockchain Cloud Architecture for IoT," *IEEE Access*, vol. 6, 2018.

[197] V. Sharma, I. You, F. Palmieri, D. N. K. Jayakody, and J. Li, "Secure and Energy-Efhcient Handover in Fog Networks Using Blockchain-Based DMM," *Ieee Communications Magazine*, vol. 56, no. 5, 2018.

[198] J. Wang, M. Li, Y. He, H. Li, K. Xiao, and C. Wang, "A blockchain based privacy-preserving incentive mechanism in crowdsensing applications," *Ieee Access*, vol. 6, pp. 17 545–17 556, 2018.

[199] L. Li, J. Liu, L. Cheng, S. Qiu, W. Wang, X. Zhang, and Z. Zhang, "Creditcoin: A privacy-preserving blockchain-based incentive announcement network for communications of smart

vehicles," *IEEE Transactions on Intelligent Transportation Systems*, vol. 19, no. 7, pp. 2204–2220, 2018.

[200] Z. Lu, W. Liu, Q. Wang, G. Qu, and Z. Liu, "A privacy-preserving trust model based on blockchain for VANETs," *IEEE Access*, vol. 6, 2018.

[201] L. Zhou, L. Wang, Y. Sun, and P. Lv, "BeeKeeper: A Blockchain-Based IoT System with Secure Storage and Homomorphic Computation," *IEEE Access*, vol. 6, 2018.

[202] Y. Rahulamathavan, R. C. Phan, S. Misra, and M. Rajarajan, "Privacy-preserving blockchain based iot ecosystem using attribute-based encryption," *2017 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS)*, no. October, 2017.

[203] K. Fan, Y. Ren, Y. Wang, H. Li, and Y. Yang, "Blockchain-based efficient privacy preserving and data sharing scheme of content-centric network in 5g," *IET communications*, vol. 12, no. 5, pp. 527–532, 2018.

[204] N. Z. Aitzhan and D. Svetinovic, "Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams," *IEEE Transactions on Dependable and Secure Computing*, vol. 15, no. 5, pp. 840–852, 2016.

[205] R. Guo, H. Shi, Q. Zhao, and D. Zheng, "Secure attribute-based signature scheme with multiple authorities for blockchain in electronic health records systems," *IEEE access*, vol. 6, pp. 11 676–11 686, 2018.

[206] J. Kang, R. Yu, X. Huang, S. Maharjan, Y. Zhang, and E. Hossain, "Enabling Localized Peer-to-Peer Electricity Trading among Plug-in Hybrid Electric Vehicles Using Consortium Blockchains," *IEEE Transactions on Industrial Informatics*, vol. 13, no. 6, 2017.

[207] J. Kang, R. Yu, X. Huang, M. Wu, S. Maharjan, S. Xie, and Y. Zhang, "Blockchain for secure and efficient data sharing in vehicular edge computing and networks," *IEEE internet of things journal*, vol. 6, no. 3, pp. 4660–4670, 2018.

[208] R. Agrawal, P. Verma, R. Sonanis, U. Goel, A. De, S. A. Kondaveeti, and S. Shekhar, "Continuous security in iot using blockchain," in *2018 IEEE international conference on acoustics, speech and signal processing (ICASSP)*. IEEE, 2018, pp. 6423–6427.

[209] J. Gu, B. Sun, X. Du, and S. Member, "Consortium Blockchain-Based Malware Detection in Mobile Devices," *IEEE Access*, vol. 6, 2018.

[210] B. Z. H. Zhao, M. Ikram, H. J. Asghar, M. A. Kaafar, A. Chaabane, and K. Thilakarathna, "A decade of mal-activity reporting: A retrospective analysis of internet malicious activity blacklists," in *Proceedings of the 2019 ACM Asia Conference on Computer and Communications Security*, 2019, pp. 193–205.

[211] M. Ikram, P. Beaume, and M. A. Kâafar, "Dadidroid: An obfuscation resilient tool for detecting android malware via weighted directed call graph modelling," *arXiv preprint arXiv:1905.09136*, 2019.

[212] P. Mamoshina, L. Ojomoko, Y. Yanovich, A. Ostrovski, A. Botezatu, P. Prikhodko, E. Izumchenko, A. Aliper, K. Romantsov, A. Zhebrak, I. Ogu, and A. Zhavoronkov, "Converging blockchain and next-generation artificial intelligence technologies to decentralize and accelerate biomedical research and healthcare," *Oncotarget*, vol. 9, pp. 5665–5690, 01 2018.

[213] G. J. Mendis, M. Sabounchi, J. Wei, and R. Roche', "Blockchain as a service: An autonomous, privacy preserving, decentralized architecture for deep learning," *CoRR*, vol. abs/1807.02515, 2018. [Online]. Available: http://arxiv.org/abs/1807.02515

[214] G. J. Mendis, Y. Wu, J. Wei, M. Sabounchi, and R. Roche, "A blockchain-powered decentralized and secure computing paradigm," *IEEE Transactions on Emerging Topics in Computing*, p. 1–1, 2020. [Online]. Available: http://dx.@doi.org/10.1109/TETC.2020.2983007

[215] J. Weng, J. Weng, J. Zhang, M. Li, Y. Zhang, and W. Luo, "DeepChain: Auditable and Privacy-Preserving Deep Learning with Blockchain-based Incentive," *IEEE Transactions on Dependable and Secure Computing*, vol. 14, no. 8, pp. 1–1, 2019.

[216] M. Shen, X. Tang, L. Zhu, X. Du, and M. Guizani, "Privacy-preserving support vector machine training over blockchain-based encrypted iot data in smart cities," *IEEE Internet of Things journal*, pp. 1–1, 2019.

[217] A. Goel, A. Agarwal, M. Vatsa, R. Singh, and N. Ratha, "DeepRing: Protecting Deep Neural Network with Blockchain," *Proc. of IEEE Conference on Computer Vision and Pattern Recognition Workshops (CVPRW)*, pp. 1–8, 2019.

[218] A. Fadaeddini, B. Majidi, and M. Eshghi, "Secure decentralized peer-to-peer training of deep neural networks based on distributed ledger technology," *The Journal of Supercomputing*, no. 0123456789, 2020. [Online]. Available: https://@doi.org/10.1007/s11227-020-03251-9

[219] W. Meng, E. W. Tischhauser, Q. Wang, Y. Wang, and J. Han, "When intrusion detection meets blockchain technology: a review," *Ieee Access*, vol. 6, pp. 10 179–10 188, 2018.

[220] R. Masood, D. Vatsalan, M. Ikram, and M. A. Kaafar, "Incognito: A method for obfuscating web data," in *Proceedings of the 2018 world wide web conference*, 2018, pp. 267–276.

[221] M. Kang and J. Kang, "A novel intrusion detection method using deep neural network for in-vehicle network security," in *2016 IEEE 83rd Vehicular Technology Conference (VTC Spring)*, May 2016, pp. 1–5.

[222] M. Sakurada and T. Yairi, "Anomaly detection using autoencoders with nonlinear dimensionality reduction," in *Proceedings of the MLSDA 2014 2Nd Workshop on Machine Learning for Sensory Data Analysis*, ser. MLSDA'14. New York, NY, USA: ACM, 2014, pp. 4:4–4:11. [Online]. Available: http://@doi.acm.org/10.1145/2689746.2689747

[223] W. Yan and L. Yu, "On accurate and reliable anomaly detection for gas turbine combustors: A deep learning approach," *arXiv preprint arXiv:1908.09238*, 2019.

[224] Y. Li, R. Ma, and R. Jiao, "A hybrid malicious code detection method based on deep learning," *International Journal of Security and Its Applications*, vol. 9, no. 5, pp. 205–216, 2015.

[225] F. Liang, W. G. Hatcher, W. Liao, W. Gao, and W. Yu, "Machine Learning for Security and the Internet of Things: The Good, the Bad, and the Ugly," *IEEE Access*, vol. 7, pp. 158 126–158 147, 2019.

[226] A. Chakraborty, M. Alam, V. Dey, A. Chattopadhyay, and D. Mukhopadhyay, "Adversarial attacks and defences: A survey," *arXiv preprint arXiv:1810.00069*, 2018.

[227] A. Agarwal, R. Singh, M. Vatsa, and N. Ratha, "Are image-agnostic universal adversarial perturbations for face recognition difficult to detect?" in *2018 IEEE 9th International Conference on Biometrics Theory, Applications and Systems (BTAS)*. IEEE, 2018, pp. 1–7.

[228] N. Akhtar and A. Mian, "Threat of adversarial attacks on deep learning in computer vision: A survey," *Ieee Access*, vol. 6, pp. 14 410–14 430, 2018.

[229] A. Goel, A. Singh, A. Agarwal, M. Vatsa, and R. Singh, "Smartbox: Benchmarking adversarial detection and mitigation algorithms for face recognition," in *2018 IEEE 9th International Conference on Biometrics Theory, Applications and Systems (BTAS)*, 2018, pp. 1–7.

[230] G. Goswami, A. Agarwal, N. Ratha, R. Singh, and M. Vatsa, "Detecting and mitigating adversarial perturbations for robust face recognition," *Int. J. Comput. Vision*, vol. 127, no. 6–7, p. 719–742, Jun. 2019. [Online]. Available: https://@doi.org/10.1007/s11263-019-01160-w

[231] G. Goswami, N. Ratha, A. Agarwal, R. Singh, and M. Vatsa, "Unravelling robustness of deep learning based face recognition against adversarial attacks," in *Proceedings of the AAAI Conference on Artificial Intelligence*, vol. 32, no. 1, 2018.

[232] A. Dorri, S. S. Kanhere, and R. Jurdak, "Blockchain in internet of things: Challenges and solutions," *CoRR*, vol. abs/1608.05187, 2016. [Online]. Available: http://arxiv.org/abs/1608.05187

[233] S. Biswas, K. Sharif, F. Li, B. Nour, and Y. Wang, "A scalable blockchain framework for secure transactions in iot," *IEEE Internet of Things journal*, 2018.

[234] J. C. Song, M. A. Demir, J. J. Prevost, and P. Rad, "Blockchain design for trusted decentralized IoT networks," in *2018 13th System of Systems Engineering Conference, SoSE 2018*, 2018.

[235] A. Reyna, C. Martín, J. Chen, E. Soler, and M. Díaz, "On blockchain and its integration with IoT. Challenges and opportunities," *Future Generation Computer Systems*, vol. 88, 2018.

[236] H. Niwa, "Why Blockchain is the future of IoT?" 2007. [Online]. Available: https://www.networkworld.com/article/3200029/internet-of-things/why-blockchain-is-the-future-of-iot.html

[237] M. S. Ferdous, M. J. M. Chowdhury, K. Biswas, N. Chowdhury, and V. Muthukkumarasamy, "Immutable autobiography of smart cars leveraging blockchain technology," *The Knowledge Engineering Review*, vol. 22, p. e3, 2020.

[238] T. Salman, M. Zolanvari, A. Erbad, R. Jain, and M. Samaka, "Security services using blockchains: A state of the art survey," *IEEE Communications Surveys Tutorials*, vol. 21, no. 1, pp. 858–880, Firstquarter 2019.

[239] T. T. A. Dinh, J. Wang, G. Chen, R. Liu, B. C. Ooi, and K.-L. Tan, "Blockbench: A framework for analyzing private blockchains," in *Proceedings of the 2017 ACM international conference on management of data*, 2017, pp. 1085–1100.

[240] K. Salah, M. H. U. Rehman, N. Nizamuddin, and A. Al-Fuqaha, "Blockchain for AI: Review and open research challenges," *IEEE Access*, vol. 7, pp. 10 127–10 149, 2019.

[241] Y. Zhang, R. Yu, S. Xie, W. Yao, Y. Xiao, and M. Guizani, "Home m2m networks: Architectures, standards, and qos improvement," *IEEE Communications Magazine*, vol. 49, no. 4, pp. 44–52, 2011.

[242] J. Zhao, Y. Chen, and W. Zhang, "Differential privacy preservation in deep learning: Challenges, opportunities and solutions," *IEEE Access*, vol. 7, pp. 48 901–48 911, 2019.

[243] P. Sundaravadivel, K. Kesavan, L. Kesavan, S. P. Mohanty, and E. Kougianos, "Smart-log: A deep-learning based automated nutrition monitoring system in the iot," *IEEE Transactions on Consumer Electronics*, vol. 64, no. 3, pp. 390–398, 2018.

[244] T. Denning, T. Kohno, and H. M. Levy, "Computer security and the modern home," *Communications of the ACM*, vol. 56, no. 1, pp. 94–103, 2013.

[245] S. Zhang, W. Li, Y. Wu, P. Watson, and A. Zomaya, "Enabling edge intelligence for activity recognition in smart homes," in *2018 IEEE 15th International Conference on Mobile Ad Hoc and Sensor Systems (MASS).* IEEE, 2018, pp. 228–236.

[246] G. Muhammad, M. F. Alhamid, M. Alsulaiman, and B. Gupta, "Edge computing with cloud for voice disorder assessment and treatment," *IEEE Communications Magazine*, vol. 56, no. 4, pp. 60–65, 2018.

[247] J. Lwowski, P. Kolar, P. Benavidez, P. Rad, J. J. Prevost, and M. Jamshidi, "Pedestrian detection system for smart communities using deep convolutional neural networks," in *2017 12th System of Systems Engineering Conference (SoSE).* IEEE, 2017, pp. 1–6.

[248] S. Mahmud, S. Ahmed, and K. Shikder, "A smart home automation and metering system using internet of things (iot)," in *2019 International Conference on Robotics, Electrical and Signal Processing Techniques (ICREST).* IEEE, 2019, pp. 451–454.

[249] S. Raskhodnikova, A. Smith, H. K. Lee, K. Nissim, and S. P. Kasiviswanathan, "What can we learn privately," in *Proceedings of the 54th Annual Symposium on Foundations of Computer Science*, 2008, pp. 531–540.

[250] C. Dwork, "Differential privacy," in *Automata, Languages and Programming: 33rd International Colloquium, ICALP 2006, Venice, Italy, July 10-14, 2006, Proceedings, Part II 33.* Springer, 2006, pp. 1–12.

[251] J. Zhao, T. Jung, Y. Wang, and X. Li, "Achieving differential privacy of data disclosure in the smart grid," in *IEEE INFOCOM 2014-IEEE conference on computer communications.* IEEE, 2014, pp. 504–512.

[252] Z. Zhang, Z. Qin, L. Zhu, J. Weng, and K. Ren, "Cost-friendly differential privacy for smart meters: Exploiting the dual roles of the noise," *IEEE Transactions on Smart Grid*, vol. 8, no. 2, pp. 619–626, 2016.

[253] C. Xu, J. Ren, D. Zhang, and Y. Zhang, "Distilling at the edge: A local differential privacy obfuscation framework for iot data analytics," *IEEE Communications Magazine*, vol. 56, no. 8, pp. 20–25, 2018.

[254] J. Liu, C. Zhang, and Y. Fang, "Epic: A differential privacy framework to defend smart homes against internet traffic analysis," *IEEE Internet of Things journal*, vol. 5, no. 2, pp. 1206–1217, 2018.

[255] M. U. Hassan, M. H. Rehmani, R. Kotagiri, J. Zhang, and J. Chen, "Differential privacy for renewable energy resources based smart metering," *Journal of Parallel and Distributed Computing*, vol. 131, pp. 69–80, 2019.

[256] Z. Wang, P. Ma, R. Wang, J. Zhang, Y. Chi, Y. Ma, and T. Yang, "Secure medical data collection via local differential privacy," in *2018 IEEE 4th International Conference on Computer and Communications (ICCC)*. IEEE, 2018, pp. 2446–2450.

[257] Ú. Erlingsson, V. Pihur, and A. Korolova, "Rappor: Randomized aggregatable privacy-preserving ordinal response," in *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*. ACM, 2014, pp. 1054–1067.

[258] Y. Xiao, Y. Shen, J. Liu, L. Xiong, H. Jin, and X. Xu, "Dphmm: Customizable data release with differential privacy via hidden markov model," *arXiv*, 2016, accessed: Mar. 27, 2023. [Online]. Available: http://arxiv.org/abs/1609.09172

[259] M. AKTURK, "Diabetes dataset," 2020. [Online]. Available: https://www.kaggle.com/datasets/mathchi/diabetes-data-set

[260] M. A. Razzaque, M. Milojevic-Jevric, A. Palade, and S. Clarke, "Middleware for internet of things: a survey," *IEEE Internet of Things journal*, vol. 3, no. 1, pp. 70–95, 2016.

[261] R. Roman and J. Lopez, "On using fog computing for personal data privacy and compliance with gdpr," *Computer*, vol. 51, no. 12, pp. 46–55, 2018.

[262] J. Konevcny, H. B. McMahan, F. X. Yu, P. Richtarik, A. T. Suresh, and D. Bacon, "Federated learning: Strategies for improving communication efficiency," in *Proceedings of the NIPS Workshop on Private Multi-Party Machine Learning*, vol. 2016. Google, 2016.

[263] H. B. McMahan, E. Moore, D. Ramage, S. Hampson, and B. A. y Arcas, "Communication-efficient learning of deep networks from decentralized data," *arXiv preprint arXiv:1602.05629*, 2017.

[264] B. Hitaj, G. Ateniese, and F. Perez-Cruz, "Deep models under the gan: information leakage from collaborative deep learning," in *Proceedings of the 2017 ACM SIGSAC conference on computer and communications security*, 2017, pp. 603–618.

[265] A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, "Medrec: Using blockchain for medical data access and permission management," in *Proceedings of the 2nd International Conference on Open and Big Data (OBD).* IEEE, 2016, pp. 25–30.

[266] S. Jiang, J. Cao, H. Wu, Y. Yang, M. Ma, and J. He, "Blockchain technology for secure sharing of patient medical records in a hospital environment," *IEEE Access*, vol. 6, pp. 65 779–65 789, 2018.

[267] Q. Yang, Y. Liu, T. Chen, and Y. Tong, "Federated machine learning: Concept and applications," *ACM Transactions on Intelligent Systems and Technology (TIST)*, vol. 10, no. 2, pp. 1–19, 2019.

[268] V. Smith, C.-K. Chiang, M. Sanjabi, and A. S. Talwalkar, "Federated multi-task learning," in *Advances in Neural Information Processing Systems 30 (NIPS 2017)*, 2017.

[269] F. Sattler, S. Wiedemann, and K.-R. Müller, "Robust and communication-efficient federated learning from non-iid data," in *Proceedings of the IEEE/CVF International Conference on Computer Vision*, 2019, pp. 4927–4936.

[270] T. Li, A. K. Sahu, A. Talwalkar, and V. Smith, "Federated optimization in heterogeneous networks," in *Proceedings of Machine Learning Research*, vol. 108, 2020, pp. 429–450.

[271] M. Abadi, A. Chu, I. Goodfellow, H. B. McMahan, I. Mironov, K. Talwar, and L. Zhang, "Deep learning with differential privacy," in *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security (CCS '16)*, 2016, pp. 308–318.

[272] A. Triastcyn and B. Faltings, "Federated learning with bayesian differential privacy," in *2019 IEEE International Conference on Big Data (Big Data)*, 2019, pp. 1299–1308.

[273] M. Chen, T. Malook, A. U. Rehman, Y. Muhammad, M. D. Alshehri, A. Akbar, M. Bilal, and M. A. Khan, "Blockchain-enabled healthcare system for detection of diabetes," *Journal of Information Security and Applications*, vol. 58, 2021.

[274] Z. L. T. Steinke‡, “The distributed discrete gaussian mechanism for federated learning with secure aggregation,” in *ICML*, 8 2021, p. 54.

[275] T. ElGamal, “A public key cryptosystem and a signature scheme based on discrete logarithms,” *IEEE transactions on information theory*, vol. 31, no. 4, pp. 469–472, 1985.

[276] B. A. Shawar and E. Atwell, “Chatbots: are they really useful?” *Journal for Language Technology and Computational Linguistics*, vol. 22, no. 1, pp. 29–49, 2007.

[277] E. Michiels, “Modelling chatbots with a cognitive system allows for a differentiating user experience.” in *PoEM doctoral consortium*, 2017, pp. 70–78.

[278] S. Ivanov and C. Webster, “Adoption of Robots, Aritificial Intelligence and Service Automation by Travel, Tourism and Hospitality Companies - A cost-benefit Analysis,” *International Scientific Conference “Contemporary tourism – traditions and innovations”, 19- 21 October 2017, Sofia University.*, pp. 1–9, 2017.

[279] M. Ikram, H. J. Asghar, M. A. Kaafar, A. Mahanti, and B. Krishnamurthy, “Towards Seamless Tracking-Free Web: Improved Detection of Trackers via One-class Learning,” *Proceedings on Privacy Enhancing Technologies*, vol. 2017, no. 1, pp. 79–99, 2016.

[280] S. S. Hashmi, M. Ikram, and M. A. Kaafar, “A longitudinal analysis of online ad-blocking blacklists,” in *2019 IEEE 44th LCN Symposium on Emerging Topics in Networking (LCN Symposium)*. IEEE, 2019, pp. 158–165.

[281] E. Carter and C. Knol, “Chatbot - an organisation’s friend or foe?” *Research in Hospitality Management*, vol. 9, no. 2, pp. 113–115, 2019.

[282] S. S. Hashmi, N. Waheed, G. Tangari, M. Ikram, and S. Smith, “Longitudinal compliance analysis of android applications with privacy policies,” in *International Conference on Mobile and Ubiquitous Systems: Computing, Networking, and Services*. Springer, 2021, pp. 280–305.

[283] Amazon, “Alexa top websites,” 2022. [Online]. Available: https://www.alexa.com/topsites

[284] “Web filter lookup,” 2022. [Online]. Available: https://www.fortiguard.com/webfilter

[285] I. Lal, “13 best chatbots to transform your conversation landscape in 2022,” 2022. [Online]. Available: https://surveysparrow.com/blog/best-chatbot-platforms/

[286] Aaron Brooks, “10 best chatbot builders in 2022,” 2022. [Online]. Available: https://www.ventureharbour.com/best-chatbot-builders/

[287] Werner Geyser, “Best ai chatbot platforms for 2022,” 2022. [Online]. Available: https://influencermarketinghub.com/ai-chatbot-platforms/

[288] Leah, “The 8 best chatbots of 2022,” 2022. [Online]. Available: https://www.userlike.com/en/blog/best-chatbots

[289] S. Barker, “15 best ai chatbot platforms to boost your conversations in 2022,” 2021. [Online]. Available: https://shanebarker.com/blog/best-ai-chatbot/

[290] S. Balkhi, “14 best ai chatbots software for your website (compared),” 2021. [Online]. Available: https://www.wpbeginner.com/showcase/best-chatbots-software-ai/

[291] Z. Group, “Top 10 best ai chatbots,” 2020. [Online]. Available: https://medium.datadriveninvestor.com/top-10-best-ai-chatbots-f68705a8f559

[292] J. Cook, R. Nithyanand, and Z. Shafiq, “Inferring tracker-advertiser relationships in the online advertising ecosystem using header bidding,” *arXiv preprint arXiv:1907.07275*, 2019.

[293] D. Inc., “What is the drift cookie security and privacy policy?” 2019. [Online]. Available: https://gethelp.drift.com/hc/en-us/articles/360019665133-What-is-the-Drift-Cookie-Security-and-Privacy-Policy-

[294] “Intercom cookie policy,” 2022. [Online]. Available: https://www.intercom.com/legal/cookie-policy

[295] Hubspot, “Cookies set on Hubspot’s websites,” p. 1, 2022. [Online]. Available: https://knowledge.hubspot.com/account/hubspot-cookie-security-and-privacy

[296] L. Inc., “Privacy policy,” 2021. [Online]. Available: https://www.livechat.com/legal/privacy-policy/

[297] T. Inc., “Privacy policy,” 2021. [Online]. Available: https://www.tidio.com/privacy-policy/

[298] A. Andreou, G. Venkatadri, O. Goga, K. P. Gummadi, P. Loiseau, and A. Mislove, “Investigating Ad Transparency Mechanisms in Social Media: A Case Study of Facebook’s Explanations,” in *NDSS*, San Diego, 2018.

[299] A. Andreou, M. Silva, F. Benevenuto, O. Goga, P. Loiseau, and A. Mislove, “Measuring the Facebook Advertising Ecosystem,” in *Network and Distribution Systems Security Symposium*, San Diego, 2019.

[300] G. Venkatadri, E. Lucherini, P. Sapiezynski, and A. Mislove, "Investigating sources of pii used in facebook's targeted advertising." *Proc. Priv. Enhancing Technol.*, vol. 2019, no. 1, pp. 227–244, 2019.

[301] A. Ghosh, G. Venkatadri, A. Mislove, and I. Kharagpur, "Analyzing Political Advertisers' Use of Facebook's Targeting Features," *Workshop on Technology and Consumer Protection (ConPro '19)*, 2019. [Online]. Available: https://facebook-targeting.ccs.neu.edu.

[302] M. Ikram, N. Vallina-Rodriguez, S. Seneviratne, M. A. Kaafar, and V. Paxson, "An analysis of the privacy and security risks of android vpn permission-enabled apps," in *Proceedings of the 2016 internet measurement conference*, 2016, pp. 349–364.

[303] M. Ikram and M. A. Kaafar, "A first look at mobile Ad-Blocking apps," *2017 IEEE 16th International Symposium on Network Computing and Applications, NCA 2017*, pp. 1–8, 2017.

[304] S. S. Hashmi, M. Ikram, and S. Smith, "On optimization of ad-blocking lists for mobile devices," in *Proceedings of the 16th EAI International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services*, ser. MobiQuitous '19, 2019, p. 220–227.

[305] O. Starov, P. Gill, and N. Nikiforakis, "Are You Sure You Want to Contact Us? Quantifying the Leakage of PII via Website Contact Forms," *PETS*, vol. 2016, no. 1, pp. 20–33, 2015.

[306] K. Gondaliya, S. Butakov, and P. Zavarsky, "SLA as a mechanism to manage risks related to chatbot services." *IEEE Intl Conference on Intelligent Data and Security*, 2020.

[307] C. Ischen, T. Araujo, H. Voorveld, G. v. Noort, and E. Smit, "Privacy concerns in chatbot interactions," in *International workshop on chatbot research and design*. Springer, 2019, pp. 34–48.

[308] M. S. I. Bhuiyan, A. Razzak, M. S. Ferdous, M. J. M. Chowdhury, M. A. Hoque, and S. Tarkoma, "BONIK: A blockchain empowered chatbot for financial transactions," in *TrustCom*, 2020.

[309] D. Biswas, "Privacy Preserving Chatbot Conversations," *Proceedings - 2020 IEEE 3rd International Conference on Artificial Intelligence and Knowledge Engineering, AIKE 2020*, pp. 179–182, 2020.

[310] W. Ye and Q. Li, "Chatbot Security and Privacy in the Age of Personal Assistants," *Proceedings - 2020 IEEE/ACM Symposium on Edge Computing, SEC 2020*, pp. 388–393, 2020.

[311] J. Bozic and F. Wotawa, “Security testing for chatbots,” in *IFIP International Conference on Testing Software and Systems*. Springer, 2018, pp. 33–38.

[312] M. Ikram, R. Masood, G. Tyson, M. A. Kaafar, N. Loizon, and R. Ensafi, “The chain of implicit trust: An analysis of the web third-party resources loading,” New York, NY, USA, p. 2851–2857, 2019. [Online]. Available: https://doi.org/10.1145/3308558.3313521

[313] “React – a javascript library for building user interfaces,” https://reactjs.org, 2022.

[314] “Angular - a platform for building mobile and desktop web applications,” https://angular.io, 2022.