INTL JOURNAL OF ELECTRONICS AND TELECOMMUNICATIONS, 2024, VOL. 70, NO. 4, PP. 785-790
Manuscript received August 7, 2023; revised October 2024. doi:10.24425/ijet.2024.149609

Lightweight mutual Authentication Protocol for IoT devices using Elliptical Curves

Vandani Verma

***Abstract*—The Internet of Things (IoT) has now permeated every aspect of modern life, requiring that all things be connected to one another and to the Internet using proper protocols. IoT, being an essential component of today's smart society is experiencing enormous problems from various security and interoperability attacks. Traditional encryption is unsuitable for low-cost IoTs because they are vulnerable to physical attacks. This paper proposes Lightweight mutual Authentication Protocol for IoT devices based on hash function using Elliptical Curve approach in which mutual authentication between RFID Tag and Reader is established through several rounds of communication. We also compare the proposed approach of authentication at both ends (Tag and Reader) in terms of efficiency and security.**

***Keywords*—reader; tag; authentication; RFID; IoT; elliptical curves**

I. Introduction

THE Internet of Things (IoT) is a new technology that identifies items as they communicate data. It allows people and things to connect at any point in time from any location, with anyone and anybody, regardless of the nature of the items. Because of this technology, a system is created, which is the connection of physical items or "things" infused with electronics, software, sensors, and network connections, allowing objects to gather and exchange data in order to further automate human life [1]. IoT has now permeated every aspect of modern life, requiring that all things be connected to one another and to the Internet using proper protocols. Applications in numerous disciplines have shown how this new way of looking at things, which greatly simplifies human existence, works. Since tags with unique identifiers are pasted on objects because they need to be identified, tags can be wirelessly identified by Radio Frequency technologies (RFID, or Radio Frequency Identification), is the most widely used technology, having experienced tremendous innovation and widespread with diverse uses. As a result, the majority of our investigations will focus on RFID as a basis for the Internet of Things.

RFID is rapidly emerging as the most intriguing technology for automatic identification in every industry area due to its low cost and ease of deployment. We may characterize the interaction between these two technologies in three categories of IoT applications. Smart cities IoT applications rely on several technologies, including RFID, Wireless Sensor Networks, and single sensors are examples of IoT elements. RFID-enabled IoT applications in warehouses and cities are more examples. RFID in logistics as part of an IoT system with WSN and single sensors is another example. Several IoT-related technologies (e.g., RFID, NFC, WSN, Wi-Fi, and Bluetooth) have significantly improved the measurement and control procedures of dynamic functions such as temperature, blood pressure, heart rate, cholesterol level, blood glucose, and so on [2]. RFID IoT enables the storage of complex data, wireless communication without line of sight, and automatic object identification and traceability. RFID technology was utilized for the first-time during WWII to identify between allied and hostile aircraft. RFID is a superior and more practical technology to work with items of diverse surfaces than outmoded barcodes, giving read/write capabilities without any visible contact and the ability to read numerous RFID tags at the same time. Researchers have investigated multiple aspects, ranging from technological advancements to RFID integration with other technologies, with the objective of streamlining IoT installations and attaining all of its capabilities in diverse businesses.

The level of safety of any system is established by flipping feed to the result, guaranteeing a relationship between key, plaintext, and ciphertext, and measuring attack complexity with linear and differential cryptanalysis. M. El-Haii et. al [3] investigated the various lightweight cryptosystems using Raspberry Pi and Arduino. According to the findings, each method is better in various respects, such as Speck for memory use, Rectangle for efficiency parameters, and Present for security, according to the findings. Yao et. al [4]used elliptic curve decisional Diffie Hellman (ECDDH) problem to address security challenges in IoT to reduce communication costs and improve execution efficiency. Yang et al. [5]used the keyword retrieval method to present a discrete, secure data administration for health tracking systems. Because different medical institutions monitor patients, distributed access between health institutions is required to make electronic health records viable. Singh et al. [6] proposed a lightweight combined algorithm that combines symmetry and asymmetry computational methods to improve the space environment. The four factors, namely data size, battery power, memory space, and processing power, are examined for threshold levels, and the suitable lightweight encryption, either symmetric or asymmetric, is applied. Nonetheless, a thorough description of the cypher framework,

Author is with Department of Mathematics, Amity Institute of Applied Sciences, Amity University Uttar Pradesh, Noida, India (e-mail: vandaniverma@yahoo.com).

key dimensions, block dimension, and privacy metrics is necessary. Al salami et al. [7] proposed a lightweight encryption algorithm for smart homes that provides privacy and security while maintaining a high level of performance and lowering overhead expenses. Biryukov et al. [8] conducted an extensive analysis of lightweight cryptographic basics and highlighted the benefits and drawbacks of IoT. He additionally emphasizes the necessity for ultra-lightweight cryptography and IoT cryptography specialized techniques.

II. BACKGROUND CONCEPTS

A. *Elliptical curves [9]*

Let the characteristics of the field F be ≠ 2, 3. Also consider a cubic polynomial $\alpha^3 + p\alpha + q$ where p, q ∈ F, with no multiple roots. Then the set of points (α, β) ∈ F that fulfils the equation $\beta^2 = \alpha^3 + p\alpha + q$ where I known as the point of infinity on the elliptical curve over field F. Assume E is an elliptical curve in the real number field, and U and V are two locations on E [10]. Now we define the negative of U and the sum U + V as follows:

Case 1: If U is the point at infinity and U+V is defined as V, we define -U to be I. This means that I become the additive identity of the point group. This suggests that neither V nor U is the infinite point.

Case 2: The negative of point U is the same as its negative y-coordinate which implies – (α, β) = (α, -β). As a result, anytime (α, β) appears on the curve, the point (α, -β) appears as well.

Case 3: If the x-coordinates of U and V differ, it is simple to see that the line l = UV crosses the curve at V, in this instance W = V, or at U, in that case W = U. Let us therefore define U + V as -W. That is, it is the mirror image of the third point of intersection with respect to the x-axis.

Case 4: If U = - V, which implies V has the same x-coordinate but a minus y-coordinate, then U + V = I, where I is the point of infinity.

Case 5: The final alternative is U = V. Then define U + V = - W as the tangent line to the curve at U and the sole other point of intersection of l with the curve as w. (W is considered to be U if the tangent line has “double tangency” at U, i.e. if U is a point of inflection).To find U + V, draw a chord through U and V, and take U + V to be the point symmetric with respect to x-axis, to the third point where the line through U and V intersects the curve. Use the tangent line to the curve at point U to determine 2U (assuming U and V are the same place), and 2U is the point symmetric to the third point where that tangent line crosses the curve.

B. *Architecture of IoT:*

The three layers of an IOT system architecture[11] (or application layer) are discussed as follows:

1) Perception layer:

It is the data source and the center of IOT. In this layer, sensors, wireless sensor networks (WSN), tags and reader-writers, RFID systems, cameras, global positioning systems (GPS), intelligent terminals, electronic data interface (EDI), objects, and other technologies sense and collect information from the physical environment.

2) Network Layer:

This layer, often known as the transport layer, contains the access network and the core network and enables fully transparent data transmission. The information from the perception layer can be sent to the upper layer using the existing mobile communication network, radio access network, wireless sensor network (WSN), and other communications equipment such as global system for mobile communications (GSM), general packet radio service (GPRS), worldwide interoperability for microwave access (WiMax), wireless fidelity (WiFi), Ethernet, and so on. Simultaneously, this layer delivers an efficient, dependable, and reliable network infrastructure platform to upper layer and large-scale industry applications.

3) Service Layer:

This layer, also known as the application layer, consists of the data management sub-layer and the application service sub-layer. The data management sub-layer processes complex data and uncertain information, such as restructuring, cleaning, and combining, and provides directory service, market to market (M2M) service, Quality of Service (QoS), facility management, geomatics, and other services through service-oriented architecture (SOA), cloud computing technologies, and other means. The application service sub-layer converts information to content and provides a suitable user interface for upper-level systems, applications, and end users, such as logistics and supply, disaster warning, environmental monitoring, agricultural management, and production management, among others.

TABLE I
DESIGN REQUIREMENTS OF IOT CRYPTOGRAPHY

Design requirements	Description
Type	They are Block cipher or sponge and as IoT devices execute many functions; a versatile primitive is required.
Block Size	96 bits is the bare minimum, larger sizes (M28 bits) must be preferred.
Key Size	At least 128 bits, because lesser keys may provide opponents simple access to the system.
Relevant Attacks	A far more conservative security model must be adopted as compared to classical ciphers.
SCA resilience	It is critical to install SCA countermeasures since loT devices can be physically attacked by adversaries in some instances.
Cryptographic Requirements	encryption, hashing, authentication
Implementation	The algorithm must be reasonably efficient on a variety of microcontrollers.

C. *Types of attack on different IoT layers [12] :*

1) Attacks on Perception Layer:

a) Eavesdropping: This type of attack attempts to steal information delivered through a network and utilize insecure transmission for confidentiality violation.
b) Node Capture: This attack completely seizes control of a crucial node, like a gateway node, and compromises it.
c) Fake Node and Malicious: Nodes stop sending actual data, endangering availability, and integrity by doing so.
d) Replay Attack: Attacker compromises authentication by stealing true information from the sender.
e) Timing Attack: weak computing capabilities of devices are used to extract secrets confidentiality.

2) Attacks on Network Layer

f) Denial of Service Attack: This attack prevents legitimate users from gaining access to devices or other system resources, posing availability and authorization issues.
g) Man-in-The-Middle Attack: This attack captures and modifies communications while also violating confidentiality, integrity, and authentication.
h) Storage Attack: The user's information may be modified to inaccurate details as a result of information replication at storage.
i) Exploit Attack: Takes control of the system and steals data from a network. Occurs because of security flaws in an application, system, or hardware, resulting in a violation of confidentiality.

3) Attacks on Application layer

a) Cross Site Scripting: An attacker modifies the application's contents to compromise its integrity.
b) Malicious Code Attack: This attack damages the system and has unintended consequences, jeopardizing its confidentiality, integrity, and availability.
c) Mass Data dealing: The capacity for bulk data dealing results in network disruption and data loss, placing availability under threat.

D. Need of lightweight cryptography for IoT [13]

For the following reasons, IoT needs lightweight cryptography:

a) Efficient end-to-end communication: End nodes must be equipped with a symmetric key method to ensure end-to-end security. It is critical for resource constrained IoT devices to have a cryptographic process that consumes less resources. End-device implementation of a lightweight symmetric key method consumes less energy
b) Applicability to resource-constrained devices: Lightweight cryptographic primitives use up less space than traditional primitives. As a result, even on resource-constrained devices, lightweight cryptographic primitives would expand the possibility of more network connections.
c) Scalability: Scalability becomes a major challenge with the widespread deployment of IoT devices in many applications. Lightweight cryptographic algorithms are simple to implement across a wide range of devices, allowing for smooth deployment and maintenance.
d) Real-time processing: Real-time processing is critical in certain IoT applications. Heavy cryptography processes may cause delays and impair IoT device responsiveness. Lightweight cryptographic algorithms are meant to be quick and use minimal processing time as possible.
e) Security: While lightweight cryptography is designed for resource-constrained devices, it nevertheless provides enough security for the majority of IoT applications. It seeks to achieve an appropriate balance between resource effectiveness and cryptographic resilience, ensuring that IoT devices are appropriately protected against a wide range of security threats.

III. PROPOSED LIGHT WEIGHTAUTHENTICATION PROTOCOL

In this section, we propose mutual authentication protocol between RFID Tag and Reader based on elliptical curve cryptography where both authenticate each other through several rounds of communication:

A. Setup Phase:

In this phase both reader and tag are familiarized with the public parameters namely F_q (Finite field of size q), a, b (elliptic curve parameters E, $\beta^2 = \alpha^3 + p\alpha + q$ on F_q, P (Generator point) and hash function H. The reader then selects a random value for his secret key: $y \in Zq$ and computes the public key as $Y = yP$. It also maintains the tag's secret key as $x \in Zq$ and public key $X = xP$ as well as the ordered pair (x, X) in its database.

B. Authentication Phase:

Authentication process carried out between the reader and the tag as follows:

Step 1: The reader picks a random number $r_1 \in Zq$ and perform operations

$$S_1 = r_1^{-1} P \text{ and } S_2 = S_1 \oplus y X.$$

Then, S_2 is communicated to the tag.

Step 2: *T*ag on receiving S_2 decide on a randomized number $r_2 \in Zq$ and with the help of private key *x* and the public key *X*, Tag computes

$$T_1 = r_2^{-1} P, T_2 = S_2 \oplus xY,$$
$$T_3 = r_2^{-1} T_2 \text{ and } T_4 = T_1 \oplus xY$$

Now, T_3 and T_4 are forwarded to the reader.

Step 3: Reader on receiving T_3 and T_4 perform operations

$$S_3 = T_4 \oplus yX \text{ and } S_4 = r_1^{-1} S_3$$

checks *if* $S_4 = T_3$.

If T_3 is equal to S_4 then Tag is authentic or else the communication is discontinued.

In case of authentic tag, reader computes $S_5 = H(S_3)$ and forwards it to tag.

Step 4: Tag on receiving S_5 checks *if* $S_5 = H(T_1)$.

If found true, tag confirms that reader is authentic, and communication is established.

TABLE II
READER TAG AUTHENTICATION PHASE

(i) Reader		**Tag**
$r_1 \in Z_q$ $S_1 = r_1^{-1} P$ $S_2 = S_1 \oplus y X$	S_1 →	$r_2 \in Zq$ $T_1 = r_2^{-1} P$ $T_2 = S_2 \oplus xY$ $T_3 = r_2^{-1} T_2$ $T_4 = T_1 \oplus xY$
	← T_3, T_4	
$S_3 = T_4 \oplus yX$ $S_4 = r_1^{-1} S_3$ checks *if* $S_4 = T_3$		
If Tag is authentic, then server computes $S_5 = H(S_3)$	S_5 →	checks *if* $S_5 = H(T_1)$ If found true, *then Server is authentic*

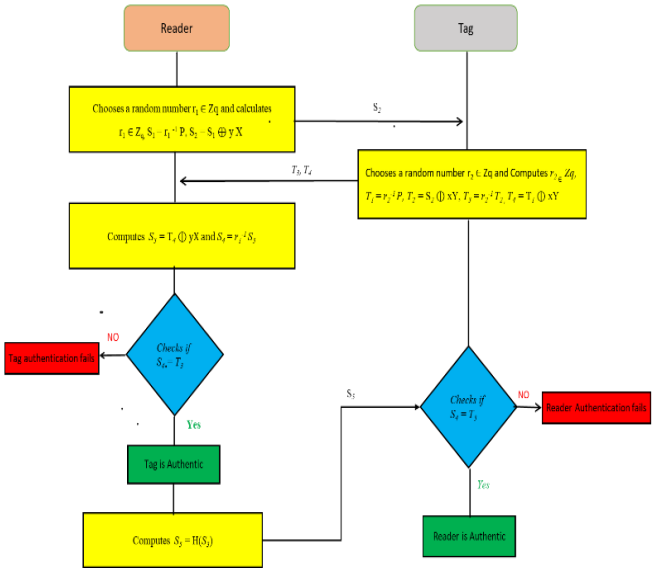

Fig. 1. Proposed mutual Authentication Protocol

IV. SECURITY ANALYSIS

The following is a security analysis of the proposed scheme (Figure1) is as follows:

A. Availability:

The proposed algorithm is easily accessible. No more changes to the private key are necessary to run the proposed protocol. As a result, the execution procedure will go off without a hitch. So, our technique ensures availability.

B. Mutual Authentication:

Without knowing the values of r_1, or the random number selected by the reader and the reader's private key, we are unable to produce the S_1 in our proposed protocol. Only the reader is aware of these values, which were not transmitted to the tag. As a result, both values can preserve their concealment. Values can thus only be kept on the reader. The values of r_2, or the randomized number selected by the tag and secret key of the tag, are also required in order to determine the values of T_3 and T_4. Therefore, the method we provide supports mutual authentication.

C. Anonymity:

Different secret keys that were never shared throughout the whole procedure exist between the tag and the reader. The reader's private key is y, and the tag contains a secret key x. They are both impossible to reach. Consequently, our suggested methodology ensures anonymity.

D. Cloning Attack:

Both the tag and the reader in our proposed technique have unique private keys of their own. Any hacker attempting to obtain these secret keys will fail since there is no linkage between the secret keys. The hacker is thus unable to do so. Consequently, our proposed technique can defeat cloning attacks.

E. Impersonation Attack:

If we follow our proposed protocol, the hacker cannot produce S_5 without knowing S_1, S_2, S_3, and S_4 because the hacker has no understanding of x, r_1, y, and r_2. In order to prevent impersonation attempts, our suggested strategy is effective.

F. Location Tracking Attack:

If the hacker attacks the reader's private key y, the hacker will never be able to obtain the tag's secret key x or the random variables r_1 and r_2 determined by the reader and the tag. As a result, no proof of the interaction between the reader and the tag exists. As a result, our suggested solution can withstand the danger of location monitoring.

G. Replay Attack:

We can see in our suggested protocol that the computed value of S_1 was replayed to tag, and therefore S_4 cannot be acquired by receiving the operations T_2 and S_2 since the reader is unaware of the tag's private key x and random number r_2. As a result, by comparing S_4 to S_2, the tag is unable to identify the hacker. Similarly, by confirming the matching of S_3, the reader is no longer capable of locating the hacker and can detect the replay attack. As a result, our proposed technique can survive a replay attack.

H. DoS Attack:

Since the tag x's secret key isn't transmitted throughout the authentication process, it doesn't need to be updated. Therefore, the presented protocol overcomes DoS attack.

I. Reader Spoofing Attack:

Because the attacker is uninformed of the tag secret key x and y (the reader's private key), he is unable to clone the reader to the tag. As a result, reader-to-tag impersonation is not feasible. As a result, our suggested protocol is resistant to reader spoofing attacks.

J. Forward Security:

If we assume that the private key of the tag can be obtained. Then because of the unawareness about the random numbers r_1 and r_2, there is no confirmation if the messages T_1 and T_2 are being transmitted among them. Hence, our proposed scheme provides forward security.

V. RESULT AND DISCUSSION

Here we discuss the security analysis and effectiveness of the proposed approach to RFID authentication schemes existing in literature on the basics of various system requirements and calculations required for the construction like addition over elliptical curve, total no. of communications, random number requirements and multiplication Zq and Elliptic curve over ECC for construction of the schemes. For the simplicity we consider

- AT-1: Availability
- AT-2: Mutual authentication
- AT-3: Anonymity
- AT-4: Cloning Attack
- AT-5: Impersonation Attack
- AT-6: Location Tracking Attack
- AT-7: Replay Attack
- AT-8: DoS Attack
- AT-9: Reader Spoofing/ Masquerade Attack
- AT-10: Forward security
- AT-11: Confidentiality
- AT-12: Scalability
- PR: Proposed

From Table III we can see that our proposed scheme is more secure than [14], [15], [16], [17], [18], [20], [21], [22], [24] and

[25] as it can overcome all the probable attacks (discussed in detail section 4). Although we can also see that [19] & [23] have the same security features as our proposed scheme, so to show the effectiveness of the proposed approach we compare the execution time taken to calculate hash functions in each scheme as given in Table IV.

TABLE III
SECURITY ANALYSIS

Ref # / Attack	AT-1	AT-2	AT-3	AT-4	AT-5	AT-6	AT-7	AT-8	AT-9	AT-10	AT-11	AT-12
[14]	x	x	x	x	x	√	√	√	x	x	x	x
[15]	x	x	√	x	√	√	√	√	x	√	x	x
[16]	√	√	x	√	√	x	√	√	√	x	√	x
[17]	√	√	x	√	√	√	√	√	√	√	√	x
[18]	√	√	x	x	√	√	√	x	√	√	√	√
[19]	√	√	√	√	√	√	√	√	√	√	√	√
[20]	*	√	*	*	*	*	*	*	x	√	√	*
[21]	√	√	√	√	√	√	√	√	x	x	√	√
[22]	√	√	√	√	√	√	√	√	x	√	√	√
[23]	√	√	√	√	√	√	√	√	√	√	√	√
[24]	x	√	x	x	x	x	x	x	x	x	√	√
[25]	*	√	√	x	√	√	√	x	*	x	x	x
PR	√	√	√	√	√	√	√	√	√	√	√	√

** Information not provided in research paper*

TABLE IV
EXECUTION TIME

Ref #	H_T	H_R	Total	Execution Time (in ms)
[14]	2	5	$2H_T + 5H_R$	0.0161
[15]	2	3	$2H_T + 3H_R$	0.0115
[16]	4	6	$4H_T + 6H_R$	0.023
[17]	3	5	$3H_T + 5H_R$	0.0184
[18]	5	7	$5H_T + 7H_R$	0.0276
[19]	2	4	$2H_T + 4H_R$	0.0138
[20]	4	3	$4H_T + 3H_R$	0.0161
[21]	2	2	$2H_T + 2H_R$	0.0092
[22]	2	2	$2H_T + 2H_R$	0.0092
[23]	2	2	$2H_T + 2H_R$	0.0092
[24]	2	4	$2H_T + 4H_R$	0.0138
[25]	2	4	$2H_T + 4H_R$	0.0138
PR	1	1	$1H_T + 1H_R$	0.0046

The table illustrates the execution time for each method while using the same environment as [19] to run our suggested approach. We assessed in the previous section that [19] and [23] have the same security properties, but now we observe that the execution time of [19] is $2H_T + 4H_R$ which equals 0.0138ms.

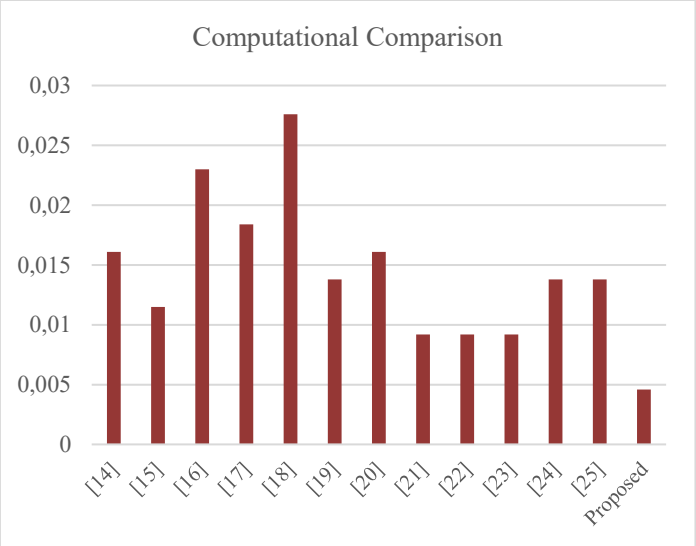

Fig. 2. Computational Comparison

Furthermore, [23] takes 0.0092ms to execute owing to $2H_T + 2H_R$. However, if we look at our suggested strategy, it only takes $1H_T + 1H_R$ or 0.0046ms to execute. As a result, our technique requires reduced execution time while maintaining full security.

VI. CONCLUSION

Traditional cryptographic primitives take up more space than lightweight cryptographic primitives, but lightweight cryptographic algorithms are simple to install and maintain across a wide range of devices as they are designed to be as quick and as efficient as possible. Here we have presented lightweight mutual authentication protocol for RFID tag and reader based on elliptical curves which is designed for low-resource devices. It has also been shown that the proposed scheme is faster as compared to [14], [15], [16], [17], [18], [19], [20], [21], [22], [23], [24] and [25] and provides more security for the vast majority of IoT applications.

VII. REFERENCES

[1] M. Shukla, J. Lin, and O. Seneviratne, "BlockIoT: Blockchain-based Health Data Integration using IoT Devices," in *AMIA Annu Symp Proc.2021*, 2021, pp. 1119–1128. Accessed: Jan. 30, 2023. [Online]. Available: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8861710/

[2] M. M. Modiri, J. Mohajeri, and M. Salmasizadeh, "GSLHA: Group-based Secure Lightweight Handover Authentication Protocol for M2M Communication," *The ISC International Journal of Information Security*, vol. 12, no. 2, pp. 101–111, Jul. 2020, http://doi.org/10.22042/ISECURE.2020.213482.507

[3] M. El-hajj, H. Mousawi, and A. Fadlallah, "Analysis of Lightweight Cryptographic Algorithms on IoT Hardware Platform," *Future Internet 2023, Vol. 15, Page 54*, vol. 15, no. 2, p. 54, Jan. 2023, http://doi.org/10.3390/FI15020054

[4] X. Yao, Z. Chen, and Y. Tian, "A lightweight attribute-based encryption scheme for the Internet of Things," *Future Generation Computer Systems*, vol. 49, pp. 104–112, Aug. 2015, http://doi.org/10.1016/J.FUTURE.2014.10.010

[5] Y. Yang, X. Zheng, and C. Tang, "Lightweight distributed secure data management system for health internet of things," *Journal of Network and Computer Applications*, vol. 89, pp. 26–37, Jul. 2017, http://doi.org/10.1016/J.JNCA.2016.11.017

[6] S. Singh, P. K. Sharma, S. Y. Moon, and J. H. Park, "Advanced lightweight encryption algorithms for IoT devices: survey, challenges and solutions," *J Ambient Intell Humaniz Comput*, pp. 1–18, May 2017, http://doi.org/10.1007/S12652-017-0494-4/METRICS

[7] S. Al Salami, J. Baek, K. Salah, and E. Damiani, "Lightweight encryption for smart home," *Proceedings - 2016 11th International Conference on Availability, Reliability and Security, ARES 2016*, pp. 382–388, Dec. 2016, http://doi.org/10.1109/ARES.2016.40

[8] A. Biryukov and L. Perrin, "State of the Art in Lightweight Symmetric Cryptography," *ArXiv*, 2017.

[9] V. Verma and D. Gupta, "An efficient signcryption algorithm using bilinear mapping," in *Proceedings of the 10th INDIACom; 2016 3rd International Conference on Computing for Sustainable Global Development, INDIACom 2016*, 2016.

[10] P. Mishra, Renuka, and V. Verma, "Identity Based Broadcast Encryption Scheme with Shorter Decryption Keys for Open Networks," *Wirel Pers Commun*, vol. 115, no. 2, 2020, http://doi.org/10.1007/s11277-020-07606-6

[11] X. Jia, Q. Feng, T. Fan, and Q. Lei, "RFID technology and its applications in Internet of Things (IoT)," in *2012 2nd International Conference on Consumer Electronics, Communications and Networks, CECNet 2012 - Proceedings*, 2012, pp. 1282–1285. http://doi.org/10.1109/CECNet.2012.6201508

[12] V. Chegeni, H. Haj Seyyed Javadi, M. Reza, M. Goudarzi, and A. Rezakhani, "Providing a Hybrid Cryptography Algorithm for Lightweight Authentication Protocol in RFID with Urban Traffic Usage Case," vol. 13, no. 1, pp. 73–85, 2021, http://doi.org/10.22042/isecure.2020

[13] L. M. Shamala, G. Zayaraz, K. Vivekanandan, and V. Vijayalakshmi, "Lightweight Cryptography Algorithms for Internet of Things enabled Networks: An Overview," *J Phys Conf Ser*, vol. 1717, no. 1, p. 012072, Jan. 2021, http://doi.org/10.1088/1742-6596/1717/1/012072

[14] J. ; Yang, J. Park, H. Lee, K. Ren, and K. Kim, "Mutual authentication protocol for low-cost RFID.," in *In Proceedings of the Workshop on RFID and Lightweight Cryptography*, Graz, Austria, Jul. 2005, pp. 17–24.

[15] C. C. Tan, B. Sheng, and Q. Li, "Secure and Serverless RFID Authentication and Search Protocols," *IEEE Trans Wirel Commun*, vol. 7, no. 4, pp. 1400–1407, Apr. 2008, http://doi.org/10.1109/TWC.2008.061012

[16] S. Cai, Y. Li, T. Li, and R. H. Deng, "Attacks and Improvements to an RIFD Mutual Authentication Protocol and Its Extensions," in *Proceedings of the Second ACM Conference on Wireless Network Security*, in WiSec '09. New York, NY, USA: Association for Computing Machinery, 2009, pp. 51–58. http://doi.org/10.1145/1514274.1514282

[17] J. S. Cho, Y. S. Jeong, and S. O. Park, "Consideration on the brute-force attack cost and retrieval cost: A hash-based radio-frequency identification (RFID) tag mutual authentication protocol," *Computers & Mathematics with Applications*, vol. 69, no. 1, pp. 58–65, Jan. 2015, http://doi.org/10.1016/J.CAMWA.2012.02.025

[18] P. Gope and T. Hwang, "A Realistic Lightweight Anonymous Authentication Protocol for Securing Real-Time Application Data Access in Wireless Sensor Networks," *IEEE Transactions on Industrial Electronics*, vol. 63, no. 11, pp. 7124–7132, 2016, http://doi.org/10.1109/TIE.2016.2585081

[19] K. Mansoor, A. Ghani, S. A. Chaudhry, S. Shamshirband, S. A. Khan Ghayyur, and A. Mosavi, "Securing IoT-Based RFID Systems: A Robust Authentication Protocol Using Symmetric Cryptography", http://doi.org/10.3390/s19214752

[20] H. Shen, J. Shen, M. K. Khan, and J. H. Lee, "Efficient RFID Authentication Using Elliptic Curve Cryptography for the Internet of Things," *Wirel Pers Commun*, vol. 96, no. 4, pp. 5253–5266, Oct. 2017, http://doi.org/10.1007/S11277-016-3739-1/METRICS

[21] Z. Zhang and Q. Qi, "An efficient RFID authentication protocol to enhance patient medication safety using elliptic curve cryptography," *J Med Syst*, vol. 38, no. 5, pp. 1–7, Apr. 2014, http://doi.org/10.1007/S10916-014-0047-8/METRICS

[22] M. S. Farash, O. Nawaz, K. Mahmood, S. A. Chaudhry, and M. K. Khan, "A Provably Secure RFID Authentication Protocol Based on Elliptic Curve for Healthcare Environments," *J Med Syst*, vol. 40, no. 7, p. 165, 2016, http://doi.org/10.1007/s10916-016-0521-6

[23] V. Kumar, R. Kumar, A. A. Khan, V. Kumar, Y. C. Chen, and C. C. Chang, "RAFI: Robust Authentication Framework for IoT-Based RFID Infrastructure," *Sensors*, vol. 22, no. 9, May 2022, http://doi.org/10.3390/s22093110

[24] M. Safkhani, P. Peris-Lopez, J. Cesar Hernandez-Castro, N. Bagheri, and M. Naderi, "Cryptanalysis of Cho et al.'s Protocol, A Hash-Based Mutual Authentication Protocol for RFID Systems," *IACR Cryptology ePrint Archive*, vol. 2011, no. 2011, pp. 1–7, 2011, Accessed: Apr. 27, 2022. [Online]. Available: https://eprint.iacr.org/2011/331.pdf

[25] B. Liu and X. Su, "An Anti-Collision Algorithm for RFID Based on an Array and Encoding Scheme," *Information*, vol. 9, no. 3, 2018, http://doi.org/10.3390/info9030063