Received: December 5, 2022. Revised: December 29, 2022.

INASS

International Journal of
Intelligent Engineering & Systems

http://www.inass.org/

Lightweight Authentication Enhancement Using Arnold Chaotic Map and Markov-Chain for Internet of Things Applications

Waleed Kareem. Ahmed[1]* **Rana Saad Mohammed[2]**

[1,2] *Computer Science Department, Mustansiriya University, Education College, Baghdad, Iraq*
* Corresponding author's Email: waleed.kareem.ahmed.b@uomustansiriyah.edu.iq

Abstract: The Internet of Things (IoT) was a new concept that connected various physical things to the internet. The IoT is fast expanding and will soon significantly impact everyday life. Although the increasing number of connected IoT devices is simplifying life, they risk our data. Radiofrequency identification (RFID) assists in the automated identification of connected IoT devices. Furthermore, the primary challenges for RFID tag-connected technology are privacy and security. With the improving safety of solutions RFID for many apps, RFID necessitates a centralized database widening. Blockchain techniques are speedily establishing themselves together as a new distributed and decentralized replacement. And it provides enhanced transparency, data security, immutability, dependability, and lower maintenance costs. Because of its inherent benefits, RFID is projected to play a significant part in enabling identifying technology on the IoT. However, due to its association with sensor technology, it has the potential to be applied in a wide range of industries. Security, however, is one of the more complex components of creating an RFID system. RFID Security focuses around authentication and privacy concerns. From the previous works, we found that the computing cost and uptime are higher. To solve these problems, we offer improving lightweight authentication using Arnold Chaotic map and Markov chain for IoT applications. The proposed method uses random algorithms (Markova chain, Arnold map chaotic, and ECC), which add high security. We also used blockchain technology to transfer keys through a non-security channel. Based on parameters such as (communication cost, throughput rate, storage requirements, transmission delay, and computational cost) the results of the proposed RFID protocol were compared with several RFID-based security solutions. As a result, the proposed lightweight scheme is more efficient and secure than existing RFID systems in terms of performance, according to simulation results, and is fully compatible with actual applications.

Keywords: Arnold chaotic map, Markov chain, ECC, Authentication, Blockchain technique.

1. Introduction

The IoT links "everything to the Internet," as the name indicates [1]. Therefore, the IoT does influence lives every day. The internet of things (IoT) is a cutting-edge wireless technology model that connects various physical devices to the internet, allowing data to be collected and distributed without human interaction. In addition, to identifying these linked devices, identification approaches like RFID, QR codes, and other sensor technology can be utilized [5, 6]. IoT applications include industrial control, intelligent supply chains, intelligent retail, intelligent buildings, intelligent grids, intelligent cities, medical information networks, and telehealth [7, 8]. It is assumed that the communication between the different IoT components is insecure. Therefore, one of the most difficult challenges for IoT technology is providing secure network communication between IoT components. Because IoT security methods may have vulnerabilities, it is vulnerable to a range of known attacks. Consequently, a secure authenticating method based on lightweight cryptographic algorithms is necessary [1, 2].

RFID is the most sophisticated approach for automatic identification utilizing RF (radio waves). The RFID technology may also be used to track or identify many products simultaneously [9, 10]. For example, identifying friend or Foe (IFF) technology

was first applied to airplanes during World War II. Due to its ability to scan hundreds of tags at once and the lack of a sight line needed for reading RFID tags, the RFID system has also supplanted the barcode system. RFID is currently being used in large-scale automated identifying applications such as monitoring and tracking, medical hospital environment, automatic payment, supplier management, access control, the IoV (internet of vehicles), and VCC (vehicle cloud computing) [3]. The three main elements are readers RFID, interrogators, tagging RFID, and the RFID system's backend server or host computers [1, 4].

Safety for RFID-based automotive systems is crucial because it concerns human lives, and everything has benefits and risks. Cryptography evolved from the necessity for data security. Cryptography is a means of preventing unauthorized access to data by converting it to a new format. There are two encryption algorithms: asymmetric key encrypting and symmetric key encryption. To encrypt and decode messages using asymmetric cryptographic encryption, 20 distinct public and private keys, are required. In contrast, symmetric encryption methods use the same cryptographic key to encrypt and decrypt ciphertext and plaintext [5, 6].

Most IoT solutions today have a central server-client architecture, allowing users to communicate with cloud servers online [3]. Additionally, efficient systems are vulnerable to malicious data manipulation by unreliable individuals, which could result in the flow of altered and made-up data [4]. On the other hand, cloud apps that store, transmit, and analyze IoT data are subject to network attacks such as bogus data manipulation, injection, and single-node failure [7]. To summarize, privacy and security were the most pressing concerns concerning IoT development. [6] discusses how blockchain-based decentralized structures might aid in the solution of the IoT application security dilemma. Blockchain technology is advantageous in centralized businesses for overcoming challenges such as low reliability, high costs, low security, and lousy efficiency [8].

The concept underlying IoT and its various manifestations is the omnipresence of items in which they can interact and connect to generate multiple services. The most recent IoT breakthroughs have contributed to the construction of smart cities. Consequently, only verified and certified equipment should have a connection to an IoT for it to function correctly. Otherwise, it is exposed to a wide range of security concerns, such as data manipulation, theft, and identity theft [9]. Traditional security approaches cannot secure data security on the IoT due to the enormous demand for computing.

Nevertheless, because IoT equipment is low-powered and has limited processing capabilities, its architecture differs fundamentally from the internet. As a consequence, existing cryptographic safety techniques are limited in their employ. Directly increasing computing requirements for IoV is not scalable nor practicable. The state-of-the-art approaches presented by several researchers (briefly mentioned throughout the literature review phase) were not suited for real-time implementation due to the high computing cost. Furthermore, the methods are unsuccessful for devices that use a small amount of energy [10, 11]. This paper tries to solve this problem by making the RFID protocol use lightweight cryptographic functions. These functions are Arnold chaotic map, Markov chain, and Elliptic-curve (ECC) for data verification to authenticate and secure the connection, as well as SHA256 to ensure the integrity of information. We also used the concept of blockchain based on SHA256 to create a dependable and secure storage solution.

Here is a summary of our research contribution:
1. Random algorithms were used (Arnold chaotic map, markov chain, ECC) in the server and the tag, which added more complexity, and for this our method is safe.
2. We provide a superior methodology compared with previous works.
3. Because all security requirements have been met, the suggested protocol may achieve robust security.
4. The validated equations have also been modified. Performance criteria, such as connection cost, computational cost, throughput rate, transmission delays, and storage needs, are superior to those of existing protocols.

The content of this article has the following structure. Section 2 is the technology of Blockchain; section 3 gives Blockchain features; section 4 is the related works; section 5 is the suggested method; section 6 provides Discussion and results; last section 7 is the conclusion.

2. The technology of blockchain

The IoT extends internet access beyond computers and humans to cover most of our daily objects. The IoT allows us to connect billions of devices simultaneously, improving data interchange and our lives. Although the benefits of the IoT appear boundless, there are significant impediments to adoption in the real world because of its centralized server/client paradigm. For example, many IoT devices on the network may generate scalability and security issues. Under the server/client topology, all

devices should be connected and authorized through the server, providing a single failure point. Therefore, moving the IoT system in a decentralized direction might be desirable. Blockchain is a well-known decentralization technique. Blockchain is a powerful method that can solve various IoT issues, including security, by decentralizing computation and administration processes [11].

There are numerous meanings of blockchain. According to [7, 12], the blockchain is "a distributed database for the record, over any transactions or public ledger, or connections undertaken and exchanged amongst participating parties." A minority of a system's participants confirm each transaction on the public ledger. After the information has been entered, it cannot be erased. The blockchain records every transaction that ever occurred [13].

As a result, BC (blockchain) technologies have emerged as a viable alternative for addressing IoT and intelligent home safety and privacy issues. By pooling assets from all operating nodes, the lack of centralized management of BC promotes usability and reliability, eliminating the problem of a single failure point. Additionally, many IoT applications require the inherent anonymity of BC, especially in Smart Homes where user identities should be kept secret. The BC technique also makes it possible to create a secure network with many diverse devices spread out among shady parties, which is essential for IoT systems [14].

3. The related works

Debiao He and B. Kumar suggested a reliable authentication method that ensures user anonymity in Markov chain-based WSNs. The Markov chain was a random process that may be applied to a system where the next event only depends on the system's present state while still following a chain of connected occurrences. During user authentication, the base station verifies that the user was permitted to obtain the data from the sensor node via an unsecured connection. The security assessment demonstrated that the suggested system was secure from numerous attacks, including forgeries, parallel session threats, user impersonation, etc. [15].

Yi-Pin Liao and C.-M. Hsiao suggested a secure RFID authenticating solution based on ECC linked to an ID-verifier transmission protocol. In contrast hand, security continued to be one of the more challenging aspects of creating the RFID system. RFID security was centered on authentication and privacy concerns. A security evaluation based on an efficient and persuasive formal methodology was used to establish that the chosen solution met the criteria. They also used evolution to assess efficiency based on communication costs, storage needs, and processing expenses. They also anticipated that the study's findings would apply to other authentication technologies comparable to RFID systems instead of simply RFID [16].

Umair Khalid and M. Asim presented an adaptable decentralized authentication and access control method for a lightweight IoT network. These IoT devices generate massive amounts of personal and sensitive data. As a consequence, assuring the system's safety and performance necessitates the use of safety gadgets. The proposed method, based on blockchain technology, maximizes distributed nature and cryptographic capabilities while reducing latency. The proposed method might be employed in a variety of IoT apps. Furthermore, secreted criteria and an assault model are being established to assess and evaluate the approach's capacity to meet these needs. To avoid the massive energy usage of PoW when verifying each block [17].

Muhammad Tahir and M. Sardaraz studied to describe a new probability-based technique for authenticating and authorizing Blockchain-enabled IoT devices. In healthcare data, security and security, as well as other regulatory responsibilities, were all critical issues. Extensive simulations using the AVISPA and Cooja simulators were used to study and assess the suggested model. Compared to current frameworks, tests show that the proposed framework enables improved access control and mutual authentication, decreasing connection and compute costs [18].

Prema K. V and Vidya Rao proposed employing two pairs of dynamic ECC to achieve signature and encrypting operations. Because they were connected to the internet, these low-resource devices were exposed to various security and privacy issues. The technique was assessed using the Raspberry Pi 3 devices in the client-server scenario. Experiments were used to establish the time essential for the hashing method, key creation, signature validation, signature generation, decryption, and encryption. Compared to cBLAKE2b, the proposed DECLADE required 13.76 percentage points, 2.57 percentage points, 18.36 percentage points, 6.12 percentage points, 9.91 percentage points, and 6.08 percentage points less time than mBLAKE2b with LWDSA. In addition, it did both theoretical and real-time safety assessments of man-in-the-middle, replay, and denial-of-service attacks [19].

Aida Akbarzadeh and M. Bayat proposed a lightweight authenticating system based on Chebyshev chaos maps. They employed a hierarchical architecture in the suggested approach to

provide varying access limits for distinct components. The IoT network's devices had processing and storage limitations. After that, they offered a formal analysis based on BAN logic to demonstrate the safety of their approach. They also compared the performance and privacy of their suggested technique to those of current solutions. Compared to alternative methods, the results demonstrated the suggested scheme's efficacy and safety [20].

Tran Khanh Dang and Chau D. M. Pham suggested utilizing ECC with a reciprocity privacy-preserving authentication method to improve resource effectiveness and privacy for participating devices. Existing authentication mechanisms were challenging to deploy owing to IoT device resource limits. However, the accuracy of the suggested authenticating approaches is established through formal analysis using BAN-logic, which indicated that session key agreement and mutual authentication between participants can be done securely. The novel protocol is secure and appropriate for low-power computers [21].

Leki Chom Thungon and N. Ahmed proposed a quick key exchange and authentication method for 6LoWPAN to authenticate resource-constrained sensing equipment quickly. Three-factor authentication was used in conventional wireless sensor networks. These issues cause a significant problem for the IoT due to resource-constrained devices' limited processor and memory capacity. However, the findings of automated verification of internet safety schemes and applications. The ProVerif tools verify the suggested method's safety claim against threats, including replaying and man-in-the-middle assaults—those who examine the logical correctness of the proposed authentication technique using Burrows-Abadi-Needham Arithmetic [22].

4. The suggested method

We develop a new IoT approach for RFID systems to enhance lightweight authentication. Addressing all security issues with current RFID-based devices while outperforming blockchain- and ECC-based alternatives in terms of storage, communication, computation costs, throughput, and transmission delays.

Our proposed approach uses random (ECC, Arnold chaotic, Markov chain) algorithms that add more randomness. However, these algorithms are hard to hack with high security. Therefore, we use random algorithms (ECC, Arnold chaotic, Markov chain) to generate more secure keys. There are two variables (X, Y) for the server and the tag generated from random algorithms (Arnold chaotic, Markov chain). We also used Blockchain technology that transfers data or keys between the server and the tag through an insecure channel. Blockchain technologies are rapidly establishing themselves as a new distributed and decentralized alternative. It provides enhanced data protection, reliability, immutability, translucence, and lower costs for maintenance. However, data transferred among servers and the tagging is also not protected, the same as in previous systems.

By validating the legality and legitimacy of the transactions and striving to preserve the information you want to protect, blockchain technology raises the bar for safety in technological activities that take place online. Although traditional operations run by banks and governments have better security and protection, the Blockchain system distinguishes itself from standard encryption approaches that entirely conceal data by allowing access to the data it contains at any time and from any location.

However, these are vulnerable devices that may be attacked in some manner. The decentralization system of blockchain technology is available to incorporate a framework for translucence. For these interested in it, the technique is built on the use of encryption to preserve data, eliminate approaches of manipulation or forgery, and is not limit arrival to it. So, assaulting the system is practically impossible; to assault the blockchain technique network, you'd require to modify the data of thousands of computers dispersed around the globe.

The three elements of the proposed solution are readings, tagging, and backup servers, with the reader functioning as an intermediary in the information flow between tagging and server. As a result, the recommended strategy only considers tagging and server connections. It is assumed that the connection between the reader and the server is secure. On the other hand, it is assumed that the connection between the reader and the tags is insecure.

There are two parts to the recommended authenticator: (1) setup and (2) authorization—the degree of authentication, the notations, and the variables used in the setting up of our suggested method.

The following parameters were used in the suggested protocols:

- n and q were numbers prime.
- F(q): A finite field of rank q and size n existed.
- EC: Elliptic Curve defined by $Y^2 = X^3 + aX + b$ from domain finite f(q), where (a) and (b) are constants.

Table 1. The suggested protocol's authentication stage

Server (X_{se}, P_{se}, X_{ta}, I_{ta}, Aa , Ab ,An, MC)	**Tag (X_{ta}, I_{ta}, Aa ,Ab ,An, MC)**
Generate h_2= AC ⊕ MC $H_2 = h_2 P_E$	
Blockchain $\{H_2\}$ →	
	Generate $h_1 = AC \oplus MC$ $H_1 = h_1 P_E$ X= AC Y= MC $TK_{ta1} = (X\ h_1\ R_2)$ $TK_{ta2} = (P_{se}\ h_2\ Y)$ $Auth_{ta}= TK_{ta2}+H(H_2 \oplus TK_{ta1})+ I_{ta}$
← Blockchain $\{H_1, Auth_{ta}\}$	
X= AC Y= MC $TK_{se1}= H((h_2\ X\ H_1) \oplus H_2)$ $TK_{se2}= (X_{se}\ H_2\ Y)$ $I_{ta} = (Auth_{ta} – TK_{se1}– TK_{se2})$ Search X_{ta} $Auth_{se}= H(H_1 \oplus TK_{se2}) + h_2\ I_{ta}$	
Blockchain $\{ Auth_{se}\}$ →	
	Check $Auth_{ta} = H(H_1 \oplus TK_{se2}) + X_{ta}\ H_2$

- P_E: The E (Elliptic curve) generating point from order n.
- X_{se}: The server's secret key.
- P_{se}: the public key of a server, where ($P_{se} = X_{se}\ P_E$).
- X_{ta}: This is the private key for the tag.
- I_{ta} is a tag's public key and is used whenever ($I_{ta} = X_{ta}\ P_E$).
- AC: this is the Arnold chaotic map.
- MC: this is the Markov chain.

4.1 Setup phase

The server conducts the following actions during the setup phase:

- First, the elliptic curve domain variables [q; P_E; a; n; b] are given.
- [Ab; An; Aa] are chaotic map domain variables.
- Finally, the Markov chain domain parameters, or [MC], are defined.
- A parameter X_{se} = AC is randomly selected from the Arnold chaotic mapping (AC) for the server's private key, and $P_{se} = X_{se}P_E$ was derived as the server's public key.
- A random parameter X_{ta} =AC is selected from the Arnold chaotic mapping (AC) for the tag's private key, and $I_{ta} = X_{ta}P_E$ was derived as the tag's public key.
- The server saves the perimeters of elliptic curves [Ab; An; Aa]; [q; P_E; a; n; b]; [MC]; [X_{ta}; I_{ta}]; and [X_{se}; P_{se}].
- Tag saves the variables of the elliptic curve [Ab; An; Aa]; [q; P_E; a; n; b]; [MC] and [X_{ta}; I_{ta}].

4.2 Authentication stage

Mutual authentication occurs between tagging and server throughout this level of authentication, and the procedures are described below. Table 1 depicts the authenticating step of the preferred technique.

A. Server to Tagged: blockchain $\{H_2\}$. A server generates a random number $h_2 = MC \oplus AC$, then computes $H_2 = h_2\ P_E$ and transmits blockchain $\{H_2\}$ into the tag.
B. Tagged to server: blockchain $\{H_1\}$, $\{Auth_{ta}\}$. Tag chooses a number at random $h_1 = MC \oplus AC$, then it calculates $H_1 = h_1\ P_E$ =, where Y and X are from MC and AC values, respectively. It also calculates $TK_{ta2} = (P_{se}\ h_2\ Y)$, $Auth_{ta}= TK_{ta2}+H(H_2 \oplus TK_{ta1})+ I_{ta}$ and $TK_{ta1} = (X\ h_1\ R_2)$, where TK_{ta2} and TK_{ta1} were the key temporary, H was hashing value, $Auth_{ta}$ is the authenticate for tags, and then it transmits blockchain$\{H_1\}$, $\{ Auth_{ta} \}$ to the side server.
C. Server to Tagged: blockchain $\{ Auth_{se} \}$. The server again computes new variable $I_{ta} = (Auth_{ta} – TK_{se1}– TK_{se2})$, $TK_{se2}= (X_{se}\ H_2 Y)$, and $TK_{se1}= H(h_2 X H_1) \oplus H_2)$. where Y and X are from MC and AC values, respectively. The server validation of the database of X_{ta}. If the matched value is unavailable, the server will interrupt the communication until the tag has been allowed and the server has calculated the result.
   $Auth_{se}$ is the server's authorizer and transmits the blockchain's result $\{Auth_{se}\}$ into a tag. Its formula is $Auth_{se} = (H\ (H_1 \oplus TK_{se2}) + h_2\ I_{ta})$.
D. $Auth_{ta} = H(H_1 \oplus TK_{se2}) + X_{ta}\ H_2$ and determine if the result is $Auth_{se}$ or not. The communication is cancelled if the tag cannot locate a similar outcome, but the server is still permitted.

5. Discussion and results

In this section, several current multiple authentication systems, including those developed by Liao and Hsiao [16], He [23], S. Kumar [5], Wei G and Qin Y [24] and Lee and Chien [25], were compared to the proposed scheme in terms of communication costs,

computation costs, and storage costs. Also compared by throughput rate and transmission delays. Below are the detailed comparison data and analysis.

5.1 Computational cost

The server and tagging approaches are used to calculate the computing cost. The server and tag runtime times are both 0.00002949s and 0.0006569s. Table 2 shows the median GF(2m) runtime in micro secs as measured by LiDIA [6].

Table 2. shows the runtime of an average GF(2m) in microseconds using LiDIA

Extension "m"	Squaring	Adding	Inversion	Multiplied
163	2.3	0.6	96.2	10.5

Table 3. Computational cost entity

Entity	Tag	Server
He [23]	Two adds, & five elliptic vectors Multiplications, Two inversions, runtime of total = 2 (T/20) + 5T + T2 * 9 = T (23.1) = 0.064 (23.1) = 1.4784 sec.	One subtract, Seven elliptic vectors multiply, , four inversions & three adds runtime of total = 1(T′/20) +7T′ + 4(9T′) + 3(T′/20) =(43.2) T′ = 43.2 * 0.001124 = 0.0485568 sec.
Liao and Hsiao [16]	Three adding and five multiply of elliptical vectors runtime of total =3 (T/20) +5 (T) =T (5.15) = 0.064 * (5.15) = 0.3296 sec.	Two subtract, five multiply Of elliptic vector, & one adds runtime of total = 2 (T′/20) +5(T′) + 1(T′/20) = (5.15) T′ = (5.15) *(0.001124)= 0.0057886 sec.
S. Kumar [5]	Two-hashing, seven vector multiplications, & five adds runtime of total = 2H +7 (T) + 5 (T/20) = (7.25) T = 0.064 (7.25) = 0.464 sec.	Two hashing, three adds , seven multiplied of elliptic vector , & two subtract runtime of total = 2 H + (3T′/20) + 7 (T′) + 2 (T′/20) = (7.25) T′ = (0.001124) * (7.25) = 0.008149 sec.
Lee and chien [25]	Four inversions, seven vectors multiplications, Six adds, & two hashing. runtime of total = 4 (9T) +7 (T) + 6 (T/20) + 2 (H) = 36 (T) + 7 (T) + 3T/10 + 2 (H) = T (43.3) = (0.064) 43.3 = 2.7712 sec.	Two hashing, one subtract, Seven multiply of elliptic Vectors, Five adds, & Four inversions runtime of total = 2 (H)+ (T′/20) + 7 (T′) + 5 (T′/20)+ 4 (9T′) = 2 (H) + 7 (T′) + (6T′/20) + 36 (T′) = T′ (43.3) = 0.001124 * 43.3 = 0.0486692 sec.
Wei G and Qin Y [24]	4SM +1TA	4SM +1TA
Suggested method	three adds, six vector multiplications, & two hashing runtime of total = 6 (T) + 2 (H) + 3 (T/20) = T (6.001) = (6.001) * (0.0006569) = 0.003942 sec	two hashing six multiply of vector, &one adds, two subtract runtime of total = 2 (H) + 6 (T) + (T′/20) + 2 (T′/20) = T′ (6.001) = (6.001) * (0.00002949) = 0.0001769 Sec.

If "T" denotes the computed multiplication for the runtime using tags, therefore "T/5," shown in Table 3, represents a predicted running time for squares operations, i.e., 10.5 and 2.3, which is about multiplying by one-fifth. Thus, T/20 stands for the estimated runtime at subtracting, T/20 for the predicted runtime at adding, and 9T for the anticipated runtime at inversion. Assume that T' denotes the computed multiplication for the runtime using servers. Therefore "T'/5," indicates a predicted running time for squares operations. Thus, T'/20 stands for the estimated runtime at subtracting, T'/20 for the expected runtime at adding, and 9T' for the anticipated runtime at inversion. Considering that some basic operations (e.g., XOR) take very little time and can be ignored.

Furthermore, build on the notations above according to [5]. The computation cost of our suggested protocol is similar to the costs of four present schemes, as displayed in Table 2. The data indicate that the suggested strategy is superior to others.

5.2 Analysis of communication costs

In the proposed approach, we reduce the size of the message from 640 to 306 bits. However, we use

the Blockchain technique in the process, which comprises the new hash, the data, and the prior hashing. Since this method was developed to use encryption to safeguard the data, prevent forging or tampering, and prevent gaining access to it. Attacking the system is virtually impossible. This result in a lengthy message, but blockchain technology has several benefits, including high security, stability, unbreakability, and decentralization. To attack the blockchain technique network, you need to alter the data of thousands of machines scattered worldwide.

As a result, the additional connection costs are always recovered when weighed against the enhanced safety of the blockchain authentication process. The server transmitted blockchain $\{H_2\}$ message and also blockchain $Auth_{se}= (H (H_1 \oplus TK_{se2}) + h_2 I_{ta})$ message. Because of this, the total cost of the connection to the server is (562 + 1792) bits, or 2354 bits. The messages sent by the tagging were blockchains $\{H_1\}$ and $Auth_{ta}= TK_{ta2}+H(H_2 TK_{ta1})+ I_{ta}$. The various communications expenses for the tags (306) + (1536) = 1842 bits due to the suggested technique.

Table 4 compares the communication cost in the proposed methodology to the other four used techniques.

5.3 Storage requirement

Storage requirements are the amount of space required to store data in tags and servers during the authentication process. In the proposed scheme, the tag stores variables system such as [Ab; An; Aa]; [q; P_E; a; n; b]; [MC] and [X_{ta}; I_{ta}]. As specified at the setup stage. Thus, the tag's saves need was ([15 + 25 + 15] + [30 + 15 + 50 + 15 + 25] + [10] + [50 + 50]) bit = 300 bit.

Table 4. Comparative analysis of communication costs entity

Entities	**Tag**	**Server**	**Totals (Tag +Server)**
Liao & Hsiao [17]	640 bits	640 bits	1280 bits
He [24]	640 bits	640 bits	1280 bits
Lee and Chien [26]	640 bits	640 bits	1280 bits
S. Kumar [5]	640 bits	640 bits	1280 bits
Wei G and Qin Y[24]	640 bits	640 bits	1280 bits
Wei G and Qin Y [25]	640 bits	640 bits	1280 bits
Suggested Method	1842 bits	2354 bits	4196 bits

Table 5. A storage cost comparison

Entity	**Tagged**	**Servers**	**Totals (Tagged+ Servers)**
Liao and Hsiao [16]	1760 bits	(1440+480m) bits	(3200+480m) bits
He [23]	1600 bits	(1440+320m) bits	(3040+320m) bits
Lee and chien [25]	1600 bits	(1440+320m) bits	(3040+320m) bits
S. Kumar [5]	1600 bits	(1440+320m) bits	(3040+320m) bits
Wei G and Qin Y[24]	x	x	x
Suggested method	300 bits	300 + 100m	(600+100m) Bits
Liao and Hsiao [16]	1760 bits	(1440+480m) bits	(3200+480m) bits

On the other hand, a server stores the variables such as [Ab; An; Aa]; [q; P_E; a; n; b]; [MC]; [X_{ta}; I_{ta}]; and [X_{se}; P_{se}]. Assuming "m" tagged were present in the systems, the server's saving needs are ([15 + 25 + 15] + [30 + 15 + 50 + 15 + 25] + [10] + [50m + 50m] + [50 + 50]) = (300 + 100m) bits.

Table 5 compares the storage costs of our proposed approach to another four techniques in utilizing.

5.4 Throughput rate

The network throughput can be defined as the number of packets successfully transmitted within the specified transmission time [26]. It is precisely expressed as follows:

Table 6. Rate of throughput

Entity	**Throughput (bps)**
B.D. Deebak [26]	5700
Srinivas [27]	4800
Lu [28]	5200
Suggested approach	11713457.3

Table 7. Delay of transmission

Entity	**Transmission delay (sec)**
B.D. Deebak [26]	0.03
Srinivas [27]	0.04
Lu [28]	0.06
Suggested approach	0.000209

$$TP_R = \frac{\sum_{i=1}^{N}(Q_i^r * ml_i)}{T_w} \quad (1)$$

where T_w is the total execution time in sec, Q_i^r is the number of packets received, and ml_i is the message length of i^{th} packet.

The throughput of the proposed system reached (11713457.3) and was calculated using the throughput equation mentioned above. As the number of packets in the system (3), the total size of the packets (2680 bits), and the total time taken to perform the authentication (0.00068639s). Through the results, the efficiency of the proposed system was proven from previous studies through its throughput. As shown in Table 6.

5.5 Transmission delay

The transmission delay is measured as the average of time. It takes data packets for travel from the source to the destination [26].

$$T_D = \sum_{i=1}^{T_P} \frac{(RT_i - ST_i)}{T_P} \quad (2)$$

Where T_D is transmission delay, (i) denotes the number of transmitted packets. T_P the overall number of packets sent, respectively. RT_i and ST_i the packets' receiving and sending times are represented.

The transmission delay of the proposed system reached (0.000209s) and was calculated using the transmission delay equation mentioned above. As the number of packets in the system (3), the packets' receiving and sending times (0.00002949s), (0.0006569s). Through the results, the efficiency of the proposed system was proven from previous studies through its transmission delay. As shown in Table 7.

6. Conclusions

These days, blockchain and IoT approaches are blending. The blockchain first received attention as the portion of a wave of digital coins that represented a challenge to existing payment systems. But the information exchanges, not the blockchain processes, caught the IoT advocates' attention. In networks where interconnected objects dynamically connect, such as the IoT, blockchain is a decentralized distribution, anti-hacking, or event-recording system that is highly advantageous for addressing major problems. Because of the importance of security in IoT, several techniques have been offered in this field.

Lately, W. K. Ahmed and Rana Saad. Suggested a lightweight RFID protocol using Blockchain and Elliptic-Curve for Internet of Things applications. However, we discovered W.K. Ahmed and Rana Saad, scheme flaws in the computational cost is higher and the time of execution is more. Therefore, in this paper, we propose to improve lightweight authentication using Arnold Chaotic Map and Markov-Chain for IoT applications to address these issues.

The proposed scheme performance has been evaluated based on computational expenses, communication costs, storage requirements, throughput, and transmission delays. It has been compared with the other current protocols. Comparing computational costs reveals that the proposed protocol has a lower computational cost than the other current procedures. Comparing communication costs shows that the recommended protocol has good communication cost. The requirement of storage study reveals that the proposed scheme requires less storage than Liao, He, S. Kumar, Lee, and Hsiao. The throughput rate and transmission delay usage are lower than other related systems. So, the suggested method is more secure and efficient than current RFID systems and suitable for practical applications.

We concluded in the suggested method that there are two processes of authenticating: the first is a significant authentication in our technique that occurs between the server and the tag as a consequence of the calculations and their complexity. This authenticate method uses a blockchain and secures variables or data transmitted across an unsecured channel. As a result, our solution delivers excellent security, privacy, and data efficiency while impervious to modification or manipulation.

In the future, to increase the system's efficiency and reduce the time taken for the authentication process, we will use a lightweight hash function.

Conflict of interest

The authors declare no conflict of interest.

Author contributions

Author 1: Data collection, concept, analysis, methodology, writing—original draft preparation, software, and writing—review, and editing. Author 2: The Supervision, validation, review, investigation, and writing—review and editing

Acknowledgments

We thank Mustansiriyah University for it helps to us with our research.

Reference

[1] M. Shariq and K. Singh, "A novel vector-space-based lightweight privacy-preserving RFID authentication protocol for IoT environment", *Springer US*, Vol. 77, No. 8, pp.8532–8562, 2021.

[2] E. L. Mohaisen and R. S. Mohammed, "Stream cipher based on chaotic maps", In: *Proc. of IEEE First International Conference of Computer and Applied Sciences (CAS)*, Baghdad, Iraq, pp. 256–261, 2019.

[3] S. F. Aghili, H. Mala, P. Kaliyar, and M. Conti, "SecLAP: Secure and lightweight RFID authentication protocol for Medical IoT", *Future Generation Computer Systems*, Vol. 101, pp. 621–634, 2019.

[4] R. S. Mohammed, A. H. Mohammed, and F. N. Abbas, "Security and Privacy in the Internet of Things (IoT): Survey", In: *Proc. of IEEE 2nd International Conference on Electrical, Communication, Computer, Power and Control Engineering (ICECCPCE)*, Mosul, Iraq, pp. 204–208, 2019.

[5] S. Kumar, H. Banka, B. Kaushik, and S. Sharma, "A review and analysis of secure and lightweight ECC-based RFID authentication protocol for Internet of Vehicles", *Transactions on Emerging Telecommunications Technologies*, Vol. 32, No. 11, p. e4354, 2021.

[6] W. K. Ahmed and R. S. Mohammed, "Lightweight Authentication Methods in IoT: Survey", In: *Proc. of IEEE International Conference on Computer Science and Software Engineering (CSASE)*, Duhok, Iraq, pp. 241–246, 2022.

[7] A. H. Mohammed and M. M. Jafer, "Secure web of things based on a lightweight Algorithm", In: *Proc. of IEEE First International Conference of Computer and Applied Sciences (CAS)*, Baghdad, Iraq, pp. 216–221, 2019.

[8] Y. Zhong, M. Zhou, J. Li, J. Chen, Y. Liu, Y. Zhao, and M. Hu, "Distributed blockchain-based authentication and authorization protocol for smart grid", *Wireless Communication and Mobile Computing*, Vol. 2021, p.15, 2021.

[9] R. Khalaf, A. Mohammed, E. Essa, and H. Ali, "Controlling smart home activities Using IoT", In: *Proc. of International Conference on Computing and Information Science and Technology and Their Applications (ICCISTA)*, Kirkuk, Iraq, pp. 1–6, 2019.

[10] L. Vishwakarma and D. Das, "SCAB-IoTA: Secure communication and authentication for IoT applications using blockchain", *Journal of Parallel and Distributed Computing*, Vol. 154, pp. 94–105, 2021.

[11] H. F. Atlam, A. Alenezi, M. O. Alassafi, and G. B. Wills, "Blockchain with Internet of things: Benefits, challenges, and future directions", *International Journal of Intelligent Systems & Applications*, Vol. 10, No. 6, pp. 40-48, 2018.

[12] R. M. A. Hussein, R. S. Mohammed, and A. H. Mohammed, "Security Challenges and Cyber-Attacks for Internet of Things", In: *Proc. of IEEE Babylon International Conference on Information Technology and Science (BICITS)*, Babil, Iraq, pp. 81–85, 2021.

[13] A. Stanciu, "Blockchain based distributed control system for edge computing", In: *Proc. of International Conference on Control Systems and Computer Science (CSCS)*, Bucharest, Romania, pp. 667–671, 2017.

[14] M. Ammi, S. Alarabi, and E. Benkhelifa, "Customized blockchain-based architecture for secure smart home for lightweight IoT", *Information Processing & Management*, Vol. 58, No. 3, p. 102482, 2021.

[15] D. Singh, B. Kumar, S. Singh, and S. Chand, "An Efficient and Secure Authentication Scheme using Markov Chain for Wireless Sensor Networks", In: *Proc. of IEEE 8th International Advance Computing Conference (IACC)*, Greater Noida, India, pp. 33–38, 2018.

[16] Y. P. Liao and C. M. Hsiao, "A secure ECC-based RFID authentication scheme integrated with ID-verifier transfer protocol", *Ad Hoc Networks*, Vol. 18, pp. 133–146, 2014.

[17] U. Khalid, M. Asim, T. Baker, P. C. K. Hung, M. A. Tariq, and L. Rafferty, "A decentralized lightweight blockchain-based authentication mechanism for IoT systems", *Cluster Computing*, Vol. 23, No. 3, pp. 2067–2087, 2020.

[18] M. Tahir, M. Sardaraz, S. Muhammad, and M. S. Khan, "A lightweight authentication and authorization framework for blockchain-enabled IoT network in health-informatics", *Sustainability*, Vol. 12, No. 17, p. 6960, 2020.

[19] V. Rao and P. KV, "DEC-LADE: Dual elliptic curve-based lightweight authentication and data encryption scheme for resource constrained smart devices", *The Institution of Engineering and Technology*, Vol. 11, No. 2, pp. 91–109, 2021.

[20] A. Akbarzadeh, M. Bayat, B. Zahednejad, A. Payandeh, and M. R. Aref, "A lightweight hierarchical authentication scheme for internet of things", *Journal of Ambient Intelligence and Humanized Computing*, Vol. 10, No. 7, pp. 2607–2619, 2019.

[21] C. D. M. Pham and T. K. Dang, "A lightweight authentication protocol for D2D-enabled IoT systems with privacy", *Pervasive and Mobile Computing*, Vol. 74, p. 101399, 2021.
[22] L. C. Thungon, N. Ahmed, S. C. Sahana, and M. I. Hussain, "A lightweight authentication and key exchange mechanism for IPv6 over low-power wireless personal area networks-based Internet of things", *Transactions on Emerging Telecommunications Technologies*, Vol. 32, No. 5, pp. 1–17, 2021.
[23] D. He, N. Kumar, N. Chilamkurti, and J. H. Lee, "Lightweight ECC Based RFID Authentication Integrated with an ID Verifier Transfer Protocol", *Journal of Medical Systems*, Vol. 38, No. 10, pp. 1-6, 2014.
[24] G. Wei, Y. Qin, and W. Fu, "An Improved Security Authentication Protocol for Lightweight RFID Based on ECC", *Journal of Sensors*, Vol. 2022, 2022.
[25] C. I. Lee and H. Y. Chien, "An elliptic curve cryptography-based RFID authentication securing e-health system", *International Journal of Distributed Sensor Networks*, Vol. 11, No. 12, 2015.
[26] B. D. Deebak and F. A. Turjman, "Lightweight authentication for IoT/Cloud-based forensics in intelligent data computing", *Future Generation Computer Systems*, Vol. 116, pp. 406–425, 2021.
[27] J. Srinivas, S. Mukhopadhyay, and D. Mishra, "Secure and efficient user authentication scheme for multi-gateway wireless sensor networks", *Ad Hoc Networks*, Vol. 54, pp. 147–169, 2017.
[28] Y. Lu, L. Li, H. Peng, and Y. Yang, "An anonymous two-factor authenticated key agreement scheme for session initiation protocol using elliptic curve cryptography", *Multimedia Tools and Applications*, Vol. 76, No. 2, pp. 1801–1815, 2017.