electronics

Article

Identifying Adversary Impact Using End User Verifiable Key with Permutation Framework

Mohd Anjum [1], Sana Shahab [2], Yang Yu [3,*] and Habib Figa Guye [4]

[1] Department of Computer Engineering, Aligarh Muslim University, Aligarh 202002, India
[2] Department of Business Administration, College of Business Administration, Princess Nourah Bint Abdulrahman University, P.O. Box 84428, Riyadh 11671, Saudi Arabia
[3] Centre for Infrastructure Engineering and Safety (CIES), University of New South Wales, Sydney, NSW 2052, Australia
[4] Department of Information Science, College of Informatics, Bule Hora University, Hagere Maryam 144, Ethiopia
* Correspondence: yang.yu@uts.edu.au

Abstract: In the Internet of Things (IoT), security is a crucial aspect that ensures secure communication, transactions, and authentication for different applications. In IoT security, maintaining the user interface and platform security is a critical issue that needs to be addressed due to leaky security distribution. During communication, synchronisation and security are important problems. The security problems are caused by the adversary impact and vulnerable attacks, leading to service failure. Therefore, the Permutated Security Framework (PSF) is designed to manage security in the IoT by providing secure communication, transactions, and authentication for different applications. The PSF uses time intervals to manage transaction security. These intervals are secured using end-verifiable keys generated using the conventional Rivest–Shamir–Adleman (RSA) technique in IoT-based communication-related applications. In this approach, the key validity is first provided for the interval, and in the latter, the access permitted time modifies its validity. The security of transactions is managed by dividing time into smaller intervals and providing different levels of security for each interval. By using time intervals, the framework is adaptable and adjustable to changes in the system, such as user density and service allocation rate, adapting parallel transactions per support vector classifications' recommendations. The proposed framework aims to synchronise interval security, service allocation, and user flexibility to mitigate adversary impact, service failures, and service delays while improving the access rate and transactions. This allows for more flexibility and better management of transaction security. The proposed framework reduces adversary impact (10.98%), service failure (11.82%), and service delay (10.19%) and improves the access rate by 7.73% for different transactions.

Keywords: Internet of Things; RSA; security; support vector machine; wireless sensor networks

Citation: Anjum, M.; Shahab, S.; Yu, Y.; Guye, H.F. Identifying Adversary Impact Using End User Verifiable Key with Permutation Framework. *Electronics* **2023**, *12*, 1136. https://doi.org/10.3390/electronics12051136

Academic Editors: Tomasz Rak and Dariusz Rzońca

Received: 28 January 2023
Revised: 23 February 2023
Accepted: 23 February 2023
Published: 26 February 2023

1. Introduction

The Internet of Things (IoT) is a rapidly growing technology that connects everyday devices to the internet, allowing them to collect and share data. It encompasses a wide range of devices, from smartphones and laptops to home appliances, industrial equipment, and even automobiles. It helps to increase the communication process among users and organisations. This technology has the potential to revolutionise many industries by enabling more efficient and automated processes, improved decision-making, and new business models. IoT is widely used in smart applications to enhance the system's overall performance and provide a better user experience [1]. As the number of connected devices grows, so do security and privacy concerns. Additionally, IoT systems are distributed and open; therefore, they are vulnerable to various security threats such as hacking, data breaches, and unauthorised access. IoT nodes transfer lightweight data among the users

and provide a better authentication process. Security is a major concern in IoT due to the large amount of data that needs to be managed. IoT is used in smart devices and wireless sensor networks (WSN) to enhance user services [2]. Proper authentication processes are used to address security issues, such as Authentication and Key Agreement (AKA) schemes. AKA schemes are applied in IoT to identify unauthorised persons from accessing the personal information of users [3]. A secret session key is shared with the users for the authentication process, and authentication will be declined without the key. AKA helps protect users from attackers by providing a better authentication process and maximising the system's performance by ensuring users' security and privacy. WSN is also used in security issues to find the users' exact location and identify intruders. While authenticating, a device's current location is traced, which helps to finalise the authentication process [4,5].

The IoT is widely utilised in various applications to improve communication among organisations and users and provide better services. Data processing is one of the main tasks in IoT, which helps to improve user performance [6]. IoT enables users to transfer data or information from one person to another using smart devices. Data transaction or transfer allows users to send information from their current location without travelling [7]. However, data transfer may also cause some security threats, and a proper authentication process is needed to ensure a secure data processing system [8]. Privacy and security are major concerns in IoT while transferring data. To address these concerns, technologies such as radiofrequency identification (RFID) are used in IoT to enhance security and privacy. RFID interacts with tags of the information and provides a better solution to security issues [9]. RFID tags have electronic product codes for each transaction, which helps to track the exact whereabouts of the data being transferred. WSN is also used in IoT and has nodes that identify the information's frequency and bandwidth. Using WSN in IoT applications makes the users' communication process safe and secure [4,10].

Synchronised security measures play a crucial role in every IoT application. WSN is used in IoT to ensure the users' security and prevents data processing errors. Independent nodes identify security errors and eliminate unwanted threats [11]. WSN captures the users' location by analysing the network's frequency and bandwidth, which plays a vital role in the authentication process. WSN also synchronises the security process by reducing the latency rate in services and providing better services to the users at the needed time [12,13]. RFID is also used in IoT for communication, where interacting tags are identified based on the device's frequency and ensure the users' security [14]. Electronic Product Code is used in every transaction process to track the data's whereabouts and secure the users' information from attackers. RFID is analysed by a classification, which is performed based on certain features of the users. AKA ensures the security of the users in a synchronised form by providing a secret session key to users from the device for an authentication process. The session key helps users to prevent cyber-attacks [11,15].

The proposed PSF aims to manage security in the IoT by providing secure communication, transactions, and authentication for different applications. One of the key features of the PSF is the use of time intervals, which are secured by end-verifiable keys generated using the conventional RSA technique. In this approach, the PSF creates unique security keys for different IoT devices and applications by permuting the elements of a set. These keys are then used to encrypt communications and authenticate transactions between devices. However, unlike the conventional approach, the proposed approach uses time intervals to generate the permuted keys. The keys are generated at specific time intervals and are valid for a limited period. This approach allows for more frequent updates to the security keys, which helps keep communications and transactions more secure. Even if a key is compromised, it will only be valid for a short time and will be replaced by a new key shortly. The RSA technique is used to generate the keys so that they are end-verifiable, which means that the authenticity of the key is verified at the end of the communication, which ensures that the communication is secure. It is a widely used and widely accepted encryption method. It creates a pair of public and private keys used to encrypt and decrypt data, respectively. In the PSF, the same pair of keys is used to encrypt and decrypt the

data. This ensures that only authorised devices can communicate with each other and that transactions are secure. Additionally, the PSF includes a mechanism for updating and revoking the keys at regular intervals, which allows for the secure management of IoT devices over time. The time intervals at which the keys are generated and updated can be adjusted based on the specific requirements of the application. This allows for a more dynamic and adaptive approach to security, which can help keep communications and transactions more secure overall.

The paper is structured into the following sections: Section 1 introduces an overview of the problems of security in the IoT and the need for a framework to manage security in this context, introducing the PSF and its key features, such as the use of time intervals and end-verifiable keys generated using the RSA technique. Section 2 illustrates the review of existing research on security in the IoT and identifies the key contributions. Section 3 provides a detailed description of the proposed PSF, including the initial system setup and the RSA algorithm used to generate the keys, and explains how the PSF synchronises interval security, service allocation, and user flexibility to improve the access rate and transactions. Section 4 presents the results of the research, including the performance parameters of the PSF, such as adversary impact, service failure, service delay, access rate, and service transactions, and compares the PSF with the existing system based on all the performance parameters and analyses the results. Lastly, Section 5 summarises the key findings of the research and describes the contributions of the PSF to managing security in the IoT.

2. Related Works

This literature survey explores the various studies and research conducted on IoT security and privacy issues. With the increasing popularity of IoT and the integration of interconnected devices and systems, it has become imperative to address the concerns surrounding the security and privacy of data transmitted over these networks. Various authentication solutions have been proposed to address these concerns, but they often fall short in terms of efficiency and practicality as compared to the proposed model. In this related work, we will delve into the various studies conducted in this field and examine the proposed solutions and their effectiveness. We will also explore the potential of new technologies, such as blockchain and elliptic curve cryptography, in addressing these issues and the challenges that still need to be addressed.

Biswas et al. [16] proposed a scalable blockchain framework for secure IoT transaction processes using a peer network. One of the biggest challenges of combining IoT and blockchain technology is the scalability of the ledger and the speed at which transactions can be executed within a blockchain system. The network's scalability is improved by balancing the ledger and execution time during the transaction process. A peer network assists the system in understanding every detail of the transaction and identifying the gap between ledger bridges. The proposed solution addresses the scalability issues associated with integrating IoT and blockchain by implementing a scalable local ledger that limits the number of transactions entering the global blockchain while maintaining peer validation at both the local and global levels. Experiment results show that the proposed framework increases transaction security while decreasing network storage size and blockchain weight. Currently, smart home environments are vulnerable to security breaches; therefore, Yu et al. [17] created a secure and efficient three-factor authentication protocol for IoT-enabled smart homes to address the security weaknesses found in Kaur and Kumar's protocol. Elliptic curve cryptosystems are used in the proposed protocol to ensure the users' security and privacy. The formal and informal security analysis process is done in the proposed framework for improving users' privacy. Compared with other existing privacy-preserving protocols, the proposed framework increases the users' overall security and improves the system's efficiency. Asheralieva et al. [18] designed a mobile edge computing network mechanism for IoT-based applications to provide system security and scalability. The proposed method uses the peer technique to identify the blocks of the shared nodes and

provide better communication to the users during the transaction process. The proposed system uses a new consensus mechanism in which each peer votes on the outputs of each block task in its shard, using a reputation-based coalitional game model (RBCGM). RBCGM is also used here to improve the overall services of the system. Huang et al. [19] introduced a new efficient revocable large universe multi-authority attribute-based encryption to address the security issues related to controlling access to data in constantly changing IoT environments. This method supports user-attribute, which is used in a security process. Integrating a cloud computing system also increases the network's overall security. The proposed scheme supports user-attribute revocation, prevents collusion attacks, and protects against the collusion attack of revoked and non-revoked users. It satisfies both forward and backward security requirements, making it suitable for large-scale collaborations across multiple domains in the dynamic and cloud-assisted IoT. It increases the overall performance of the network by ensuring the security of the users from attackers.

Sadri et al. [20] proposed an anonymous two-factor authentication protocol for preserving the integrity and confidentiality of the transmitted messages in WSNs for the IoT that addresses the security vulnerabilities of the existing state-of-the-art protocol proposed by Wu et al. [21]. A WSN is used in the proposed protocol to extend the system's lifetime. The proposed method analyses formal and informal problems to secure the authenticating user process and provide better communication services and are secure against various known attacks such as sensor and user trace, sensor capture, offline password guessing, and replay attacks. Dorri et al. [22] established a lightweight, scalable blockchain method for IoT applications that address traditional blockchain technology's computational and scalability limitations. The proposed blockchain method uses a distributed time-based consensus algorithm, which helps reduce latency and system delay rates. It helps to manage blockchain delays and provides better services to users. Compared with other methods, the proposed lightweight, scalable blockchain method strongly protects from various security attacks. Simulation studies indicate that it reduces packet overhead and delay and increases the overall performance and blockchain scalability compared to relevant baselines. Vishwakarma et al. [23] developed a novel communication and authentication method for providing identification, authentication, secure communication, and data integrity in the IoT network. Blockchain and a hybrid cryptosystem technique are used in the proposed scheme to enhance the security system of the applications. Angular distance based on the cluster approach is used here to analyse the system's securities. Analytical results show that the proposed secure communication and authentication method reduced the computation time and protected systems from various cyberattacks such as impersonation, message replay, man-in-the-middle, and botnet attacks.

Peneti et al. [24] introduced a method for managing security, privacy, and confidentiality in next-generation networks such as IoT and 6G by combining blockchain and a grey wolf-optimised modular neural network approach. The proposed method creates user-authenticated blocks to manage security and privacy properties, and the neural network is used to optimise latency and computational resource utilisation in IoT-enabled smart applications. A simulation study is performed to display the over-efficiency of the system with respect to the multi-layer perceptron and deep learning networks, and it is shown to have low latency and high security (99.12%). Majumder et al. [25] introduced a constraint application protocol based on elliptic curve cryptography. It establishes a secure session key between IoT devices and a remote server using lightweight elliptic curve cryptography to overcome the limitations of key management and multicast security in constraint application protocol, which is used for communication between lightweight resource constraint devices in an IoT network. The proposed approach provides a constraint application protocol implementation for authentication in IoT networks, and it is found to be lightweight and secure after analysing various cryptographic attacks. Lin et al. [26] introduced a new settlement model for IoT data exchange services that use blockchain technology to overcome the limitations of traditional centralised models. The proposed model includes a Bitcoin-based time commitment scheme and an optimised practical Byzantine

fault-tolerant consensus protocol named ReBFT to ensure fairness and accountability in the decentralised network. It also ensures users a safe and secure transaction process and prevents unauthorised authentication. Several experiments are conducted to verify the feasibility of the proposal. Compared with existing protocols, the proposed scheme raises the feasibility and service efficiency.

Attarian et al. [27] proposed a communication protocol for secure and anonymous mHealth transactions using a combination of onion routing, blockchain smart contracts, and the user datagram protocol to protect the security and privacy of clients' identities. The blockchain approach is used in the proposed protocol to ensure the structure and architecture of the application. The proposed protocol aims to address challenges of anonymity, untraceability, unlinkability, and unforgeability in healthcare transactions and can detect malicious clients who send false data and helps to eliminate those details from the database. The proposed protocol ensures the security and privacy of the users while transacting data. Experimental outcomes and privacy proofs show that the proposed protocol has a reasonable computational cost and provides sufficient protection for IoT-based mHealth transactions. Yazdinejad et al. [28] discussed the challenges of IoT, such as security and energy consumption. They proposed a solution to mitigate these challenges by combining blockchain and software-defined networks in IoT networks. The proposed architecture uses a cluster structure with a new routing protocol. It utilises both public and private blockchains for peer-to-peer communication between IoT devices and software-defined network controllers, which eliminates proof-of-work and uses an efficient authentication method, making it suitable for resource-constrained IoT devices. Software-defined network controller plays a vital role in this protocol, which helps ensure the users' security while processing data. The experimental results show that this proposed architecture performs better throughput, delay, and energy consumption than other routing protocols. Compared with other security methods, the proposed protocol increases users' scalability, security, and privacy and reduces the computation cost with the help of the blockchain technique.

Srinivas et al. [29] proposed a new lightweight chaotic map-based authenticated key agreement protocol (CMAKAP) for the industrial environment that aims to increase security using a fuzzy extractor technique for biometric verification. The authentication process is done based on the user's biometrics, personal information, and smart cards, which help to prevent the users from being unauthorised. The real-or-random method is used here to analyse the security issues in the applications. The scheme also supports adding new devices, changing passwords/biometrics, and revoking smart cards. Formal security analysis and simulation studies were conducted, and it was found that the proposed scheme provides superior security compared to other existing methods. Pham et al. [30] introduced a mutual privacy-preserving authentication protocol (MPPAP) by using an elliptic curve cryptography approach to improve security and protect the privacy of IoT devices while also being efficient in resource consumption. It helps to provide better communication services to the users. A secret session key is shared with the users for the authentication process, ensuring the users' security and privacy. The proposed model extends previous works and includes a distributed network architecture and secure communications. The protocol has been formally proven correct, is resilient to attacks, and has low energy consumption. Then, the overall summary of the existing works is summarised in Table 1.

Table 1. Summary of the related works.

Reference	Method(s)	Purpose	Efficiency
Biswas et al. [16]	Scalable blockchain framework	To address the scalability issues associated with integrating IoT and blockchain.	Increases transaction security while decreasing network storage size and blockchain weight.
Yu et al. [17]	Three-factor authentication protocol	To address the security weaknesses found in Kaur and Kumar's protocol.	Increases the users' overall security and improves the system's efficiency.
Asheralieva et al. [18]	Reputation-based coalitional game model (RBCGM)	To identify the blocks of the shared nodes and provide better communication.	Improves the overall services of the system.
Huang et al. [19]	Revocable large universe multi-authority attribute-based encryption	To address the security issues related to controlling access to data in constantly changing IoT environments.	Ensures the security of the users from attackers.
Sadri et al. [20]	Anonymous two-factor authentication protocol	To address the security vulnerabilities.	Preserves the integrity and confidentiality of the transmitted messages.
Wu et al. [21].	Three-factor authentication protocol	To analyse both formal and informal problems to secure the authenticating user process.	Manages data security and confidentiality.
Dorri et al. [22]	A lightweight, scalable blockchain method	To address the computational and scalability limitations of traditional blockchain technology.	Reduces latency and system delay rates.
Vishwakarma et al. [23]	Blockchain and a hybrid cryptosystem technique	To resolve integrity and security-related issues.	Reduces the computation time and protect systems from various cyberattacks.
Peneti et al. [24]	Blockchain and grey wolf-optimised modular neural network approach	To optimise latency and computational resource utilisation.	Low latency and high security
Majumder et al. [25]	Constraint application protocol	To overcome the limitations of key management and multicast security in a constraint application protocol.	Secures the information from different cryptographic attacks.
Lin et al. [26]	Byzantine fault-tolerant consensus protocol	To overcome the limitations of traditional centralised models.	Ensures users a safe and secure transaction process and prevents unauthorised authentication
Attarian et al. [27]	Combination of onion routing, blockchain smart contracts	To protect the security and privacy of clients' identities	Addresses challenges of anonymity, untraceability, unlinkability, and unforgeability in healthcare transactions and can detect malicious clients
Yazdinejad et al. [28]	Blockchain and software-defined networks	To propose a solution to mitigate these challenges by combining blockchain and software-defined networks.	Better performance in throughput, delay, and energy consumption than other routing protocols.
Srinivas et al. [29]	Lightweight chaotic map-based authenticated key agreement protocol (CMAKAP)	To increase security by using a fuzzy extractor technique for biometric verification.	The proposed scheme provides superior security compared to other existing methods.
Pham et al. [30]	mutual privacy-preserving authentication protocol (MPPAP)	To improve security and protect the privacy of IoT devices	Proven correct and resilient to different attacks while having low energy consumption.

3. Proposed Permuted Security Framework

The design goal of PSF is to improve the user flexibility rate of the IoT applications by reducing adversary fewer services in IoT combined end-user applications. This platform provides secure transactions, authentication, and communication for various end-user industrial applications. Its experience in controlling security is synchronising the IoT platform and user interface. It provides different security threats to be distributed for secure and dependable transactions through the IoT network. The proposed PSF is illustrated in the IoT environment as in Figure 1. The cloud and security have the connections that are used to manage data security. Here, security techniques are utilised to manage data security.

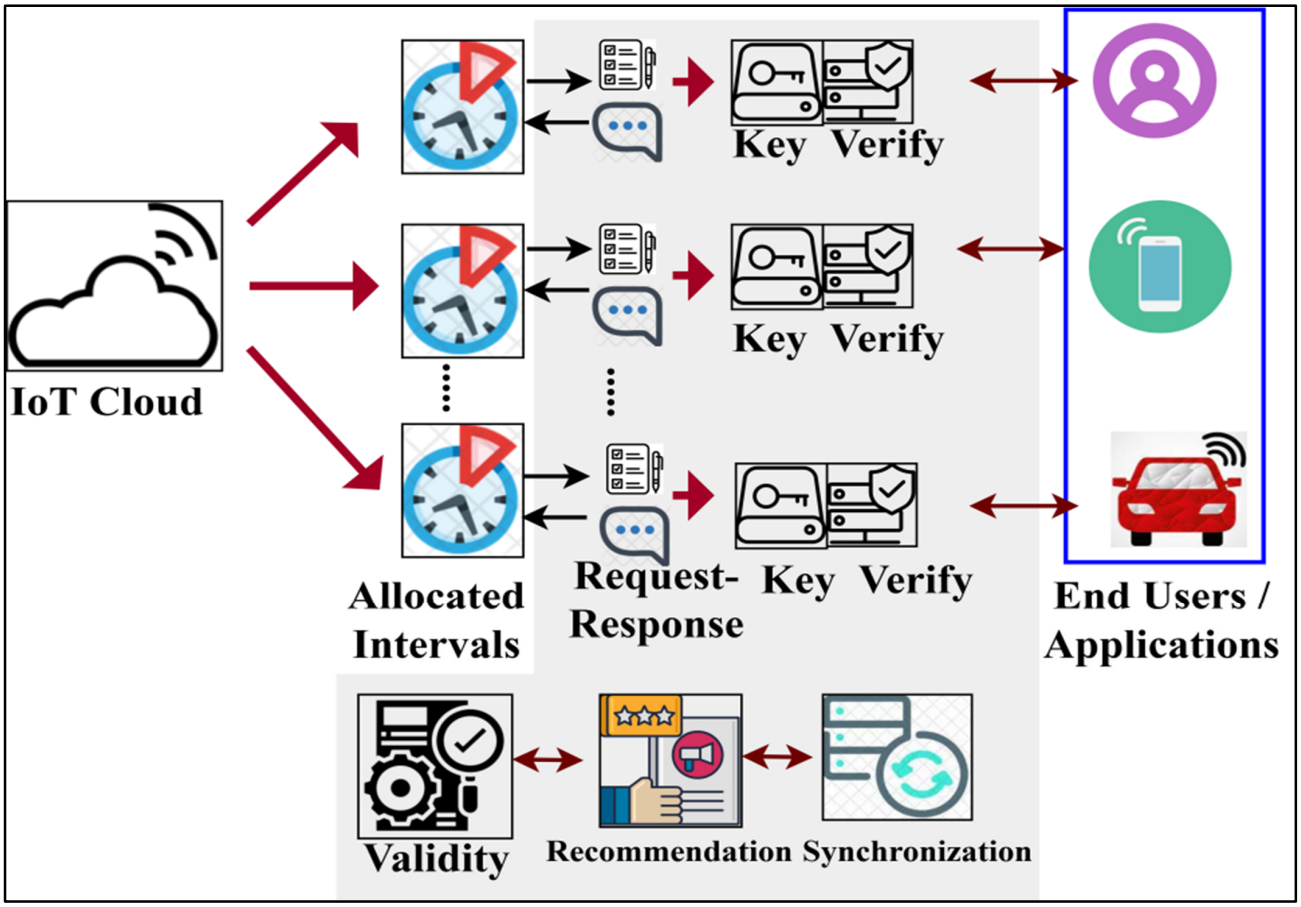

Figure 1. Proposed permuted security framework in IoT environment.

The proposed framework can provide secure data collection and security distribution for synchronisation between end-user applications and the platform using transaction time intervals. In this manner, the data transactions, authentication, and communication through the IoT platform are secured from permitting adversary fewer services to improve user flexibility harmoniously and the service allocation rate of smart end-user applications, as shown in Figure 1. The function of PSF assisted in providing a secure data collection and distribution security. Data collection from the IoT cloud and user side is performed, and security is the distribution to both sender and receiver. The applications and processing centres are linked through IoT. Permutated security in the IoT platform and the user interface is administered to prevent leaky security distribution, adversary fewer services, and service failures. The IoT environment ensures data transactions between the applications and processing centres. The operations of the IoT cloud and user interface in the platform are used for synchronisation, transactions, and authentication. Synchronising fewer services for the applications and processing centres is processed and analysed using learning.

Initial System Setup

The IoT network is determined using two terminals: the IoT cloud and the user interface. The IoT cloud terminals collect data, and user interface terminals administer security and another mitigating adversary impact. The IoT cloud terminals communicate with $I_{oT} = \{1, 2, \ldots, z\}$ set of services that can access data from all the end-user applications from the smart technology. The above I_{oT} transmits various quantities of data in the different time interval $D_T = \{1, 2, \ldots, T\}$. Let n represent the number of adversaries and fewer services in the end-user applications. Based on the above definition, the number of data transfers per unit of time is i such that the collection of secure data transaction $\exists_i$ is estimated as:

$$\exists_i = \left\{ \begin{array}{c} \begin{array}{c} I_{oT} \times i \times T \; \forall \; I_{oT} \rightarrow D_T, \text{ if } n = 0 \\ A_{fs} \times \frac{z-n}{I_{oT}} \times T \; \forall \; (I_{oT}, n) \rightarrow D_T, \text{ else } n \neq 0 \end{array} \\ \text{such that} \\ I_{oT} \rightarrow D_T = \prod_{i=1}^{I_{oT}} i_n \\ \text{and} \\ (I_{oT}, n) \rightarrow D_T = \sum_{i=1}^{s} i_n - A_{fs} \sum_{i=1}^{n} i_n \\ \text{and} \\ A_{fs} = \frac{A_{ft}}{A_{ft}+i} \end{array} \right\} \quad (1)$$

In Equation (1), the variables A_{fs} and A_{ft} denote the adversary's fewer service rate and data transmission in D_T. The expressions $I_{oT} \rightarrow D_T$ and $(I_{oT}, m) \rightarrow D_T$ show the mapping of the IoT cloud and the user interface terminals at the different time interval D_T. The data synchronisation or information from the IoT architecture is concealed into two levels: IoT cloud network for security. The IoT cloud terminal, the transmission of data, and $\exists_i$ are the sum-up metrics for securing the collection for the mapped D_T, where it satisfies. For data collection, the user interface terminal provides synchronisation and secure authentication. The synchronisation of data between $I_{oT} \in i$ and n are operated with the help of their mapping and transaction time. According to Equation (1), the given condition $n > I_{oT}$ specifies less and insufficient data from the IoT network. The different time mapping for the IoT cloud and the sequential process $\exists_i$ rely upon $(z \times i)$, which is the evaluating condition for synchronisation.

$$T_n = \prod_{i=1}^{s} \frac{\mu_n}{T_i}; \text{ where } \urcorner\exists_i = \frac{\exists_i}{(i-n)} - (\mu - A_{ft}) \quad (2)$$

Based on the above equation, variables T_n and $\urcorner\exists_i$ represent the different mapping time instances and sequential collection of data. The above-derived equations are the reliable synchronisation of the security distribution (S_r), where it is evaluated for each access level of D_T. This estimation is observed for identifying the function $n \neq 0$ and $n = 0$ for all D_T using the conventional RSA technique. This RSA cryptography analysis is an approach to public-key cryptography, and it is based on random contours over each access level in that network. The collection of the secured data sequence βT_n and $\urcorner\exists_i$ such that the S_r is defined for all the output for the centre level O_u. The linear output of security distribution of $\urcorner\exists_i$ in T_n is the synchronising observation for augmenting $(z \times i)$. The O_u and result (Z) are important in defining S_r. The different instances of IoT cloud inputs for the determination of $\urcorner\exists_i$ for both $I_{oT} \rightarrow D_T$ and $(I_{oT}, n) \rightarrow D_T$ include different mappings sequences. If the IoT cloud is accessed in the mapping time, it is one; otherwise, it is zero. Figure 2 presents the synchronisation mapping for linear access.

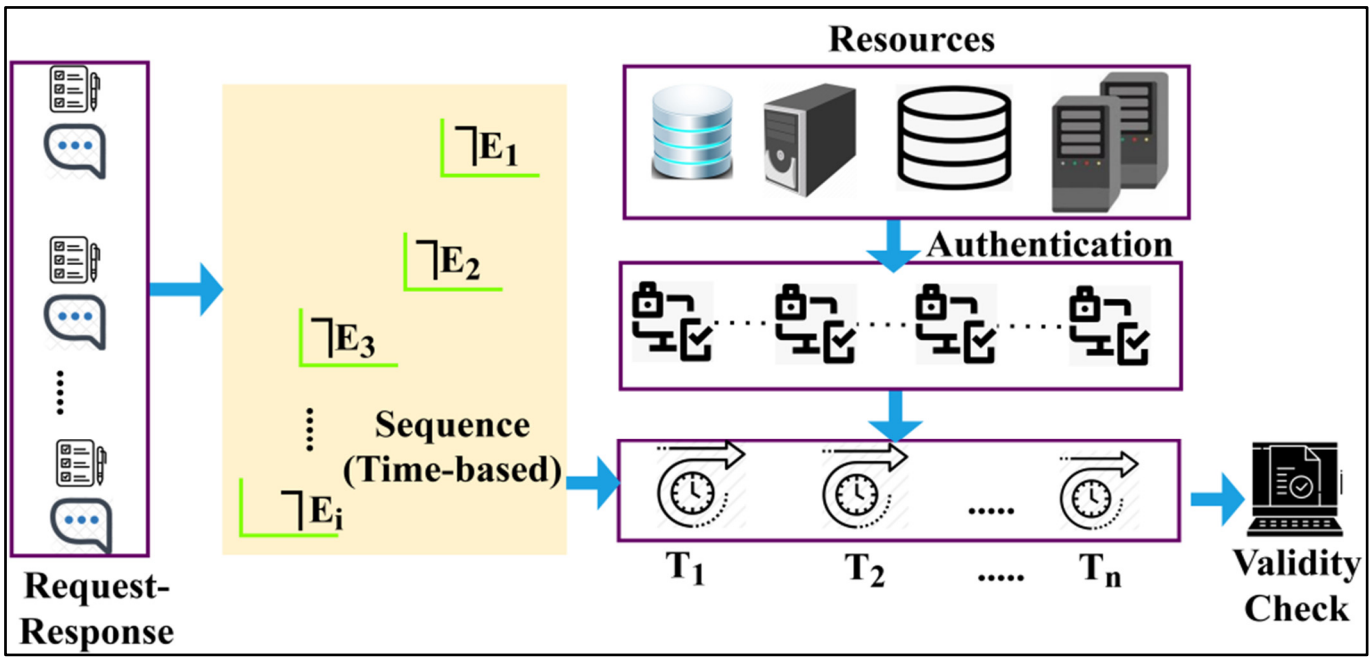

Figure 2. Synchronisation mapping process.

The proposed framework performs a mapping based on $\exists E_i$ indifferent transactions T_n. The available resources are authenticated using sequence-based validations to improve the transactions. The proposed framework performs a validity check if the transaction is authenticated. Therefore, the mapping process is performed for $I_{oT} \rightarrow D_T$, whereas synchronisation is achieved as $(I_{oT}, n) \rightarrow D_T$, as shown in Figure 2. This is performed to achieve a solution until $n \neq 0$. The solution of the centre-level access output in the first mapping $I_{oT} \rightarrow D_T$ produces a linear limitable result whereas $(I_{oT}, n) \rightarrow D_T$ extracts solution of z with $n \neq 0$. The following equation shows the centre-level access output, and the final result of Z for $I_{oT} \rightarrow D_T$ is estimated. These estimations have functioned for both the conditions of A_{ft} and the conditional estimation of $\mu = 1$ or $\mu = 0$ in D_T. Hence, the output is accessed for the entire distributed time instance D_T. From the above mapping condition, n serves as an IoT cloud input, and the synchronisation of A_{fs} in $I_{oT} \rightarrow D_T$ mapping is given as:

$$\left.\begin{array}{c} O_u{}^1 = \exists_{i1} T_1 + n_1 \mu_1 \\ O_u{}^2 = \exists_{i2} T_2 - A_{ft1} + \exists_{i1} \mu \\ O_u{}^3 = \exists_{i3} T_3 - A_{ft2} + \exists_{i2} \mu \\ \vdots \\ O_u{}^t = \exists_{it} T_{D_T} - A_{ftT-1} + \exists_{itT-1} \mu \end{array}\right\} \quad (3)$$

Instead,

$$\left.\begin{array}{cc} Z_1 = O_u{}^1 & Z_1 = \exists_{i1} T_1 + n_1 \mu_1 \\ Z_2 = O_u{}^2 - A_{fs1} i_2 & Z_2 = \exists_{i2} T_2 - A_{ft1} + \exists_{i2} \mu - A_{fs1} i_2 \\ Z_3 = O_u{}^3 - A_{fs2} i_3 & Z_3 = \exists_{i3} T_3 - A_{ft2} + \exists_{i3} \mu - A_{fs2} i_3 \\ \vdots & \vdots \\ Z_{D_T} = O_u{}^t - A_{fsT-1} i_{T-1} & Z_{D_T} = \exists_{it} T_{D_T} - A_{ftT-1} + \exists_{itT-1} \mu - A_{fsT-1} i_{T-1} \end{array}\right\} \quad (4)$$

From the above equation, the linear access solution for each level of data transactions is determined as $Z = \exists_i T - A_{ftt} + \exists_i \mu - A_{fs} n$ and $n = 0$, then $\mu = 1$ and $\exists_{it} T_{D_T} = n \exists_i$ and therefore, $Z = n \exists_i T + n \exists_i = n \exists_i (T + 1)$ is the reliable solution and $S_r = 1$. Here, the synchronisation of such IoT cloud systems is retained at once. The secure transaction requires $\{S_r, \beta, I_{oT}\}$ for each level of access D_T and this data provides security for the IoT

information. Therefore, $(I_{oT}, n) \rightarrow D_T$ mediate solution and results are estimated as in the following equations, respectively.

$$\left.\begin{array}{c} {O_u}^1 = \exists_{i1} \\ {O_u}^2 = \exists_{i2} - A_{fs1} - \mu_{i_1} i_1 \\ {O_u}^3 = \exists_{i3} - A_{fs2} + \mu_{i_2} i_2 \\ \vdots \\ {O_u}^t = \exists_{iT} - A_{fsT-1} - \mu_{i_{T-1}} i_{T-1} \end{array}\right\} \quad (5)$$

where in Equation (5), Equation (6) is derived.

$$\left.\begin{array}{c} Z_1 = {O_u}^1 = \exists_{i1} \\ Z_2 = {O_u}^2 + T_{n_1} - \urcorner\exists_{i1} = \exists_{i2} - A_{fs1} - i_1 + T_{n_1} - \urcorner\exists_{i1} \\ Z_3 = {O_u}^3 + T_{n_2} - \urcorner\exists_{i2} = \exists_{i3} - A_{fs2} i_2 + T_{n_2} - \urcorner\exists_{i2} \\ \vdots \\ Z_T = {O_u}^t + T_{n_t} - \urcorner\exists_{iT} = \exists_{iT-1} - A_{fsT-1} - \mu_{i_{T-1}} + T_{n_{t-1}} - \urcorner\exists_{iT-1} \end{array}\right\} \quad (6)$$

The solution, as in the above-derived equations, is obtained by verifying the functions $\urcorner\exists_i = (z - n)\exists_i$ and $\mu = 1$ or $\mu = 0$ in each level-by-level manner. If $\mu = 0$, then $Z_T = \exists_i - \mu_{i_{T-1}} i_t - \urcorner\exists_i$ is the final output, and if $\mu = 1$, then $A_{ft} = 0$, and therefore, the output is $Z = \exists_i + T_n - \urcorner\exists_i$. Hence, if $I_{oT} \rightarrow D_T$, then $Z = n\,\exists_i(T + 1)$ is the output and $Z = \exists_i + T_n - \urcorner\exists_i$ is the segregated result. From this output, $S_r = \left[\frac{\mu - A_{fs} \times A_{ft}}{n}\right]$ is the synchronisation value, and this can be updated with all the outputs of ${O_u}^t$ and Z_T in Equations (5) and (6). This condition is not relevant for the first estimation as in Equations (4) and (5) because it depends upon all mapped I_{oT} to the D_T. Therefore, the S_r together with β and I_{oT} is accessed by the IoT platform, and hence it remains consistent. The following instance of collecting data S_r on its existing D_T defines the leaky security distribution of acquiring data. In this condition, the consequence of transactions is observed in $n > i$, and then the collection from $z \in I_{oT}$ is halted to prevent each data access level from sender and receiver in the synchronisation, recommendation, and validation process. The security distributions in the synchronisation of information from the IoT network pass it on to the end-verifiable key to their participation in the D_T. This overcomes permitting adversaries fewer services and PSF by collecting unwanted or incorrect data. At the same time, user flexibility is high. The controlled PSF makes certain service delays data synchronisation within the IoT architecture. In the data synchronisation process, the transaction follows the synchronisation of user interface terminals. The user interface depends on (β, S_r, I_{oT}) for synchronising data through end-user applications and the IoT platform. This data security distribution is administered based on the synchronisation recommendation and S_r Simultaneously. In this distribution of security process, the end-to-end verifiable authentication, the keys are distributed between the terminals. Using the RSA algorithm, the following steps are to generate an end-verifiable key:

1. Select two large prime numbers X and Y such that $X \neq Y$, randomly and autonomous of each other.
2. Compute
$$z = XY \quad (7)$$
3. Compute the quotient function
$$\varnothing(z) = (X - 1)(Y - 1) \quad (8)$$
4. Select an integer ε such that $I_{oT} < \varepsilon < \varnothing(z)$, which is relatively prime to $\varnothing(z)$.
5. Compute $\complement_d$ such that
$$\complement_d \varepsilon \equiv 1; (\mathrm{mod}\ (\varnothing(z))) \quad (9)$$

The key generation process for T_n is illustrated in Figure 3.

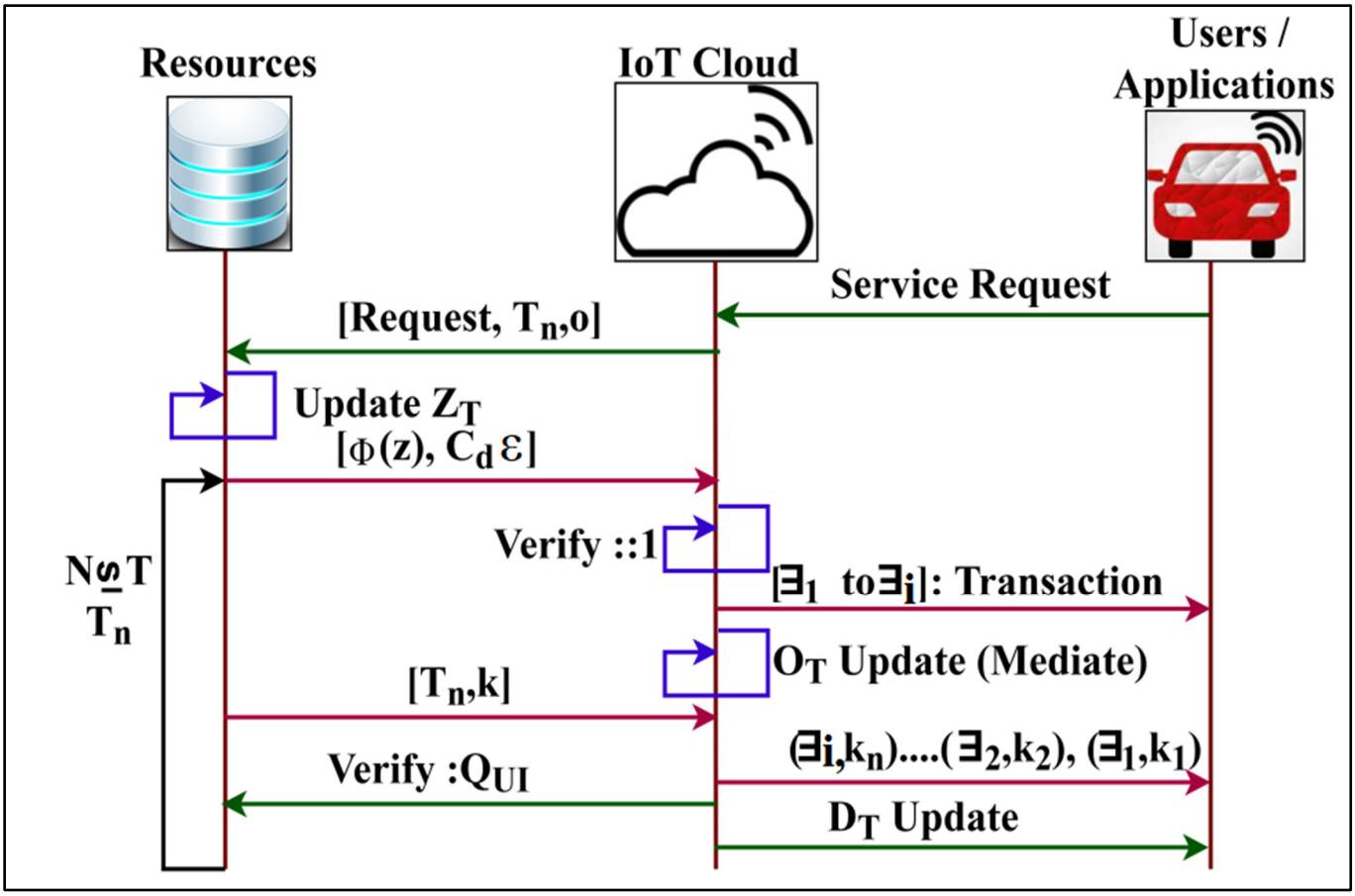

Figure 3. Key generation process in T_n.

The key generation process pursues in Equations (7)–(9) for the requests through the IoT cloud. The secure transactions for $\exists_i$ is verified for $N = T_n$ such that O_T is a mediate update. Based on this update, the D_T is performed by verifying Q_{UI} such that $[T_n, k]$ is true, and hence the key assigning is sequential. This ensures maximum authentication for the T_n for which D_T is updated using the β factor, depicted in Figure 3. The public key consists of the z, the modulus, and ε is the variable representing the public exponent for sometimes performing encryption, whereas the private key consists of z, the modulus, and ε for the private exponent and sometimes performs decryption, which can be hidden. The transmission of data from sender to receiver keeps the private key secret. X and Y are exposed since the factors of z and allow computation of $\complement_r$ have given ε.

$$\left.\begin{array}{c} Q_{ICT} = \complement_r \times \mu_i \times I_{oT} \text{ and } Q_{UI} = \complement_r \times \beta \\ \text{such that,} \\ Q_{ICT} :\rightarrow D_T \text{ and } D_T :\rightarrow \beta \; \forall \; I_{oT} \\ Q_{ICT} :\rightarrow D_T \text{ and } D_T : \rightarrow (\beta - \mu_i \times z) \forall \; (z - n) \end{array}\right\} \quad (10)$$

Based on the above equation, $\complement_r$ is the random number computation from which the two large prime numbers $\complement_f$ are fetched for synchronisation. Equation (10) differentiates the rationality of D_T for either I_{oT} Or $(z - n)$ as classified by the support vector classifications. Now, each level of session access keys k is distributed as:

$$k = Q_{ICT} * P_{UI} * |\complement_f| = Q_{UI} * P_{ICT} |\complement_f| \quad (11)$$

Each level of accessing this session key is valid until the condition $T \in D_T$ after which K is synchronised based on $\complement_r$. Here, the key validity is generated as:

$$\left.\begin{array}{c} K(\exists_i) = G(S_r|\beta|\exists_i|\complement_f|K) \\ \text{and} \\ \text{Security distribution} = \{(Q_{ICT} \oplus K(\exists_i) \oplus \complement_f \oplus D_T),\ z\} \end{array}\right\} \quad (12)$$

Equation (12) specifies the security distribution relies on the condition of $z \in I_{oT}$ and β in the D_T. These metrics turn into verifying sequences in the end-user applications. Here, D_T is linked with the k; hence, the changes of D_T is existing in $\complement_r$. The user side verifies entire security features to improve overall efficiency. The analysed synchronising data is valid if the $T \in D_T$ is access level. This access level is computed in different points, such as permitting overlapping and pursued instances of the following sessions. The classification process is presented in Figure 4.

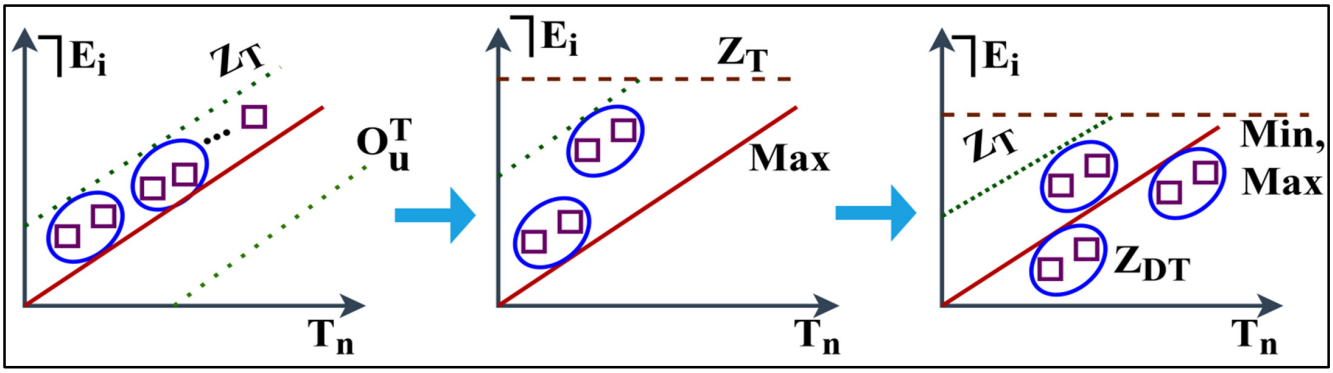

Figure 4. Classification process.

In the classification process, the access level is defined based on the previous $\exists_i$ such that Z_T defines the updates and maximum deviation. This process is differentiated based on Z_{DT} and Z_T for which the classifier performs min-max alignment. The process is restricted for T_n that is stuck under Z_T updates wherein D_T is true. This is required in the other processes to reflect multiple instances and improve access levels, as shown in Figure 4. In this IoT framework, user access level authentication is prohibited from decreasing the complexity of communication and extra service delay. The user interface terminal performs a synchronisation verification check as in the following equation. This security verification check makes certain appropriate k, D_T, and $\exists_i \in z \in I_{oT}$ is synchronised.

$$\left.\begin{array}{c} [(I_{oT} \to D_T) \oplus T_n \oplus Y \oplus \complement_f] = \left[\exists_i \oplus T \in D_T \oplus \frac{\complement_r}{I_{oT}} \oplus \beta\right],\ \forall\ \exists_i \text{ in } D_T \\ [Q_{ICT} \oplus \mu \oplus I_{oT}] = [Q_{UI} \oplus \beta \oplus \complement_r],\ \forall\ z \in I_{oT} \to D_T \\ G(S_r|\beta|\exists_i) = H(\neg\exists_i \oplus T_n \oplus S_r),\ \forall\ \neg\exists_i = z\exists_i \end{array}\right\} \quad (13)$$

The authentication and key verification process, Equations (12) and (13), adapts for $I_{oT} \to D_T$ where the grouping changes as in Equation (1) do not match for the above condition. Therefore, the mediate output of $O_u{}^t$ decides the different data transmission intervals and, therefore, the mapping. Based on the integrity of the end-user applications is verified and IoT cloud service instances and autonomous authentication are not lined up properly; therefore, the delay does not happen. The concurrent sequence and instances-related data integrities are verified by PSF without requiring extra computations. In addition, concurrency and integrity-related synchronisation minimise the number of computations during the verification. The classification procedure maximises the IoT cloud and user-side integrity and check. On the processing side, sequences are denoted by the user interface terminal, and security check S_r is utilised to improve the process. In the IoT cloud process, it is performed as the getting terminal by synchronising X and Y as per β and K. This synchronisation minimises the adversary impact, service failures, and service delays in

the end-user application of the IoT terminal. In Table 2, the required sessions for different transactions are tabulated.

Table 2. Required sessions for transactions.

Transactions	Mapping Instances	Access Level	Required Sessions
40	53	0.27	29
80	93	0.36	69
120	174	0.41	121
160	316	0.68	158
200	210	0.52	136
240	355	0.93	162

Table 2 presents the required sessions for different transactions. As the transactions increase, T_n is augmented based on $\neg\exists_i$ and O_u^t. This improves the synchronisation in mapping based on Z_1 to Z_T updates. The RSA-based authentication provides high Q_{ICT} in determining the session validity. As the mapping instances increase, the access is open for high users, varying the required sessions, permitting diverse T_n. Table 3 presents the session validity (%) under different access level rates.

Table 3. Session validity (%) for different access levels.

Access Level	Generated Keys	Actual Session Time (s)	Validity (%)
0.2	40	62.3	80.7
0.4	117	324.15	85.16
0.6	165	547.37	89.62
0.8	249	625.69	91.15
1	328	710.4	94.2

Table 3 presents the session validity for the proper access level from the observed data. The active sessions require keys in O_u^1 to O_u^t updates for which $\varnothing(Z)$ are required. This increases the key validity until the session is closed. Hence, $\forall\neg\exists_i$, the Z generation and $k(\exists_i)$ is retained at a maximum level using $I_{oT} \rightarrow D_T$ validation. Therefore, a maximum validity $(\%)$ for the allocated access level is generated for different keys. Figure 5 presents the self-analysis for mapping and updating instances and verification checks observed under different transactions.

An analysis of instances (mapping and update) and verification checks for different transactions are presented in Figure 5. The O_u^1 to O_u^t is assigned for different $\neg\exists_i$ and is mapped with the available resources for which Z_1 to Z_T is provided. However, Z_1 to Z_T is interrupted based on mediate O_u^t solution and hence Z_1 to Z_{DT} is updated in different instances. This is enhanced if the mapping is pursued at a high rate in $k(\exists_i)$ maximised instances. The $I_{oT} \rightarrow D_T$ is performed for Z_T to Z_{DT} modified update for improving precise response. Therefore, the verification checks are extended for the session validity and $k(\exists_i)$ instances. This is performed under different Q_{ICT} in Z_T to Z_{DT} chances requiring high verification checks. In Figure 6, the session validity for different access levels is presented.

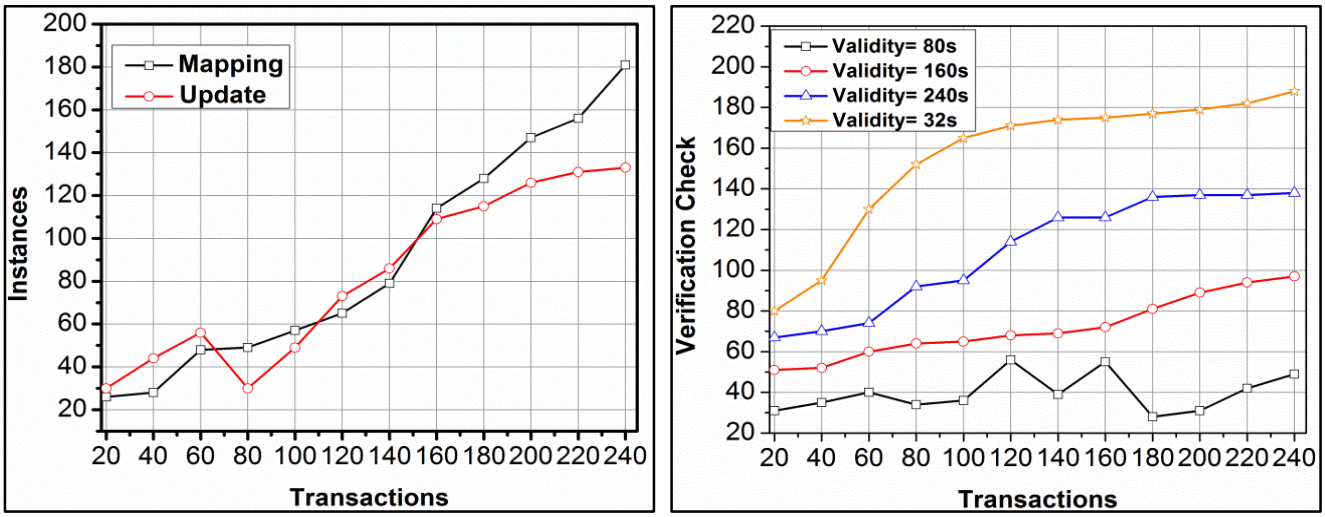

Figure 5. Mapping and updating, and verification checks under different transactions.

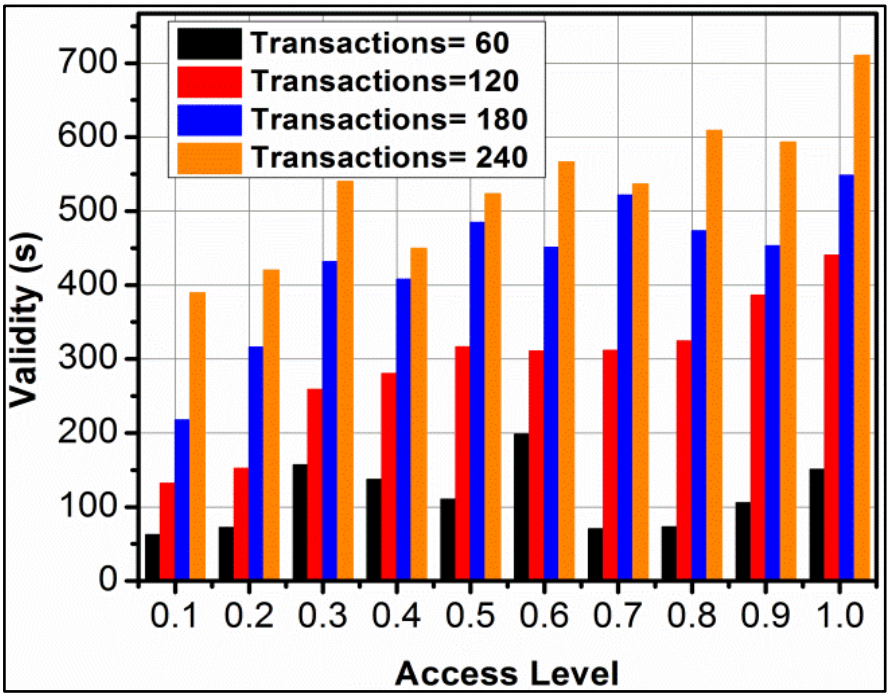

Figure 6. Session validity for different access levels.

The varying access levels require high validity as the transaction increases. In the proposed framework, the $k(\exists_i)$ is performed in different Q_{ICT}. This increases the O_u^1 to O_u^t for $I_{oT} \rightarrow D_T$ instances, increasing the validity. The notable feature is the synchronisation of Z_{DT} and Z_T in multiple instances (access) increases the validity requirement. Hence, the consecutive sequence is required to improve Z_{DT} and service distribution. Moreover, the adverse impact is reduced for extended validity-based verification checks (refer to Figure 6).

4. Results and Discussion

This section elucidates the proposed framework's performance verified using OPNET simulations. In this simulation, 80 IoT users performed 20–240 transactions through six resource servers. The request-to-response rate is varied between 0.7 and 1 with a mean transaction delay of 120 ms. This experimental scenario considers a man-in-the-middle attack for deceiving the transactions. With this setup, the metrics of adversary

impact, service failure, service delay, access rate, and service transactions are compared for analysis. In the comparative analysis, the following methods are considered: CMAKAP [29], RBCGM [18], and MPPAP [30]. The NETMASTER CXC-150 modem is utilised for internet access, Linux IPTables Firewall, Microsoft DNS server, Linux open VPN server, web server, Windows 2008-IIS 7.0.

4.1. Adversary Impact

The comparative analysis for adversary impact is presented in Figure 7 with the existing methods. The $T_n \forall \neg\exists_i$ is assessed for $n \neq 0$ and $n = 0$ conditions under different transactions for reducing the adversary impact. In the proposed framework, the synchronisation is performed for S_r and βT_n. The synchronisation is performed to prevent $(Z \times i)$ augmentation that injects the adversaries. However, the different instances for the above augmentation are classified using support vectors based on k and P_{UI}. Therefore, the adversary injecting instances in Z_{DT} are updated from which O_u^t is split, and new allocations are made. The classifications performed for $\exists_i$ and $(A_{fs} - \mu)$ such that the consecutive occurrence is reduced. Therefore, the classification is instigated until Z_1 to Z_T is performed for O_u^1 to O_u^t such that Z_{DT} is true. The authentication using RSA performs secured transactions without breaching $\neg\exists_i$ and hence the impact is less. Moreover, for k, $K(\exists_i)$ is induced by balancing $I_{oT} \rightarrow D_T$ in retaining T_n. Therefore, for T_n and O_u^1 to O_u^t, validity is improved in defining less adversary impact for transactions and access levels.

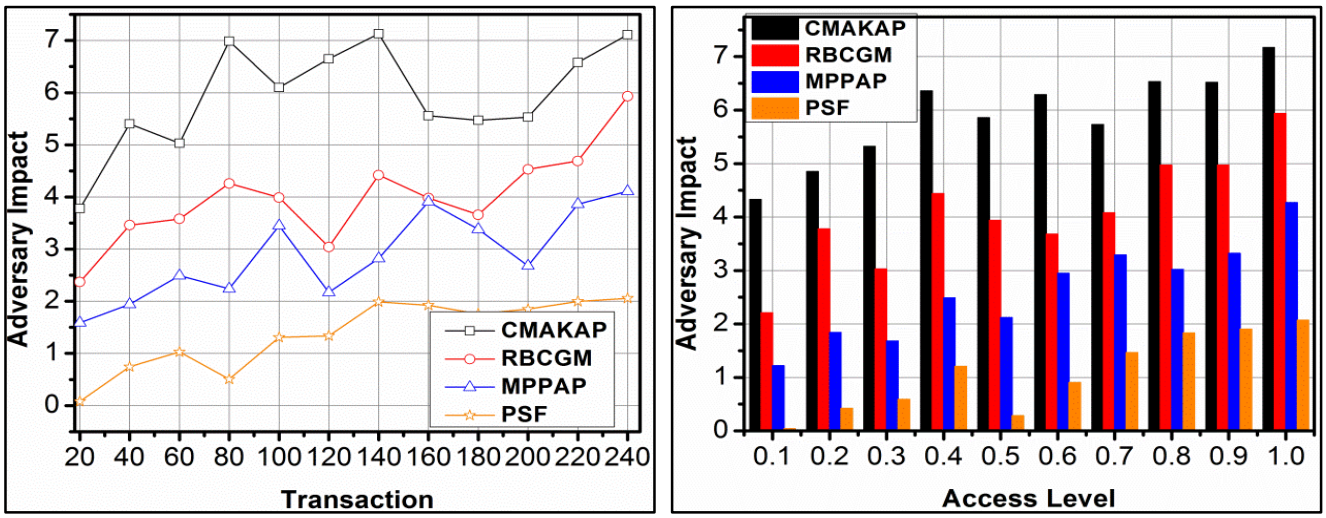

Figure 7. Adversary impact analysis.

4.2. Service Failure

In Figure 8, the efficiency analysis of service failure under various transactions and access levels is presented. The proposed framework reduces service failure based on Z_1 to Z_T and k verification. First, the (i_{T-1}) in O_u^t is identified as improving T_n and $\exists_i$. If the Z_T is outraged by Z_{DT}, then the classification process is instigated, for which Q_{ICT} is performed. The classification for $-\neg\exists_i$ and $\mu = 1$ condition distinguishes multiple adversaries impacted $\neg\exists_i$. Hence, $K(\exists_i)$ is extended $\forall\ (T+1)$ in $Z = n$, and hence the sessions are secured. In this process, Z_{DT} is performed, requiring new $z \in I_{oT}$ such that T_n is retained. As the T_n is retained, the available instances improve the Q_{ICT} for the consecutive $n > i$ interval. Hence, (β, S_r, I_{oT}) are consecutively shared in retaining the session. Therefore, the change in $\neg\exists_i$ or $\varnothing(Z)$ requires a high k, to prevent the failure of the session. This is recursive for S_r in different transactions, preventing additional failures. The security is administered by validating $C_d \varepsilon \equiv 1$ such that $Q_{ICT} :\rightarrow D_T$ is verified under different users as well. Therefore, the service failures are reduced in the proposed framework, achieving fair results.

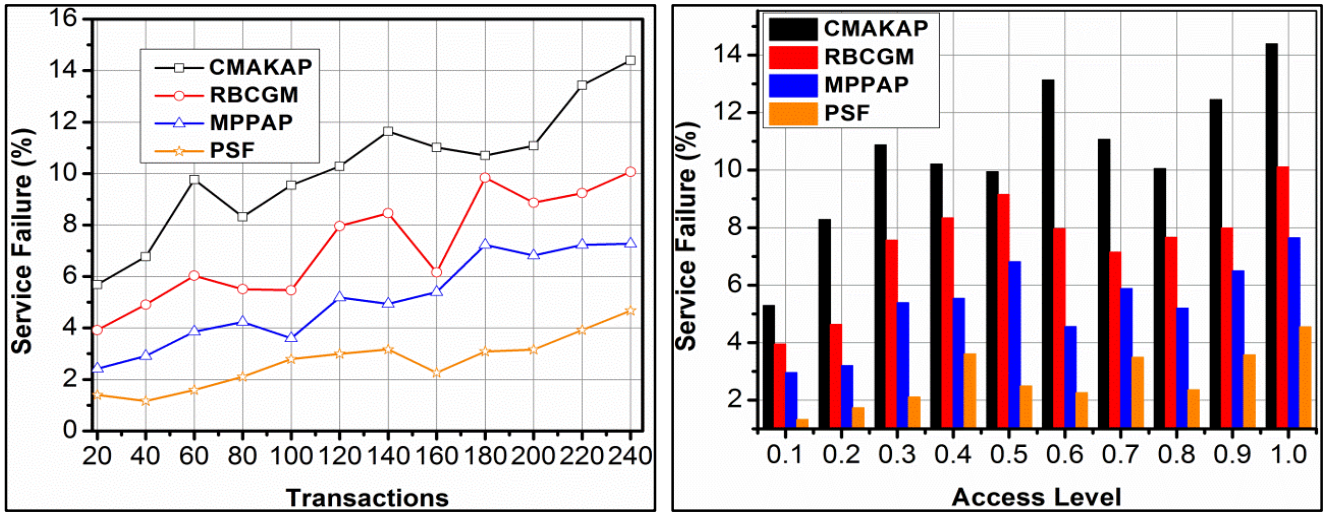

Figure 8. Service failure analysis.

4.3. Service Delay

The proposed framework achieves less service delay compared to the other methods. In the proposed framework, $\exists_i$ maximised by reducing failures, and hence reassignment (resource) is less required. The Z_1 to Z_T based on O_u^1 to O_u^t as in Equation (3) shows up as delay without increasing failures. In the Q_{ICT} definition, $Q_{UI} = C_r \times \beta$ and $(\beta - \mu_i)$ are first validated for conventional service allocations. Contrarily, if a failure occurs, then $(\mu_i \times z)\ \forall (z - n)$ is validated for detecting the time requirement. The classifier learning devices Z_1 to Z_T as in Equation (6) for Z_{DT} for identifying S_r. Based on S_r, the allocations are performed. In this allocation, two conditions are verified, namely $\neg\exists_i = n\exists_i$ and $n = 0$, and hence the allocations are validated. These validations improve the swiftness in $\exists_i$, in a concurrent manner, under T_n, reducing additional time. The classifier instance now relies on Z_1 to Z_T as in Equation (6) for improving the response. Therefore, the delay is confined $\forall\ \mu = 1$ verified for the above conditions. This is common for different transactions and access levels, achieving less delay, as presented in Figure 9.

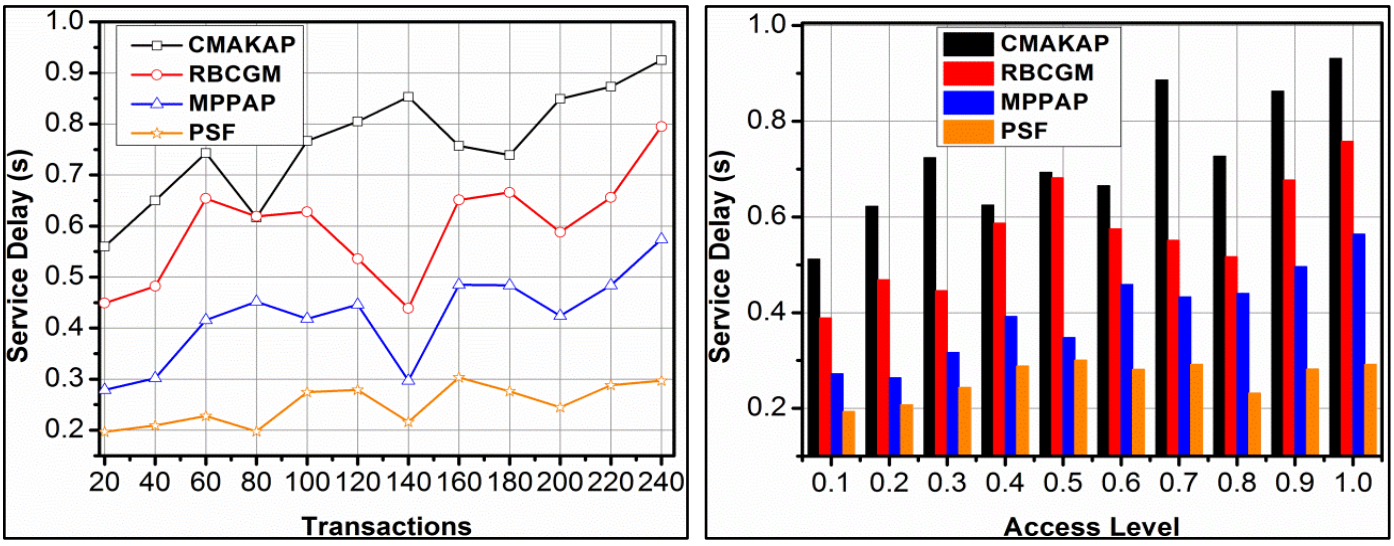

Figure 9. Service delay analysis.

4.4. Access Rate

The proposed framework achieves a high access rate for different transactions and access levels, which is shown in Figure 10. The adversary impacts are mitigated based on

Z and $\varnothing(Z)$ processes for securing access and service distributions. The O_u^1 to O_u^t based classifications using support vectors are performed to identify Z_{DT} in Z_1 to Z_T iterations. Further, the $K(\exists_i)$ is analysed for improving the access rate beyond the extended $\neg\exists_i - n\exists_i$ and hence the $I_{oT} \rightarrow D_T$ is improved. In different T_n, the $\neg\exists_i$ is analysed for detecting mediates in O_u^T as in Equation (5). Therefore, Z_1 to Z_T is modified depending on Q_{CT}, this modification has to satisfy two distinct conditions for retaining the access rate. First, $n \neq 0$ in either $\mu = 1$ or $\mu = 0$ such that D_T is retained. For the retained D_T, S_r is performed based on $z \in I_{oT}$, and hence the $n > i$ is achieved. If this condition is satisfied, then classification is improved to reduce the adversary impact. In the second condition, $I_{oT} < \varepsilon < \varnothing(z)$ and the authentication modes and their access levels are defined. In the proposed framework, the defined $\varnothing(z)$ is used for C_r and ε validation for maximising the access level. This leads to further access delegation regardless of the users and T_n.

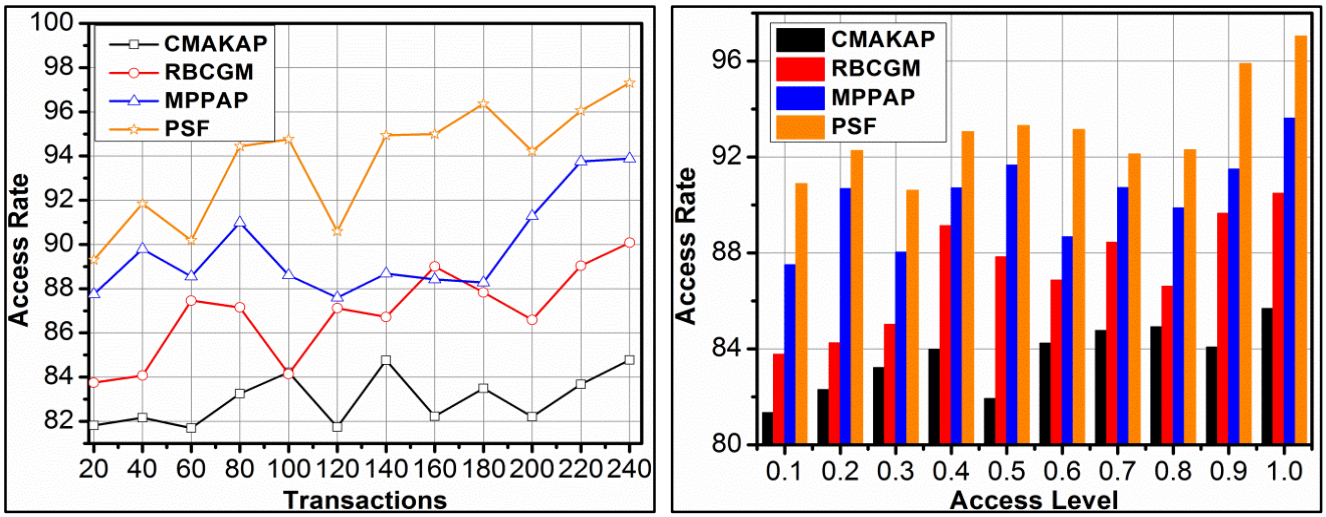

Figure 10. Access Rate Analysis.

4.5. Service Transactions

The proposed framework achieves high service transactions for different access levels, which is depicted in Figure 11. The initial T_n is required for improving service distributions without reducing the change in service allocation. In the proposed framework, $D_T = \{1 \text{ to } T\}$ is augmented to improving $\exists_i$ and hence the $n \neq 0$ is achieved. In this case, the change in T_n is achieved for multiple iterations as classified by the learning process. The Z_{DT} update in different instances is required for $(T+1)$ for $S_r = 1$, and hence the $\exists_i$ are improved. The classifier performs $(C_r \times \beta)$ and $(z - n)$ differentiation for improving service transactions. In the proposed framework, the validation is performed under different instances for $|C_f|$. The $D_T :\rightarrow \beta \; \forall \, I_{oT}$ mapping increases T_n for leveraging the distribution. Therefore, for varying access levels, the transactions are improved without increasing the overhead. The procedure is general for various Z_{DT} overwhelming service failures. Then, various transactions and access level-related comparative analyses are shown in Tables 4 and 5.

The proposed framework reduces adversary impact, service failure, and service delay by 10.98%, 11.82%, and 10.19%, respectively. Contrarily, it improves the access rate by 7.73%.

The proposed framework achieves 11.16% less adversary impact, 12.34% less service failure, 10.19% less service delay, 7.1% high access rate, and 10.12% high service transaction.

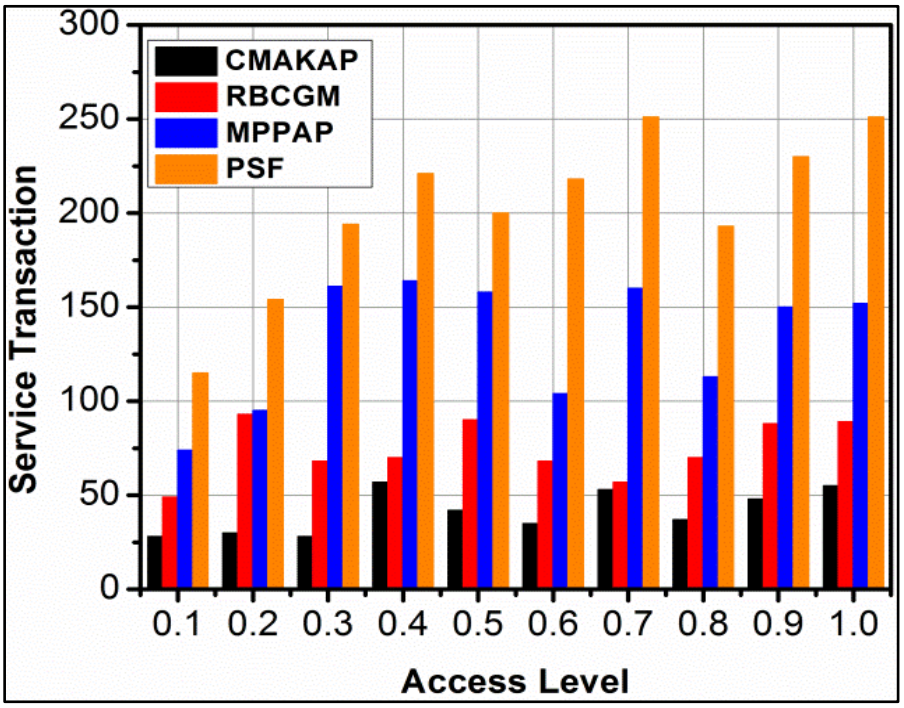

Figure 11. Service transaction analysis.

Table 4. Comparative analysis summary for transactions.

Metrics	CMAKAP	RBCGM	MPPAP	PSF
Adversary Impact	7.11	5.93	4.11	2.0575
Service Failure (%)	14.4	10.07	7.28	4.673
Service Delay (s)	0.925	0.795	0.574	0.2967
Access Rate	84.77	90.08	93.89	97.311

Table 5. Comparative analysis summary for access level.

Metrics	CMAKAP	RBCGM	MPPAP	PSF
Adversary Impact	7.17	5.94	4.27	2.0718
Service Failure (%)	14.39	10.11	7.65	4.547
Service Delay (s)	0.931	0.758	0.564	0.2918
Access Rate	85.68	90.48	93.62	97.037
Service Transaction	55	89	152	251

5. Conclusions

This article presents an access and transaction adaptable PSF for mitigating the adversary impact over dense IoT services. The secure transaction sequence between the users/applications and the resources through the cloud is linearly mapped and synchronised for providing high-level access. The sessions are distinguished based on access time intervals and authenticated using RSA. In the classification process, support vectors are employed for handling linear and synchronised access between the users. The proposed framework fits the user and transaction flexibility without deviating from data collection and update. For ease of service allocation, the classifications are performed based on failing and mapping updates. This is considered by the classifier for improving the end-to-end verification checks. Based on the verification validity, the session intervals are modified,

and hence the synchronisation is retained. The proposed framework reduces adversary impact, service failure, and service delay by 10.98%, 11.82%, and 10.19%, respectively. Contrarily, it improves the access rate by 7.73% for different transactions.

Author Contributions: Conceptualisation, M.A. and S.S.; methodology, M.A. and S.S.; software, M.A. and S.S.; validation, M.A., S.S. and Y.Y.; formal analysis, Y.Y.; resources, S.S.; data curation, H.F.G. and S.S.; writing—original draft preparation, M.A. and S.S.; writing—review and editing, H.F.G., S.S. and Y.Y.; visualisation, S.S. and Y.Y. All authors have read and agreed to the published version of the manuscript.

Funding: This research was supported by the Princess Nourah bint Abdulrahman University Researchers Supporting Project number (PNURSP2023R259), Princess Nourah bint Abdulrahman University, Riyadh, Saudi Arabia.

Data Availability Statement: Experiments are performed on simulator for real scenarios.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Mishra, S.; Tyagi, A.K. The role of machine learning techniques in internet of things-based cloud applications. In *Artificial Intelligence-Based Internet of Things Systems*; Springer: Berlin, Germany, 2022; pp. 105–135.
2. Li, Y.; Cao, B.; Peng, M.; Zhang, L.; Zhang, L.; Feng, D.; Yu, J. Direct Acyclic Graph-Based Ledger for Internet of Things: Performance and Security Analysis. *IEEE/Acm Trans. Netw.* **2020**, *28*, 1643–1656. [CrossRef]
3. Tournier, J.; Lesueur, F.; Le Mouël, F.; Guyon, L.; Ben-Hassine, H. A survey of IoT protocols and their security issues through the lens of a generic IoT stack. *Internet Things* **2021**, *16*, 100264. [CrossRef]
4. Javanmardi, S.; Shojafar, M.; Mohammadi, R.; Nazari, A.; Persico, V.; Pescapè, A. FUPE: A security driven task scheduling approach for SDN-based IoT–Fog networks. *J. Inf. Secur. Appl.* **2021**, *60*, 102853. [CrossRef]
5. Li, D.; Cai, Z.; Deng, L.; Yao, X.; Wang, H.H. Information security model of block chain based on intrusion sensing in the IoT environment. *Clust. Comput.* **2019**, *22*, 451–468. [CrossRef]
6. Xu, X.; Wang, X.; Li, Z.; Yu, H.; Sun, G.; Maharjan, S.; Zhang, Y. Mitigating Conflicting Transactions in Hyperledger Fabric-Permissioned Blockchain for Delay-Sensitive IoT Applications. *IEEE Internet Things J.* **2021**, *8*, 10596–10607. [CrossRef]
7. Shamieh, F.; Wang, X.; Hussein, A.R. Transaction Throughput Provisioning Technique for Blockchain-Based In-dustrial IoT Networks. *IEEE Trans. Netw. Sci. Eng.* **2020**, *7*, 3122–3134. [CrossRef]
8. Wang, J.; Wei, B.; Zhang, J.; Yu, X.; Sharma, P.K. An optimised transaction verification method for trustworthy blockchain-enabled IIoT. *Ad Hoc Netw.* **2021**, *119*, 102526. [CrossRef]
9. Lee, K.; Yim, K. Study on the transaction linkage technique combined with the designated terminal for 5G-enabled IoT. *Digit. Commun. Netw.* **2021**, *8*, 124–131. [CrossRef]
10. Li, H.; Pei, L.; Liao, D.; Wang, X.; Xu, D.; Sun, J. BDDT: Use blockchain to facilitate IoT data transactions. *Clust. Comput.* **2021**, *24*, 459–473. [CrossRef]
11. Rachit; Bhatt, S.; Ragiri, P.R. Security trends in Internet of Things: A survey. *Sn Appl. Sci.* **2021**, *3*, 121. [CrossRef]
12. Al-Otaibi, Y.D. Distributed multi-party security computation framework for heterogeneous internet of things (IoT) devices. *Soft Comput.* **2021**, *25*, 12131–12144. [CrossRef]
13. Djedjig, N.; Tandjaoui, D.; Medjek, F.; Romdhani, I. Trust-aware and cooperative routing protocol for IoT security. *J. Inf. Secur. Appl.* **2020**, *52*, 102467. [CrossRef]
14. Hodgson, R. Solving the security challenges of IoT with public key cryptography. *Netw. Secur.* **2019**, *2019*, 17–19. [CrossRef]
15. Oh, M.-K.; Lee, S.; Kang, Y.; Choi, D. Wireless Transceiver Aided Run-Time Secret Key Extraction for IoT Device Security. *IEEE Trans. Consum. Electron.* **2019**, *66*, 11–21. [CrossRef]
16. Biswas, S.; Sharif, K.; Li, F.; Nour, B.; Wang, Y. A Scalable Blockchain Framework for Secure Transactions in IoT. *IEEE Internet Things J.* **2018**, *6*, 4650–4659. [CrossRef]
17. Yu, S.; Jho, N.; Park, Y. Lightweight Three-Factor-Based Privacy-Preserving Authentication Scheme for IoT-Enabled Smart Homes. *IEEE Access* **2021**, *9*, 126186–126197. [CrossRef]
18. Asheralieva, A.; Niyato, D. Reputation-Based Coalition Formation for Secure Self-Organized and Scalable Sharding in IoT Blockchains with Mobile-Edge Computing. *IEEE Internet Things J.* **2020**, *7*, 11830–11850. [CrossRef]
19. Huang, K. Secure Efficient Revocable Large Universe Multi-Authority Attribute-Based Encryption for Cloud-Aided IoT. *IEEE Access* **2021**, *9*, 53576–53588. [CrossRef]
20. Sadri, M.J.; Asaar, M.R. An anonymous two-factor authentication protocol for IoT-based applications. *Comput. Netw.* **2021**, *199*, 108460. [CrossRef]
21. Wu, F.; Li, X.; Xu, L.; Vijayakumar, P.; Kumar, N. A Novel Three-Factor Authentication Protocol for Wireless Sensor Networks with IoT Notion. *Ieee Syst. J.* **2021**, *15*, 1120–1129. [CrossRef]

22. Dorri, A.; Kanhere, S.S.; Jurdak, R.; Gauravaram, P. LSB: A Lightweight Scalable Blockchain for IoT security and anonymity. *J. Parallel Distrib. Comput.* **2019**, *134*, 180–197. [CrossRef]
23. Vishwakarma, L.; Das, D. SCAB-IoTA: Secure communication and authentication for IoT applications using block-chain. *J. Parallel Distrib. Comput.* **2021**, *154*, 94–105. [CrossRef]
24. Peneti, S.; Kumar, M.S.; Kallam, S.; Patan, R.; Bhaskar, V.; Ramachandran, M. BDN-GWMNN: Internet of Things (IoT) Enabled Secure Smart City Applications. *Wirel. Pers. Commun.* **2021**, *119*, 2469–2485. [CrossRef]
25. Majumder, S.; Ray, S.; Sadhukhan, D.; Khan, M.K.; Dasgupta, M. ECC-CoAP: Elliptic curve cryptography based constraint application protocol for internet of things. *Wirel. Pers. Commun.* **2021**, *116*, 1867–1896. [CrossRef]
26. Lin, W.; Yin, X.; Wang, S.; Khosravi, M.R. A Blockchain-enabled decentralised settlement model for IoT data exchange services. In *Wireless Networks*; Springer: Berlin, Germany, 2020; pp. 1–15.
27. Attarian, R.; Hashemi, S. An anonymity communication protocol for security and privacy of clients in IoT-based mobile health transactions. *Comput. Netw.* **2021**, *190*, 107976. [CrossRef]
28. Yazdinejad, A.; Parizi, R.M.; Dehghantanha, A.; Zhang, Q.; Choo, K.K.R. An energy-efficient SDN controller ar-chitecture for IoT networks with blockchain-based security. *IEEE Trans. Serv. Comput.* **2020**, *13*, 625–638. [CrossRef]
29. Srinivas, J.; Das, A.K.; Wazid, M.; Kumar, N. Anonymous Lightweight Chaotic Map-Based Authenticated Key Agreement Protocol for Industrial Internet of Things. *IEEE Trans. Dependable Secur. Comput.* **2018**, *17*, 1133–1146. [CrossRef]
30. Pham, C.D.; Dang, T.K. A lightweight authentication protocol for D2D-enabled IoT systems with privacy. *Pervasive Mob. Comput.* **2021**, *74*, 101399. [CrossRef]