Journal of Theoretical and Applied Information Technology
15th September 2022. Vol.100. No 17

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

IMPROVING LIGHTWEIGHT AUTHENTICATION USING NEW TECHNIQUES FOR IOT

WALEED KAREEM AHMED[1] , RANA SAAD MOHAMMED[2]
[1,2] University of Mustansiriya , College of Education, Department of Computer Science, Iraq
E-mail: [1] waleed.kareem.ahmed.b@uomustansiriyah.edu.iq,
[2] drranasaad@uomustansiriyah.edu.iq

ABSTRACT

The Internet of Things (IoT) is a new paradigm that uses an Internet to communicate a wide range of physical objects with the cyber scientist. The Internet of Things (IoT) is rapidly growing and would soon have a big influence on our daily lives. While the growing amount of linked IoT gadgets makes our lives easier, it actually puts our personal information at danger. For IoT devices, radio frequency identification (RFID) aids in the automated identification of connected devices. However, both privacy and security for RFID tag-connected technologies are the key issues. The increasing security of radio frequency identification (RFID) solutions for a variety of RFID applications that require a centralized database expansion, as compared to a standard central database, blockchain technologies are rapidly establishing itself with a new decentralized and distributed alternative that offers improved data security , dependability, transparency, the immutability, and lower maintenance costs. RFID is expected to play a major role in enabling identification technologies in the Internet of Things due to its inherent benefits. However, because of its connection with sensor technology, it may be used in the broad range of sectors. On the other hand, one of the most challenging parts of developing a RFID system appeared for being security. Authentication and privacy concerns are at the heart of RFID security. Elliptic curve cryptosystem (ECC) related algorithms are commonly regarded as the best option among PKC approaches due to their small key sizes and effective calculations. Recently W.K. Ahmed et al . proposed a New Lightweight BLOCKCHAIN and ECC-Based RFID Authentication Protocol for IOT. We found the weaknesses of W.K. Ahmed et al protocol by computation cost high and running time high. In order to solve these problems. In this paper, we introduce Improving lightweight authentication using New techniques for IoT. Our protocol uses techniques from them blockchain, ECC, Arnold map chaotic, and Markova chain. We implemented our suggested programming using python language. after comparing storage cost, communication cost, and computation cost with other protocols, our protocol is more secure and performance efficient than the existing RFID protocols and is well suited for practical applications.
Keywords: *ECC, Arnold map chaotic, blockchain technique, authentication, Markov chain*

1. INTRODUCTION

As the name implies, the Internet of Things (IoT) connects "everything to the Internet" [1]. Every day, the Internet of Things has an impact on our lives. IoT is a unique paradigm in ubiquitous wireless communications that connects numerous physical devices or items to the cyber world through the internet, allowing data to be gathered and transmitted without the need for human involvement [2–4]. Different identification methods, as like QR codes, RFID, as well as other sensor technologies, can be used to identify these linked devices [5, 6]. Smart supply chains, industrial control, smart retail, smart cities, smart grids, smart buildings, telemedicine information systems and telehealth are only a few examples of IoT applications [7, 8]. The connectivity between the various IoT components is presumed to be insecure. A main challenge for IoT technology was ensuring safe network connectivity between IoT components. Because IoT may have certain flaws in its security procedures, it is subject to a variety of known threats. As a result, a safe authentication technique based upon lightweight cryptographic techniques is required[1].

RFID (radio frequency identification) has been the most advanced technique for automated identification using radio waves (RF). The RFID method is also useful for simultaneously tracking or identifying several items [9, 10]. RFID technology was originally utilized for IFF (Identifying Friend or Foe) airplanes during World War II [11]. Furthermore, the RFID system replaces the barcode system due to features such as its ability to scan hundreds of tags at once and the lack of sight line need for read RFID tags. Presently, RFID is now

being utilized into large-scale applications of automated identification, such as the medical hospital environment, monitoring and tracking, automated payment, access control, supplier management, vehicular cloud computing (VCC) , and the Internet of Vehicles (IoV) [2]. RFID tagging, RFID readers or interrogators, and the backend servers or host computer were the three essential components of the RFID system [1][3].

Because everything has advantages and disadvantages, security for RFID-based automotive systems is a serious problem because it concerns human lives. 16,17 Cryptography was born out of the need for data security. Cryptography is a method of protecting data from unwanted access by changing it to a different format. 18,19 Asymmetric key encryption and symmetric key encryption are two types of encryption algorithm. Asymmetric cryptographic encryption requires 20 different keys, including public and private the keys, to encrypted and decode communications. 12,21 Symmetric encryption algorithms, on the other hand, employ the same cryptography key for encryption and decode plaintext and ciphertext[4][5].

Most IoT solutions now use a centralized server-client architecture, in which users communicate to cloud servers over the Internet [3]. Moreover, centralized systems are vulnerable to harmful information manipulation through untrusted individuals, which might lead to the flow of manipulated and fabricated data [4]. Network attacks like fake data injection, data manipulation, and single nodes failure, the on other side, are vulnerable to clouds applications which store, forward, and analyze IoT data [5]. To summarize, the most pressing issues about IoT development were privacy and security. [6] points out how blockchain-based decentralized architectures can help solve the challenge for IoT application security. In centralized companies, blockchain technology is favorable to overcoming problems of poor dependability, high cost, the low security, and poor efficiency [10, 11]. [6].

The omnipresent of things is the notion underpinning IoT and its different forms, where they may connect and interact to develop a wide range of services. The Internet of Things' most recent advancements aided smart city development. As a result, just authenticated and approved devices should have access to a IoT of order for it to work without interruption. Otherwise, it becomes vulnerable to a variety of security threats, including data theft, data manipulation, and identity theft [4,5]. Because of the tremendous demand for compute, traditional security techniques are unable to protect information integrity in the Internet of Things. Furthermore, because Iot systems are low-powered but also have limited computing capability, their design differs significantly from that of the Internet [6]. Therefore, existing cryptographic security measures are limited in their use. It is not scalable nor practicable to directly increase computing demand for IoV [7,8]. Due to the substantial computational cost, the state-of-the-art techniques provided by various researchers (briefly detailed during literature review section) were not appropriate for real time applications [9–11]. The approaches are ineffective for gadgets that consume relatively little energy [7][8]. To resolve the above issue, the RFID protocol employed lightweight cryptographic functions ECC, Markov chain, and Arnold chaotic map for verification of data for authenticating and secure connection, and SHA256 to assure data integrity. We've also used the SHA256-based blockchain idea to create a reliable and secure storage system.

In brief, our contribution to a study is as follows:

1. We found the weaknesses of W.K. Ahmed et al protocol by computation cost high and running time high.
2. We propose an improved scheme that overcomes the problems of their scheme W.K. Ahmed et al.
3. The proposed protocol is able to achieve strong security as all security requirements are fulfilled.
4- The authentication equations have also been improved Performance parameters, that is, computational cost, communication cost, and storage requirements are better than existing protocols.

the remainder of this essay is structured as follows. section 2 blockchain technique, section 3 blockchain's qualities include, section 4 related work, section 5 proposed method, section 6 results and discussion, section 7 conclusion.

2. BLOCKCHAIN TECHNIQUE

An Internet of Things (IoT) is expanded internet connectivity beyond humans and computers to include most of our everyday things. The Internet of Things offers the ability to link billions of items at once, enhancing data exchange needs and so enhancing our lives. Although the advantages in the Internet of Things seem limitless, owing to its centralized server/client method, there are several barriers to adoption into the real world. For example, high numbers of IoT items in the network might cause scalability and security difficulties. All devices should be linked and authorized through the

server under the server/client structure, which provides a one point of failure. Therefore, taking the IoT system along the decentralized road might be the best option. Blockchain is a well-known decentralization technique. Blockchain is a strong technology which decentralizes computing and management processes, but it has the potential to solve many IoT challenges, including security[9].

The blockchain has several definitions. so according [7][10], The blockchain which "a distributed database for records, or public ledger, over any transactions or connect that have been conducted and shared between participating parties." Every transaction of the public ledger is confirmed by a minority of the system's members. Information cannot be deleted after it has been submitted. Every transaction that has ever taken place is recorded on the blockchain[11].

As a result, BC technologies becomes as appealing solution for tackling the IoT but also Smart Home privacy and security problems (Jurdak & Gauravaram, Dorri, Kanhere, 2017). The lack of a centralized control of BC ensures usability and dependability by combining assets from all running nodes, avoiding the problem of a one point of failure. Furthermore, BC's intrinsic anonymous feature is critical for many IoT application deployment, notably in Smart Homes were user identities must be kept private. The BC method also provides a secured network with many heterogeneous devices across untrusted parties, which is a critical need in IoT systems [12].

3. BLOCKCHAIN'S QUALITIES INCLUDE:

The blockchain has a lot of properties that make it appealing to the IoT for solving many of its problems. According to [13], blockchain features include the following:

1. Immutability: One of the main benefits of blockchain was the ability to create immutable ledgers. Every centralized database is susceptible to corruption, necessitating reliance on a third party to maintain data integrity. A transaction cannot be modified once it has been agreed upon and documented.
2. Decentralization: The loss of centralized control enables scalability and resilience by using every contributing nodes' resources and reducing many-to-one data flows, lowering latency and avoiding the one point of failure issue which arises in the centralized model.
3. Anonymity: Anonymity allows users to hide their identify and keep their personal information secret.
4. Better Security: Since there is no one point of failure which can bring the entire down the network, blockchain delivers better security.
5. Increased Capacity: Among the most important aspects for blockchain technology was that it may boost a network's capabilities. Thousands of machines working together could have more computing power that a few centralized servers.

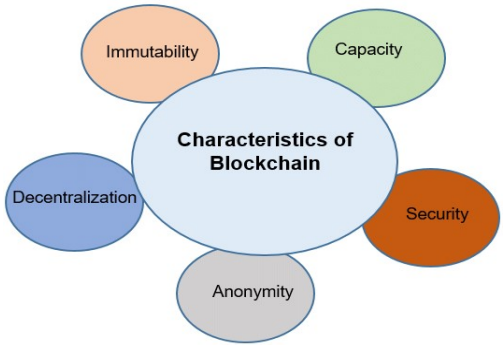

Figure 1: blockchain's qualities include

4. RELATED WORK

To address the drawbacks of previous systems, Debiao He et al [14] propose a new ECC-based RFID authenticating methodology that includes an ID verifier transmission protocol. Many newly reported ECC-based RFID authenticating systems have major security issues. To show the proposed authentication scheme's solid security characteristics, a detailed security analysis was conducted. Furthermore, the performance of suggested authentication technique is assessed in terms the communication, the computational, and storage needs.

Yi-Pin Liao et al [15] proposed a secure ECC-based RFID authenticating approach connected to an ID-verifier communication protocol. On the other hand, many of the most challenging parts of developing the RFID system appear for be security. Authentication and privacy concerns are at the heart of RFID security. The recommended solution may be proved to fulfill the requirements needed through a security analysis was based on an effective and compelling formal approach. Furthermore, they also employed evolutionary to do an efficiency study based on storage requirements, communication costs, and computing costs. They also expect that the outcomes of this study will be relevant to other authentication applications that are

similar to RFID systems, rather than just RFID systems.

Umair Khalid et al [16] describe a decentralized authenticating and access control mechanism for lightweight Iot systems that may be used in a variety of circumstances. These Internet of Things (IoT) technologies produce a tremendous amount of sensitive and personal data. As a result, ensuring the safety and efficacy of the system requires that these devices be safe. The proposed method is based on blockchain technology has taken more use of cryptographic capability and distributed nature, whereas fog computing is employed to reduce latency. The suggested technique may be used in a number of IoT applications. In addition, safety standards and an attack model are developed to evaluate and evaluate our approach's ability to achieve these requirements. To avoid PoW's enormous energy consumption when confirming each block.

Muhammad Tahir and colleagues [17] This paper presents the new authenticating and authorization approach of Blockchain-enabled IoT devices using a probability model. In healthcare information, privacy and security, and other regulatory duties, are all essential factors. To examine and evaluate the proposed model, exhaustive simulations with both the AVISPA tools as well as the Cooja simulators were employed. Tests demonstrate that the suggested framework enables robust mutual authentication, enhances access control, and reduces both connection and computing cost in comparison to existing frameworks.

To implement the digital signatures and encrypting operations, Vidya Rao as well as Prema K. V [18] suggest using two sets of dynamically elliptic curves. Those low-resource gadgets are subject to a range for security and privacy risks since they are linked to the Internet. In client-server model, the approach is evaluated using the Raspberry Pi 3 device. The length of time necessary for the hashing algorithm, key creation, signature generation, signature validation, decryption, and encryption was determined through experiments. When compared to cBLAKE2b, the proposed DECLADE took 13.76 percentage, 2.57 percent, 18.36 percentage, 6.12 percent, 9.91 percentage, and 6.08 percentage less time, respectively, then LWDSA with mBLAKE2b. Its safety evaluations of man-in-the-middle attack, replay attack, and denial-of-service attack are undertaken both theoretically and in real time.

Aida Akbarzadeh et al. [19] proposed lightweight Chebyshev Chaotic Maps authenticating mechanism. In the suggested solution, they leverage a hierarchical framework to implement different access restrictions for various components. The IoT network's devices were limited in terms both storage and processing. They then offer a formal analysis utilizing BAN logic to establish the security in their technique. They also compare their suggested method's performance and privacy to that of existing systems. The results support the proposed scheme's effectiveness and safety when compared to competing methods.

Chau D.M. Pham and Tran Khanh Dang [20] proposed using elliptic curve cryptography (ECC) with a reciprocal privacy-preserving authenticating mechanism to achieve resource effectiveness and ensure privacy for participating devices. Existing authenticating approaches are difficult to deploy due to resource constraints of IoT devices. Formal analysis utilizing BAN-logic [49] is used to demonstrate the correctness of the provided authentication procedures, indicating that mutual authenticating and session key agreement among the participants may be done securely. As the result, the novel protocol is secure and appropriate for low-power devices.

Leki Chom Thungon et al [21] proposed a lightweight key exchanging and authenticating mechanism for 6LoWPAN to quickly authenticate resource-constrained sensor devices. In traditional wireless sensor networks, three-factor authenticating is employed. These issues are a substantial overhead in the Internet of Things due from resource-constrained devices' limited memory and processing capabilities. The suggested method's safety claim against threats such as replay for man-in-the-middle assaults is supported by the findings from automated validating of internet secure protocols and applications, and the ProVerif tools. Those who also employ Burrows-Abadi-Needham Arithmetic to assess the logical correctness of the recommended authentication system.

5. PROPOSED METHOD

We proposed Improving lightweight authentication utilizing New techniques for IoT of RFID systems, which addresses all of the security issues with current RFID-based systems and surpasses alternative blockchain and ECC-based protocols in terms of storage cost, computation cost, and communication cost.

We employed Blockchain technology in our suggested solution, which adds great security to the data exchanged between the servers and the tags and also serves as a preliminary authentication for our method. As a result, communication costs are

high, but we can use Blockchain technology to safeguard data and authorization, and blockchain technologies are quickly establishing themselves as a new decentralized and distributed alternative which provides improved data safety, dependability, transparency, immutability, and lesser maintenance costs. Data sent between the servers and the flag also isn't safeguarded, as it was in prior protocols.

Blockchain is a system that helps give a high level of security in technological transactions taking place from over Internet by confirming the authenticity and legality of these transaction, and acting to preserve the data that you wish to safeguard. Unlike traditional encryption methods, which completely block information, Blockchain technology is distinguished by the fact that the data it contains can be regarded at any time and from any location, despite the reality that traditional processes owned by governments and banks have high levels of safety and protection. Those are, however, systems which can be hacked in some way. As for the decentralized network of Blockchain technologies, it is provided to everyone to include a framework with transparency for those interesting in it, as that technology was based on using of encryption to safeguard information, avoid methods of tampering or forging and does not limit access to it. so the idea of attacking the system is nearly hard, in order to attack the blockchain technology system, you'd have to update the information of thousands of devices spread around the world.

Tagging, readings, and backup servers are the three components of the proposed approach, with the readers acting as an intermediate in data flow between tagged and servers. As a consequence, the suggested method only takes into account tag and server connections. On the other hand, the connection between the server and the reader is assumed to be secure. On the other hand, the connection between reader and tags is assumed to be secure.

The proposed authenticator has two parts: (1) setup as well as (2) authorization. The authentication stage, as well as the notations and parameters used in the setting of our recommended approach.

The parameters using in the proposed protocols were as follows:

- n, q: These were prime numbers.
- F(q): There was the finite field with ranking n and size q.
- E: Elliptic curve, define via y2 = x3 + ax + b of the finite field F(q), with constants a and b.
- P: The generation point for the elliptic curve (E) from order n.
- Xs: An secret key of the server.
- Ps: a server the public key, whenever Ps = Xs P.
- Xt: That's the tag's private key.
- It: this is a public-key of tag, whenever It = Xt P

5.1 Setup Stage

During the setup step, the server performs the following tasks:

- The domains variables of elliptic curves [q; a; P; b; n] are specified.
- Chaotic map domain variables, that is; [Cb; Cn; Ca] are defined.
- Markov chain domain variables, this is, [M] is specified.
- A random parameter Xs = C is selected for the server's private key from the chaotic mapping (C) as well as Ps = XsP was calculated as that for the server's public key.
- A random parameter Xt =C In is selected for the tag's private key from chaotic mapping (C) as well as IT = XtP was calculated as that for tag's public key.
- Server keeps elliptic curve perimeters [q; a; P ; b; n]; [Cb; Cn; Ca]; [Xt; It]; [M]; and [Xs ;Ps].
- Tag keeps elliptic curve perimeters [q; a; P ; b; n]; [Cb; Cn; Ca]; [Xt; It] and [M] .

5.2 Authentication Stage

During this level of authenticating, mutual authentication happens between the tag and the server, and the mechanisms were explained below. The authenticating stage of the recommended approach is depicted in Figure 2.

Server (Xs, Ps, Xt, It, Ca ,Cb ,Cn,M)	Tag (Xt, It, Ca ,Cb ,Cn,M)

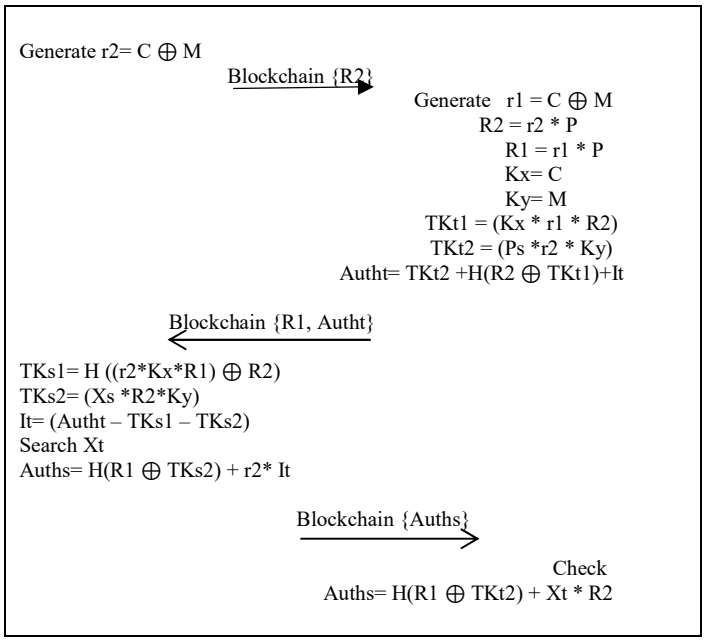

Figure 2: Authentication phase of proposed protocol

1) Server → Tagging: blockchain {R2}. A server random generated numbered r2 = C ⊕ M, then it calculates R2 = r2P and delivers blockchain {R2} into tag.
2) Tagging→ servsr: blockchain {R1, Autht}. Tag select a number at randomly r1 = C ⊕ M, then it computes R1 = r1P =(Kx, Ky), where Kx and Ky they are from values C and M, respectively. It also calculating TKt2 = (Ps * Ky*r2), TKt1 = (Kx * R2* r1), and Autht= TKt2 +H(R2⊕ TKt1)+It ,wherever TKt1 and TKt2 were temporary A keys, H was hash values, Autht was the authenticating for tagging and then it sends blockchain{R1, Atht} into the server.
3) Server→ Tagging: blockchain{Auths}. A servers again calculatig new numbered TKs2= (Xs * Ky* R2), It= (Autht – TKs1 – TKs2), and TKs1= H (R2 ⊕ Kx * R1 *r2. the server checks the database from Xt, if the matching value is not found, the server would then terminate the connection until the tag has being permitted and the server has computed the value. Auths= r2* It + H(R1⊕ TKs2) is wherever Auths was the server's authorisation and sends the value of blockchain{Auths} into tag.
4) Auths= H(R1 TKt2) + Xt * R2 and Auths= H(R1 TKt2) + Xt * R2 evaluate if the result Auths. If the tag cannot find an equal value, the connection will be terminated; otherwise, the server will be authorized.

6. RESULTS AND DISCUSSION

In this part, the proposed protocol was compared to a number of current multifactor authentication systems, including Liao and Hsiao[11], W.K.Ahmed et al [8], He et al[23], Lee et al[24], and S. Kumar et al[3], with terms of communication costs, calculation costs, and storage costs. The particular comparative results and analysis are listed below.

6.1 Computational cost

The computational cost is determining via the server and tag methods. The server and tag run times are 0.00002949 and 0.0006569, respectively. Table 1 displays the average GF(2m) running time in microseconds using LiDIA [6].

If "T" as the estimated runtime for multiplication in Tagged, then "T/5," as indicated in Table 2, shows the estimated runtime of square operation, that is, for multiplying it is 10.5, and for squares it is 2.3, which is nearly one-fifth of multiplying. As a result, T/20 represents the projected runtime of adding, T/20 represents the expected runtime for subtracting, and 9T represents the estimated runtime for inversion. If Server's multiplication time is T′, the estimated runtime for squaring is T′/5, the estimated runtime with adding is T′/20, its estimated runtime for subtracting is T′/20, as well as the estimated runtime on inversion is 9 T′. We believe that the time spent for some basic processes (XOR operations) is very low and may be overlooked. In addition, according into[25] and[26]. Based on the foregoing notations, our proposed protocol's calculation cost is equivalent to a costs of four current protocols, as shown by Table 2. The findings suggest that the proposed method is better than others.

Table 1. GF(2m) average runtime through microseconds used LiDIA.

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

Table 2: Entity of computational costs.

Entity	Tag	Server
Liao and Hsiao [15]	3 adding and 5 Multiplications of elliptical vectors Total runtime =3 (T/20) + 5T =T5.15 = (0.064)5.15 = 0.3296 sec.	1 adds, 5 elliptic vector multiply, & 2 subtract Total runtime = 1(T′/20) +5T′ + 2(T′/20) = T′5.15= 0.001124* 5.15 = 0.0057886 sec.
He et al [23]	2 adds, 2 inversions, & 5 elliptic vector multiplications Total runtime = 2(T/20) +T2*9 + 5T = T23.1 = (0.064) 23.1 = 1.4784 sec.	3 adds, 4 inversions 7 elliptic vector multiply, &1 subtract Total runtime = 3(T′/20) + 4(9T′) +7T′+ 1(T′/20) = T′ 43.2 = 0.001124*43.2 = 0.0485568 sec.
Lee et al [24]	7 vector multiplications, 6 adds, 4 inversions, & 2 hashing. Total runtime = 7T+6(T/20) + 4(9T) + 2(H) = 7T+3T/10 + 36T +2H = T 43.3 = (0.064)43.3 = 2.7712 sec.	5 adds, 2 hashing, 7 elliptic Vector multiply, 1 subtract, & 4 inversions Total runtime = 5(T′/20) +2H+ 7T′ + (T′/20) + 4(9T′) = (6T′/20) +2H + 7T′ + 36T′ = T′43.3 = 0.001124*43.3 = 0.0486692 sec.
S. Kumar et al [4]	5 adds, 7 vector multiplications, & 2 hashing Total runtime = 5(T/20) +7T +2H = T7.25 = (0.064)7.25 = 0.464 sec.	3adds,2hashing ,7 elliptic Vector multiply, & 2 subtract Total runtime = (3T′/20) +2 H +7T′ + 2(T′/20) = T′ 7.25 = 0.001124*7.25 = 0.008149 sec.
W.K.Ahmed et al [8]	5 adds, 6 vector multiplications, & 2 hashing Total runtime = 5(T/20) +6T +2H = T6.25 = 6.25 *0.0007211 = 0.004506 sec.	3 adds, 2 hashing 6 vector multiply, & 2 subtract Total runtime = 3(T′/20) + 2H + 6T + 2(T′/20) = T′ 6.25 = 0.0001038*6.25 = 0.00064875 Sec.
Suggested method	3 adds, 6 vector multiplications, & 2 hashing Total runtime = 3(T/20) +6T +2H = T6.001= 6.001*0.0006569 = 0.003942 sec	1 adds, 2 hashing 6 vector multiply, & 2 subtract Total runtime = (T′/20) + 2H + 6T + 2(T′/20) = T′ 6.001 = 0.0001038*6.001 = 0.0001769 Sec.

Table 3: Comparison analysis of communication costs Entity.

Entity	Servers	Tags	Totals (Servers+Tags)
Liao and Hsiao [15]	640 bits	640 bits	1280 bits
He et al [23]	640 bits	640 bits	1280 bits
Lee et al [24]	640 bits	640 bits	1280 bits
S. Kumar et al [4]	640 bits	640 bits	1280 bits
W.K. Ahmed et al [8]	2354 bits	1842 bits	4196 bits
Suggested method	2354 bits	1842 bits	4196 bits

Table 4: Comparison for storage costs.

Entity	Servers	Tagging	Totals (Servers+Tagging)
Liao and Hsiao [15]	(1440+480m) bits	1760 bits	(3200+480m) bits
He et al [23]	(1440+320m) bits	1600 bits	(3040+320m) bits
Lee et al [24]	(1440+320m) bits	1600 bits	(3040+320m) bits
S. Kumar et al [4]	(1440+320m) bits	1600 bits	(3040+320m) bits
W. Ahmed et al [8]	300 + 100m	300 bits	(600+100m) bits
Suggested method	300 + 100m	300 bits	(600+100m) bits

6.2 Communication Cost Analysis

In our suggested protocol, we decrease the message of 640 bits into 306 bits. But in our technique we employ Blockchain technology which includes the data, the new hash, and the previous hash. as that technology was based on using of encryption to safeguard information, avoid methods of tampering or forging and does not limit access to it. so the idea of attacking the system is nearly hard, in order to attack the blockchain technology system, you'd have to update the information of thousands of devices spread around the world. This leads into a large message length, however Blockchain technology provides a lot of advantages, such as high security, dependability, unbreakability, and decentralization. so, the increased connecting cost is never a loss compared into the added safeguard of the blockchain authenticity process if it was considered a primary authenticating of the proposed method. The messages sent by the server were blockchain [[R2 = P * r2]] as well as blockchain {{Auths = H (TKs2⊕ R1) + r2 * It}}. Consequently, the total connecting cost in server

equals (562 + 1792) bits = 2354 bits, and the messages transmit by the tag were blockchain {R1 = r1P = (kx, ky)} as well as blockchain {Autht = It + TKt2+ H (R2 ⊕ TKt1)} Consequently, of a suggest method, the many communications cost for the tag (1536 + 306) bits = 1842 bits.

The transmission costs for our suggested approach are compared to the other four methodologies in use in Table 3

6.3 Storage Requirement

Storage need refers to the amount of space required to store information with in tagging and servers and during authentication phase. In our suggested protocol, the tag keeps system variables, like as, [q; a; P; b; n]; [Cb; Cn; Ca]; [Xt; It] and [M]. At its memory, as stated through the setup stage. Thus, the saves requirement of the tag was ([30 + 15 + 50 + 15 + 25] + [15 + 25 + 15] + [50 + 50]) + [10] bits = 300 bits. on either side, the server keeps variables, like as, [q; a; P; b; n]; [Cb; Cn; Ca]; [Xt; It]; [M]; and [Xs; Ps]. Assuming that "m" tags are present in the system, the server's saves requirements were ([30 + 15 + 50 + 15 + 25] + [15 + 25 + 15] + [50m + 50m] + [10] + [50 + 50]) bits = (300 + 100m) bits.

The storing costs of our suggested solution are compared to other four methodologies in use in Table 4.

7. CONCLUSION

Blockchain with Internet of Things (IoT) techniques are merging these days. The blockchain originally gained notice as part of a surge of crypto currencies that posed a threat to traditional transaction methods. But it was the data transfers, not the blockchain operations, that drew the attention the IoT campaigners. Blockchain is a decentralized an anti-hacking, distributed, or event tracking method that looks to be highly beneficial for addressing major concerns in networks where linked objects automatically communicate with one another, i.e., the Internet of Things. Many strategies have been presented in this area due to the relevance of security in IoT. In this article, Recently W.K. Ahmed et al . proposed a New Lightweight BLOCKCHAIN and ECC-Based RFID Authentication Protocol for IOT. We found the weaknesses of W.K. Ahmed et al protocol by computation cost high and running time high. In order to solve these problems. we also proposed an Improving lightweight authentication using New techniques for IOT. Performance analysis in the suggested protocol has being done on the base of computational cost, communication costs, as well as storage requirement and is comparison with the others five existing protocols. Computational cost comparative shows that suggested protocol has lower computational cost than comparative with another five existing protocols. Communication cost comparative indicates suggested protocol had the same communication overhead W.K. Ahmed et al. Storage requirement analysis shows that suggested protocol has lower storage requirement than Liao, He et al, S. Kumar et al, Lee et al and Hsiao's protocol while same as W.K. Ahmed et al protocols. our protocol is more secure and performance efficient than the existing RFID protocols and is well suited for practical applications.

In our proposed system, there are two authentication processes, the first authentication between the server and the tag resulting from the computations and its complexity, and this is the main authentication in our method. The second authentication is through a blockchain that protects data or variables over an insecure channel. Thus our system provides high security, privacy and data efficiency and is not subject to alteration or tampering.

in the Future, experiments with the work will be conducted on a wider scale for other IoT application types.

REFERENCES:

[1] M. Shariq and K. Singh, *A novel vector-space-based lightweight privacy-preserving RFID authentication protocol for IoT environment*, vol. 77, no. 8. Springer US, 2021.

[2] S. F. Aghili, H. Mala, P. Kaliyar, and M. Conti, "SecLAP: Secure and lightweight RFID authentication protocol for Medical IoT," *Futur. Gener. Comput. Syst.*, vol. 101, pp. 621–634, 2019.

[3] R. S. Mohammed, A. H. Mohammed, and F. N. Abbas, "Security and Privacy in the Internet of Things (IoT): Survey," *2nd International Conference on Electrical, Communication, Computer, Power and Control Engineering, ICECCPCE 2019*. pp. 204–208, 2019, doi: 10.1109/ICECCPCE46549.2019.203774.

[4] 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," *Trans. Emerg. Telecommun. Technol.*, vol. 32, no. 11, pp. 1–19, 2021, doi: 10.1002/ett.4354.

[5] W. K. Ahmed and R. S. Mohammed, "Lightweight Authentication Methods in IoT: Survey," in *2022 International Conference on Computer Science and Software Engineering*

(CSASE), 2022, pp. 241–246.

[6] Y. Zhong *et al.*, "Distributed blockchain-based authentication and authorization protocol for smart grid," *Wirel. Commun. Mob. Comput.*, vol. 2021, 2021.

[7] L. Vishwakarma and D. Das, "SCAB-IoTA: Secure communication and authentication for IoT applications using blockchain," *J. Parallel Distrib. Comput.*, vol. 154, pp. 94–105, 2021.

[8] W. K. Ahmed. and R. S. Mohammed, "New Lightweight BLOCKCHAIN and ECC-Based RFID Authentication Protocol for IOT," to be published in Journal,under publication, pp. 1–9, 2022.

[9] H. F. Atlam, A. Alenezi, M. O. Alassafi, and G. B. Wills, "Blockchain with Internet of things: Benefits, challenges, and future directions.," *Int. J. Intell. Syst. Appl.*, vol. 10, no. 6, 2018.

[10] R. M. Abdul-Hussein, R. S. Mohammed, and A. H. Mohammed, "Security Challenges and Cyber-Attacks for Internet of Things," in *2021 1st Babylon International Conference on Information Technology and Science (BICITS)*, 2021, pp. 81–85.

[11] A. Stanciu, "Blockchain based distributed control system for edge computing," in *2017 21st International Conference on Control Systems and Computer Science (CSCS)*, 2017, pp. 667–671.

[12] M. Ammi, S. Alarabi, and E. Benkhelifa, "Customized blockchain-based architecture for secure smart home for lightweight IoT," *Inf. Process. Manag.*, vol. 58, no. 3, p. 102482, 2021.

[13] A. Dorri, S. S. Kanhere, and R. Jurdak, "Blockchain in internet of things: challenges and solutions," *arXiv Prepr. arXiv1608.05187*, 2016.

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

[15] 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.

[16] 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 Comput.*, vol. 23, no. 3, pp. 2067–2087, 2020.

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

[18] V. Rao and P. KV, "DEC-LADE: Dual elliptic curve-based lightweight authentication and data encryption scheme for resource constrained smart devices," *IET Wirel. Sens. Syst.*, vol. 11, no. 2, pp. 91–109, 2021.

[19] A. Akbarzadeh, M. Bayat, B. Zahednejad, A. Payandeh, and M. R. Aref, "A lightweight hierarchical authentication scheme for internet of things," *J. Ambient Intell. Humaniz. Comput.*, vol. 10, no. 7, pp. 2607–2619, 2019, doi: 10.1007/s12652-018-0937-6.

[20] C. D. M. Pham and T. K. Dang, "A lightweight authentication protocol for D2D-enabled IoT systems with privacy," *Pervasive Mob. Comput.*, vol. 74, p. 101399, 2021, doi: 10.1016/j.pmcj.2021.101399.

[21] L. Chom Thungon, N. Ahmed, S. Chandra 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," *Trans. Emerg. Telecommun. Technol.*, vol. 32, no. 5, pp. 1–17, 2021, doi: 10.1002/ett.4033.

[22] 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. 2014, doi: 10.1007/s10916-014-0116-z.

[23] C.-I. Lee and H.-Y. Chien, "An elliptic curve cryptography-based RFID authentication securing e-health system," *Int. J. Distrib. Sens. Networks*, vol. 11, no. 12, p. 642425, 2015.

[24] Z. Xu, W. Liang, K.-C. Li, J. Xu, and H. Jin, "A blockchain-based roadside unit-assisted authentication and key agreement protocol for internet of vehicles," *J. Parallel Distrib. Comput.*, vol. 149, pp. 29–39, 2021.

[25] P. Chandrakar, A. Jain, S. Balivada, and R. Ali, "A secure authentication protocol for vehicular ad-hoc networks," in *2019 IEEE International Conference on Electrical, Computer and Communication Technologies (ICECCT)*, 2019, pp. 1–7.