Intelligent Automation & Soft Computing
DOI: 10.32604/iasc.2023.029397
Article

Cryptographic Algorithm for Enhancing Data Security in Wireless IoT Sensor Networks

A. Bhavani and V. Nithya*

Department of ECE, SRM Institute of Science and Technology, Kattankulathur, 603203, Chennai, Tamilnadu, India
*Corresponding Author: V. Nithya. Email: nithyav@srmist.edu.in
Received: 02 March 2022; Accepted: 06 April 2022

Abstract: Wireless IoT Sensor Network can handle audio, video, text, etc., through the interconnection of ubiquitous devices. The entertainment and application-centric network relies on its autonomous nodes for handling large streams of multimedia data. Security breaches and threats due to insider attacks reduce the data handling and distribution capacity of the nodes. For addressing the insider attacks problem, Session-Critical Distributed Authentication Method (SCDAM) is proposed. The proposed method relies on short-lived concealed authentication based on an improved elliptic curve cryptography (ECC) algorithm. In this authentication, the session time and the interrupts are accounted for, providing end-to-end authentication. The session keys are distributed before and after each interrupt from which the shared data is authenticated. This authentication process uses a linear hash process, ensuring non-repetition of keys in the consecutive sessions. This proposed authentication method is capable of providing improved sessions, less data distribution loss, and complexity.

Keywords: Insider attacks; elliptic curve cryptography; hash function; session authentication; IoT

1 Introduction

Nowadays, the Internet of Things (IoT) played a crucial role and going to change in this world [1]. Approximately, the usage of IoT devices will be reached around 22 billion by 2025. Due to the tremendous cost-saving reason, most industries utilize various IoT devices for their application purposes [2]. IoT devices are incorporated by several organizations and individuals with wireless sensors to create multiple smart applications. Each IoT device depends on wireless sensor technology, which causes supply chain management, smart cities, smart buildings, smart homes, and intelligent agriculture [3,4]. Along with this, the Y-O-Y growth and structure analysis of various industries, the wireless IoT sensor market has been reached globally in 2020–2026 [5]. IoT devices collect the data from local conditions or environments with wireless technology, and the gathered information is transmitted via the powerful platform or components. The IoT sensors are distributed in various geographic locations that are communicated via the gateways, central hubs, and servers. The main reason for incorporating the wireless sensor with IoT is that it consumes minimum maintenance and low power function [6,7]. Although the

IoT devices are distributed in various locations, it also collects enormous data volumes by making the proper interactions. The heterogenous environment-based data collection causes security-related issues.

The IoT devices are gathering sensitive information like healthcare details, bank and business transactions, etc. This information needs to be secured from unauthorized access [8]. Due to the heterogeneous device location, the communication path or information may be accessed by unauthorized users. Distribution denial of service (DDoS) attacks [9] is pervasive while sharing the data from one location to another [10]. The wireless IoT sensor networks are created with minimum security features that are more difficult to handle. Therefore, the security of wireless IoT sensor devices-based communication should be managed by applying the different security mechanisms [11,12]. The created system must be recognizing the unauthorized users, unauthorized activities, malicious attack detection, and prediction of DDoS and insider attacks [13,14]. Several supervised learning techniques are utilized to predict unwanted activities in the IoT based data sharing process [15]. These algorithms consume high overhead, high false positives, never considering the device service attributes, difficulty predicting the type of attacks [16] and low response levels [17].

The security algorithm should be crated for handling the wireless IoT sensor data security and node distribution by considering this problem definition. Hence this paper uses the Session-Critical Distributed Authentication Method (SCDAM) for addressing the insider attacker problem. The SCDAM algorithm authentication process is improved by applying the Elliptic Curve Cryptography (ECC) approach [18]. During the authentication process, session time and interrupts are utilized to establishing the end-to-end authentication process. The session keys are distributed before and after each interrupt from which the shared data is authenticated. This authentication process uses a linear hash process, ensuring non-repetition of keys in the consecutive sessions. The discussed SCDAM with the ECC algorithm establishes the security and addresses the insider attack with less data distribution loss, complexity, and improved sessions. This wireless IoT sensor device-based data handling process is implemented using the NS2 simulations. The entire paper is prepared as follows, Section 2 dealing with the different researcher opinions regarding wireless IoT sensor data handling. Section 3 analyses the working process of SCDAM with ECC based IoT data sharing and handling; excellence of the system is evaluated in Section 4. The end of the work is summarized in Section 5.

2 Related Works

Maram et al., 2019 applied SIMON block cipher lightweight cryptographic (SIMON-LC) algorithm for managing data security in IoT applications [19]. This paper uses SIMON cipher characteristics to enhancing the speed of the process. Integrating the advanced encryption standard algorithm with the SIMON block cipher algorithm maximizes data security with minimum encryption time, execution time, and memory consumption.

Zhang et al., 2019 managed the UNICODE data security and privacy in the Internet of things using intelligent security algorithm [20]. Here, substitution S-box is utilized to handling the various UNICODE data such as image, video, audio, and text. This process works in a dynamic and key-dependent manner that improves the overall data security in IoT applications. The effective utilization of substitution-based S-box enhances overall system performance.

Adhikari et al., 2017 developed the RFID authentication process in IoT using the Elliptic Curve Cryptographic approach (RFID-ECC) This work analyzed the various security weaknesses for improving the overall IoT data security [21]. A radio frequency identification scheme is developed by utilizing the Elliptic curve cryptography (ECC) approach by considering the security weakness. This process enhances the overall security requirements with minimum cost. Elhoseny et al., 2019 created the secure IoT communication framework in the content-centric network by applying the elliptic curve cryptography

[22]. The security was ensured by designing the certificateless public key infrastructure for resource-constrained IoT communication. The lightweight cryptosystem is incorporated with the elliptic curve cryptography to effectively manage data security and effectively eliminate the intermediate cryptographic attacks.

Wang et al., 2018 developed a secure IoT healthcare-based data transmission model by applying various cryptographic algorithms [23]. This process creates the hybrid encryption scheme by integrating the 1-D or 2-D discrete wavelet transform with Adleman, Shamir, Rivest, and the advanced encryption standard algorithm. The hybrid encryption algorithm was encrypting the transmitting IoT data, which includes both text and images. The combination of encryption algorithms is difficult to identify by the intermediate attackers. Then the introduced hybrid encryption scheme manages the patient confidentiality, capacity, and imperceptibility effectively.

Manikandan et al., 2018 introducing the one round cipher algorithm [ORCA] for managing the multimedia data security in IoT applications [24]. The algorithm generates the key dynamically, and the dynamic permutation table, round substitution table, and two pseudo-random metrics are utilized. These table pieces of information are being used to create the ciphertext used to maintain multimedia data security. The cipher scheme's effective utilization improves the overall IoT data security with maximum speed, flexibility, simplicity, and low error propagation.

Deebak et al., 2019 developed the random coefficient selection and mean modification approach for managing the security in the IoT framework [25]. This approach uses multiple discrete coefficients to analyze the data randomly to ensure data security. This process ensures high robustness and minimizes the region-related attacks successfully. The utilization of normalized cross-correlation relative values helps to eliminate the intermediate attacks with a 0.95 correlation value.

Sudhakaran et al., 2020 managed data security in IoT-related wireless sensor networks by applying the hybrid secure routing mechanism [26]. Flexible security is ensured using the two-fish symmetric key method in the global sensor networks. This process is achieved by authenticating the user based on the authentication and encryption model [27]. In addition to this, the eligibility weight function is applied to validate the sensor nodes. After that, Ad-hoc On-demand multipath distance vector and multipath optimized link-state routing protocol are utilized to transmitting the data via the authenticated node. This process manages security and multipath diversity.

2.1 Problem Definition

In the wireless IoT sensor networks, security, and data privacy is one of the significant challenges. The incorporation of sensor technologies in IoT devices can collect a huge volume of data that consists of text, audio, video, etc. This information is transmitted from the organized location to the processing place for ensuring a specific application. The data transmission should be authenticated before initiating the process because it eliminates intermediate attacks and access. According to the various researcher's opinions, several cryptographic and encryption techniques are utilized to authenticate the data before making the transaction.

Further, the secure key generation process is also defined for maintaining data security and privacy. Although the discussed methods fail to resolve the security breaches and threats due to the insider attacks, they reduce the nodes' data handling and distribution capacity. In this work, Session-Critical Distributed Authentication Method (SCDAM) with Elliptic Curve Cryptography (ECC) approach is applied to ensure the discussed problem definition for addressing the insider attacker problem.

2.2 Insider Attack Problem

The insider attack problem is nothing but the malicious attacks in the network by the authorized person. Compared with the external attacks, the insider attack has a specific advantage because the authorized person has a network architecture structure and policies. Most organizations plan to create security measurements for external attacks and fewer mechanisms for managing the internal attacks. Due to the fewer security precautions of internal attacks, sensitive data has been stealing by injecting the Trojan viruses. Then the insider attack hacks the system's full processing capacity, storage, and system overloading. According to the NOKIA report in 2019, almost 33% of IoT devices are infected. This information is gathering, according to the 150 million devices-based network traffic details.

Although the IoT devices are integrated with the wireless technology, it has weak security measures that cause to access the sensitive files. The unwanted threatening files are injected into IoT devices and creating damage to the process. Once the insider attack accesses the IoT devices, that will make a severe risk in healthcare and smart home applications. The insider attack blocks the user from accessing the information; it also affects the entire system, platform, and stealing the user's sensitive details.

The wireless sensor IoT devices collect the multimedia data; therefore, the IoT devices handle the massive volume of data with nodes' distribution capacity. Hence, the effective cryptographic technique called session-critical distributed authentication method with Elliptic curve cryptography approach is applied to handling the insider attack problem. Then the detailed working process of SCDAM with ECC algorithm is elaborated in the following section.

3 Session-Critical Distributed Authentication Method (SCDAM)

In this work, session-critical distributed authentication method (SCDAM) with elliptic curve cryptography (ECC) approach is applied to manage the data security in wireless sensor IoT devices. This method generates the key value for both sender and receiver according to the ECC method that addresses the user authentication. During the authentication process, session time and interrupts are accounted for via the end-to-end authentication process. Here, the one-time password-based authentication scheme is applied to provide data security to each session. This process manages the IoT data security for every session also eliminate the insider attack problem. The session key is engendered based on the time stamp. The previous session keys do not work on the current session; this causes the introduced method to robust against the insider and reply attacks. In addition to this, the ECC-based end-to-end authentication process and linear hash function establish further dictionary attacks in the wireless sensor IoT device.

3.1 One-time Password Scheme for Session Authentication

Wireless sensor IoT devices are used to collect the various information used to create a smart application. The gathered details are transmitted from one location to another; data security and privacy should be managed. The information is stored and sent in a distributed environment that requires the authentication process to ensure safety. Authentication is nothing but verifying user identities while accessing the IoT data, applications, and resources. The authentication process manages the trusty relationship and enables accountability. The wireless sensor IoT device information is transmitted by creating the one-time password scheme because it can only reduce the insider attack problem. The system generates a list of passwords that secretly communicated with the sender and receiver. The sender only selects the password from the list, which is saved in the server. The selection password is changed according to the user choice, which means the password is disclosed that causes the elimination of the insider attacks. The one-time authentication process has two steps: registration (the IoT device users register their details to the server and get the list of passwords for further transactions) and login & authentication (server authenticates the user to access the data).

3.2 Registration

The first step of the session-critical distributed authentication process is registration. Here, every wireless sensor IoT device users share their secrete key to the server. The secret key is denoted as SEED. For every timestamp T, the server generates the session ($\mathfrak{SK}$) by using random number $\mathfrak{D}$. Therefore, the session key is denoted as

$$\mathfrak{SK} = \mathfrak{D}||T \tag{1}$$

With the help of the session key and secrete key, the server computes the key value as $\mathfrak{K} = SEED \oplus \mathfrak{SK}$ that is sent to the user. The computed $\mathfrak{K}$ value is transmitted to the user, and then the user estimate the session key $\mathfrak{SK}$ value as,

$$\mathfrak{SK} = SEED \oplus \mathfrak{K} \tag{2}$$

Afterward, the user generates the initial key $\mathfrak{IK}$ value from the randomly generated secret key $\mathfrak{E}$ value. The $\mathfrak{IK}$ value is formed using Eq. (3).

$$\mathfrak{IK} = \mathfrak{E} \oplus SEED \tag{3}$$

After determining the secrete key $\mathfrak{E}$ and session key $\mathfrak{SK}$, the number of times N should be determined, and details are transmitted to the server. The transmission should be done by performing the

$\mathfrak{IK} \oplus \mathfrak{SK}$ and $N \oplus \mathfrak{SK}$.

The server was retrieving the N and $\mathfrak{IK}$ values from the user transmitted details such as $\mathfrak{IK} \oplus \mathfrak{SK}$ and $N \oplus \mathfrak{SK}$. Then the server computing the password by using the initial key $\mathfrak{IK}$ and linear hash function as follows,

$$P_0 = H^N(\mathfrak{IK}) \tag{4}$$

In Eq. (4), H is denoted as the linear hash function, which means the data's dynamic structure implements the hash table while generating passwords. The password is generated $P_0 = P_0 \oplus \mathfrak{SK}$. The generated password P_0 and N value is saved in the server database. The server saves the entire IoT device session details in their memory, giving each user a session I.D. to access the details. This process enables authentication while accessing the IoT details in the distributed environment. Along with P_0, P_1 and P_2 is computed using Eq. (5).

$$P_1 = H^{N-1}(\mathfrak{IK}); P_2 = H^{N-2}(\mathfrak{IK}) \tag{5}$$

The generated passwords P_0, P_1 and P_2 are XOR with the respective session key $\mathfrak{SK}$ and transmitted to the user for getting the password list. The XOR process is represented in Eq. (6)

$$\left.\begin{array}{l} P_0 \oplus \mathfrak{SK} \\ P_1 \oplus \mathfrak{SK} \\ P_2 \oplus \mathfrak{SK} \end{array}\right\} \tag{6}$$

The received values represented in the Eq. (6) are again XOR with the session key $\mathfrak{SK}$ to get the original password values P_0, P_1 and P_2. Here, the registration process itself enhances authentication by ensuring end-to-end authentication. For every key transmission enables the secrete while making the communication between the user and the server. This secrete communication process robust to the insider attack in the wireless sensor IoT device-based data transmission or communication.

Here, the client hashes the $\mathfrak{IK}$ values for N times, and the estimated value is compared with the password. If both values are equal, then the authentication ensures that IoT communication is terminated by considering the intruder. Once the wireless Sensor IoT device user registration is completed, it will be

ready to transfer the information from one location to another. The IoT device data has been accessed by login and authentication manner. The secure data access process is discussed as follows.

3.3 Login and Authentication

User authentication is the most critical step in validating user identity and providing access to the user. If the user logging to access the data t^{th} time, the server creates the new session key $\mathfrak{SK}$. The $\mathfrak{SK}$ generation is depending on the timestamp T and random number $\mathfrak{D}$. Here, the server estimates the password by using the hash function (H) and initial key $\mathfrak{IK}$ that is defined in Eq. (7)

$$P_{t-1} = H^{C+1}(\mathfrak{IK}); \tag{7}$$

Here, C is computed from N-t, H is hash function. By using the P_{t-1} value, server performs the XOR operation with the session key for authentication purpose such as $P_{t-1} \oplus \mathfrak{SK}$ and $\mathfrak{SK} \oplus SEED$. The computed values are sent to the user; by using these values, the user calculates the session key value according to Eq. (8)

$$\mathfrak{SK} = P_{t-1} \oplus (P_{t-1} \oplus \mathfrak{SK}) \tag{8}$$

The computed $\mathfrak{SK}$ value is checked with the user timestamp value. If the value is valid, then the user estimates the SEED value using Eq. (9)

$$SEED = \mathfrak{SK} \oplus (\mathfrak{K}) \tag{9}$$

In Eq. (9), $\mathfrak{K} = SEED \oplus \mathfrak{SK}$. The estimated SEED value is checked with the sever memory to verify the user identity. If the computed SEED value is matched with the database value, then the server's authenticity is verified effectively.

Once the user verifies the server identity, then the session key is XORed $(\mathfrak{SK} \oplus P_t)$ With a password that is sent to the server. The server computes the password from the session key $P_t = \mathfrak{SK} \oplus (\mathfrak{SK} \oplus P_t)$. From the estimated P_t value, P_{t-1} is computed by taking the hash value of P_t. If both P_t and P_{t-1} is matched, then the user is verified. Then the server updates the user information, N with C; here, C = N − t. The server's next password has been generated and transmitted to the user for accessing the next login and data access process. The following password is generated using Eq. (10).

$$P_{t+1} = \mathfrak{SK} \oplus (\mathfrak{SK} \oplus P_{t+1}). \tag{10}$$

The computed P_{t+1} value is stored in the database to make the next login and wireless sensor IoT data access secure. The session key distribution is maintained at every timestamp and eliminates the insider attack problem due to updating passwords in every access. In this work, the secrete key and session key played a vital role in enabling secure data access. After verifying the user details with the server database, the security is further enhanced by authorizing the user information using the Elliptic Curve Cryptography (ECC) approach.

3.4 Elliptic Curve Cryptography Based Authentication

It is one of the public-key cryptography approaches in which the encryption key is known to the public, and the decryption secretes key is kept private. The ECC approach provides security and data privacy while accessing the IoT data. The above discussed one-time critical session-based process ensures the user and server authenticity. During the user verification process, end-to-end authentication is performed to access the data from the third-party server.

The introduced method relies on short-lived concealed authentication based on an improved elliptic curve cryptography (ECC) algorithm. Here, the public and private keys are generated according to the

elliptic curve equation that reduces traditional prime number involvement. The elliptic curve based generated keys are robust and complex to guess by third parties. The algorithm consumes minimum computing power and resource usage but ensures a high level of data security. The elliptic curve equation $G(p)$ is formed according to Eq. (11).

$$Y^2 = X^3 + ax + b \tag{11}$$

In Eq. (11), Y^2 is denoted as an elliptic curve, a and b are the real numbers. With the help of these parameters, the public key and private key are generated. As discussed earlier, the user randomly chooses the secret key from [2, n − 2], and the public key is defined based on the elliptic curve. The ECC-based selected key values are transmitted between user and server for making the authentication purpose. These ECC-related key values enhance overall system security in the fastest manner. The registration, login, and authentication process are then performed to enhance wireless sensor IoT security. The detailed algorithm steps are illustrated in Table 1.

Table 1: Algorithm Steps for a session-critical distributed authentication method (SCDAM)

Key Generation
Step 1: Generate the public and private key value according to the elliptic curve $G(p)$
Registration
Step 2: The secrete key SEED shared to the server
Step 3: Generate the session key $\mathfrak{SK} = \mathfrak{D}\|\|T$ using random number and timestamp
Step 4: Transmit the session key to the user in the form of $\mathfrak{K} = SEED \oplus \mathfrak{SK}$, and the user gets the session key by performing the $\mathfrak{SK} = SEED \oplus \mathfrak{K}$
Step 5: Generate $\Im\mathfrak{K} = \mathfrak{E} \oplus SEED$ by user // initial key
Step 6: transmit the $\Im\mathfrak{K} \oplus \mathfrak{SK}$ and $N \oplus \mathfrak{SK}$ information to the server
Step 7: Server generate the password to the user for every session using $P_0 = H^N(\Im\mathfrak{K})$
Step 8: Then the next passwords $P_1 = H^{N-1}(\Im\mathfrak{K}); P_2 = H^{N-2}(\Im\mathfrak{K})$ are computed using the linear hash function. The choice of the password depends on the user.
Step 9: generated passwords P_0, P_1 and P_2 are XOR with the respective session key $\mathfrak{SK}$ and transmitted to the user for getting the password list.
Step 10: client hashes the I.K. values for N times, and the estimated value is compared with the password
Step 11: If the matches are found, the users are validated to access the IoT device information.
Login and Authentication
Step 12: Generate the session I.D. value according to the user logging activities.
Step 13: compute the user entered password details $P_{t-1} = H^{C+1}(\Im\mathfrak{K})$
Step 14: server validate the details and $\mathfrak{SK} = P_{t-1} \oplus (P_{t-1} \oplus \mathfrak{SK})$ information is transmitted to the user.
Step 15: If the value is valid, then the user estimates the SEED: $SEED = \mathfrak{SK} \oplus (\mathfrak{K})$
Step 16: The estimated SEED value is checked with the sever memory to verify the user identity.
Step 17: This process helps to improve the end-to-end authentication process.
Step 18: The server computes the password from the session key $P_t = \mathfrak{SK} \oplus (\mathfrak{SK} \oplus P_t)$.
Step 19: The estimated P_t value, P_{t-1} is computed as $P_{t+1} = \mathfrak{SK} \oplus (\mathfrak{SK} \oplus P_{t+1})$
Step 20: If both P_t and P_{t-1} is matched, then the user is verified.

The wireless sensor IoT device information is accessed by authenticating the user and server successfully based on the algorithm steps. Here, the initial key generation depends on the Elliptic Curve Cryptography (ECC) approach, which is more secure and difficult to guess by intermediator. The full

registration, login, and authentication depend on the secrete key and session key, which maintains the overall data security. In addition to this, the generated session key values with password values are varied, difficult to guess by the authenticated person for every session. The passwords are selected only by the user, which is various from every time session access. Therefore, the created system resolves the insider attack problem effectively.

4 Results and Analysis

This section evaluates the session-critical distributed authentication method (SCDAM) with elliptic curve cryptography (ECC) approach-based data security and privacy in wireless sensor IoT data transmission. This approach utilizes the session key for every transaction, and the key helps to authenticate the user and server while accessing the details. In this work, insider attack problems are considered because the IoT devices are weak to security metrics.

The SCDAM approach has distinct passwords P_0, $P_1 \ldots P_n$ during the registration phase. Among the passwords, the user only selects the respective password, which is accessed by the insider. In this work, the shared password information is also encrypted by applying the XOR operation with the session key. Therefore, the introduced SCDAM with the ECC method robustness to the insider attack. This discussed system is implemented using NS2 simulation, Network Simulator (Version 2), widely known as NS2, is simply an event-driven simulation tool that has proved useful in studying the dynamic nature of communication networks. Simulation of wired as well as wireless network functions and protocols (e.g., routing algorithms, TCP, UDP) can be done using NS2. In general, NS2 provides users with a way of specifying such network protocols and simulating their corresponding behaviours and the attack frequency has varied from 50, 75, 100, 125 and 150 KB/s. Here attack frequency is nothing but the amount of data spent/second towards launching the attacks.

Different wireless sensor IoT devices are utilized during this process because the multimedia data such as text, audio, and video-related information are used. These data are collected by applying different IoT devices such as motion sensors, environment sensors, sockets, cameras, and smartphones. These IoT devices are utilizing the wearable technologies that are being used in various smart applications. Therefore, security should be examined while making the data transmission process. Then the introduced system utilizes the effective security mechanism from starting of the registration to data access. Therefore, the system's excellence is validated with the percentage of affected packets while attacks on the received packet. The obtained results are compared with existing works such as SIMON block cipher lightweight cryptographic (SIMON-LC) [19], RFID with Elliptic Curve Cryptographic approach (RFID-ECC) [21], and one round cipher algorithm (ORCA) [24]. Then the respective resultant percentage of affected packets analysis is shown in Fig. 1.

Fig. 1 demonstrated that the percentage of affected packets value of session-critical distributed authentication method (SCDAM) with elliptic curve cryptography (ECC) approach that is compared with the SIMON block cipher lightweight cryptographic (SIMON-LC) [19], RFID with Elliptic Curve Cryptographic approach (RFID-ECC) [21], and one round cipher algorithm (ORCA) [24]. From the results, SCDAM has a 44.88% value on average, in case of the SIMON-LC increases from 64.57%, RFID-ECC having 58.83%, and ORCA having 52.25%. Among the methods, SCDAM with the ECC approach attains the minimum affected packet values that mean it has only 1.23% increases when the packets' size increases gradually. The effective utilization of the session key and user selection passwords reduces the impact of the insider attacker. In addition to this, the resilience of the introduced security scheme should be examined during the frequency of attacks are varied. The resilience factor determines how effectively the wireless sensor IoT device withstands while collecting the various data even though it

has different facing attacks. The system's efficiency is compared with the number of attack frequency with the node's resilience captured. Then the obtained result is shown in Fig. 2.

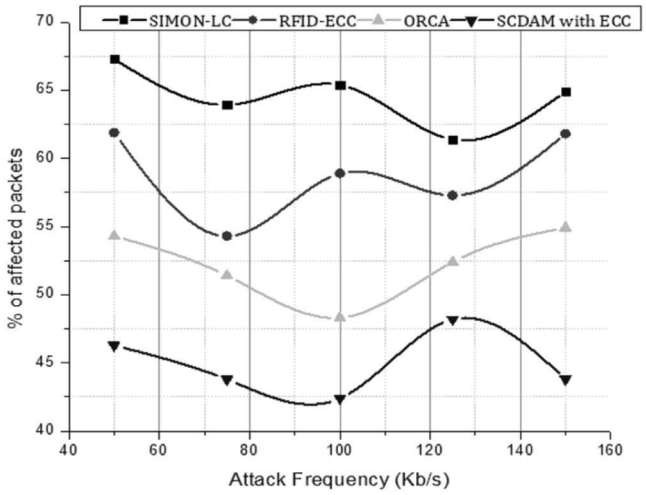

Figure 1: Attack frequency *vs*. percentage of affected packet

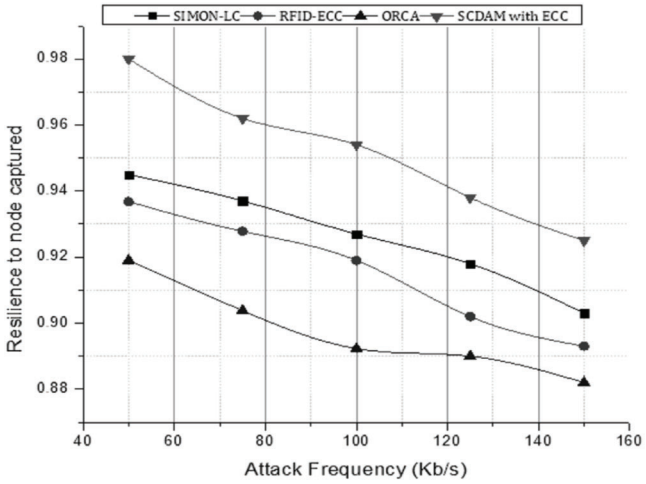

Figure 2: Attack frequency *vs*. resilience to node capture

Fig. 2 demonstrated that the resilience of node captured value of session-critical distributed authentication method (SCDAM) with elliptic curve cryptography (ECC) approach that is compared with the SIMON block cipher lightweight cryptographic (SIMON-LC) [19], RFID with Elliptic Curve Cryptographic approach (RFID-ECC) [21], and one round cipher algorithm (ORCA) [24]. From the results, SCDAM has a 44.88% value on average, in case of the SIMON-LC increases from 64.57%, RFID-ECC having 58.83%, and ORCA having 52.25%.

Among the methods, SCDAM with ECC approach decreases the values from 0.98 to 0.925, whereas SIMON-LC's resilience decreases from 0.94 to 0.90, RFID-ECC decreases from 0.93 to 0.89, and ORCA decreases from 0.91 to 0.88. Hence the SCDAM with ECC attains a 5.9% higher resilience than compared to other existing methods. The introduced method uses the $Y^2 = X^3 + ax + b$ elliptic curve to

generate the fundamental values that are difficult to guess by the intermediate user. In addition to the password, users are selected to create complexity when the insider tries to get the session and secret key.

Therefore, the introduced system able to withstand its data transfer performance when different numbers of attacks present. Although the system must receive the amount of data, even the IoT device is influenced by attacks. Therefore, the aggregated throughput is measured at the receiver end. Then the obtained throughput value is shown in Fig. 3.

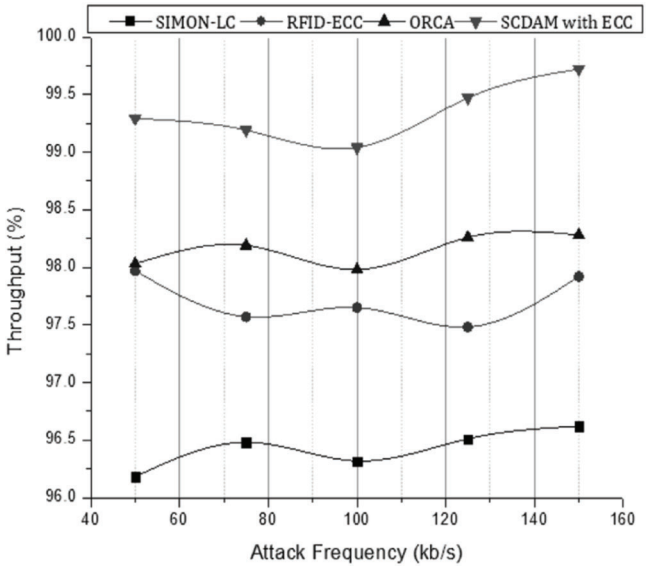

Figure 3: Attack frequency *vs*. throughput

In this process, the SCDAM with ECC algorithm uses the encryption process for every transmission performed during the registration, login, and authentication process. The transmission uses the session key that violates the insider attack also several attacks. The secure transaction process not only maintains data security also increases the throughput value. Then the Fig. 3 illustrated that the throughput value of session-critical distributed authentication method (SCDAM) with elliptic curve cryptography (ECC) approach that is compared with the SIMON block cipher lightweight cryptographic (SIMON-LC) [19], RFID with Elliptic Curve Cryptographic approach (RFID-ECC) [21], and one round cipher algorithm (ORCA) [24]. The obtained throughput is examined with different attack frequency. Compared to other methods, SCDAM with the ECC method has a higher throughput value of 11.24%.

Further, the average residual energy value of the wireless sensor IoT device should be examined. Even though the IoT devices are withstanding and can process the different attacks, it should have high residual energy. The energy of the IoT device does not lose during this authentication process. The efficiency of the residual energy of the different number of attack frequencies is computed, and the resultant value is demonstrated in Fig. 4.

Then the Fig. 4 illustrated that the residual energy value of session-critical distributed authentication method (SCDAM) with elliptic curve cryptography (ECC) approach that is compared with the SIMON block cipher lightweight cryptographic (SIMON-LC) [19], RFID with Elliptic Curve Cryptographic approach (RFID-ECC) [21], and one round cipher algorithm (ORCA) [24]. The SCDAM with the ECC method has a high residual energy value compared to other methods.

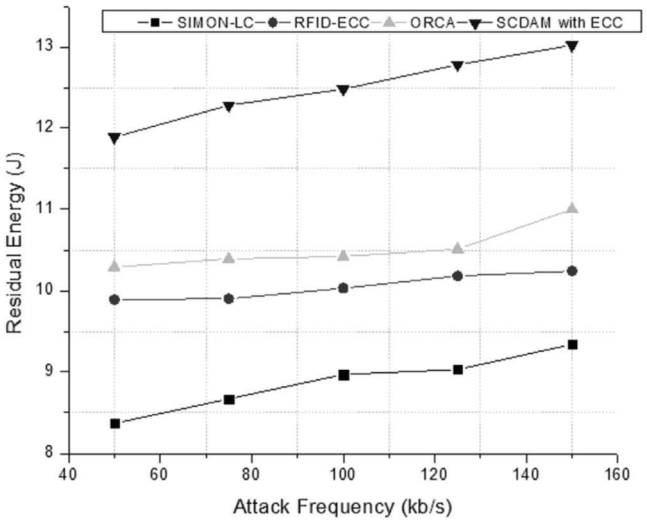

Figure 4: Attack frequency *vs*. residual energy

5 Conclusion

Thus the paper analyzing the session-critical distributed authentication method (SCDAM) with elliptic curve cryptography (ECC) approach based on data security in wireless sensor IoT device. Initially, the user keys such as public and private key values are generated according to the elliptic curve equation, which is more secure. The generated keys are then shared between the users and the server by registering, login, and authentication. For every session, the server and user utilize the secrete and session key to encrypt the user shared information. After authenticating the user and server, the password has been created by the server. The generated password is transmitted to the user in terms of the encrypted format. Among the passwords, the user selects the password and access the IoT details. During this process, the linear hash is utilized to generate the inside intruder's complicated password to guess. Thus the system manages the end-to-end authentication with minimum complexity and high throughput. In the future, optimized encryption techniques are utilized to improve data security in the IoT environment.

Funding Statement: The authors received no specific funding for this study.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] A. Alam and S. Tanweer, "Efficient and secure data transmission approach in cloud-manet-iot integrated framework," *Wireless Personal Communication*, vol. 132, pp. 1232–1251, 2020.

[2] D. Durand, G. Thomas, L. Visagie and M. Booysen, "Evaluation of next-generation low-power communication technology to replace gsm in iot-applications," *IET Communications*, vol. 13, no. 16, pp. 2533–2540, 2019.

[3] J. Liaoliang, T. Li, X. Li and M. Atiquzzaman, "Anonymous communication via anonymous identity-based encryption and its application in iot," *Wireless Communications and Mobile Computing*, vol. 121, pp. 568–581, 2018.

[4] S. Mukherjee, K. Sankar and M. Biswas, "Networking for IoT and applications using existing communication technology," *Egyptian Informatics Journal*, vol. 19, no. 2, pp. 107–127, 2018.

[5] A. Adnan, G. Kousiouris, P. Haris and S. Juan, "Real-time probabilistic data fusion for large-scale iot applications," *IEEE Access*, vol. 6, pp. 10015–10027, 2018.

[6] L. Richard, P. Joseph and S. Sumanth, "Wearable iot data stream traceability in a distributed health information system," *Pervasive and Mobile Computing*, vol. 40, pp. 692–707, 2017.

[7] S. Peerasak, N. Nuttapun and N. Nitigan, "Smart farm monitoring via the blynk iot platform: Case study: Humidity monitoring and data recording," in *16th Int. Conf. on ICT and Knowledge Engineering (ICT&KE)*, Singapore, vol. 1, pp. 1–6, 2018.

[8] G. Dimitris, I. Kounelis, R. Neisse and I. Naifovino, "Security and privacy issues for an iot based smart home," in *40th Int. Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*, India, pp. 1292–1297, 2017.

[9] S. Sam, M. Mikail, S. Rathore and H. Jong, "Distributed denial of service attacks and its defenses in IoT: A survey," *The Journal of Supercomputing*, vol. 1, pp. 1–44, 2019.

[10] L. Dongxing, W. Peng, D. Wenping and F. Gai, "A blockchain-based authentication and security mechanism for iot," in *27th Int. Conf. on Computer Communication and Networks (ICCCN)*, Canada, pp. 1–6, 2018.

[11] W. Haiping, S. Changxia, L. Yanling, Q. Hongbo, S. Lei *et al.,* "IoT information sharing security mechanism based on blockchain technology," *Future Generation Computer Systems*, vol. 101, pp. 1028–1040, 2018.

[12] A. Afsheen, R. Latif, H. Abbas and F. Aslamkhan, "Malicious insiders attack in iot based multi-cloud e-healthcare environment: A systematic literature review," *Multimedia Tools and Applications*, vol. 77, no. 17, pp. 21947–21965, 2017.

[13] F. Syed, N. Naeem, B. Zubair, C. Valliand, A. Ibrahim *et al.,* "Modelling and evaluation of malicious attacks against the iot mqtt protocol," in *IEEE Int. Conf. on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, China, pp. 748–755, 2017.

[14] X. Liu, F. Liang, M. Zuchao and R. Weizhi, "Detection of multiple-mix-attack malicious nodes using perceptron-based trust in iot networks," *Future Generation Computer Systems*, vol. 101, pp. 865–879, 2019.

[15] A. Muna, L. Hawawreh, M. Nourmoustafa and E. Elenasitnikova, "Identification of malicious activities in industrial internet of things based on deep learning models," *Journal of Information Security and Applications*, vol. 41, pp. 1–11, 2018.

[16] F. Faezeh, M. Sayadhaghighi, A. Jolfaei and M. Alazab, "Artificial intelligence for detection, estimation and compensation of malicious attacks in nonlinear cyber-physical systems and industrial iot," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 4, pp. 2716–2725, 2020.

[17] S. Manikandan and M. Chinnadurai, "Effective energy adaptive and consumption in wireless sensor network using distributed source coding and sampling techniques," *Wireless Personal Communication*, vol. 118, pp. 1393–1404, 2021.

[18] N. Alassaf, A. Gutub and S. Parah, "Enhancing speed of SIMON: A light-weight-cryptographic algorithm for iot applications," *Multimedia Tools Applications*, vol. 78, pp. 32633–32657, 2019.

[19] B. Maram, J. Gnanasekar and G. Manogaran, "Intelligent security algorithm for unicode data privacy and security in iot," in *Int. Conf. on Intelligent Systems*, China, vol. 13, pp. 3–15, 2019.

[20] X. Zhang, X. Sun, W. Sun, T. Xu and P. Wang, "Deformation expression of soft tissue based on bp neural network," *Intelligent Automation & Soft Computing*, vol. 32, no. 2, pp. 1041–1053, 2022.

[21] S. Adhikari and S. Ray, "A lightweight and secure iot communication framework in content-centric network using elliptic curve cryptography," in *Recent Trends in Communication, Computing, and Electronics. Lecture Notes in Electrical Engineering*, Singapore, vol. 524, pp. 524–545, 2019.

[22] M. Elhoseny, G. Ramírezgonzalez, O. Abuelnasr, S. Shawkat, N. Arunkumar *et al.,* "Secure medical data transmission model for iot-based healthcare systems," *IEEE Access*, vol. 6, pp. 20596–20608, 2018.

[23] M. Wang, Z. Zhou and C. Ding, "Blockchain-based decentralized reputation management system for internet of everything in 6g-enabled cybertwin architecture," *Journal of New Media*, vol. 3, no. 4, pp. 137–150, 2021.

[24] S. Manikandan and M. Chinnadurai, "Virtualized load balancer for hybrid cloud using genetic algorithm," *Intelligent Automation & Soft Computing*, vol. 32, no. 3, pp. 1459–1466, 2022.

[25] F. Deebak, L. Bakkiam, R. David and M. Faditurjman, "A hybrid secure routing and monitoring mechanism in iot-based wireless sensor networks," *Ad Hoc Networks*, vol. 97, pp. 2021–2032, 2019.

[26] S. Sudhakaran, P. Pradeep, M. Malathy and A. Chidambaranathan, "Authorisation, attack detection and avoidance framework for iot devices," *IET Networks*, vol. 9, no. 5, pp. 209–214, 2015.

[27] P. Sudhakaran, "Energy efficient distributed lightweight authentication and encryption technique for iot security," *International Journal of Communication Systems*, vol. 5, no. 3, pp. 256–276, 2020.