Hindawi
Wireless Communications and Mobile Computing
Volume 2022, Article ID 8051905, 15 pages
https://doi.org/10.1155/2022/8051905

Research Article

Security-Level Improvement of IoT-Based Systems Using Biometric Features

Masoud Moradi,[1] Masoud Moradkhani ,[2] and Mohammad Bagher Tavakoli[1]

[1]*Department of Electrical Engineering, Arak Branch, Islamic Azad University, Arak, Iran*
[2]*Department of Electrical Engineering, Ilam Branch, Islamic Azad University, Ilam, Iran*

Correspondence should be addressed to Masoud Moradkhani; moradkhani.m@ilam-iau.ac.ir

Received 22 July 2021; Revised 14 December 2021; Accepted 27 December 2021; Published 25 February 2022

Academic Editor: Deepak Gupta

The Internet of Things (IoT) is reported as a main research topic in the current decade. It will be possible to connect smart devices to each other using IoT, a platform such as the Internet. However, the expansion and intrusion of such a large network raises some new security issues and risks related to the disclosure of user confidential information where these devices are subject to hacker threats and intrusions. Traditional security systems were password based. In this paper, after reviewing the actions taken in this regard, the improvement level of biometric security compared with traditional password-based methods will be proven in section three using the Markov model. By considering the results of the evaluation, the probability of occurrence of security problems is decreased by 90.71% by applying biometric features. Then, multi-layer security architecture with biometric features and coding systems is suggested to increase security. In the first layer, the fingerprint recognition algorithm is dependent on the module, and the U.are.U 5100 module provides more security than others. In the second layer, the Hash mechanism of the MD5 algorithm is, on average, 63.21% more efficient. By determining the properties of the first two architectural layers and ultimately for the IoT application layer, empirical methods and hardware platforms for the Internet of things are used. Concerning the simulation results, the suggested mechanism enhances the system security by 120.38% on average, which is 106.23, 110.45, and 144.46% of relative improvement compared with IoT sensors, controller layer mechanisms, and application layer mechanisms, respectively.

1. Introduction

Internet of Things (IoT) [1] is one of the new popular technologies in the modern era whose security and confidentiality is still a controversial topic in this field. IoT primarily requires the precise mechanisms of confidentiality, integrity, authentication, and access control model. The current Internet is constantly under attack due to technical, legal, and human problems. This issue leads to hundreds of new security challenges that should be addressed in detail. Another challenge in this area is that the IoT applications are on the rise. In this article, a brief review of security issues related to IoT and the impact of this technology on the digital divide are presented. According to a May 2014 report by the Pew Research Center, the IoT will have significantly grown by 2025. According to a research by the Gartner Institute in 2020, nearly 26 billion identifiable devices could be part of this global computer network. According to Gartner, more than 50% of Internet connections are accomplished through IoTs. The market value of IoT equipment increased from less than $ 1 billion in 2015 to $ 48 billion in 2025. HIS Research also reports a 6-fold increase in sales of IoT products over the next decade. According to the agency forecasts, the supply of products, e.g., sensors for pedestrian identification and traffic status applications, estimates of the state, and amount of water and air pollution in 2026, will be 1.4 billion units. IHS predicts that the IoT market will grow from a base cost of 15.4 billion devices in 2015 to 30.7 billion in 2020 and 75.4 billion in 2025 [2]. Given the rapid growth in the number of IoT devices according to International Data Corporation (IDC), the market for IoT is expected to reach $ 41 billion by 2020 [3]. The security and privacy of IoT [4] are intended to

protect against malicious attacks and any unauthorized use of users' private information on the Internet, which has always been a major challenge in cyberspace. Theft of confidential information from the business servers, private photos from private clouds, and video content from IP-connected home cameras are typical examples of Internet hackers destroying security. Sharing personal shopping habits, disclosing people's residential information, and giving personal details to unauthorized people are behaviors that affect privacy. The impact of the challenge will be certainly enhanced by increasing the number of IoT-connected devices and services. As security threats increase, users need new authentication techniques to increase security. Many applications and services have emerged in various monitoring, medical, military care, etc. Fields using IoT technology. Moreover, the rapid growth of the sensor industry in mobile and smart devices entails users' permanent connection as a standard feature in the near future. As a result, the importance of IoT security and privacy is reported as an urgently necessary requirement, specifically for the IoT infrastructure with high level of security. Fingerprint is a reliable biometric feature that is addressed in a wide range of applications requiring authentication. Biometric systems such as fingerprints provide tools to create reliable reports and protect the privacy of authorized users [5].

In this paper, one or more of the biometric features such as fingerprint and multi-layer security architecture can be used to increase security and reliability of system from the security risk perspective. On the other hand, for the implementation of the proposed approach, the partial method and the Arduino hardware platform are used. This controller's performance can be upgraded based on the algorithms to support a variety of IoT sensors and communication platforms. Furthermore, another improvement is the simultaneous use of biometric sensors and back-up communication paths to address security threats in each layer of the IoT. The main contributions of this paper are as follows:

(i) Security improvement by combining sensors for biometric features identification such as fingerprint sensors and voice biometric systems. The system can also be upgraded by other biometric features such as the user's face.

(ii) IoT Controller section theory, where the Arduino controller is used with the capability of intelligence algorithms to resolve possible errors.

(iii) Security improvement in the IoT communication layer by applying redundant mechanisms for transferring information from the Arduino controller to the Internet infrastructure.

(iv) Security enhancement for user authentication and confirmation, a combination of password and biometric features are used to identify the person and allow access to the IoT. Along with simulating and implementing biometric identification models, cryptographic models are used to increase system security with the secure storage of biometric data. Biometric templates must be stored with a hash-based private key to merely provide access for the registered user.

(v) Recording biometric features should be done in a secure part of the reliable hardware so that it is not accessible to other users except the system administrator. The encrypted form of the biometric data is merely stored in the system. Moreover, once a user is erased, their biometric data are also erased from the device where rooting the device should not compromise the biometric data.

(vi) Using Markov model for improvement biometric authentication.

(vii) Combine hash algorithm with biometric technique for more security improvement.

The rest of this paper is structured as follows. Section 2 contains the research related to authentication and cryptography in the context of the Internet of Things. Using the Markov model, the improvement level of biometric securities compared with conventional password-based methods will be proven in Section 3. The proposed method and the related models are presented in Section 4. Simulation and details of simulation are given in Section 5 Finally, the conclusion is proposed in section six.

2. Related Work

In this section, the research study is reviewed from different perspectives of IoT security-related research based on fingerprint biometrics and the applied research in the area, such as medical research, is initially reviewed [6]. Then, the studies associated with IoT authentication and encryption are addressed accompanied by the reviewing the practical uses of security-sensitive applications Different types of platforms associated with security, such as cloud computing, the Arduino platform, and the cloud platform are reviewed.

In Ref. [7], a prototype-based framework for IoT-enabled health care systems is presented. The solution uses smart gateway architecture to facilitate data storage and processing, as well as the cloud as a support infrastructure for analysis and decision-making. The security of this solution depends on the security features and capabilities of the operating system. Another solution is suggested in Ref. [8]. In this context, Raspberry Pi devices are used as fog nodes. It is also guaranteed through the use of an authentication process based on the role of data confidentiality. In this context, the cloud environment is used to some extent for data storage. Also Ref. [9] discusses the hierarchical framework for use in the field of health along with the security of its data. In this method, information related to the analysis of health data is stored separately in the cloud and fog infrastructure. The solution also uses the MAPE-K-based model to support computations related to running various programs as well as data encryption. In addition, Ref. [10] suggests a low-energy health monitoring framework. This method is used to facilitate and secure the process of sending

the analyzed IoT data to the fog environment. In this solution, IoT devices also have processing power and are able to process raw data. They also have the ability to discharge data to different nodes in order to reduce energy consumption. In the fog layer is a distributed database for classifying and securing data. Hu [11] Provides a security framework for use in face recognition systems. In this solution, a central cloud is responsible for managing all available resources. Small tasks are also unloaded to process the fog infrastructure. Upon completion of tasks in fog, only the results will be sent back to the cloud for analysis and storage. In Ref. [12], another framework has been developed to provide data-sharing capabilities for users. In this proposed framework, each user operation is managed by the core of the Spark platform embedded in the cloud environment. In this method, encryption and authentication techniques have been used to provide security. Finally, an one-pass architecture is proposed that proposes PaaS capability for combining fog nodes and IoT devices [13]. This method helps with messaging communications as well as authentication. This solution supports horizontal integration between gateways and cloud data centers as well as task migration. Table 1

The authors in Ref. [14] suggested a system including NodeMCU ESP8266 microcontroller with a Wi-Fi connection for IoT driver applications. Android applications have features such as history control, navigation, registration menu, and speech recognition control. In this research, system security consists of a unique biometric and speech authentication mechanism. However, compared with the mechanism in our paper, the suggested mechanism is proposed only in the layer of IoT sensors. Authors in their study designed a low-cost biometric system for IoT devices using limited resources to be able to save the memory and computation costs [15]. The suggested system utilizes an algorithm based on the block logic operation to reduce biometric property measurement. However, the introduced mechanism is only proposed in the layer of IoT sensors compared with the suggested one in our article.

In their study, Karimian et al. discuss the cost of using biometric systems and suggest frameworks for their improvement [16]. In this regard, Srianusha et al. proposed a system for fingerprint engine start. This system allows only authorized users to drive the vehicle via scanning their fingerprints. Users can enter the system and register by letting the system scan their fingerprints. In this research, Atmega 328 and esp8266 wifimodule microcontrollers are used. We can refer to the single-layer security mechanism approach in the sensors layer as one of the limitations of this study. In this paper, by considering the reviews regarding the related activities, in contrast with traditional security systems, we seek to utilize biometric properties on the platform of multi-layer security architecture. In other words, a multilayer security architecture, including biometric features and coding systems, is proposed. In the first, second, and application IoT layers, fingerprint recognition algorithm, Hash algorithm, and hardware platforms for the Internet of things are used, respectively.

In Ref. [17] a lightweight algorithm is presented to ensure the security of the cloud computing environment. The proposed algorithm uses the 16 byte block encryption technique to encrypt the data. In this algorithm, Faistel network with permutation and replacement architecture are used to complicate the cryptographic process. This solution has the power to run with the length of the private key and the number of different cycles. The results of the evaluation indicate that the implementation time of the solution is low. But the problem with these private key-based solutions is that they require an encryption key exchange, which can compromise security and privacy. In Ref. [18] several different encryption techniques have been used to secure cloud storage space. For this purpose, an encryption system based on AES algorithm and asynchronous key transfer system for data or information exchange is provided. Elliptic curve encryption technique has also been used to exchange information between the user and the server. The solution has been able to achieve a relatively good execution time in the process of sending and receiving data, although in this evaluation, the volume of data is considered very small. The authors in Ref. [19] presented a two-step encryption solution to secure data storage in the cloud. In this solution, the main data are divided into two parts, which are encrypted by a common key. The cryptographic key is based on the model of chaos theory. This solution can increase the encryption time while increasing security, but the required time for splitting and combining data has not been investigated. In Ref. [20], blockchain is used for a security solution based on cloud computing. Accordingly, to ensure data security, data are stored in the form of blockchain blocks. For any data to be stored in block form, it will require the approval of more than half of the servers, so it will be virtually impossible to make unwanted changes. But this type of security will have problems; for example, if the user wants to delete or change the data, it will be very costly. Another problem is how to store different types of data in the form of blockchain blocks because the blockchain is originally designed to store data related to transactions. In Ref. [21], the performance of some symmetric cryptographic algorithms has been studied in terms of runtime parameters and memory consumption. The results show that DES and Blowfish algorithms are more efficient in encryption and decryption time as well as memory consumption. The articles [22, 23] provide an overview of the most important cryptographic solutions that can be used in cloud computing and the Internet of Things. The results of these studies indicate the need for algorithms and solutions that can create a kind of compromise between security and service quality parameters, so that due to the limited resources of processing nodes in the IoT devices, the use of encryption technique has the least negative impact on providing services.

Authors in Ref. [24] provides a secure decision-making solution for the Internet of Things based on cloud computing. Accordingly, machine learning alongside IoT based on fog computing has been used to provide a safe experience in healthcare systems. Blockchain has also been used to secure the framework. In this solution, data related to patients' physiological signals are first collected using

Table 1: Shows summarizing the metrics and limitations of various methods.

Method	Decentralized management	Security features			Platform independence	Ability to integrate in...		
		Security	Authentication	Integrity		Cloud	Fog	IoT
Rahmani [7]	✓	✓	✓	✗	✗	✓	✓	✓
Dubey [8]	✓	✓	✓	✗	✗	✗	✓	✓
Azimi [9]	✓	✓	✓	✗	✗	✓	✓	✓
Gia [10]	✓	✓	✓	✗	✗	✗	✓	✓
Hu [11]	✗	✗	✗	✗	✗	✓	✓	✓
Suneetha et al. [12]	✗	✗	✓	✗	✗	✓	✓	✓
Jaberi, et.al. 2021	✗	✗	✓	✓	✓	✗	✓	✓
Proposed	✓	✓	✓	✓	✓	✓	✓	✓

intelligent devices and sent to fog nodes. In this case, the fog nodes use their processing power to use machine learning to examine the physiological signals received and to make decisions about patients who may have problems. After the diagnosis of this group of patients, a warning message is sent to the relevant doctor. In this case, blockchain is used to secure the data stream. The authors in Ref. [25] provided a survey on IoT-based healthcare system. For this purpose, a comprehensive review of the applications, problems, and challenges of these systems has been conducted. The result of this study is the need for the development of traditional health models with the help of IoT infrastructure. In this way, a permanent connection can be established between the patient and the medical centers through IoT sensors. But, in the meantime, there are security and privacy challenges that require new research and solutions to provide secure algorithms that require low resources.

Also in Table 2 contribution of some related works are shown.

3. Biometric Security Using Markov Model

In the traditional systems, security depended on password-based approaches. In this section, the level of security improvement in biometric-based systems compared with traditional password methods will be proven.

In order to evaluate the security, we introduce a Markov process to describe a security attack model based on the Markov transition matrix. A security threat is a stochastic process; therefore, we model it as a Markov chain.

3.1. Two-State Markov Model. The probability of transition from one state to another is defined based on the vulnerabilities present in the current state. An attacker misuses various vulnerabilities to reach a security threat state and, ultimately, reaches the ultimate failure. Not applying security measures, the system has two states, as shown below:

(i) S state for secure state

(ii) F state for failure state

3.1.1. Two-State Markov Model in the State of Inability for Recovering Security Threat. In the Markov model shown below, "a" probability indicates the probability of transition from a secure state to a failure state. Since in this model, recovering the security threat is not possible, the system enters the failure state (fault state) during the security threat. In the Markov chain, the sum of probabilities of outgoing edges from each state is equal to one (see Figure 1).

3.1.2. Two-State Markov Model Able to Recover Security Threat. In this Markov chain, since recovering the security threat is possible, there is a "b" probability for a system in failure state to return and recover from security error state to a secure state (see Figure 2).

(i) "a" probability: it indicates the transition probability from a secure state to a threat state.

(ii) "b" probability: it indicates the return and recovery probability of the system from a security error state to a secure state (detection and correction of security threat).

3.2. Three-State Markov Model. By applying the suggested mechanism, we focus on the observable and measurable states and develop three states [27].

(i) State "S" for the secure state of the system

(ii) State "T" for the threat state of the system

(iii) State "F" for the failure state of the system

Figure 3 presents the suggested pattern of Markov for modeling security threats and attacks with the probability of transition between states.

The probabilities of transition between states in the Markov model are as follows:

(i) Probability "a": indicates the probability of transition from a secure state of the system to a threat state.

(ii) Probability "b": indicates the probability of threat elimination and return of the system from a threat state to a secure state.

(iii) Probability "c": indicates the probability of transition from the system's threat state to failure state and occurrence of security error (in the case of not identifying the security threat).

Table 2: Related works in the field of IoT security.

Reference paper	Year	Contribution
[17]	2021	In this solution, a lightweight algorithm based on block cryptography is used to provide security in fog computing.
[19]	2020	A two-step encryption solution is provided to secure the data stored in the cloud. In this solution, the main data are divided into two parts, which are encrypted by a common key.
[22]	2020	In this article, the authors provide an overview of the most important cryptographic solutions that can be used in fog computing. The results of these studies indicate the need for algorithms and solutions that can create a kind of compromise between security and service quality parameters.
[24]	2020	A framework for use in health care systems along with machine learning for decision-making based on patient data is provided. Also, blockchain has been used to secure the data stream.
[26]	2020	This paper first examines the infrastructure, protocol, and application of the Internet of Things. Then, security problems in the IoT environment are expressed. It also identifies some emerging techniques that can be used to address IoT security issues. In this study, the authors conclude that machine learning, blockchain, and artificial intelligence are the new approaches to solving the problem of IoT security.
[14]	2020	The authors provided a system including a microcontroller with android application that has features for history control and speech recognition. For securing this system, they are using a unique biometric and speech authentication mechanism.
[15]	2019	Authors in this paper provided a low-cost biometric system for IoT devices that used limited resources to reduce memory and computation costs. The proposed system utilizes an algorithm based on the block logic operation to reduce biometric property measurement.
[21]	2019	A number of symmetric cryptographic algorithms have been investigated in terms of performance. Solutions in terms of runtime parameters and memory consumption have been investigated. The purpose of this study was to determine the capabilities and limitations of each cryptographic algorithm.
[18]	2018	In this research, an encryption system based on AES algorithm and asynchronous key transfer system for data exchange is presented. This solution can be used to secure infrastructure with limited processing resources.
[20]	2018	Blockchain has been used as a security solution based on cloud computing. To ensure data security, data are stored in the form of blockchain blocks.

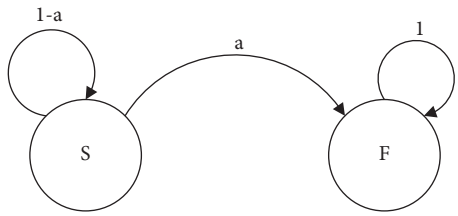

Figure 1: Markov model before the proposed mechanism and impossibility of security threat.

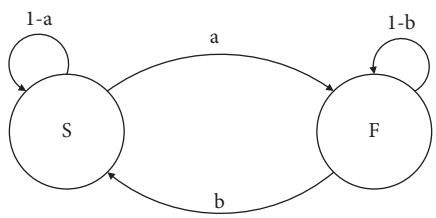

Figure 2: Markov model before the suggested mechanism.

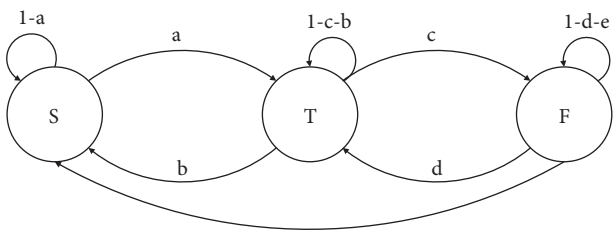

Figure 3: Three-state Markov model.

(iv) Probability "d": indicates the probability of return of the system from security error occurrence state to threat state (detection of security threat).

(v) Probability "e": indicates the probability of return and recovery of the system from security error occurrence to secure state (detection and correction of security threat).

This security model contains every element of a security attack, including attack, defense, and system recovery. In this article, due to some reasons, we will not introduce the direct transition from state S to state F, because several stages exist for the detection and correction of security threats in the proposed mechanism.

Since security threats, as error occurrence factors, lead to the system entering an undesired state, there are two states of detection and correction to deal with security threats.

In the above model, probabilities "b" and "d" indicate the correction probabilities of the security threats (probability "b" indicates the probability for system return from a threat state to a secure state after correction of the threat state and probability "d" indicates the probability of system return from security error occurrence to threat state in the case of error correction of the threat state).

3.3. Transition Probability Matrix for States of Security Evaluation. The transition probability matrix for a Markov chain with n states is a $n \times n$ matrix in which the element

$p[i, j]$ is the probability of transition from state i to state j in the range [1, 28].

3.3.1. Transitions Probability Matrices of the Two-State Markov Model in the Mode of the Impossibility of Security Threat Recovery. In the transition probability matrix, the sum of values of each row is equal to one. Hence, based on the Markov chain, the transition probability matrix is obtained, as shown in Figure 4.

3.3.2. Transition Probability Matrix of the Two-State Markov Model with the Possibility of Threat Recovery. In this case, in the Markov chain, there is a probability of b for recovery of the security threat. Therefore, the transition probability matrix is obtained (see Figure 5).

3.3.3. Transition Probability Matrix of the Three-State Markov Model. Figure 6 presents the suggested pattern for modeling security threats and attacks based on the Markov chain and the transition probability matrix.

3.4. The Failure Probability of the System and Security Hacking. Based on the Markov chain and transition probability matrix, the probability of the system failure and security hacking is shown as $P(F)$ and obtained by the below equations:

(a) The probability of system failure and security hacking in the first Markov model

$P(F) = P(s).a + P(F).1$

$P(S)$: The probability of the system being at the secure state

$P(F)$: The probability of the system being at the hacking state and failure of the firewall

b. The probability of system failure and security hacking in the second Markov model

$P(F) = P(s).a + P(F).(1 - b)$

c. The probability of system failure and security hacking in the third Markov model

$P(F) = P(s).a.P(T).c + P(F).(1 - d - e)$

$P(T)$: The probability of the system being at the threat state

4. The Proposed Mechanism

Security improvement in different systems is based on the following three mechanisms:

(i) Authentication Algorithm

(ii) Hash Algorithm

(iii) Encryption Algorithm

The proposed mechanism in this paper is based on a combination of Hash and Authentication mechanisms.

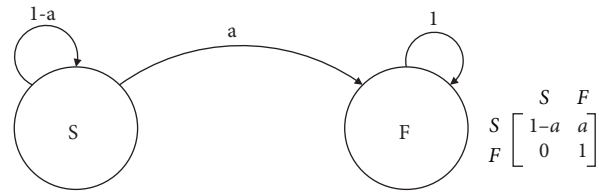

Figure 4: The Markov chain and transitions probability matrix before suggested mechanism and impossibility of security threat recovery.

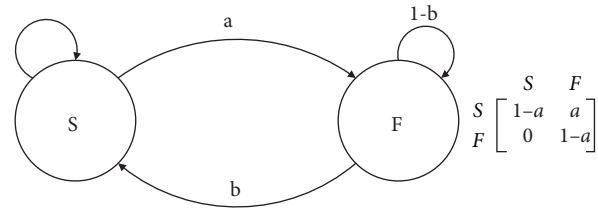

Figure 5: Markov chain and transitions probability matrix before the suggested mechanism and the possibility for recovery of the security threat.

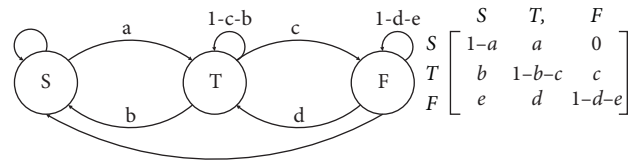

Figure 6: The Markov chain and transition probability matrix with the suggested mechanism.

4.1. First Layer of Security Architecture: Authentication. If the fingerprint is accepted by the controller, the confirmation signal is sent through the transmitter module to the IoT system, which can also include a wireless receiver pair and a similar controller. The flowchart of the IoT platform transmitter function is shown in Figure 7. In this algorithm, the fingerprint is initially received by the relevant module via the IoT controller for receiving and authentication of the user and after comparing the received data, the data are compared with the approved biometric features database. If the user authentication is verified, the connection to the infrastructure will be established.

As shown in Figure 8, a fingerprint image is captured by a scanner or sensor and the sensor converts it into a data format.

The Nest Scenario is similar to the baseline scenario based on the hardware perspective except that the VeriFinger fingerprint identification algorithm is used. A set of minutiae points is used in the VeriFinger fingerprint identification algorithm. The first step in fingerprint authentication is fingerprint image sampling. In the fingerprint sensor, the characteristics of the points with the matched fine lines are taken from the fingerprint image, and they are referred to as minutiae points. In biometrics and fingerprint scanning, minutiae refer to specific plot points on a fingerprint. This includes characteristics such as ridge bifurcation or a ridge ending on a fingerprint. These features store

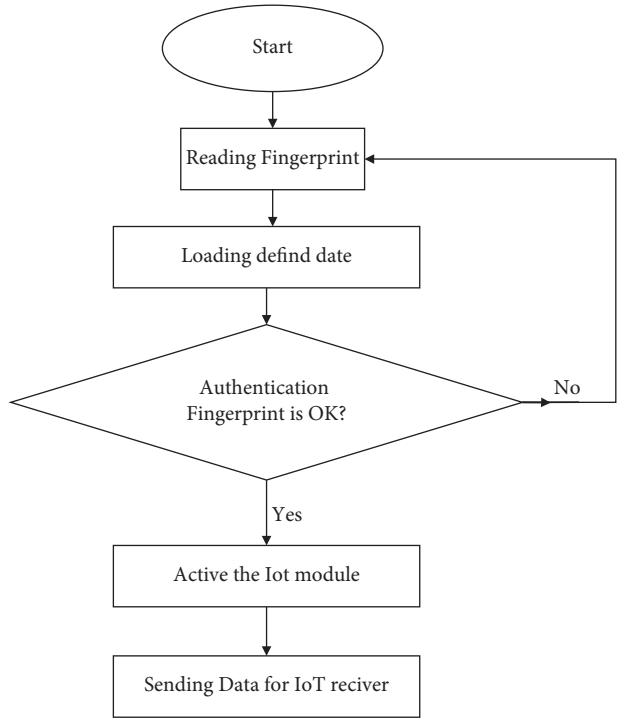

Figure 7: System failure probability in the first Markov model.

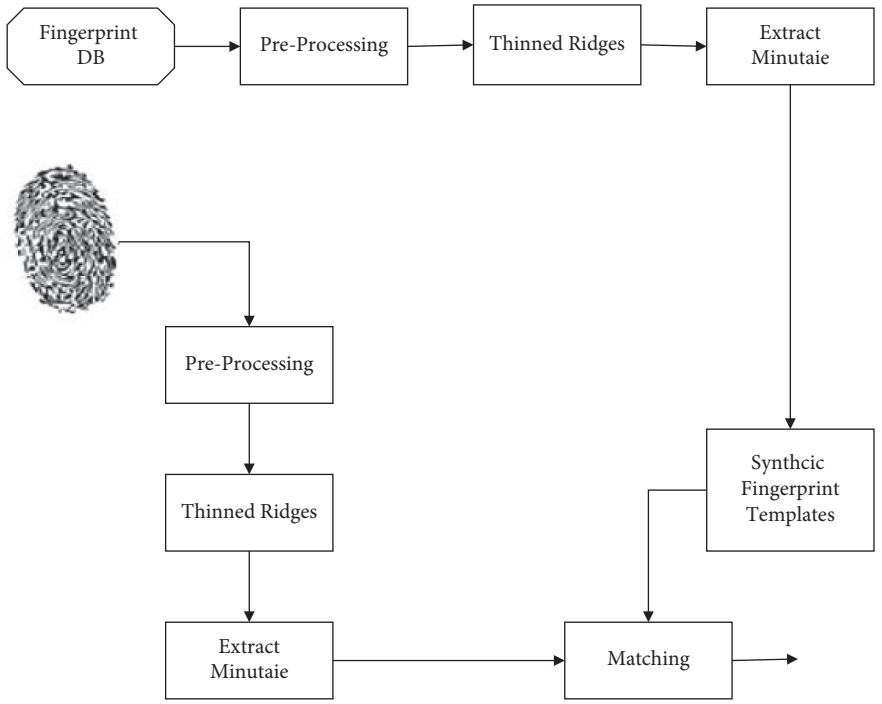

Figure 8: System failure probability in the second Markov model.

each individual finger in a database and differentiate them from other recorded fingerprints. Fingerprint is initially matched with the entries in the database which have general features similar to the tested fingerprint. If the matching operation with this group does not produce a positive result, the next record with the most similar general features would be selected and the process continues with the same basis until either the successful result is achieved or the end of the database is announced.

Three fingerprint samples are taken from one finger to produce more accurate and higher quality results. Each of the three images is processed to extract its features. The

three sets of features are then analyzed and subdivided into a single set of features written in the database. Accordingly, the recorded features will be more reliable and the fingerprint identification quality is significantly enhanced. The flowchart in Figure 9 illustrates the VeriFinger fingerprint identification algorithm step by step.

4.2. Second Layer of Security Architecture: Hashing. In subsequent scenarios, in addition to security enhancement by the fingerprint sensor at the IoT sensor layer, hash and encoding algorithms are used. Figure 10 schematically illustrates the mechanism of combining hash and biometric fingerprint encoding algorithms.

The fingerprint sensor and encryption in this scenario are combined with the MD5 algorithm. The MD5 algorithm returns a 128-bit digital fingerprint as an output where the message means the biometric feature of the IoT user (see Table 3).

4.3. Third Layer of Architecture: IoT Controller. User authentication based on each one of the biometric properties, such as voice biometric and cryptosystem, is according to the below items:

IoT controller supports below elements regarding encryption algorithms.

(i) Authenticated encryption with associated data (AEDA): GCM, EAX, ChaChaPoly
(ii) Encrypted blocks: AES256, AES192, AES128
(iii) Encryption modes: XTS, GCM, EAX, CTR
(iv) Hash algorithms: BLAKE2b, BLAKE2s, SHA3_512, SHA3_256, SHA512, SHA256
(v) Extendable output functions: SHAKE256, SHAKE128
(vi) Message authentication: MAC-, GHASH, Poly1305
(vii) Public-key algorithms: P521, Ed26619, Curve25519
(viii) Random number generation: RNG

Based on the statistics of Ref. [6], the application of some of these algorithms is listed as follows:

Encryption algorithms
Hash algorithms
Authentication algorithms

4.4. Combining Biometric and Hashing. Multiple authentication to enhance user authentication along with coding mechanisms has been proposed as a new approach in this study. Primary authentication is done using biometric identification, which demonstrates the highest level of security compared to other methods of identification. The main advantage of this approach is reported to provide unique information, i.e., the biological features of the individuals, and remove the problem of replay attacks. The use of encryption-based systems also prevents replay attacks and eavesdropping. The proposed architecture includes the following components:

(i) Biometric authentication by scanning the relevant biological features
(ii) Sending the scan result to the database
(iii) Encrypting the data to the database
(iv) Comparing the encrypted data with the samples in the database
(v) Performing the compliance and authenticity steps
(vi) Approving and allowing the user to communicate in case of matching
(vii) Monitoring of the IoT data

To improve security, the security threats are classified as follows:

(i) Security threats in the identification layer
(ii) Security threats of the control algorithms
(iii) Security threats in the network communications layer (IoT Infrastructure)

Figure 11 shows how to combine biometric and hashing features to increase security:

5. Evaluation

5.1. System Configuration. The details and configuration of hardware's instrument are shown in Table 4.

Also, the raspberry Pi 4 details are described in Table 5.

5.2. Simulation Details. The simulated data are extracted from the Arduino IDE (A compiler of commands for programming IoT sensors) and Fritzing V0.9.2 b (simulating the hardware needs to communicate with the sensors) simulation software and the proposed algorithm is evaluated with different benchmark test structures. Then, the IoT security models are analyzed. The Arduino controller is an open source platform. This unique feature contributes to find relevant libraries for each module or sensor. User authentication is based on each of the biometric features such as audio biometric and cryptographic system to increase security. To analyze and evaluate the proposed method, various simulation scenarios are presented related to the security of IoT-based systems. In Scenario 1, the level of security is checked by the fingerprint sensor authentication mechanism. The components of this scenario can be seen in Figure 12:

Schematic of IoT implementation based on fingerprint biometrics is illustrated in Figure 13:

Considering the evaluation results, the VeriFinger algorithm and encryption algorithms both affect the security authentication on the Internet of things. These parameters are selected based on the interactions between security, efficiency, and system cost. From the perspective of VeriFinger algorithm modules, U.are.U 5100 and Verifier 300 modules have the most and least level of security. For

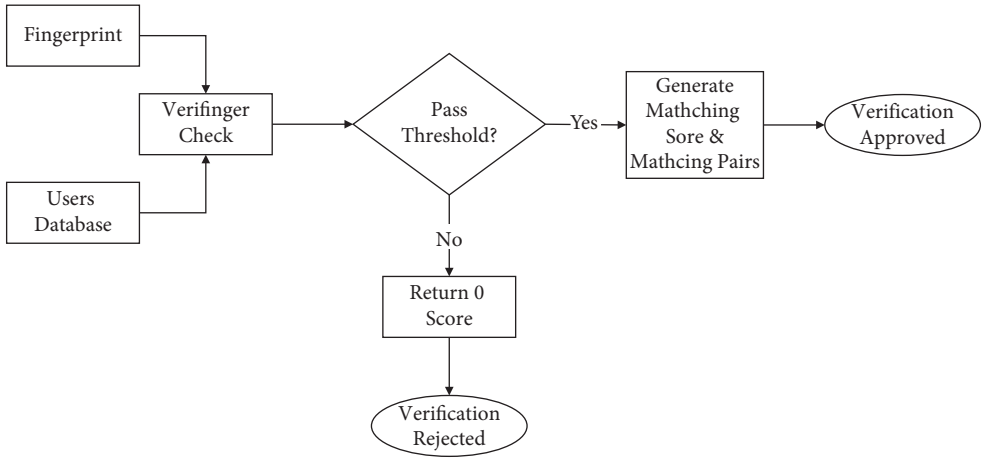

Figure 9: The transmitter module flowchart.

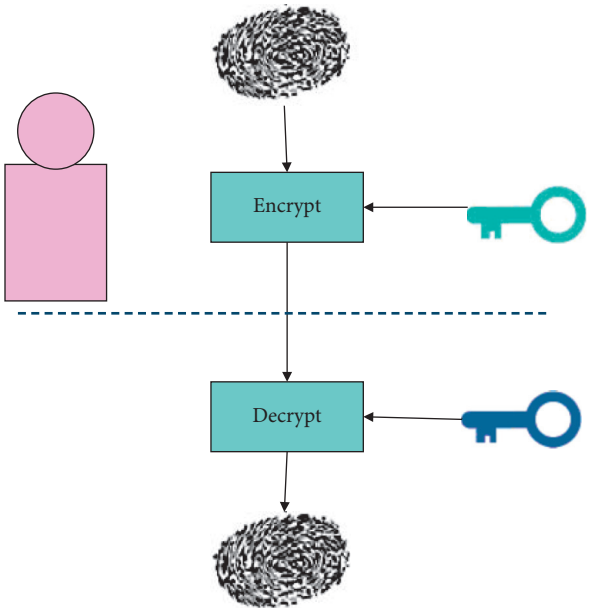

Figure 10: Biometric data matching steps.

Table 3: Comparing the characteristics of MD5 and SHA1 algorithms.

Function	MD5	SHA1
Block length	512 bit	512 bit
Algorithm length	128 bit	160 bit
Rotation steps	64 steps	80 steps
Initialization variables	4	5
Collision complexity	2^{54}	2^{80}

moderate security purposes, the FS80 module can be used based on efficiency and costs.

The fingerprint identification algorithm of VeriFinger is evaluated regarding authentication mechanisms; on the other hand, the efficiency and security of this algorithm are dependent on other fingerprint modules. In this regard, based on the agreement accuracy and agreement speed of fingerprint reading, U.are.U 5100 module has

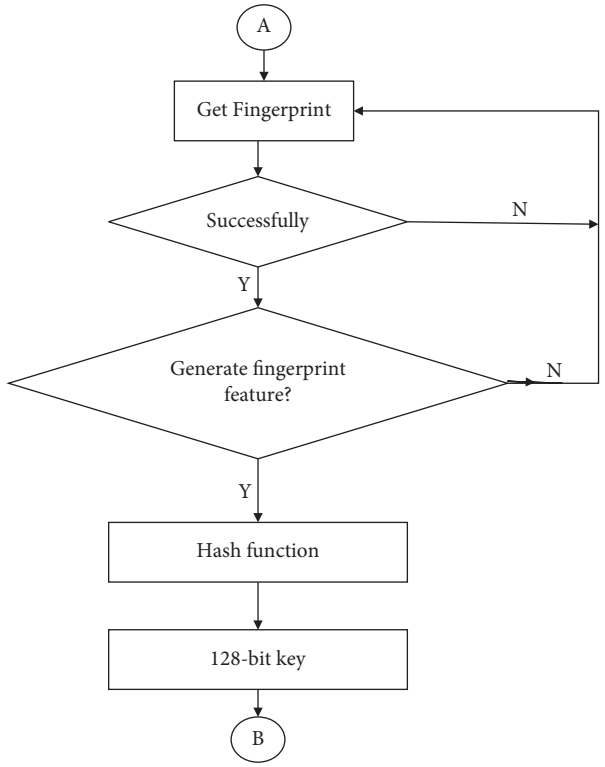

Figure 11: VeriFinger fingerprint identification algorithm.

more security than modules FS80 and Verifier 300. Hence, in the following sections, the fingerprint recognition authentication mechanisms are simulated based on the U.are.U 5100 module. Concerning Hash mechanisms, the strongest Hash mechanism is based on security evaluation in different conditions of algorithms, namely, MD5 and SHA1.

To check the performance of the MD5 and SHA1 encoding algorithms, the encoding time parameter is used, which is a function of the fingerprint file size (see Figure 14).

Comparing the computation time required for MD5 algorithm coding relative to SHA1 is 63.21% on average (see Table 6).

Table 4: Details and configuration of hardware's instrument.

IoT Device	Finger Pulse Oximeter Jumper JPD-450F, 1.6 V, with Bluetooth v4.2.
Master node	Laptop dell E6520, intel core i7- CPU 2760QM @ 2.40 GHz, 8 GB RAM DDR3
Worker node	Raspberry pi 4, ARM Cortex-A72

Table 5: Raspberry Pi 4 details.

Broadcom BCM2711, Quad core Cortex-A72 (ARM v8) 64 bit SoC @ 1.5 GHz
4 GB LPDDR4-3200 SDRAM
2.4 GHz IEEE 802.11ac wireless, bluetooth 5.0, BLE
2-Lane MIPI CSI camera port
Gigabyte ethernet 10/100/1000 Mbit/s
2-Lane MIPI CSI camera port
OpenGL ES 3.1, vulkan 1.0
5V DC via USB-C connector

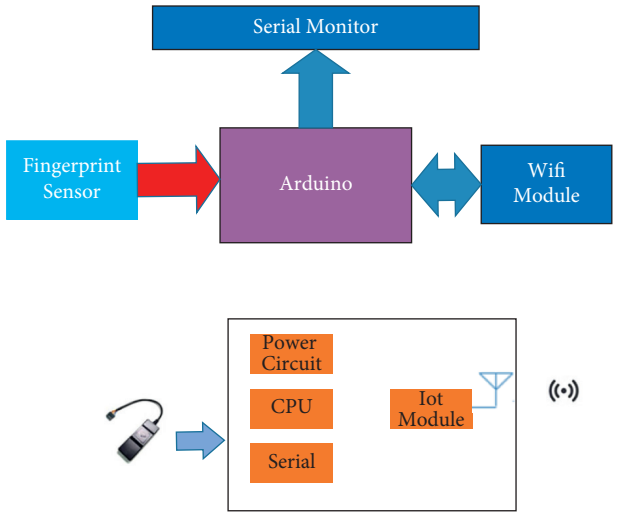

Figure 12: Combining hash and fingerprint biometric encryption algorithms.

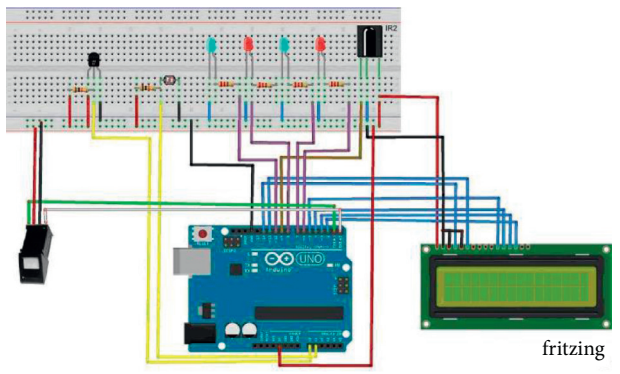

Figure 13: Comparison of the performance of MD5 and SHA1 encoding algorithms by the fingerprint file size.

Thus, by applying the biometric properties and a combination of applied innovations in IoT layers, the probability of security problems reduced by 90.71% on average. On the other hand, to keep the efficiency of these MD5 and SHA1 algorithms from the perspective of the time required for coding, using the MD5 algorithm, leads to a 63.21% reduction in the delay time of system efficiency improvement.

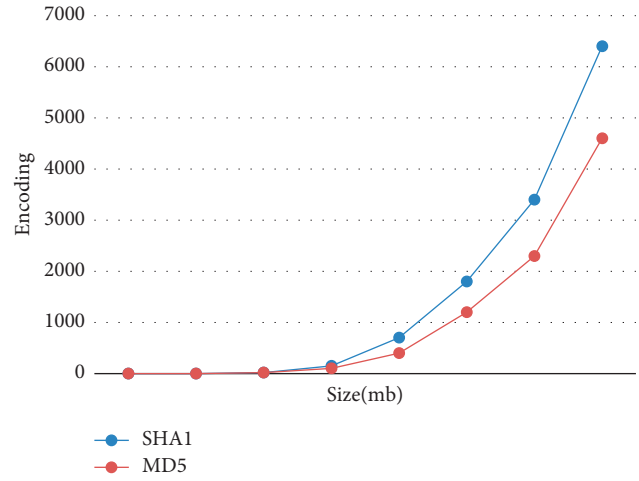

Figure 14: Increasing security by combining biometric and hashing features.

Table 6: Summary of comparing the time required for coding.

File size(KB)	Time MD5/SHA1 (%)
8	67.65
16	69.35
32	36.63
64	74.07
128	52.85
256	66.88
512	67.56
1024	70.70
Average	63.21

5.3. Evaluation of the Two Proposed Methods. Based on the study [29], the security resulted from traditional systems, such as password compared with biometric properties, like the fingerprint, as shown in Table 7.

5.3.1. Evaluation of Security of the Two-State Markov Model in the State of the Impossibility of Security Threat Recovery. Before the suggested mechanism and impossibility of security threat, concerning the obtained equation, the probability of the system being at the hacking state and firewall failure is obtained from the below relationship:

$$P(F) = P(s0) \cdot A + (F0) \cdot 1. \quad (1)$$

Table 7: Evaluation of Users' accounts.

Security rating	Password (%)	Fingerprint (%)
Very secure	23.4	31.9

Based on different values of a, which is the occurrence probability of security threat, and initial value of $P(S0)$, which according to the security results of traditional systems, is assumed as password and biometric property, two tables are generated, as shown below. It should be noted that the initial value of $P(F0)$ is the supplement of state $P(S0)$. See Tables 8 and 9.

The probability of system failure and security hacking of the first Markov model in two states of using password compared with using fingerprint biometric can be observed in Figure 15.

5.3.2. Evaluation of the Two-State Markov Model Security with the Possibility of Security Threat Recovery. Before applying the proposed mechanism and with security threat recovery, considering the acquired equation, the probability of the system being at hacking state and firewall failure is obtained from the below relationship:

$$P(F) = P(s0) \cdot a + P(F0) \cdot (1 - b). \quad (2)$$

By considering the probability of security threat occurrence and initial values $P(S0)$, which are assumed based on the security results from traditional systems, such as password and biometric property, Tables 10–13 are obtained based on different values of a and b.

The probability of system failure and security hacking of the second Markov model using password compared with using fingerprint biometric can be observed in Figure 16.

5.3.3. Security Evaluation of the Three-State Markov Model. By applying the proposed mechanism, which is measured based on the initial values of states $P(s0)$, $P(T0)$, $P(F0)$, and coefficients of e, d, c, and a:

$$P(F) = P(s0)a \cdot P(T0) \cdot c + P(F0) \cdot (1 - d - e). \quad (3)$$

The result was much higher than the first and second models, which were obtained using fingerprint biometrics instead of passwords, thus reducing the probability of system hacking by an average of 83.12%.

5.4. Evaluation Results of Different Markov Models

5.4.1. Evaluation Result of Security Failure Probability in the First Markov Model. As seen in Table 14, applying the biometric fingerprint leads to an average decrease of 94.99% in the probability of system hacking compared with using a password.

5.4.2. Evaluation Result of Security Failure Probability in the Second Markov Model. Averaging the evaluation results shows that using biometric fingerprint reduces the probability of system hacking by 94.02% on average.

5.4.3. Evaluation Result of Security Failure Probability in the Third Markov Model. Applying the biometric fingerprint reduces the system hacking probability by 83.12% on average.

5.5. Evaluation Result of Security Failure Probability. Overall, the probability of security problem occurrence in three Markov models reduces by 90.71% on average by applying the biometric properties (see Table 15).

Table 8: Evaluation of security in the first model of Markov with the assumption of using password.

a	$P(S0)$	$P(F0)$	$P(F)$
0.10	23.4	76.6	78.94
0.20	23.4	76.6	81.28
0.30	23.4	76.6	83.62
0.40	23.4	76.6	85.96
0.50	23.4	76.6	88.3
0.60	23.4	76.6	90.64
0.70	23.4	76.6	92.98
0.80	23.4	76.6	95.32
0.90	23.4	76.6	97.66

Table 9: Evaluation of security in the first model of Markov with the assumption of using fingerprint biometric.

a	$P(S0)$	$P(F0)$	$P(F)$
0.10	31.9	68.1	71.29
0.20	31.9	68.1	74.48
0.30	31.9	68.1	77.67
0.40	31.9	68.1	80.86
0.50	31.9	68.1	84.05
0.60	31.9	68.1	87.24
0.70	31.9	68.1	90.43
0.80	31.9	68.1	93.62
0.90	31.9	68.1	96.81

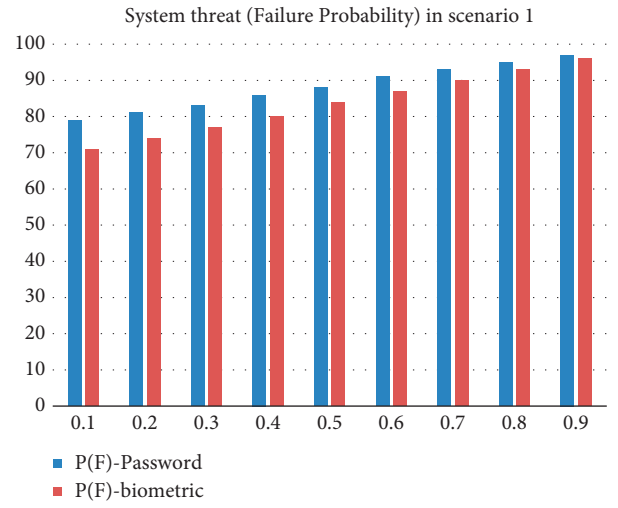

Figure 15: Block Diagram of Scenario Modules 1 (fingerprint sensor authentication in IoT).

Table 10: Evaluation of security in the second Markov model with the assumption of using a password (constant value of b and variable a).

a	b	$P(S)$	$P(F)$	$P(F)$
0.10	0.90	23.4	76.6	10
0.20	0.90	23.4	76.6	12.34
0.30	0.90	23.4	76.6	14.68
0.40	0.90	23.4	76.6	17.02
0.50	0.90	23.4	76.6	19.36
0.60	0.90	23.4	76.6	21.7
0.70	0.90	23.4	76.6	24.04
0.80	0.90	23.4	76.6	26.38
0.90	0.90	23.4	76.6	28.72

Table 11: Evaluation of security in the second Markov model with the assumption of using a password (constant value of a and variable b).

a	b	$P(S)$	$P(F)$	$P(F)$
0.10	0.10	23.4	76.6	71.28
0.10	0.20	23.4	76.6	63.62
0.10	0.30	23.4	76.6	55.96
0.10	0.40	23.4	76.6	48.3
0.10	0.50	23.4	76.6	40.64
0.10	0.60	23.4	76.6	32.98
0.10	0.70	23.4	76.6	25.32
0.10	0.80	23.4	76.6	17.66
0.10	0.90	23.4	76.6	10

Table 12: Evaluation of security in the second Markov model with the assumption of using biometric (constant value of b and variable a).

a	b	$P(S)$	$P(F)$	$P(F)$
0.10	0.90	31.9	68.1	10
0.20	0.90	31.9	68.1	13.19
0.30	0.90	31.9	68.1	16.38
0.40	0.90	31.9	68.1	19.57
0.50	0.90	31.9	68.1	22.76
0.60	0.90	31.9	68.1	25.95
0.70	0.90	31.9	68.1	29.14
0.80	0.90	31.9	68.1	32.33
0.90	0.90	31.9	68.1	35.52

Table 13: Evaluation of security in the second Markov model with the assumption of using biometric (constant value of a and variable b).

a	b	$P(S)$	$P(F)$	$P(F)$
0.10	0.10	31.9	68.1	64.48
0.10	0.20	31.9	68.1	57.67
0.10	0.30	31.9	68.1	50.86
0.10	0.40	31.9	68.1	44.05
0.10	0.50	31.9	68.1	37.24
0.10	0.60	31.9	68.1	30.43
0.10	0.70	31.9	68.1	23.62
0.10	0.80	31.9	68.1	16.81
0.10	0.90	31.9	68.1	10

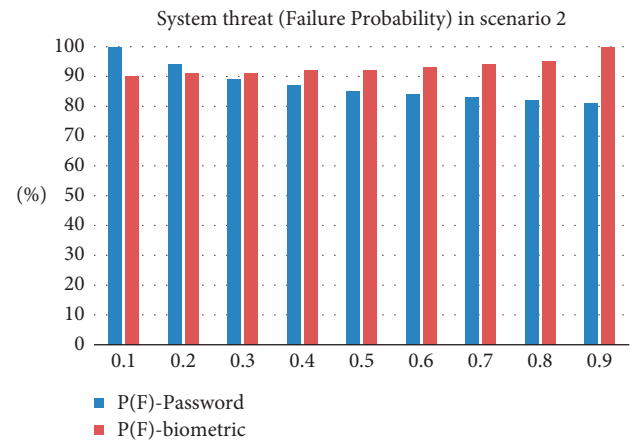

Figure 16: Schematic of implementing the IoT application.

Table 14: Evaluation result of security failure probability in the first Markov model.

a	$P(F)$-Password	$P(F)$-Biometric	System threat (failure probability) in model 1 (%)
0.10	78.94	71.29	90.31
0.20	81.28	74.48	91.63
0.30	83.62	77.67	92.88
0.40	85.96	80.86	94.07
0.50	88.3	84.05	95.19
0.60	90.64	87.24	96.25
0.70	92.98	90.43	97.26
0.80	95.32	93.62	98.22
0.90	97.66	96.81	99.13
Average			94.99

Table 15: Security failure probability by applying the biometric properties.

System threat (failure probability) (%)	
Model 1	94.99
Model 2	94.02
Model 3	83.12
Average	90.71

5.6. Simulation Scenarios. As mentioned in previous sections of the article, we assume the below scenarios by considering the schematic of Figure 13:

(i) Facing security threats by fingerprint recognition in the first layer of IoT

(ii) Facing security threats by the hash mechanism in the second layer of IoT

(iii) Facing security threats by software and hardware mechanisms in the application layer of IoT

(iv) Facing security threats by applying the suggested mechanism in the article, including the aggregation of the above mode in all three architectural layers of IoT

In the following, we examine the results of each scenario from the security perspective and study the improvement level of the suggested system.

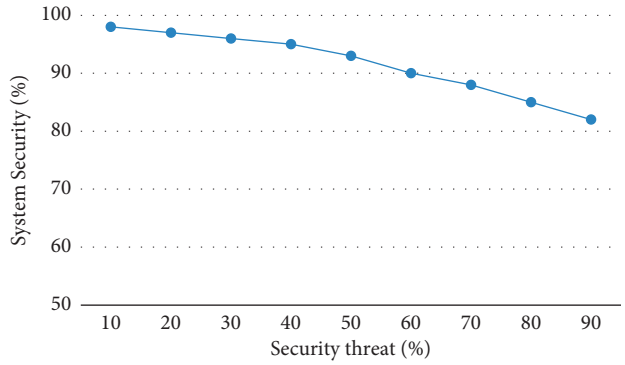

Figure 17: System security in the first scenario for different levels of security threats.

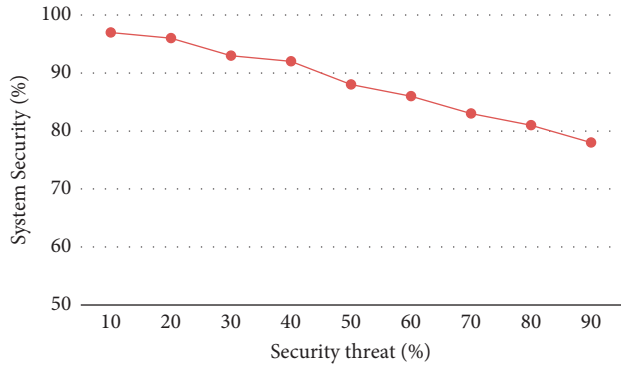

Figure 18: System security in the second scenario for different levels of security threats.

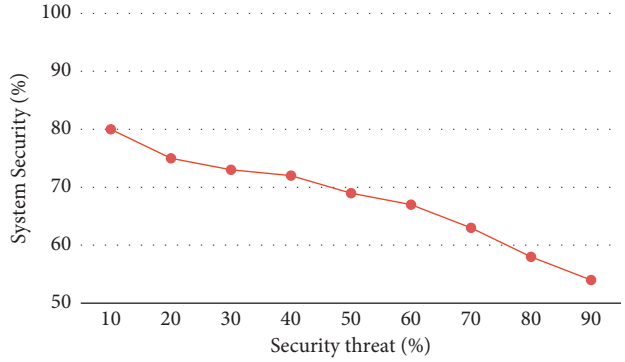

Figure 19: System security in the third scenario for different levels of security threats.

5.6.1. First Scenario: Facing the Security Threats by Fingerprint Recognition in the First Layer of IoT. In this case, biometric properties are applied only in the sensors' layer, and on average, the system security is 91.34% (see Figure 17).

5.6.2. Second Scenario: Facing the Security Threats by the Hash Mechanism in the Second Layer of IoT. In this case, the hash mechanism in the second IoT layer is used to face security threats, and the system security is 88.02% on average (see Figure 18).

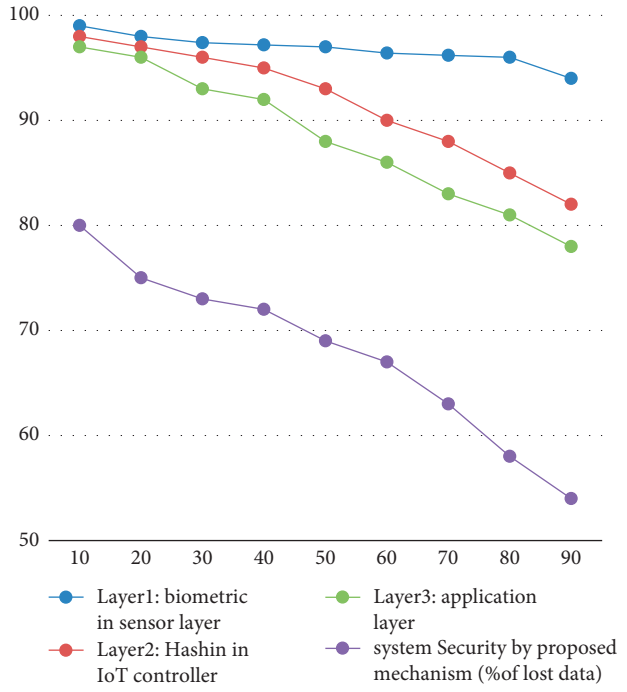

Figure 20: Comparison of system security in the suggested mechanism with available scenarios.

Table 16: Comparison results.

Security threat (%)	System security improvement (relative to each layer)		
	Layer 1: Biometric in sensor layer	Layer 2: Hashing in IoT controller	Layer 3: Application layer
10	101.33	101.33	122.80
20	102.32	103.29	130.58
30	102.08	105.84	133.46
40	102.72	106.20	136.66
50	105.14	109.91	139.73
60	107.13	111.98	143.80
70	108.75	116.25	154.07
80	112.41	119.26	164.19
90	114.22	120.04	174.83
Average	106.23	110.45	144.46
		120.38	

5.6.3. Third Scenario: Facing Security Threats with Software and Hardware Mechanisms in the Application Layer of IoT. In this scenario, security measures are applied in the application layer. Due to the weakness of this layer, system security is 67.89% on average (see Figure 19).

5.6.4. Fourth Scenario: Facing the Security Threats by Applying the Suggested Mechanism in the Article, Including the Aggregation of above Mode in All Three Architectural Layers of IoT. In this case, which is suggested by

this paper, a combination of three above scenarios is proposed, and the system security is 96.82%, on average, and the improvement level of security in this scenario compared with previous modes can be seen in Figure 20:

The relative comparison of results is observed in Table 16:

6. Conclusion

IoT is expected to expand user connectivity and ease daily life; however, serious security challenges are considered in using this technology for distributed authentication. Moreover, integrating with biometrics in IoT design raises concerns about the cost and implementation of a user-friendly design. Furthermore, user authentication in the IoT environment is one of the most important challenges, especially in accessing important data. Current user authentication approaches on the IoT are either less flexible or inflexible. For authentication, the security of password-based systems decreases over time due to human error and the complexity of malicious attacks. According to the proposed mechanism in this paper, which is a combination of biometrics and coding, the security of the system has been improved by an average of 96.82%. Based on simulation states, the proposed method improves the system security by 120.38% on average, which shows 106.23, 110.45 and 144.46% improvement for the IoT sensor layer, controller layer and application layer, respectively [30–35].

Data Availability

The data are available upon request to the corresponding author.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

References

[1] P. Aufner, "The IoT security gap: a look down into the valley between threat models and their implementation," *International Journal of Information Security*, vol. 19, no. 1, pp. 3–14, 2019.

[2] Gartner, "Gartner Says the Internet of Things Will Transform the Data Center, (2014http://www.gartner.com/newsroom/id/2684616.

[3] IoT. Analytics, "Why the Internet of Things Is Called Internet of Things: Definition, History, Disambiguation," (2014) https://iot-analytics.com/internetof-things-definition.

[4] D. Ferraris and C. Fernandez-Gago, "TrUStAPIS: a trust requirements elicitation method for IoT," *International Journal of Information Security*, vol. 19, 2019.

[5] M. Trik, S. Pour Mozafari, and A. M. Bidgoli, "An adaptive routing strategy to reduce energy consumption in network on chip," *Journal of Advances in Computer Research*, vol. 12, no. 3, pp. 1–12, 2021.

[6] H.-T. Nguyen, Q.-D. Ngo, and V.-H. Le, "A novel graph-based approach for IoT botnet detection," *International Journal of Information Security*, vol. 19, 2019.

[7] A. M. Rahmani, "Exploiting smart e-Health gateways at the edge of healthcare Internet-of-Things: a fog computing approach," *Future Generation Computer Systems*, vol. 78, pp. 641–658, 2018.

[8] H. Dubey, "Fog computing in medical internet-of-things: architecture, implementation, and applications," *Handbook of Large-Scale Distributed Computing in Smart Healthcare*, Springer, Berlin, Germany, 2017.

[9] I. Azimi, "HiCH: hierarchical fog-assisted computing architecture for healthcare IoT," *ACM Transactions on Embedded Computing Systems*, vol. 16, pp. 1–20, 2017.

[10] T. N. Gia, "Low-cost fog-assisted health-care IoT system with energy-efficient sensor nodes," in *Proceedings of the 2017 13th International Wireless Communications and Mobile Computing Conference (IWCMC)*, Valencia, Spain, June 2017.

[11] P. Hu, "Fog computing based face identification and resolution scheme in internet of things," *IEEE Transactions on Industrial Informatics*, vol. 13, pp. 1910–1920, 2016.

[12] V. Suneetha, S. Suresh, and J. Viswa, "A novel framework using Apache spark for privacy preservation of healthcare big data," in *Proceedings of the 2020 2nd International Conference on Innovative Mechanisms for Industry Applications (ICIMIA)*, Bangalore, India, March 2020.

[13] S. Jebri, "lightweight Algorithm to secure data transmission in IoT systems," *Wireless Personal Communications*, vol. 116, pp. 2321–2344, 2021.

[14] F. Afandi and R. Sarno, "Android application for advanced security system based on voice recognition, biometric authentication, and internet of things," in *Proceedings of the 2020 International Conference on Smart Technology and Applications (ICoSTA)*, pp. 1–6, Surabaya, Indonesia, February 2020.

[15] W. Yang, S. Wang, G. Zheng, J. Yang, and C. Valli, "A privacy-preserving lightweight biometric system for internet of things security," *IEEE Communications Magazine*, vol. 57, no. 3, pp. 84–89, 2019.

[16] N. Karimian, M. Tehranipoor, D. Woodard, and D. Forte, "Unlock your heart: next generation biometric in resource-constrained healthcare systems and IoT," *IEEE Access*, vol. 7, pp. 49135–49149, 2019.

[17] F. Thabit, "A new lightweight cryptographic algorithm for enhancing data security in cloud computing," *Global Transitions Proceedings*, vol. 2, pp. 91–99, 2021.

[18] A. Hussain, C. Xu, and M. Ali, "Security of cloud storage system using various cryptographic techniques," *International Journal of Mathematics Trends and Technology*, vol. 60, pp. 45–51, 2018.

[19] R. F. Abdel-Kader, S. H. El-Sherif, and R. Y. Rizk, "Efficient two-stage cryptography scheme for secure distributed data storage in cloud computing," *International Journal of Electrical and Computer Engineering*, vol. 10, pp. 3–1, 2020.

[20] C. Esposito, "Blockchain: a panacea for healthcare cloud-based data security and privacy," *IEEE Cloud Computing*, vol. 5, pp. 31–37, 2018.

[21] Wani and Q. P. Abdul Raoof, "Performance evaluation and analysis of advanced symmetric key cryptographic algorithms for cloud computing security," *Soft Computing: Theories and Applications*, Springer, Berlin, Germany, 2019.

[22] V. Agarwal, A. K. Kaushal, and L. Chouhan, "A survey on cloud computing security issues and cryptographic techniques," *Social Networking and Computational Intelligence*, Springer, Berlin, Germany, 2020.

[23] B. Umapathy, "A survey ON cryptographic algorithm for data security IN cloud storage environment," *European Journal of Molecular & Clinical Medicine*, vol. 7, no. 9, 2020.

[24] A. Banerjee, "A secure IoT-fog enabled smart decision making system using machine learning for intensive care unit," in *Proceedings of the 2020 International Conference on Artificial Intelligence and Signal Processing (AISP)*, Amaravati, India, January 2020.

[25] K. Jaiswal and V. Anand, "A survey on IoT-based healthcare system: potential applications, issues, and challenges," *Advances in Biomedical Engineering and Technology*, Springer, Berlin, Germany, 2021.

[26] B. K. Mohanta, "Survey on IoT security: challenges and solution using machine learning, artificial intelligence and blockchain technology," *Internet of Things*, vol. 11, p. 100227, 2020.

[27] N. T. Le and D. B. Hoang, "Security threat probability computation using Markov chain and common vulnerability scoring system," in *Proceedings of the 28th International Telecommunication Networks and Applications Conference (ITNAC)*, Sydney, Australia, November 2018.

[28] H. A. Kholidy, A. Erradi, S. Abdelwahed, and A. Azab, "A finite state hidden Markov model for predicting multistage attacks in cloud systems," in *Proceedings of the 2014 IEEE 12th International Conference on Dependable, Autonomic and Secure Computing*, pp. 14–19, Dalian, China, August 2014.

[29] H. Wimberly and L. M. Liebrock, "Using Fingerprint Authentication to Reduce System Security: An Empirical Study," in *Proceedings of the IEEE Symposium on Security and Privacy*, Berkeley, CA, USA, May 2011.

[30] V. A. Bharadi and G. M. DSilva: Online Signature Recognition Using Software as a Service (SaaS) Model on Public Cloud. 2015 International Conference on Computing Communication Control and Automation, (2015).

[31] D. Choi, S. Seo, Y. Oh, and Y. Kang, "Two-factor fuzzy commitment for unmanned IoT devices security," *IEEE Internet of Things Journal*, vol. 6, no. 1, pp. 335–348, 2019.

[32] A. F. Jabeen, "Development and implementation using Arduino and Raspberry Pi based Ignition control system," *Advances in Computational Sciences and Technology*, vol. 10, no. 7, pp. 1989–2004, 2017.

[33] M. Mehrnezhad, E. Toreini, S. F. Shahandashti, and F. Hao, "Stealing PINs via mobile sensors: actual risk versus user perception," *International Journal of Information Security*, vol. 17, no. 3, pp. 291–313, 2017.

[34] R. Vijaysanthi, N. Radha, M. J. Shree, and V. Sindhujaa, "Fingerprint authentication using raspberry Pi based on IoT," in *Proceedings of the 2017 International Conference on Algorithms, Methodology, Models and Applications in Emerging Technologies (ICAMMAET)*, India, Chennai, February 2017.

[35] M. Trik, S. Pour Mozaffari, and A. M. Bidgoli, "Providing an adaptive routing along with a hybrid selection strategy to increase efficiency in NoC-based neuromorphic systems," *Computational Intelligence and Neuroscience*, vol. 2021, Article ID 8338903, 8 pages, 2021.