Alkadhim Journal for Computer Science, Vol. 2, No. 1 (2024)

Open Access ISSN: 3007-1437 (Online), ISSN: 3007-1429 (Print)

IRAQI Academic Scientific Journals

Alkadhim Journal for Computer Science (KJCS)

Journal Homepage: https://alkadhum-col.edu.iq/JKCEAS

KJCS ALKADHIM JOURNAL FOR COMPUTER SCIENCE

A Robust Privacy Preserving Authentication Scheme for IOT Environment by 5G Technology

[1,2,*]ALI D. KHALAF

[1]Department of Computer Engineering, Faculty of Engineering, Shahid Chamran University of Ahvaz, Ahvaz, Iran.

[2]Missan Oil Company ,Missan-Iraq

Article information

Article history:
Received: November, 08, 2023
Accepted: February, 23, 2024
Available online: March, 14, 2024

Keywords:
IOT,
Authentication,
security,
privacy,
ECC algorithm

Corresponding Author:
Ali D. Khalaf
alialdelfy52@gmail.com

DOI:
https://doi.org/10.53523/ijoirVolxIxIDxx

Abstract

In recent years, secure communication between the interconnected components of the internet of things has become an important and worrying issue due to some attacks on the IoT. The Internet of Things (IOT) is the integration of things with the world of the Internet, where this integration takes place by adding devices or programs to be smart and, as a result, they will be able to communicate with one another and participate in all elements of life quite efficiently. Accordingly, we've developed an authentication protocol for the IoT ecosystem; it's primary function is to ensure the safety of data exchange between the many devices that make up the IoT. Our proposed protocol is based on the elliptic curve cipher (ECC) algorithm, which greatly aids in protecting IoT components from physical assault. Our informal protocol analysis demonstrates that our solution not only protects users' privacy by concealing their devices' identities but also thwarts impersonation, counterattacks, and tracking and suggestion attacks directed at IoT devices. Security characteristics of the proposed protocol are also explicitly examined with the help of the (SCYTHER) program. In addition, the effectiveness of the suggested protocol is evaluated by determining both its excess costs and its communication costs. Therefore, it appears that the protocol is vastly superior than the many other equivalent protocols by assessing its performance and security.

1. Introduction

In recent years, the world has witnessed many developments, and these developments have facilitated many things as well These developments in information technology and devices have led to the rapid deployment of billions of interconnected devices and smart services in critical infrastructures such as health, transportation[1], environmental control and data transmission over the network Need or reference to any kind of interaction between humans and computers or interaction between humans themselves where Brings confidence and convenience to consumers.

Therefore, companies specializing in information technology began to live in a terrible rush towards the so-called Internet of things or internet of beings [2]. As it is the integration of things with the world of the Internet, where this integration takes place by adding hardware or software to be Intelligent and as a result are able to communicate

with each other and participate very effectively in all aspects everyday life [3]. As a result, it will enable us to give new modes of communication among humans and things, and even between things themselves Thus, this leads to changing the old traditional life to a better and better lifestyle, but not to be It's that easy because there are still many risks and challenges and many problems that need to be addressed Processing and security in order to realize the full potential and to provide a good and safe life for users[4] , therefore, privacy and authentication are important things that must be available in IoT devices, so in our research, we address a protocol that preserves the privacy of the Internet of Things and is secure against attacks[5].

2. Related Works

In the past years and to this day, researchers have reached and are still reaching to provide protocols to provide security, privacy and authentication for users in the Internet of things environment. There are two classes of authentication protocols for securing the IoT environment depending on the type of connection:

1) Devices (Internet of Things devices) .

2) Achieving communication between internet of things devices and the server.

El.hajj et al [6], Das et al [7], Ferrag et al [8] they scanned several authentication processes for the internet of things environment. Where this protocol was developed using different technologies an The digital signature, along with private and public key cryptography are all good examples of this, and physical uncopiable functions (PUF), in addition to the mechanism that relies on (AKA).

2.1 The mechanism that depends on the AKA mechanism

In a similar vein, the use of a password or other kind of authentication to restrict access to a computer system is a security risk. Many methods, also known as [9, 10], [11], have been developed to ensure users' security and privacy in the context of the Internet of Things.

In 2008, Jeong et al. [12] introduced an AKA protocol that makes use of an OTP and a smart card to secure domestic settings. Their system is similar to that of Jeong et al. [12], in that it protects users from a wide range of scyther attacks, but unlike Jeong et al. However, they are vulnerable to security issues like smart card theft and unauthorized access. Additionally, non-authentication occurs because the mutual authentication protocol between the gateway and the smart device is not implemented. The ability to monitor and conceal the identity of a genuine plaintext user during transmission via an open network card and one-time password was broken. Security flaws such as smart card attacks and offline password guessing were taken. A scheme (also known as safe) that employs a card-based one-time password was proposed and lightweight AKA method based on ECC Smart Home Networks was developed. In 2011 by vaidya et al[13], but it was vulnerable to password guessing attacks, insider impersonation, and going offline.In 2015, Santos et al. [14] reported a secure AKA method using ECC in smart home contexts; nevertheless, their protocol was not safe against stolen validators and internal assaults.

In 2019, Shuai et al. [15] propose a minimal AKA mechanism dependent on The security of smart houses may be proven with ECC.

In 2020, Wazid et al. [16] introduced symmetric-key cryptography and an efficient AKA scheme based on to the retail function of smart homes; however, Lyu et al. [17] discovered in their scheme that the Scheme of Wazid et al. [16] is vulnerable to compromised servers and desynchronization attacks.

2.2 The mechanism that depends on the Private key mechanism

Private keys are used to encrypt and decode data in symmetric, asymmetric, and cryptocurrency cryptography. Only the keys generator or authorized parties should have access to them.

In 2015 Sun et al[18]. presented a key agreement authentication system utilizing function hashes and the Advanced Encryption Standard (AES), but it does not use authentication-safe methods. Since protecting individual confidentiality was not a priority for the writers.

In 2017 Jan et al. [19] proposed a key agreement and protocol based on payloads. Using the Internet's sensor network while retaining user anonymity (AES). An enhanced authentication technique for domestic systems was created by in 2017 Song et al. [20] They employed Message Authentication Codes (MAC) to send and receive information.

2.3 The mechanism that depends on the public key:

A free key is a large number that is used for encryption and is made available to the public through a central repository or directory. Public keys can be generated by computer programs, but more commonly they are issued by a trusted, designated authority and posted online for all to see. In comparison to the IoT method (RSA), elliptic curve cipher(ECC) is the current standard for authentication protocols[21] - [26] due to its suitability for low-power devices.

In 2015 Klare and Soo [23] first presented an ECC-based Internet-based key agreement and authentication framework. Things where it was claimed that the protocol included basic safety features. However, research by Chang et al. [26] into the kalra and sood protocol [23] revealed that it lacks essential security features like authentication and consensus on a shared session key. An enhanced protocol has been developed to address the security concerns with the Kalra and Sood method [23].

In 2017, Wang et al. [24] demonstrated that the procedure developed by Zhang et al. By eliminating the need for a password and modifying the method in which individual messages are tallied, they made the protocol better for Zhang et al[27].Kalra and Sood's [23] method was studied . In 2018 by Kumari et al. [28], who found that it fails to provide device anonymity, mutual authentication, and session key agreement. To cut a long story short, we have a problem. The problem is that we have kumari et al[28] will not be successful without access to the internet and protection from internal threats. Recently, Maarof et al.[25] looked at their enhanced ECC-based key agreement methodology.

2.4 The mechanism that depends on the signature

It's a mathematical technique for making sure anything digital is what it claims to be.It improves security and attempts to address issues with digital communications, such as impersonation and tampering. The Prediction-Based Authentication (PBA) protocol proposed.

in 2016 by Liu et al[29], is based on the Merkel signature tree scheme(MSS) [30] storage and Merkel signature tree scheme(MSS) and self-storage, and it is capable of withstanding packets and attacks(DoS), though its authors did not investigate the issue of privacy.Scheme(MSS) gives a lengthier signature and a longer key, and in 2018 salmdamli et al [31] investigated the 3-5- The mechanism that depends on PUF

In many respects, PUFs are the inanimate counterpart of biometrics in that they are novel physical security primitives that provide unclonable and intrinsic instance-specific measurements of physical items.Since they can produce and store secrets safely, we can use them to quickly build a physical information security infrastructure.Neither of the two PUF-based authentication approaches proposed for IOT architecture by Aman et al in 2017, [32] is enough to fulfill security requirements.

In 2019, Gope and Sikadar[33] proposed a master method accord for internet of things devices, and this protocol is well suited to IoT devices.

although the writers did not employ the synchronized number approach for the identification, their method is exposed to a separation attack and inadequate for guaranteeing complete confidentiality and safety.

In 2019 Chikouch et al [34], their protocol fails to resist an impersonation attack as well defined information leak attack resistance.

Although we have reviewed several protocols, authentication schemes, and major and different agreements, yet most of these protocols and schemes are insecure and vulnerable to many attacks where they cannot be blocked these attacks also call into question the ineffectiveness of some of these protocols and schemes environments that have limited resources so the weaknesses and defects in the protocols and the schemes mentioned above urge us to present a system that must be capable of resisting any security threats, so we will propose a security scheme authentication agreement scheme lightweight and has the ability to resist attacks in the Internet of things environment .

3. Preliminaries

In this section, we first explain the architecture of the internet of things system, then the security and privacy requirements in the internet of things environment, and finally the mathematics tool used in our proposed protocol.

- IOT SYSTEM ARCHITECTURE

The architecture of the internet of things consists of two main components:

1- A group of Internet of Things devices.

2- Internet of Things Server [35].

The purpose of these applications is to provide a good life, convenience and reliability for users such as smart transportation and smart communication.

- MATHEMATICAL TOOLS

we'll give you a quick primer on elliptic curves cipher (ECC) [36 – 38] algorithm, which we rely on in our research it is an algorithm proposed by Miller 1985[39] , which has been widely used in designing algorithms from that time to the present day, For the same degree of security with a lower key size [40] We assume that F_p It represents the domain of a finite

number, as is P a large prime number, and the E indicates the elliptic curve is through F_p , and this depends on the following equation : 〖 y〗^2=x^3+ax+b mod p Where (4a^3+27b^2) mod p ≠ 0 And x,y,a,b∈F_p , Let 0 It is an unlimited point, and is G a group that is additive with q and generates p , added group G contains all points of the elliptic curve, where we assume p and Q are two places on the elliptic curve The blister addition process in G is defined as P+ Q=R the numerical point in g is multiplied and defined as S.P=P+ P+⋯+P (s times).

(ECDLP),[41] is the question of the discrete logarithm of the elliptic curve is mathematically useless and is based on E and gives two P points and Q of J The primary goal of (ECDLP) is to discover an integer s that fulfills Q=s.P.

4. Proposed Scheme

Our proposed scheme will be of three stages. In the first stage, the system parameters are initialized by a server, in the second stage, registration takes place, and in the third stage, the mutual authentication process takes place with the server to start the search and perform the verification of operating operations.

The table below lists the most common notations and their expansions.

Table (1): list of notations used

Notations	Expansions
D	The IoT Device
S	Server of the system
E	An elliptic curve
G	An additive group based on E
P	A generator of G
P, q	Large prime numbers
K_s,K_p	Private and public key of S
h	The hash functions
RID_d	Real identities of the D
PID_d	Pseudonyms of the devices
r	Random integer
$Pass$	Password
‖	Concatenation operator
$\oplus$	Exclusive oR (XOR) operation
SK	Secure the key
T, T_r, ΔT	The timestamp of the signature

4.1 Initialization phase

During this phase, the server system it creates the initial system parameters and following the steps, It also refreshes the system settings to keep the machine secure.

1) The server system chooses two large primes (p, q) as well as an additive group $(G)$with the system(q) in which it is constructed (p) ,an additive set (G) contains all points of the elliptic curve$(E)$and is determined by the equation $y^2 = x^3 + ax +$ b mod p Where $a, b \in F_p$

2) The server system produces a random number $Ks \in Z^*q$ In the form of a private key, it Calculates the public key $K_p = K_s \,.\, P$

3) The server system chooses the hash functions h .

4) The server system publish the queried system parameters ={q , K_p,P , h }.

4.2 Registration Phase

This Phase aims to register the device in this phase ,the server generate real identity RID_d for the device and upload it to the device via secure channel.

4.3 Authentication Phase

In this Phase, the login is done, as the device joins S and to start the authentication system, this is implemented in the following steps :

Step 1 : The D generates a random integer $r \in Z_q^*$ and computes PID_{d1} $PID_{d1} = r.p$ and PID_{d2} $= RID_d \oplus h\,(r.\,K_p)$, Then , the D sends $\{T_1, PID_d, \sigma$d$\}$ to the S,

Where , $PID_d = \{PID_{d1}, PID_{d2}\}$ and σd = h $(T_1 \| RID_d)$

Step 2: after the S received the message $\{T_1, RID_d, \sigma$d$\}$ it first starts checking the timestamp T_1, where the timestamp is defined as follows.

assume that (T_r) it is reception time and (T) is a predetermined delay, If $(T > T_r - T)$ then the time will be correct , Otherwise, the message is rejected ,.

If the time $T_1$is correct, we calculate $RID_d$where

$RID_d = PID_{d2} \oplus h$ (r . RID_{d1}) , and checks whether σ_d = ? $h(T_1 \| RID_d)$
If this is not the case, then S refuses to send the message, otherwise , it completes the process by checking the (RID_d) with the stored one ,
If not equel , S drops the message and the device is determined as not real , , otherwise , it computes SK where ,
$SK = h\ (RID_d \| K_s)$
$SK^* = SK \oplus RID_d$
$\sigma_s = h\ (SK \| T_2)$
After that , the S send $\{T_2 , SK^*, \sigma_s\}$ to D

Step 3: After to receive D the message from S that is First check the timestamp ,Where if it is correct, then D calculates SK
Where , $SK = SK^* \oplus RID_d$
Also after that check the σ_s where
σ_s= ? $h\ (SK \| T_2\ )$
Where if so , the device will use the SK for secure communication with S.

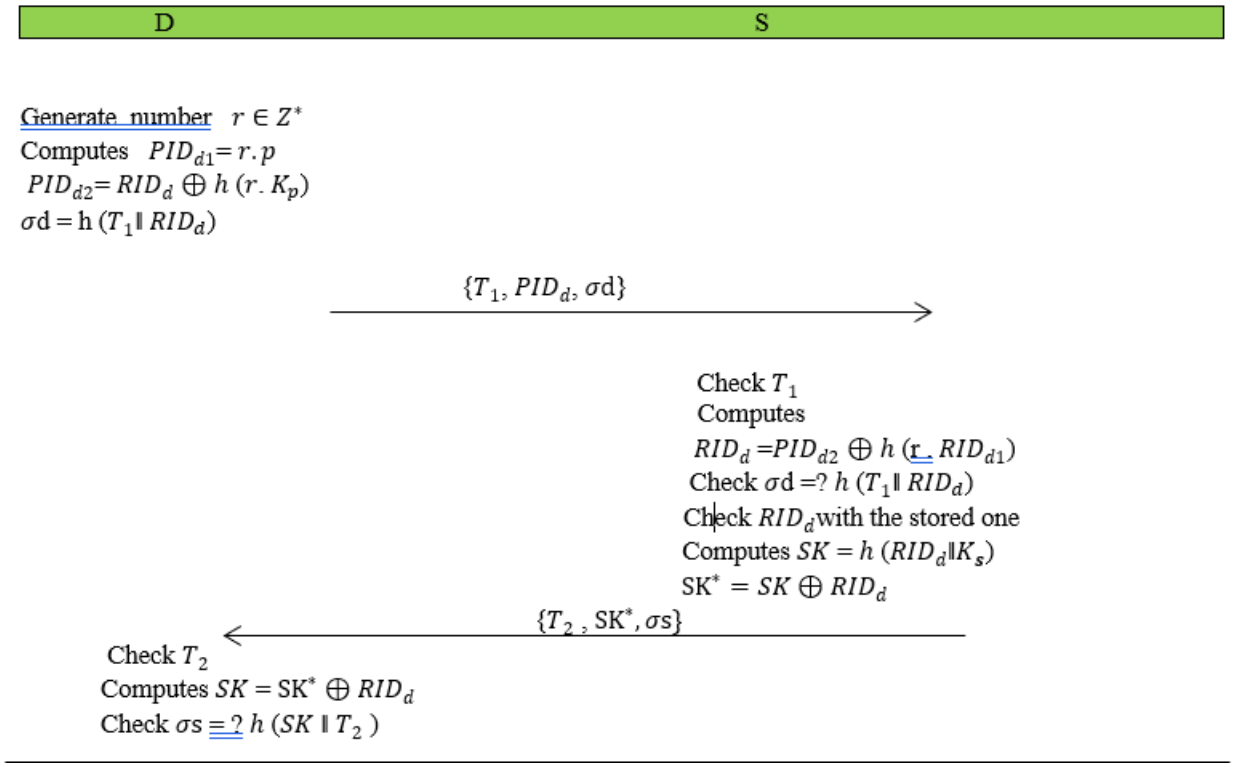

Figure (1): The steps of authentication phase

5. Security analysis and comparison:

We give a security analysis of our suggested strategy in this section, and for a purpose prove that our prtocol is of a strong security nature through elliptic curve cipher(ECC), and to make sure that the scheme meets all needs for security and privacy, so we will divide the analysis into two parts :

5.1. Formal security verification using scyther tool

In order to prove that our proposed scheme is safe against attacks, in this section we use one of the most widely used and recognized tools for security protocols and applications of the Internet of Things environment, which is (Scyther).

The Scyther is one of the most modern testing tools developed as symbols (Cremers) at the Technology Eindhoven University [42] , and it has a graphical interface in which the analysis of security protocols is performed by one click of a button, where these lines include commands that write commands in the Python language[43], in this tool the protocol description and parameters are taken The other is as an entry, and as for an exit, it provides a summary report and displays a diagram for each attack[44]. The figure(2)[45] shows the mechanism of action of this tool.

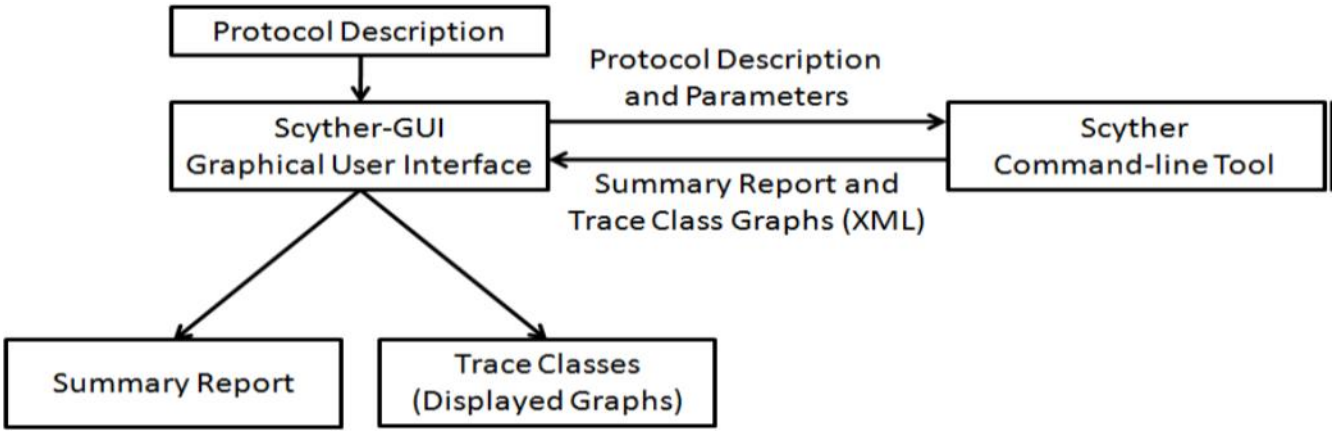

Figure (2): How does the scyther work?

Where we modeled the proposed protocol in the security protocol description language (SPDL) using scyther

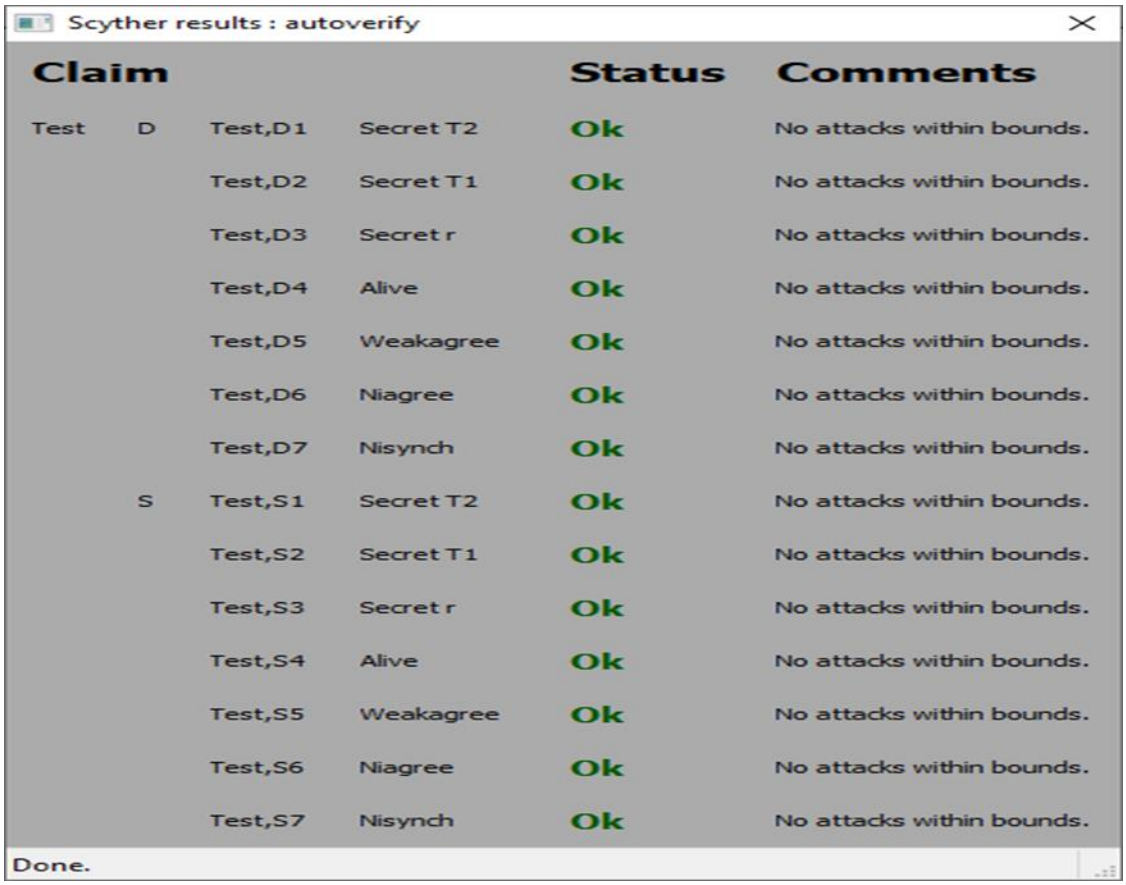

Figure (3): scythe security protocol verification

As a result, figure (3) depicts the validation of the suggested protocol using the scyther tool

5.2. Informal security analysis

In this subsection, it is shown that the proposed protocol can resist the following potential security attacks:

1) privacy and inaccessible

In the proposed protocol, the real identity 〖RID〗_d is a personal identity of D that is not explicitly exchanged on the general channel, although an interim identity is handed over by D in each session. Renew it after each session and a random number in each message that is sent to make it different. Therefore, after analyzing two different messages from the same D, it was found that the attacker could not be traced, nor could he access the location of the device. Therefore, our proposed protocol meets the requirements of preserving privacy.

2) Physical attack on an IoT device

Suppose the attacker has captured " D " and tries to spoof it, after that the attacker can extract the parameters which are the real identity, temporary etc and be stored in the memory of D However, it should be mentioned that the D is integrated with an integrated circuit that will do automated change the output's behavior (for example, a response message) As a result, every attempt to tamper is warranted. with the memory D will not allow an attacker to create a key for a session with S so the proposed protocol is resilient against physical attacks.

3) Create a session key

The session (sk) is a one-time-use symmetric key that is generated at the conclusion of the authentication process and used to encrypt data in transit between parties during a communication session. The suggested protocol accommodates this need by allowing the generation of a session key SK =h(RID-d_k-s).

4) Data confidentiality

Since the proposed protocol prevents an adversary from learning the most recent one-time identifier used in prior sessions by having the IoT device generate a new value at the conclusion of each session and sending it to the server, it provides forward confidential lity.

5) Resist impersonation attack

In the event that the opponent tried to impersonate himself at the joining stage, the inclusion of the message in the suggested scheme {T_1, 〖PID〗_d, σd} that is sent by the device to the server contains 〖 RID〗_d therefore, the attacker cannot impersonate any person who wants to join because he does not have the device alias σd = h (T_1‖ 〖RID〗_d)

6) Replay attack

In the message ((T ,T_sk, 〖PID〗_(d),σd) we use the time stamp T as the the attacker is unable to change the T in the beacon because during the investigation will be self-rejected if it is no longer valid or has expired and therefore the replay attack is inefficient in our proposed protocol.

7) Resist modification attack

In our proposed scheme, the sent messages contain {σd} ,{ σs} and in the event of any modification, the recipient reveals that the output does not match, therefore, the modification attack is not effective in our proposed scheme.

5.3. Performance analysis

We implement the related and proposed protocols from Kalra and Sood [23], Wang et al. [24], Maarof et al. [25] and kumari et al. [28] in order to assess how well our suggested protocol works and how it stacks up against other protocols. We next conduct an evaluation and comparison of the protocols' performance once we have finished the implementation procedure. In addition, a comparison of security characteristics is provided to demonstrate that the proposed protocol is more secure than competing protocols:

–T_h the
time of execution of the hash function.
– T_{ecc_m} how long it takes to perform an error-correcting code (ECC) point multiplication.

5.3.1. Computation Cost

Login and authentication are both taken into account for computational expenses since they are used more frequently than any other stages in the authentication system, as evidenced by experimental data [46] that the implementation time (computational costs) for T_h and T_(ecc_m) are 2.3μs and 22.26 × 10^2 μs , Since computation is very inexpensive and is associated with lightweight operations (such as XOR), its computational costs are ignored.

Table (2): computational costc comparison

Login and authentication phase			
Schemes	Device_Side	server_Side	Total
[23]	$4T_h + 3T_{ecc\_m}$	$5T_h + 4T_{ecc\_m}$	$9T_h + 7T_{ecc\_m} \approx 15.603 \times 10^3$ μs
[24]	$6T_h+4T_{ecc\_m}$	$6T_h+4T_{ecc\_m}$	$12T_h + 8T_{ecc\_m} \approx 17.835 \times 10^3$ μs
[25]	$5T_h+6T_{ecc\_m}$	$7T_h+5T_{ecc\_m}$	$12T_h+11T_{ecc\_m} \approx 24.513 \times 10^3$ μs
[28]	$3T_h + 4T_{ecc\_m}$	$4T_h + 4T_{ecc\_m}$	$7T_h + 8T_{ecc\_m} \approx 17.824 \times 10^3$ μs
Proposed	$3T_h + 2T_{ecc\_m}$	$4T_h + T_{ecc\_m}$	$7T_h + 3T_{ecc\_m} \approx 6.694 \times 10^3$ μs

Table (3): communication and storage cost comparison

Schemes	Number of messages	Communication cost(bits)	Storage cost(bits)
[23]	3	1760	320
[24]	3	1920	576
[25]	3	1728	320
[28]	3	1760	480
Proposed	2	1280	160

In the login and authentication phase, based on Table (2), we have compared the computational cost of our suggested scheme with that of Kalra and Sood's scheme [23], Wang et al scheme [24], Maarof et al scheme [25], and Kumari et al scheme [28].the computational cost of a scheme are Kaalra and Soood $9T_h + 7T_{ecc\_m} \approx 15.603 \times 10^3$ µs , Wang et al $8T_{ecc\_m}+12T_h \approx 17.835 \times 10^3$ µs , Maarof et al $11T_{ecc\_m}+12T_h \approx 24.513 \times 10^3$ µs , kumari et al $7T_h + 8T_{ecc\_m} \approx 17.824 \times 10^3$ µs and for our scheme are $7T_h + 3T_{ecc\_m} \approx 6.694 \times 10^3$ µs As we see that our scheme is superior to the above schemes in the computational cost, and this means that our scheme is less computational and better than the computational schemes.

5.3.2. Communication cost

Here we compare the overheads in the relevant proposed protocols, where the registration stage is performed once for every newly connected device on the Internet, and thus the cost of communication for the proposed protocols is calculated in terms of the total amount of bits sent by the entities involved in order for the verification stage to take place. Our suggested scheme's communication cost is compared to that of previously proposed systems in table (3), including the schemes of Kaalra and Soood[23], Wang et al[24], Maarof[25], and kumari[28]. Despite taking into account the cost of the schemes' connections, We have assumed in the first message that the value of timestamp((T_1) is 160 bits , and that the value of pseudonyms of the devices (PID_1) is 320 bits and (PID_2) is 160 bits and that the value of (σd) is 160 bits, So the sum of the first message is 800 bits, In the second message we also assume a value of timestamp (T_2) is 160 bits and value of Secure the key (SK) is 160 bits and value of (σs) is 160 bits So the sum of the second message is 480 bits After that, we collect the two messages, so their sum is 1280 bits , this means that the cost of communication in our scheme is higher and better than the rest of the other schemes above.

5.3.3. Storage cost

In comparison to Kalra and Sood's technique [23], our proposed scheme requires the embedded device (d_i) to store (C_K)= 320 bits of data in its memory. Wang and colleagues' plan [24] The embedded device (Id_i) must keep (C_K)=576 bits of data in its memory. Maarof and colleagues' scheme [25] The embedded device (Id_i) must store (C_K)= 320 bits of data in its memory, and the approach proposed by Kumari et al. [28] An embedded device's memory includes (C_K,Id_i) =320 + 160 = 480 bits of data. For the embedded device(D), the storage cost is taken into account.

because it has a small amount of memory towards the end of the recording phase in the schematics we have indicated, In our proposed scheme the embedded device contains the real identities of the device (RID_d) = 160 bits this means that our scheme is less than the other schemes that we refered to, which makes the cost of storing our proposal much lower

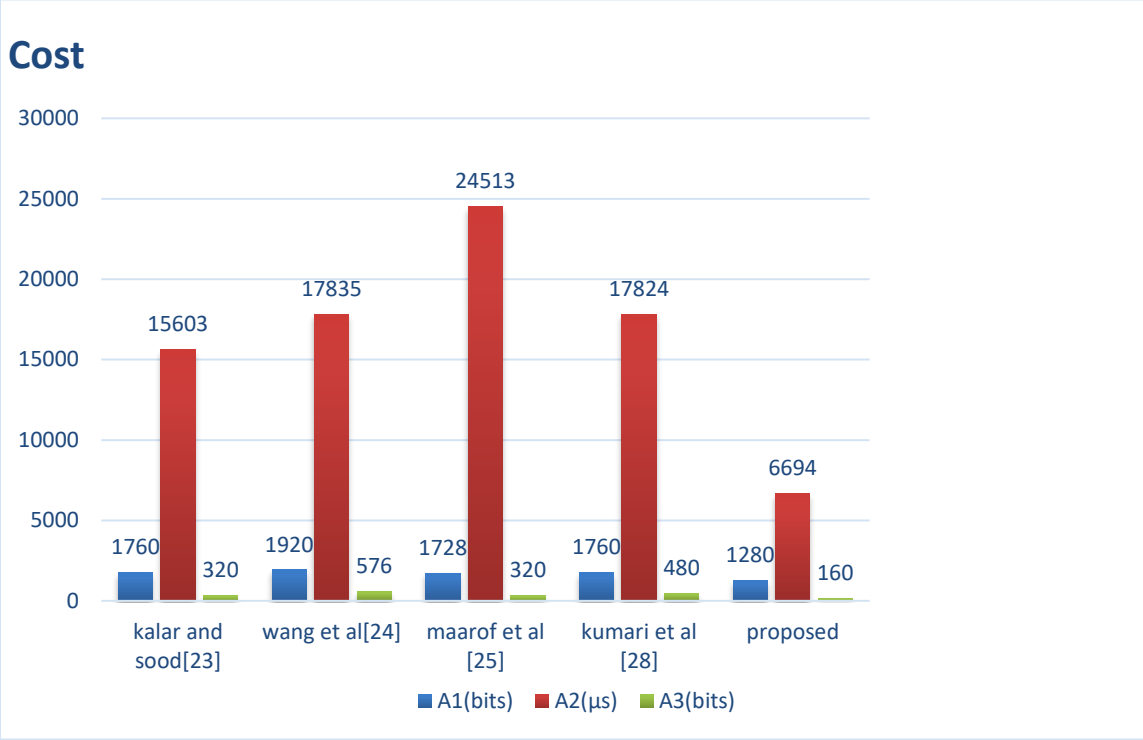

Figure (4): Performance comparison

In Figure (4), we compare the performance of our proposed scheme to schemes [23], [24], [25], and [28], assuming that A_1 is the communication cost (in bits), A_2 is the calculation cost (in s), and A_3 is the storage cost (in bits). Our scheme outperforms the other schemes because it is well suited for authenticating devices embedded in the Internet of things environment.

5.3.4. Security requirements comparison

A comparison of the security requirements between our proposed scheme and schemes Kalra and Sood's scheme [23], Wang et al scheme [24], Maarof et al scheme [25], and kumari et al scheme [28] is shown in table (4), where it appears from the table (4) that our proposed scheme can withstand different attacks otherwise. as schemes [23], [24], [25] and[28] are vulnerable to some attacks that we will mention in the table below, and therefore our proposed scheme provides the largest result of the schemes [23], [24], [25], and [28] regarding the security of the Internet of things environment.

Table (4): security features comparison

Security requirements→ Schemes↓	A_1	A_2	A_3	A_4	A_5	A_6	A_7
[23]	×	✓	×	×	×	✓	✓
[24]	✓	✓	✓	×	×	✓	✓
[25]	✓	×	×	✓	×	✓	×
[28]	✓	✓	×	✓	✓	✓	×

Proposed	✓	✓	✓	✓	✓	✓	✓

✓achieved ; × not achieved
A_1: privacy and inaccessible
A_2: physical attack on an IOT device
A_3: Create a session key
A_4: data confidentiality
A_5: resist impersonation attack
A_6: replay attack
A_7: resist modification attack

6. Conclusions

In our current era, many embedded devices are connected to the Internet to exchange data thanks to the rapid developments of the Internet of Things, so data privacy and device authentication are among the important problems occurring in Internet of things devices as a result, we proposed an improved authentication protocol in our research this depends on ECC, as it is the proposed protocol is strong, secure, and effective against various attacks as demonstrated in the informal analysis , Furthermore, the validity and security of the proposed protocol is verified through authentication tool scyther that is used in many researches. The suggested protocol is assessed by comparison with different and related protocols in relation to communication and computation. In addition, we will make more effort in the future to design biometric authentication systems that are secure and lightweight suitable for the IoT environment.

Acknowledgement: This is an optional section.

Conflict of Interest: The authors declare that there are no conflicts of interest associated with this research project. We have no financial or personal relationships that could potentially bias our work or influence the interpretation of the results.

References

[1] Yaqoob, I., Ahmed, E., Hashem, I. A. T., Ahmed, A. I. A., Gani, A., Imran, M., & Guizani, M,"Internet of things architecture: Recent advances, taxonomy, requirements, and open challenges", IEEE wireless communications, vol.24, no.3, pp .10-16, 2017.

[2] Sheng, Z., Mahapatra, C., Zhu, C., & Leung, V. C, "Recent advances in industrial wireless sensor networks toward efficient management in IoT", IEEE access, vol . 3, pp . 622-637, 2015

[3] Vermesan, O, & Friess, P,"Internet of things: converging technologies for smart environments and integrated ecosystems". River publishers, Eds, 2013,pp.145-150.

[4] Stergiou, C., Psannis, K. E., Kim, B. G., & Gupta, B." Secure integration of IoT and cloud computing. Future Generation Computer Systems",vol 78,no.4, pp.964-975,2018.

[5] Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. " Security, privacy and trust in Internet of Things: The road ahead. Computer networks" vol. 76, no.5,pp.146-164,2015.

[6] M. El-Hajj, A. Fadlallah, M. Chamoun, and A. Serhrouchni, ``A survey of Internet of Things (IoT) authentication schemes," Sensors, vol. 19, no. 5, pp. 1141, 2019.

[7] A. K. Das, S. Zeadally, and D. He, ``Taxonomy and analysis of security protocols for Internet of Things," Future Gener. Comput. Syst., vol. 89, pp. 110_125, 2018.

[8] M. A. Ferrag, L. A. Maglaras, H. Janicke, J. Jiang, and L. Shu, ``Authentication protocols for Internet of Things: A comprehensive survey," Secur. Commun. Netw., vol. 2017, pp. 1_41, 2017.

[9] K. Han, T. Shon, and K. Kim, ``Ef_cient mobile sensor authentication in smart home and WPAN," IEEE Trans. Consum. Electron., vol. 56, no. 2, pp. 591_596, 2010.

[10] S. Kumari, A. K. Das, M. Wazid, X. Li, F. Wu, K. K. R. Choo, and M. K. Khan, ``On the design of a secure user authentication and key agreement scheme for wireless sensor networks," Concurrency Comput. Pract. Exper., vol. 29, no. 23, pp. 1_24, 2017.

[11] M. Bilal and S. G. Kang, ``An authentication protocol for future sensor networks," Sensors, vol. 17, no. 5, p. 979, 2017.

[12] J. Jeong, M. Y. Chung, and H. Choo, ``Integrated OTP-based user authentication scheme using smart cards in home networks," in Proc. 41st Annu. Hawaii Int. Conf. Syst. Sci. (HICSS), Waikoloa, HI, USA, Jan. 2008, pp. 294_301.

[13] B. Vaidya, D. Makrakis, and H. T. Mouftah, ``Device authentication mechanism for smart energy home area networks," in Proc. IEEE Int. Conf. Consum. Electron. (ICCE), Jan. 2011, pp. 787_788.

[14] F. K. Santoso and N. C. H. Vun, ``Securing IoT for smart home system," in Proc. Int. Symp. Consum. Electron., 2015, pp. 1_2.

[15] M. Shuai, N. Yu, H. Wang, and L. Xiong, ``Anonymous authentication scheme for smart home environment with provable security," Comput. Secur., vol. 86, pp. 132_146, Sep. 2019.

[16] M. Wazid, A. K. Das, V. Odelu, N. Kumar, and W. Susilo, ``Secure remote user authenticated key establishment protocol for smart home environment," IEEE Trans. Dependable Secure Comput., vol. 17, no. 2, pp. 391_406, Dec. 2020.

[17] Q. Lyu, N. Zheng, H. Liu, C. Gao, S. Chen, and J. Liu, ``Remotely access `my' smart home in private: An anti-tracking authentication and key agreement scheme," IEEE Access, vol. 7, pp. 41835_41851, 2019.

[18] X. Sun, S. Men, C. Zhao, and Z. Zhou, ``A security authentication scheme in machine-to-machine home network service," Secur. Commun. Netw., vol. 8, no. 16, pp. 2678_2686, Nov. 2015.

[19] M. Jan, P. Nanda, M. Usman, and X. He, ``PAWN: A payload-based mutual authentication scheme for wireless sensor networks," Concurrency Compute, Pract. Exper., vol. 29, no. 17, p. e3986, Sep. 2017.

[20] T. Song, R. Li, B. Mei, J. Yu, X. Xing, and X. Cheng, ``A privacy preserv ing communication protocol for IoT applications in smart homes," IEEE Internet Things J., vol. 4, no. 6, pp. 1844_1852, Dec. 2017.

[21] A. A. Alamr, F. Kausar, J. Kim, and C. Seo, ``A secure ECC- based RFID mutual authentication protocol for Internet of Things," J. Supercomput., vol. 74, no. 9, pp. 4281_4294, Sep. 2018.

[22] S. Hussain, S. A. Chaudhry, O. A. Alomari, M. H. Alsharif, M. K. Khan, and N. Kumar, ``Amassing the security: An ECC-based authentication scheme for Internet of drones," IEEE Syst. J., early access, Mar. 1, 2021.

[23] S. Kalra and S. K. Sood, ``Secure authentication scheme for IoT and cloud servers," Pervas. Mobile Comput., vol. 24, pp. 210_223, Dec. 2015.

[24] C.-M. Chen, K.-H. Wang, W. Fang, T.-Y. Wu, and E. K. Wang, ``Recon sidering a lightweight anonymous authentication protocol," J. Chin. Inst. Engineers, vol. 42, no. 1, pp. 9_14, Jan. 2019

[25] A. Maarof, M. Senhadji, Z. Labbi, and M. Belkasmi, ``Authentication protocol for securing Internet of Things," in Proc. 4th Int. Conf. Eng. MIS (ICEMIS), 2018, pp. 1_7.

[26] C.-C. Chang, H.-L. Wu, and C.-Y. Sun, ``Notes on `secure authentication scheme for IoT and cloud servers,'" Pervas. Mobile Comput., vol. 38, pp. 275_278, Jul. 2017

[27]S. A. Chaudhry, ``Correcting `PALK: Password-based anonymous lightweight key agreement framework for smart grid,'" Int. J. Electr Power Energy Syst., vol. 125, Feb. 2021, Art. no. 106529.

[28] S. Kumari, M. Karuppiah, A. K. Das, X. Li, F. Wu, and N. Kumar, ``A secure authentication scheme based on elliptic curve cryptography for IoT and cloud servers," J. Supercomput., vol. 74, no. 12, pp. 6428_6453, Dec. 2018.

[29] C. Lyu, D. Gu,Y. Zeng, and P. Mohapatra, ``PBA: Prediction-based authen tication for vehicle-to-vehicle communications," IEEE Trans. Dependable Secure Comput., vol. 13, no. 1, pp. 71_83, Jan. 2016.

[30] Yehia, M., AlTawy, R., & Gulliver, T. A. "Security analysis of DGM and GM group signature schemes instantiated with XMSS-T. In Information Security and Cryptology" 17th International Conference, 2021,pp. 61-81.

[31] G. Saldamli, L. Ertaul, and B. Kodirangaiah, "Post-quantum cryptography on IoT: Merkle's tree authentication," in Proc. Int. Conf. Wireless Netw. (ICWN) , vol.3,no.4,pp. 35_41,2018

[32] M. N. Aman, K. C. Chua, and B. Sikdar, ``Mutual authentication in IoT systems using physical unclonable functions," IEEE Internet Things J., vol. 4, no. 5, pp. 1327_1340, Oct. 2017.

[33] P. Gope and B. Sikdar, ``Lightweight and privacy-preserving two-factor authentication scheme for IoT devices," IEEE Internet Things J., vol. 6, no. 1, pp. 580_589, Feb. 2019.

[34] N. Chikouche, P.-L. Cayrel, E. H. M. Mboup, and B. O. Boidje``A privacy-preserving code-based authentication protocol for Internet of Things," J. Supercomput., vol. 75, no. 12, pp. 8231_8261, Dec. 2019.

[35] A. Bander. and K. Mahmood. "Provable Privacy Preserving Authentication Solution for Internet of Things Environment ." IEEE Access,vol 9 (2021): 82857-82865.

[36] Srinadh, V., Maram, B., & Daniya, T. (2021, December). Data Security And Recovery Approach Using Elliptic Curve Cryptography. In 2021 IEEE International Conference on Computation System and Information Technology for Sustainable Solutions (CSITSS) (pp. 1-6). IEEE.

[37] Shemanske, T. R. Modern Cryptography and Elliptic Curves. American Mathematical Soc,2017,pp83.

[38] Ullah, S., Zheng, J., Din, N., Hussain, M. T., Ullah, F., & Yousaf, M. "Elliptic Curve Cryptography; Applications, challenges, recent advances, and future trends". Computer Science Review, vol.47,pp.3-12,2023.

[39] V. S. Miller, ``Use of elliptic curves in cryptography," in Proc. Conf Theory Appl. Cryptograph. Techn. Berlin, Germany: Springer, Dec. 1985, pp. 417_426.

[40] Harsha, A., & Patil, B. "A Review: Security of Data in Cloud Storage using ECC Algorithm". Bonfring International Journal of Software Engineering and Soft Computing.vol.6,no.2,pp2-10,2016.

[41] Gebregiyorgis, S. W. "Algorithms for the elliptic curve discrete logarithm and the approximate common divisor problem ",Doctoral dissertation, PhD Thesis, University of Auckland, New Zealand,2016.

[42] Bojjagani, S., Reddy, Y. P., Anuradha, T., Rao, P. V., Reddy, B. R., & Khan, M. K. (2022). Secure Authentication and Key Management Protocol for Deployment of Internet of Vehicles (IoV) Concerning Intelligent Transport Systems. IEEE Transactions on Intelligent Transportation Systems, 23(12), 24698-24713.

[43] KOZAKIEWICZ, M, & SIEDLECKA-LAMCH, O. "Some Remarks on Security Protocols Verification Tools. In Information Systems Architecture and Technology": Proceedings of 37th International Conference on Information Systems Architecture and Technology.vol.2, no.2, pp. 65-75, 2017

[44] YANG, H., OLESHCHUK, V., & PRINZ, A. "Verifying Group Authentication Protocols by Scyther. Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications" (JoWUA), vol.7,no.2, pp.3-19,2016.

[45] PATEL, R., BORISANIYA, B., PATEL, A., PATEL, D., RAJARAJAN, M., & ZISMAN, A. "Comparative analysis of formal model checking tools for security protocol verification. In International Conference on Network Security and Applications ", Springer Berlin Heidelberg vol.3, no.2, pp. 152- 163, (2010).

[46] Kilinc HH, Yanik T ."A survey of SIP authentication and key agreement schemes". IEEE Commun Surv Tutor ,vol.16,no1.2,pp.1005–1023,2014