SERBIAN JOURNAL OF ELECTRICAL ENGINEERING
Vol. 22, No. 2, June 2025, 223-241
UDC: 004.77:004.056.523 **DOI: https://doi.org/10.2298/SJEE2502223D**
Original scientific paper

Elliptic Curve Cryptography and Biometrics for IoT Authentication

Souhayla Dargaoui[1], Mourade Azrour[1], Ahmad El Allaoui[1], Azidine Guezzaz[2], Abdulatif Alabdulatif[3], Sultan Ahmad[4], Nisreen Innab[5]

Abstract: The Internet of Things (IoT) is now present in every aspect of our daily lives because of its ability to offer remote services. Unfortunately, the insecure transmission of user data in open channels caused by this significant use of IoT networks makes it vulnerable to malicious use. Hence, the security of the user's data is now a serious matter in an IoT environment. Since authentication may prevent hackers from recovering and using data transmitted between IoT devices, researchers have proposed many lightweight IoT authentication protocols over the past decades. Many of these protocols are built around two authentication factors. They cannot guarantee unlinkability and perfect forward secrecy, as well as withstand well-known attacks such as node capture, DOS attack, stolen verifier, Denning-Sacco attack, and GWN bypass. This paper proposes an Elliptic Curve Cryptography (ECC) -based authentication protocol that is anonymous and exploits three authentication factors to ensure all security services and withstand well-known attacks. Our provided protocol is secure and can resist known attacks, as demonstrated by both informal security analysis and formal security proof using ProVerif. Lastly, our protocol and other protocols are compared in terms of computational costs, communication costs, and security features.

Keywords: Authentication, IoT, Elliptic Curve Cryptography, Multi-factor security, Biometrics.

[1]IMIA Laboratory, MSIA Team, Faculty of Sciences and Techniques, Moulay Ismail University of Meknes, Errachidia, Morocco, s.dargaoui@edu.umi.ac.ma, https://orcid.org/0009-0006-8080-0252; mo.azrour@umi.ac.ma, https://orcid.org/0000-0003-1575-8140; a.elallaoui@umi.ac.m, https://orcid.org/0000-0002-8897-3565
[2]Higher School of Technology, Cadi Ayyad University, Morocco, a.guezzaz@uca.ma, https://orcid.org/0000-0003-1058-5420
[3]Department of Computer Science, College of Computer, Qassim University, Buraydah, Saudi Arabia. ab.alabdulatif@qu.edu.sa, https://orcid.org/0000-0003-0646-5872
[4]Department of Computer Science, College of Computer Engineering and Sciences, Prince Sattam Bin Abdulaziz University, Al-Kharj, Saudi Arabia, s.alisher@psau.edu.sa, https://orcid.org/0000-0002-3198-7974
[5]Department of Computer Science and Information Systems, College of Applied Sciences, AlMaarefa University, Riyadh, Saudi Arabia, ninnab@um.edu.sa, https://orcid.org/0000-0003-4412-7727

1 Introduction

The Internet of Things, known as a huge network that connects products, equipment, and databases, has improved people's daily lives by offering remote management for aspects like transportation, health care, smart grids, smart homes, and the environment [1 – 11]. A healthcare diagnosis system combining the IoT and recurrent neural networks was presented by Balasundaram et al. [12]. The purpose of the mechanism presented is to categorize health anomalies with accuracy. Amara Aditya and her team have developed an intelligent IoT-based car park that can be used to manage car parking in a smart city [13]. Their framework is designed to gather real-time data, analyze it, and provide the coordination in accessible location nearby. An important data flow is generated and exchanged daily by users over insecure wireless communication networks using this technology. Because of this, this data is at risk of being exploited improperly. To prevent malicious use of user data, multiple solutions can be placed in an IoT network. Authentication is the most crucial and effective solution.

Authentication typically stops hackers from utilizing user data, even if it is derived from a message while permitting lawful authorities to use it freely and securely. However, IoT devices, with their limitations, cannot ensure the high computation power, storage, and energy required by traditional authentication protocols. Lightweight authentication schemes have been implemented as a result. There have been a lot of lightweight authentication schemes provided in the past ten years [14 – 36]. Nevertheless, analysis has shown that most of these schemes are two-factor authentication mechanisms that fail to provide crucial security properties, including:

– Unlinkability that ensures that multiple sessions or actions of a user cannot be linked together;
– Key secrecy, which guarantees that cryptographic keys remain confidential and inaccessible to unauthorized parties;
– Perfect forward secrecy that ensures that the compromise of long-term keys does not affect the confidentiality of past session keys.
– In addition, they are vulnerable to various attacks, such as:
– Stolen verifier attacks, where attackers obtain stored authentication data (like passwords or hashes);
– Denial of Service (DoS) attacks, which aim to overwhelm or disable the service;
– Denning-Sacco attacks, which allow attackers to decrypt past communications after a key compromise;

– Node capture, where physical access to a device allows an attacker to extract sensitive information;
– GWN bypassing, where unauthorized entities circumvent the gateway node to gain access [3].

The aim of the article is to provide a lightweight authentication protocol, which enhances security over known assaults and provides the necessary security features. To handle noisy biometric data, we used the Fuzzy Extractor algorithm. The output of a fuzzy extractor is identical for noisy input sources that are nearly identical. Generally, Fuzzy Extractors consists of two procedures. The generation procedure generates an equably diffused value and public reconstruction data from a noisy signal. While the reproduction procedure reproduces the equably diffused value from a signal close enough to the initial noisy signal. Thus, we can get the same output for noisy biometric data. The provided scheme consists of the next contributions:

– We introduce a novel authentication and key-agreement system that is based on three factors. The provided scheme enables the mutual authentication between the user and the portal and between the portal and the IoT appliance. Lastly, a session key will be set up between the user and the appliance.
– The scheme being proposed uses ECC, a hash function, and random numbers as its foundations.
– The scheme's efficiency and robustness are demonstrated by informal security analysis and simulation using ProVerif.

The remainder of this article is structured as follows. The second section presents related works. Section three presents the proposed protocol. Section four presents both informal and formal assessments of security. Section five compares our system with others by analyzing computation costs, communication overheads, and security services. The paper's conclusion was reached in section six.

2 Related Work

Several authentication schemes have been provided in the last decades to ensure confidentiality and security in IoT networks. Associated with existing systems, symmetric-key algorithms have relatively small keys while requiring limited resources. Additionally, the encoded text is generally smaller than the initial one. These mechanisms appear to be the best option to implement IoT authentications. P. Gope and T. Hwang [37] came up with a practical authentication scheme for Wireless Sensor Networks (WSN) that could guarantee user privacy, untraceability, and forward/backward secrecy. A. Ghani et al. [38] carried out a cryptanalysis on [37] and found that this protocol is vulnerable to user tracking, Denial-of-Service, and stolen verifier. Additionally, A. Ghani and

his coworkers presented an improved symmetric-key authentication scheme for IoT-driven wireless networks. They showcased how their protocol can tackle the weaknesses of the Gope and Hwang scheme [37]. Their protocols [37] possess identical communication overheads, as shown by analyzing the comparison results. Nevertheless, it is 52.63% more effective than the basic scheme due to its lower computation cost [38].

Unfortunately, symmetric encryption has a kind of shortcoming unlike public-key cryptography methods that ensure authenticity, privacy, and non-repudiation. Recent research has led to build asymmetric encryption-based IoT authentication schemes. D.Q. Bala et al. [39] introduced an authentication scheme that utilizes the certificate-less public key cryptography mechanism for IoT networks. They demonstrated that the proposed framework was impervious to replay assaults node impersonation. N. Li et al. [40] used public key encryption to build a lightweight mutual authentication protocol for smart city environments. The provided protocol balances the efficiency and communication cost without compromising security. N. Li and his team showed that their scheme was more efficient than the existing ones at the time.

Despite the short key length required, elliptic curve cryptography has the same security strength as public-key encryption systems. Q. Jiang et al. in their work [41] and D. He et al. in another work [42] have showed that it is vulnerable to impersonation attacks and smart-card loss. Additionally, they illustrated that the authentication mechanism of He et al. is unable to guarantee untraceability and was susceptible to traceability raids. They devised an authentication scheme, which utilizes temporal credentials and leverages the ECC for WSN. The devised scheme fulfills the security gaps maintaining the basic protocol desirable features. Li et al. [43] evaluated the protocol provided by Q. Jiang et al. and proposed a new, considering three factors. Their scheme's performance evaluation results demonstrate that it ensures additional security services while maintaining the same computational effectiveness.

Several other techniques have been employed to enhance IoT authentication. Utilizing a physically unclonable function, M. A. Qureshi [44] provided an authentication scheme called PUF-IPA, which ensures bolstered resilience against security assaults compared to earlier schemes that use the same basics. PUF-IPA's strength is demonstrated by the analysis results. Based on Blockchain, M. T. Hammi [45] proposed an unfocused authentication protocol for IoT environments, which secures a reliable authentication of IoT appliances. The suggested scheme has been implemented using Ethereum Blockchain and C++ language. It demonstrates its effectiveness and low overhead. The main disadvantage of all solutions presented in this chapter is that two-factor authentication mechanisms are not capable of full protection as described in the introduction section.

3 The Provided Authentication Protocol

Our protocol contains five phases. The gateway initiates by selecting a random numeral KG as its private key, selecting P, a one-way hash function h(.), the Gen (.) and Rep (.) algorithms, calculating Ppub = KG.P, and publishing these elements. The notation used in our paper is illustrated in **Table 1**.

Table 1
Notations.

Notation	Description
U	User
S	Sensor
ID_i	User identity
SID_j	Sensor identity
PW_i	User password
GWN	Gateway
K_G	Gateway secret key
h (.)	One-way hashing function
SK	Session key
Gen (.)	Fuzzy extractor generation procedure
Rep (.)	Fuzzy extractor Reproduction procedure
K_u, R_u, K_s, R_s, R_g, R_G, r_1	Random numbers
T_i	Timestamp
Bio_i	User biometric model
$\oplus$	Xor procedure
$\|\|$	String concatenation procedure
P	The generator point on the elliptic curve

3.1 New sensor addition phase

The gateway, at this phase, generates the sensor identity SIDj and saves it in its databank. Then, the gateway computes the C=h (SIDj||KG), and transmits {SIDj, C, P} to the IoT device that holds them in its memory.

3.2 User registration stage

In this stage, the data must be exchanged in a secure channel. To complete this stage, the customer must go through three steps, as illustrated in Fig. 1.

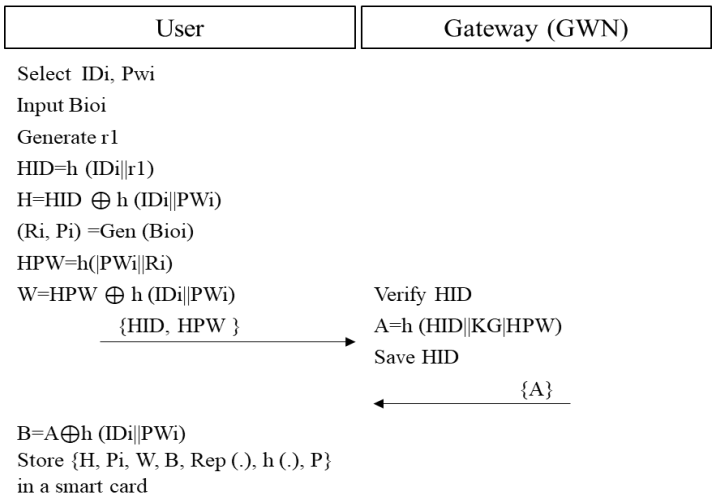

Fig. 1 – *User registration phase.*

The first step combines six subsets:

Authentication factors generation: The customer chooses its credentials IDi and PWi, adopts r1 number randomly, and provides his biometrics Bioi.

HID Generation: The user computes HID=h (IDi||r1) its pseudo identity using a hash function with the identity IDi and a random number r1. This adds randomness and avoids direct exposure of the identity.

H Calculation: To obfuscate HID, the user computes H=HID ⊕ h (IDi||PWi), concealing HID using the hash of the identity and password combination.

Fuzzy Extractor and Biometric Processing: To handle noisy biometric data while deriving consistent values, the user exploits the generation algorithm of the fuzzy extractors to produce Ri and Pi.

HPW and W Calculation: The user computes HPW=h (PWi||Ri) by combining the password and biometric randomness. Then, he computes W=HPW ⊕ h (IDi||PWi), concealing HPW with another hash.

Communication to Entrance: Finally, the customer transmits HID and HPW to the gate.

The second step contains two subsets:

Authentication parameter calculation: The gate computes A, which is a parameter that enables the authentication between this latter and the customer.

HID storage and A transmission: At this point, the gateway saves HID and communicates A to the user.

The third step contains two subsets:

Authentication parameter securing: To obfuscate the parameter A, the customer computes B using IDi and PWi.

Smart Card Storage: The user stores {H, Pi, W, B, Rep (.), h (.), P} in a smart card.

3.3 Login and authentication stage

The exchange between the network entities is carried out through an insecure broadcaster at this stage. The process of this phase is detailed below and represented in Fig. 2.

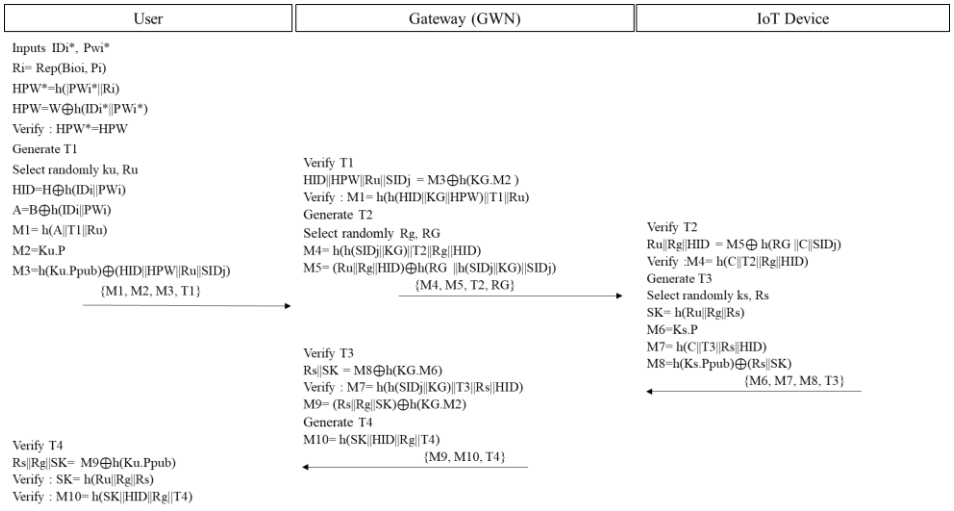

Fig. 2 – *Login and authentication stage.*

The first step contains four subsets:

Credentials providing: The user provides his ID and PWi and scans his fingerprints.

Login: The customer restores Ri upon the Rep algorithm. Later, he calculates HPW and HPW* and verifies if HPW=HPW*. If they are equal, the user elaborates on the authentication request. Otherwise, the session ends.

Authentication request elaboration: The user generates T1, Ku, Ru, and recovers HID and A from H and B. Then the user computes M1, M2, and M3.

Request transmission: lastly, the user communicates the request {M1, M2, M3, T1} to the gate.

The second step contains three subsets:

Request freshness check: To verify the request legitimacy, the gate verifies the novelty of T1. If the delay transmission is less than a threshold, the gateway starts the authentication process. Otherwise, the session ends.

User authentication: The gateway reconstructs HID, HPW, Ru, and SIDj upon M3 and checks that M1 equals h (h (HID||KG||HPW) ||T1||Ru). If this condition is valid, it constructs the authentication request that will be sent to the IoT device.

Authentication request elaboration and transmission: The gate engenders T2, Rg, and RG and computes M4 and M5, as illustrated in Fig. 1. Lastly, it transfers the request {M4, M5, RG, and T2} to the sensor.

The third step contains three subsets:

Request freshness check: The IoT device gets the request transmitted by the gate and tests the freshness of T2. If it is valid, the sensor starts the authentication process.

Gateway authentication: The sensor reconstructs Ru, Rg, and HID upon the M5 and verifies that M4 equals h (C||T2||Rg||HID). Then, it generates the session key.

Session key generation and response transmission: The sensor generates T3, ks, and Rs and computes SK, M6, M7, and M8. Finally, the sensor transmits the response {M6, M7, M8, T3} to the gate.

The fourth step contains three subsets:

Response freshness check: The gateway receives the sensor response and tests the novelty of T3. If it is valid, the gate starts the sensor authentication process.

Sensor authentication: The gateway reconstructs Rs and SK and verifies if M7 equals h (h (SIDj||KG) ||T3||Rs||HID). Then, it generates the response that will be transferred to the user.

Response generation: the gateway generates T4 and computes M9 and M10 as illustrated in Fig. 1 and transfers the response {M9, M10, T4} to the customer.

The fifth step contains two subsets:

Response freshness check: The user tests the validity of T4. If it is valid, the user starts the authentication process of the device and the gateway.

Session key computation and gateway and sensor authentication: The user retrieves Rs, Rg, and SK from M9. Then, he verifies that SK equals h (Ru||Rg||Rs) and M1 equals h (SK||HID||Rg|T4). If these qualities are valid, the authentication is successful.

3.3 Password update stage

To update the password, the customer must pass through four steps as explained below:

Credentials providing: The user provides his ID and PWi and scans his fingerprints.

Login: The customer retrieves Ri upon the Rep algorithm. Subsequently, he calculates HPW and HPW and verifies if HPW=HPW*.

New credentials computing: The user provides his new password Pwinew and computes:

$$Wnew = h(PWinew \| Ri) \oplus h(Idi \| PWinew)$$

$$Hnew = H \oplus h(IDi \| PWi) \oplus h(Idi \| PWinew)$$

$$Bnew = B \oplus h(Idi \| PWi) \oplus h(Idi \| PWinew).$$

Smart card update: The user replaces W, H, and B with the up-to-date values in the smart card.

4 Security Analysis

Relating to the Dolev-Yao threat prototype [46], we represent the hacker's abilities like this:

- The attacker can access all information communicated through a public channel.
- Spyware messages can be modified, added, replayed, and redirected by the attacker.
- The attacker can retrieve the data preserved on the smart card if he obtains this chip.
- When a device is captured, the hacker may gather all the data preserved in its memory.
- The enemy may be a lawful user.

4.1 Informal security examination

Mutual authentication

To authenticate the customer, the gate compares M1 with h(h(HID||KG||HPW)||T1||Ru). By verifying that M4 equals h(C||T2||Rg||HID), the device validates the authenticity of the gateway. After that, the device is authenticated by the gateway, comparing M7 to h (h(SIDj||KG)||T3||Rs||HID). At the end, the customer verifies that M10 equals h (SK||HID||Rg||T4) for authenticating the gateway. As a result, we propose a scheme that provides mutual authentication.

Anonymity and untraceability

Our scheme incorporates HID into M1, M3, M4, M5, and M7. The attacker, considering the threat model, can receive these messages. However, the Diffie–Hellman problem, the hash function, and the gate secret key prevent the

extraction of HID from these messages. Additionally, even if the attacker could recognize HID, it will not be able to extract IDi since it is secured by r1 and h (.). Thus, our proposed mechanism ensures user anonymity and untraceability.

Key security

To maintain session key privacy, it is crucial that only the customer and gateway may know the session key at the end of the authentication stage. GWN's trustworthiness makes it impossible for the opponent to access KG. Additionally, the CDH complexity problem makes the attacker unable to determine Ru, Rg, and Rs even when he gets access to the customer's hidden information Ku.P and Ks.P. Moreover, these values are unpredictable and fluctuate between sessions. As a result, the secrecy of session keys is guaranteed by our scheme.

Impersonation attack

Calculating M1, M2, and M3 is necessary for the attacker to imitate the customer, but it is impracticable unless he knows HID, HPW, and A. Even though the opponent can thieve the smart card and recover W, B, and H, he is still unable to recover HPW, A, and HID without knowing the user identifier and password.

To impersonate the gateway, the hacker should compute the request transferred to the device and the response transmitted to the user. However, firstly, he needs to recover HID, Ru, and SIDj that cannot be done because he does not know the gateway secret key KG.

The sensor can be impersonated by calculating M6, M7, and M8 that is unfeasible unless he has C and RG. Thus, our system is not vulnerable to this kind of attack.

Replay attack

The gate authentication process cannot be executed if the timestamp is invalid for the intercepted and replayed request {M1, M2, M3, T1}. Regardless of the opponent's attempt to alter T1 in the request, it is impossible to change the M1 value unless he knows Ru and A. The requests computed by the gateway and the IoT device cannot be replayed for the same reasons. Thus, our protocol does not allow this type of attack.

Node capture

Capturing an IoT device enables the opponent to recognize some parameters, such as SIDj, C, and P, but he may not be able to discover KG because of the hash function. Therefore, capturing a device does not affect other devices.

Denial of service

To track the customer, the opponent needs to record messages {M1, M2, M3, T1}, but the arguments of these messages adjust between sessions because of

random values and timestamp usage. As a result, he may not alter them. Thus, our scheme is robust against denial-of-service assaults.

Insider attack

This kind of assault may turn up once a lawful customer steals the credentials to construct new login applications. The forms of credentials used in our provided scheme are hidden. In this manner, the opponent may not recognize PWi even though he recovers HPW since it is hidden using Ri and the hashing function. Consequently, our scheme presents a significant resistance against insider raids.

Stolen verifier

The gateway does not include any verification table to check data correspondence. Accordingly, our scheme is resilient toward stolen verifier attacks.

Denning-Sacco

In this kind of raid, the opponent attempts to recover a long-term secret key from the earlier session key. The fact that the session key in our provided mechanism is computed utilizing arbitrary values without any long-term keys makes the occurrence of this attack impossible.

Smart-card loss

As mentioned in earlier sections, the information stored in the smart card cannot enable the opponent to complete the authentication process unless he knows the credentials and has biometrics.

Password guessing

The opponent cannot recover HPW even though he gets access to M1, M2, and M3 transmitted through public channels. Additionally, to extract PWi from HPW, the opponent should solve the CDH problem, which is practically impossible. Therefore, it is impossible to discover PWi.

Meanwhile, if the attacker gets access to the information preserved in the smart card, the attacker may recover Band W. Nevertheless, he needs IDi and Ri to recover PWi, a thing that cannot occur. Therefore, this kind of attack is not feasible in our mechanism.

GWN Bypassing

This type of attack occurs when a harmful legitimate customer or attacker completes the authentication process but does not notify the gateway to finish its work. Since the customer does not have the gateway's secret key, it is impossible to send a correct message {M4, M5, T2, RG} to the sensor Sj. Correspondingly, this attack may not be feasible in our system.

The man in the middle

To forge a lawful intercepted login request {M1, M2, M3, T1}, the attacker needs to discover Ru, Ku, IDi, and PWi, which is impossible, as explained in previous sections. Therefore, our scheme may resist this kind of assault.

4.2 Formal security examination

This first goal of this part is to explain how the ProVerif tool can be used to analyze the security of the presented mechanism. The next step is to review the results gathered from this tool. ProVerif is an automated system that validates cryptographic mechanisms that follow the Dolev-Yao model. ProVerif evaluates the security features, authentication, and observational equivalences, considering the idealization of cryptographic primitives. This tool may evaluate the scheme for an unrestricted number of sessions. Blanchet et al. [47] ‘s process calculation syntax is used to model and check the protocols.

The evaluation results are illustrated in Fig. 3. The mutual authentication process is carried out sequentially. Furthermore, the proposed scheme may ensure the session key certainty, the customer’s credentials security, and the GWN private setting.

ProVerif text output:

```
------------------------------------------------------------
Verification summary:

Query not attacker(SK[]) is true.

Query not attacker(IDi[]) is true.

Query not attacker(PWi[]) is true.

Query not attacker(KG[]) is true.

Query inj-event(UAuthenticationPhase(user[])) ==> inj-event(ULoginPhase(user[])) is true.

Query inj-event(GWNAuthentication(server[])) ==> inj-event(UAuthenticationPhase(user[])) is true.

Query inj-event(SNSessionKey(sensor[])) ==> inj-event(GWNAuthentication(server[])) is true.

Query inj-event(UserSessionKey(user[])) ==> inj-event(SNSessionKey(sensor[])) is true.

Query inj-event(SNSAuthenticationPhase(sensor[])) ==> inj-event(UserSessionKey(user[])) is true.

------------------------------------------------------------
```

Fig. 3 – *Security evaluation results.*

5 Performance and Comparative Analyses

The proposed scheme has been compared to several authentication mechanisms considering the computation overheads, the connection overheads, and the security achievements. This section provides the comparative results.

5.1 Security achievement

Table 2 summarizes the result showed informal security examination section and illustrates the security characteristics of compared schemes and their resilience against attacks. The proposed scheme presents the best performance, resists well-known assaults, and ensures all the security characteristics needed in an authentication system. Nonetheless, B. Hu et al. [48] may not demonstrate the resilience of their authentication system against DoS attacks, GWN bypassing, Insider attacks, MITM attacks, stolen verifiers, and Denning-Sacco attacks. Additionally, the protocol proposed by J. Pirayesh et al. [51] is vulnerable to DoS raids. It does not examine its resilience against insider attacks, node capture, password guessing, Denning-Sacco attacks, GWN bypassing, and smart card loss. Further, it may not prove that it secures key secrecy, unlinkability, and forward secrecy. A.K. Yadav et al. [53] do not illustrate that the proposed scheme may secure perfect forward secrecy. They only evaluate the resilience of their scheme against replay assaults and smart card loss.

Table 2

Security characteristics and resilience against assaults.

Protocol	F_1	F_2	F_3	F_4	F_5	F_6	A_1	A_2	A_3	A_4	A_5	A_6	A_7	A_8	A_9	A_{10}	A_{11}
[48]	✓	✓	✓	✓	✓	✓	✓	✓	✓	-	-	-	-	✓	✓	-	-
[49]	✓	✓	✓	✓	✓	-	✓	✓	✓	✓	✓	✓	-	✓	✓	-	✓
[50]	✓	✓	✓	✓	✓	-	✓	✓	✓	-	✓	✓	-	✓	✓	-	✓
[51]	✓	✓	-	✓	-	-	✓	✓	-	×	-	✓	-	-	-	-	✓
[52]	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	-	✓	-	✓	-	-	✓
[53]	✓	✓	✓	✓	✓	-	-	✓	-	-	-	-	-	-	✓	-	-
Our protocol	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

F1: mutual authentication, F2: Anonymity, F3: unlinkability, F4: key agreement, F5: key secrecy, F6: perfect forward secrecy, A1: Impersonation assault, A2: reply assault, A3: node capture, A4: DoS assault, A5: Insider assault, A6: Stolen verifier, A7: Denning-Sacco assault, A8: password guessing, A9: smart card loss, A10: GWN bypassing, A11: man in the middle.

5.2 Computation overheads

This subsection compares the computation requirements of our protocol's login and authentication stage with those of other ECC-based protocols. **Table 3** illustrates the comparative outcomes. The notations used are as follows:

– Th: Time needed for a hash operation.
– Tsig: Time needed for signature generation and verification by HECDSA.
– Te: Time needed for ECC multiplication.
– Ts: Time needed for symmetrical cryptography.
– Tf: Time needed for the fuzzy extractor.

Other operations require negligible execution time. According to [23, 54], Th≈0.0001 ms, Te= Tf ≈0.442 ms, Tsig≈3.1920 ms, and Ts≈0.0026 ms.

To compute the login request, accomplish the required tests, and compute the session key, the customer needs 7Th+Tf+2Te in our scheme. The gateway needs Th+2Te to examine the login demand, compute the request transmitted to the sensor, verify its response, and construct the response transmitted to the customer. The IoT sensor needs 6Th+2Te to evaluate the requests and compute the response. As a result, our scheme requires 22Th+Tf+6Te to complete the login and authentication stage. **Table 3** shows that the requirements for each compared protocol are very similar, except for [51]. Even though our protocol is not the fastest, executing only takes approximately 3 seconds.

To assess scalability, we experimented with increasing network size to simulate authentication latency. Our protocol's latency is shown in Fig. 4 for different network sizes (100, 300, 500, 1000, 3000, 5000, 10000). We believe that our protocol can handle up to 3000 users since the network latency increase is 0.1 ms per user.

Table 3
Computational overheads comparison.

Sheme	User	Gateway	Sensor	Total	Execution time (ms)
[48]	7Th+3Te	10Th+Te	6Th+2Te	23Th+6Te	2,6543
[49]	7Th+3Te+1Tf	7Th+Te	4Th+2Te	18Th+6Te+Tf	3,0958
[50]	9Th+3Te	9Th+Te	7Th+2Te	25Th+ 6Te	2,6545
[51]	-	-	-	15Th+2Tf+4Ts+ +2Tsig+6Te	9,9319
[52]	5Th+3Te	5Th+2Te+Ts	3Th+3Te+Ts	13Th+8Te+2Ts	3,5425
[53]	-	-	-	Ts+15Th+6Te	2,6561
Our protocol	7Th+Tf+2Te	9Th+2Te	6Th+2Te	22Th+Tf+6Te	3,0962

5.3 Communication costs

The result of the comparison between our protocol and the other protocols in terms of communication costs is illustrated in **Table 4**. This later shows also the total of exchanged messages all along the authentication stage in each protocol. According to [49], the size of the random number, identity, timestamp, hashed value, the length of a point in an elliptical curve, and symmetric encryption /decryption block are 128 bits, 128 bits, 32 bits, 160 bits, 320 bits, and 256 bits respectively. The result of the comparative study demonstrates that the protocols that require small computation and communication overheads, like [48] and [53], may not provide strong resilience against assaults. Nevertheless, our protocol requires tolerable computation and communication costs regarding the robustness ensured against attacks.

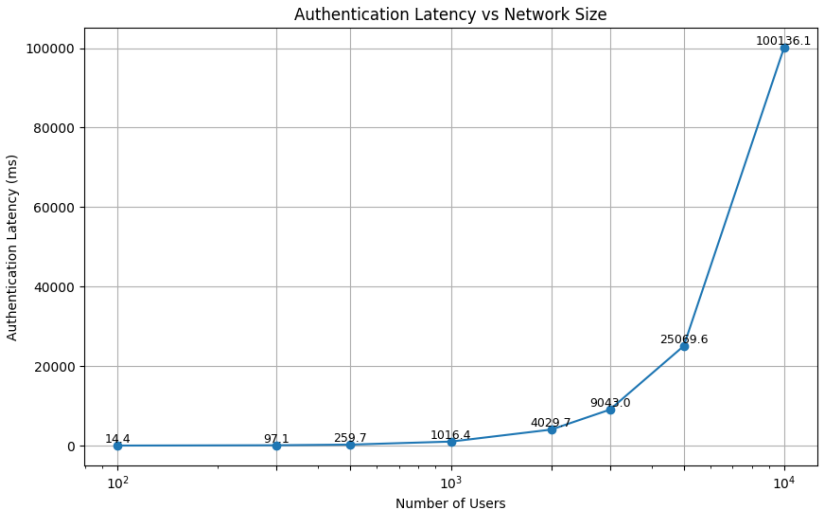

Fig. 4 – *Authentication latency with increasing network size.*

Table 4
Communication cost comparison.

Protocol	Total messages	Total communication cost
[48]	4	3456
[49]	3	2112
[50]	4	3552
[51]	3	-
[52]	6	3456
[53]	4	2144
Our protocol	4	2912

6 Conclusion

Since data security is a big issue in IoT deployments, researchers have developed different authentication systems to deal with this issue and secure users' data privacy. However, many of those protocols have flaws, especially regarding ensuring the customer's anonymity. In this paper, we combined three authentication factors to construct an ECC-driven authentication protocol that enables the anonymity of the user and ensures a high security level. Using the ProVerif tool, we have illustrated that our protocol ensures all security features. The robustness of our scheme against known attacks has also been demonstrated using informal security verifications. In the end, we contrasted our scheme with some similar protocols that were built on ECC. As a result, the provided scheme

is shown to have lower computation and communication costs, considering its robustness and security level.

7 References

[1] S. Dargaoui, M. Azrour, A. El Allaoui, A. Guezzaz, A. Alabdulatif, A. Alnajim: An Exhaustive Survey on Authentication Classes in the IoT Environments, Indonesian Journal of Electrical Engineering and Informatics, Vol. 12, No. 1, March 2024, pp. 15 – 31.

[2] S. Dargaoui, M. Azrour, A. El Allaoui, A. Guezzaz, A. Alabdulatif, A. Alnajim: Internet of Things Authentication Protocols: Comparative Study, Computers, Materials and Continua, Vol. 79, No. 1, April 2024, pp. 65 – 91.

[3] S. Dargaoui, M. Azrour, A. El Allaoui, F. Amounas, A. Guezzaz, H. Attou, C. Hazman, S. Benkirane, S. Haddou Bouazza: An Overview of the Security Challenges in IoT Environment, Ch. 13, Advanced Technology for Smart Environment and Energy, Springer, Cham, 2023.

[4] S. Dargaoui, M. Azrour, J. Mabrouki, A. El Allaoui, A. Guezzaz, S. Benkirane, A. Alabdulatif: Security Issues in Internet of Medical Things, Ch. 5, Blockchain and Machine Learning for IoT Security, 1st Edition, Chapman and Hall/CRC, New York, 2024.

[5] M. Azrour, S. Dargaoui, J. Mabrouki, A. Guezzaz, S. Benkirane, W.Shafik, S. Ahmad: A Survey of Machine and Deep Learning Applications in the Assessment of Water Quality, Ch. 38, Technical and Technological Solutions Towards a Sustainable Society and Circular Economy, Springer, Cham, 2024.

[6] S. Dargaoui, M. Azrour, A. El Allaoui, A. Guezzaz, S. Benkirane, A. Alabdulatif, F. Amounas: Applications of Blockchain in Healthcare: Review Study, Ch. 1, IoT, Machine Learning and Data Analytics for Smart Healthcare, 1st Edition, CRC Press, Boca Raton, 2024.

[7] S. Dargaoui, M. Azrour, A. El Allaoui, A. Guezzaz, S. Benkirane: Authentication in Internet of Things: State of Art, Proceedings of the 6th International Conference on Networking, Intelligent Systems & Security, Larache, Morocco, May 2023, p. 3.

[8] C. Hazman, A. Guezzaz, S. Benkirane, M. Azrour: Enhanced IDS with Deep Learning for IoT-Based Smart Cities Security, Tsinghua Science and Technology, Vol. 29, No. 4, August 2024, pp. 929 – 947.

[9] A. E. M. Eljialy, M. Y. Uddin, S. Ahmad: Novel Framework for an Intrusion Detection System Using Multiple Feature Selection Methods Based on Deep Learning, Tsinghua Science and Technology, Vol. 29, No. 4, August 2024, pp. 948 – 958.

[10] M. Azrour, J. Mabrouki, A. Guezzaz, S. Benkirane, H. Asri: Implementation of Real-Time Water Quality Monitoring Based on Java and Internet of Things, Ch. 8, Integrating Blockchain and Artificial Intelligence for Industry 4.0 Innovations, Springer, Cham, 2024.

[11] S. Dargaoui, M. Azrour, A. El Allaoui, A. Guezzaz, S. Benkirane, A. Alabdulatif, F. Amounas: Internet-of-Things-Enabled Smart Agriculture: Security Enhancement Approaches, Proceedings of the 4th International Conference on Innovative Research in Applied Science, Engineering and Technology (IRASET), Fez, Morocco, May 2024, pp. 1 – 5.

[12] A. Balasundaram, S. Routray, A. V. Prabu, P. Krishnan, P. Priya Malla, M. Maiti: Internet of Things (IoT)-Based Smart Healthcare System for Efficient Diagnostics of Health Parameters of Patients in Emergency Care, IEEE Internet of Things Journal, Vol. 10, No. 21, November 2023, pp. 18563 – 18570.

[13] A. Aditya, S. Anwarul, R. Tanwar, S. K. Vamsi Koneru: An IoT Assisted Intelligent Parking System (IPS) for Smart Cities, Procedia Computer Science, Vol. 218, 2023, pp. 1045 – 1054.

[14] C.- T. Chen, C.- C. Lee, I.- C. Lin: Correction: Efficient and Secure Three-Party Mutual Authentication Key Agreement Protocol for WSNs in IoT Environments, PLoS ONE, Vol. 15, No. 6, April 2020, p. e0234631.

[15] D. Kumar, S. Chand, B. Kumar: Cryptanalysis and Improvement of a User Authentication Scheme for Wireless Sensor Networks Using Chaotic Maps, IET Networks, Vol. 9, No. 6, November 2020, pp. 315 – 325.

[16] D. Kaur, D. Kumar, K. Kumar Saini, H. S. Grover: An Improved User Authentication Protocol for Wireless Sensor Networks, Transactions on Emerging Telecommunications Technologies, Vol. 30, No. 10, October 2019, p. e3745.

[17] J. Oh, S. Yu, J. Lee, S. Son, M. Kim, Y. Park: A Secure and Lightweight Authentication Protocol for IoT-Based Smart Homes, Sensors, Vol. 21, No. 4, February 2021, p. 1488.

[18] P. Kumar Panda, S. Chattopadhyay: A Secure Mutual Authentication Protocol for IoT Environment, Journal of Reliable Intelligent Environments, Vol. 6, No. 2, June 2020, pp. 79 – 94.

[19] M. Dammak, O. R. M. Boudia, M. A. Messous, S. M. Senouci, C. Gransart: Token-Based Lightweight Authentication to Secure IoT Networks, Proceedings of the 16th IEEE Annual Consumer Communications & Networking Conference (CCNC), Las Vegas, USA, January 2019, pp. 1 – 4.

[20] L. Kou, Y. Shi, L. Zhang, D. Liu, Q. Yang: A Lightweight Three-Factor User Authentication Protocol for the Information Perception of IoT, Computers, Materials & Continua, Vol. 58, No. 2, 2019, pp. 545 – 565.

[21] T. M. Butt, R. Riaz, C. Chakraborty, S. S. Rizvi, A. Paul: Cogent and Energy Efficient Authentication Protocol for WSN in IoT, Computers, Materials & Continua, Vol. 68, No. 2, April 2021, pp. 1877 – 1898.

[22] V. O. Nyangaresi: Lightweight Anonymous Authentication Protocol for Resource-Constrained Smart Home Devices Based on Elliptic Curve Cryptography, Journal of Systems Architecture, Vol. 133, December 2022, p. 102763.

[23] J. Cui, F. Cheng, H. Zhong, Q. Zhang, C. Gu, L. Liu: Multi-Factor Based Session Secret Key Agreement for the Industrial Internet of Things, Ad Hoc Networks, Vol. 138, January 2023, p. 102997.

[24] S. Yu, K. Park: ISG-SLAS: Secure and Lightweight Authentication and Key Agreement Scheme for Industrial Smart Grid Using Fuzzy Extractor, Journal of Systems Architecture, Vol. 131, October 2022, p. 102698.

[25] R. Krishnasrija, A. Kr. Mandal, A. Cortesi: A Lightweight Mutual and Transitive Authentication Mechanism for IoT Network, Ad Hoc Networks, Vol. 138, January 2023, p. 103003.

[26] [26] J. Lee, J. Oh, D. Kwon, M. Kim, S. Yu, N.- S. Jho, Y. Park: PUFTAP-IoT: PUF-Based Three-Factor Authentication Protocol in IoT Environment Focused on Sensing Devices, Sensors, Vol. 22, No. 18, September 2022, p. 7075.

[27] A. Kumar Yadav, M. Misra, P. Kumar Pandey, M. Liyanage: An EAP-Based Mutual Authentication Protocol for WLAN Connected IoT Devices, IEEE Transactions on Industrial Informatics, Vol. 19, No. 2, February 2023, pp. 1343 – 1355.

[28] P. Bagga, A. Mitra, A. Kumar Das, P. Vijayakumar, Y. Park, M. Karuppiah: Secure Biometric-Based Access Control Scheme for Future IoT-Enabled Cloud-Assisted Video Surveillance System, Computer Communications, Vol. 195, November 2022, pp. 27 – 39.

[29] S Kumar Dwivedi, R. Amin, S. Vollala: Design of Secured Blockchain Based Decentralized Authentication Protocol for Sensor Networks with Auditing and Accountability, Computer Communications, Vol. 197, January 2023, pp. 124 – 140.

[30] S. Rostampour, N. Bagheri, Y. Bendavid, M. Safkhani, S. Kumari, J. J. P. C. Rodrigues: An Authentication Protocol for Next Generation of Constrained IoT Systems, IEEE Internet of Things Journal, Vol. 9, No. 21, November 2022, pp. 21493 – 21504.

[31] [R. Kumar, S. Singh, P. Kumar Singh: A Secure and Efficient Computation Based Multifactor Authentication Scheme for Intelligent IoT-Enabled WSNs, Computers and Electrical Engineering, Vol. 105, January 2023, p. 108495.

[32] B. Khalid, K. N. Qureshi, K. Z. Ghafoor, G. Jeon: An Improved Biometric Based User Authentication and Key Agreement Scheme for Intelligent Sensor Based Wireless Communication, Microprocessors and Microsystems, Vol. 96, February 2023, p. 104722.

[33] R. Hajian, A. Haghighat, S. H. Erfani: A Secure Anonymous D2D Mutual Authentication and Key Agreement Protocol for IoT, Internet of Things, Vol. 18, May 2022, p. 100493.

[34] C. Patel, A. K. Bashir, A. A. AlZubi, R. Jhaveri: EBAKE-SE: A Novel ECC-Based Authenticated Key Exchange Between Industrial IoT Devices Using Secure Element, Digital Communications and Networks, Vol. 9, No. 2, April 2023, pp. 358 – 366.

[35] M. Azrour, J. Mabrouki, R. Chaganti: New Efficient and Secured Authentication Protocol for Remote Healthcare Systems in Cloud-IoT, Security and Communication Networks, Vol. 2021, No. 1, January 2021, p. 5546334.

[36] S. Dargaoui, M. Azrour, A. El Allaoui, A. Guezzaz, S. Benkirane: Machine Learning for Security Boosting in Internet of Things Environments, Ch. 8, Recent Advances in Internet of Things Security, 1st Edition, CRC Press, Boca Raton, 2025.

[37] P. Gope, 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, November 2016, pp. 7124 – 7132.

[38] A. Ghani, K. Mansoor, S. Mehmood, S. A. Chaudhry, A. Ur Rahman, M. Najmus Saqib: Security and Key Management in IoT-Based Wireless Sensor Networks: An Authentication Protocol Using Symmetric Key, International Journal of Communication Systems, Vol. 32, No. 16, November 2019, p. e4139.

[39] D. Q. Bala, S. Maity, S. Kumar Jena: Mutual Authentication for IoT Smart Environment Using Certificate-Less Public Key Cryptography, Proceedings of the 3rd International Conference on Sensing, Signal Processing and Security (ICSSS), Chennai, India, May 2017, pp. 29 – 34.

[40] N. Li, D. Liu, S. Nepal: Lightweight Mutual Authentication for IoT and Its Applications, IEEE Transactions on Sustainable Computing, Vol. 2, No. 4, October 2017, pp. 359 – 370.

[41] Q. Jiang, J. Ma, F. Wei, Y. Tian, J. Shen, Y. Yang: An Untraceable Temporal-Credential-Based Two-Factor Authentication Scheme Using ECC for Wireless Sensor Networks, Journal of Network and Computer Applications, Vol. 76, December 2016, pp. 37 – 48.

[42] D. He, N. Kumar, N. Chilamkurti: A Secure Temporal-Credential-Based Mutual Authentication and Key Agreement Scheme with Pseudo Identity for Wireless Sensor Networks, Information Sciences, Vol. 321, November 2015, pp. 263 – 277.

[43] X. Li, J. Niu, S. Kumari, F. Wu, A. Kumar Sangaiah, K.- K. R. Choo: A Three-Factor Anonymous Authentication Scheme for Wireless Sensor Networks in Internet of Things Environments, Journal of Network and Computer Applications, Vol. 103, February 2018, pp. 194 – 204.

[44] M. A. Qureshi, A. Munir: PUF-IPA: A PUF-Based Identity Preserving Protocol for Internet of Things Authentication, Proceedings of the IEEE 17th Annual Consumer Communications & Networking Conference (CCNC), Las Vegas, USA, January 2020, pp. 1 – 7.

[45] M. T. Hammi, B. Hammi, P. Bellot, A. Serhrouchni: Bubbles of Trust: A Decentralized Blockchain-Based Authentication System for IoT, Computers & Security, Vol. 78, September 2018, pp. 126 – 142.

[46] D. Dolev, A. Yao: On the Security of Public Key Protocols, IEEE Transactions on Information Theory, Vol. 29, No. 2, March 1983, pp. 198-208.

[47] B. Blanchet, B. Smyth, V. Cheval, M. Sylvestre: ProVerif 2.05: Automatic Cryptographic Protocol Verifier, User Manual and Tutorial, INRIA, Paris, 2023.

[48] B. Hu, W. Tang, Q. Xie: A Two-Factor Security Authentication Scheme for Wireless Sensor Networks in IoT Environments, Neurocomputing, Vol. 500, August 2022, pp. 741 – 749.

[49] Q. Xie, Z. Ding, B. Hu: A Secure and Privacy-Preserving Three-Factor Anonymous Authentication Scheme for Wireless Sensor Networks in Internet of Things, Security and Communication Networks, Vol. 2021, No. 1, January 2021, p. 4799223.

[50] X. Wang, Y. Teng, Y. Chi, H. Hu: A Robust and Anonymous Three-Factor Authentication Scheme Based ECC for Smart Home Environments, Symmetry, Vol. 14, No. 11, November 2022, p. 2394.

[51] J. Pirayesh, A. Giaretta, M. Conti, P. Keshavarzi: A PLS-HECC-Based Device Authentication and Key Agreement Scheme for Smart Home Networks, Computer Networks, Vol. 216, October 2022, p. 109077.

[52] M. A. Khan, B. A. Alzahrani, A. Barnawi, A. Al-Barakati, A. Irshad, S. A. Chaudhry: A Resource Friendly Authentication Scheme for Space–Air–Ground–Sea Integrated Maritime Communication Network, Ocean Engineering, Vol. 250, April 2022, p. 110894.

[53] A. Kumar Yadav, M. Misra, P. Kumar Pandey, K. Kaur, S. Garg, X. Chen: A Provably Secure ECC-Based Multi-Factor 5G-AKA Authentication Protocol, Proceedings of the IEEE Global Communications Conference (GLOBECOM), Rio de Janeiro, Brazil, December 2022, pp. 516 – 521.

[54] S. Dargaoui, M. Azrour, A. El Allaoui, A. Guezzaz, S. Benkirane, A. Alabdulatif, F. Amounas: IoT-Driven Smart Agriculture: Security Issues and Authentication Schemes Classification, Proceeding of the International Conference on Connected Objects and Artificial Intelligence (COCIA), Casablanca, Morocco, May 2024, pp. 61 – 66.