Energy Efficient Authentication Scheme for Industrial Smart Grid Environments

***Abstract*—** **Optimization of resource consumption and decreasing the response time of authentication requests is an immense urgent requirement in large Smart Grids (SG) for supporting the scalability of resources. Previous works attempted to address these issues. However, our analysis inferred that the existing schemes lack in the creation of a lightweight, secure architecture because of high operational costs. Thus, resulting in smart meters and transmission/distribution control centers consuming high electric and computing power. Further, it leads to an increase in the burden on storage memory. It also creates heavy traffic on a communication channel between smart meters and control centers, in-turn increasing the response time of devices authentication requests. As response time increases for processing authentication requests, a significant loss is incurred by the application in maintaining a quality of service. To address these shortcomings, we proposed a lightweight, secure architecture that uses crypto-modules, which optimize usage of one-way hash functions and elliptic-curve cryptography operation. We demonstrated the proposed scheme's security strength in a simulated SG environment using informal analysis by considering widely accepted AVISPA, and ProVerif tool. The result confirmed the proposed scheme security strength, and moreover, it satisfies the goal of secure design in smart grids. Further, we calculated the working cost of the proposed scheme for an enterprise-level smart grid by implementing it using standard Pairing-Based Cryptography (PBC) library on smart meters. The result of implementation proved that the proposed scheme is light in weight and removed the existing gaps. This makes the proposed scheme efficient to handle authentication requests made by smart meters that see a tremendous spike in demand occasionally. Hence, it is optimal for deployment in real-world scenarios.**

***Index Term:* Smart GridAuthentication scheme; Elliptic-curve cryptography (ECC); Internet of things; Cloud; Smart meters; Distribution control center.**

1. INTRODUCTION

o

WING to the fast advancement of cutting-edge innovation in the realm of ubiquitous computing, the Industrial Smart Grid (SG) environments has caught significant consideration from the Internet of Thing (IoT) business and network communication [1]. Therefore, to deal with exponentially growing heterogeneous data and devices in SG applications, IoT is being connected to a standard cloud platform. In such a platform, important information about individuals is stored. Therefore, the safety, privacy, and security of such data are of paramount information a standard cloud platform. In such a platform, important information about individuals is stored. Therefore, the safety, privacy, and security of such data are of paramount information [2]. Hence, unauthorized internet clients must not be allowed to access data from private cloud servers. The entire array of security strategies for SG-IoT applications can be supported by designing an efficient authentication process. Because of this, the authentication process is the principal first layer of security against potential attackers. The selection of the appropriate authentication technique relies mainly on devices and sensor configurations, both of which determine the power and energy consumption. SG-IoT devices such as smart meters (SM) and control centers (i.e., a service provider (SP)) have limited their

power and computing capabilities. This limitation is because of such devices having low memory, low power, low battery, and network confinement [3]. Therefore, the encryption techniques (i.e., appropriate authentication protocol) have to be tailored for application in the scenario. Considering the need for SG-IoT devices and sensors, the existing research attempted in the direction of designing lightweight-authentication protocols and started designing protocol based on elliptic-curve cryptography (ECC), which is one of the profitable open-key cryptographies [4]. However, in our analysis, we found that the existing schemes provided a secure authentication scheme at the cost of the high operational (i.e., computation, communication, and storage) costs. Due to the limited capacity of SG-IoT devices and the high operational cost of existing schemes, the scheme proposed by existing researchers unnecessarily consumes much electric power, storage, computation energy for computing challenges parameters, and verification process. In many cases, therefore, there are chances of overheating and damaging SG devices, which increase the cost of maintenance. Also, due to engaging in the use of additional resources in a limited SG environment, huge device authentication requests need to wait for a considerable time for authentication verification. Furthermore, by sending heavyweight communication parameters (i.e., authentication challenges), the existing high communication cost authentication system creates an additional burden on the communication channel. This is considered a significant loss. It greatly degrades the quality and performance of the SG industry while handling scalability issues and governing huge processing of large (i.e., million or zillion) number of authentication requests.

To address the aforementioned problems more efficiently, this paper presented an energy-efficient, lightweight, secure authentication protocol for SG-IoT application. Firstly, we analyzed various recent studies and identified the various factors that include ECC point multiplication that will help to reduce the operational cost. We significantly reduced the number of ECC point multiplication operation in the proposed scheme, and which helped us to make the scheme lightweight and improve the performance over existing schemes. To test the performance of the proposed scheme, we implemented standard Pairing-Based Cryptography (PBC) [5] library on a smart meter that computes the primitive timing of the various cryptography operations included in the proposed scheme and the existing schemes. Using this primitive timing, we computed the operational cost of the proposed scheme and some recent schemes and compared it. The result of the comparison shows that the proposed scheme is lightweight in designing and require lower operational cost overhead. Then, we also demonstrate that the proposed scheme is secure under the elliptic curve Diffie Hellman problem (ECDHP) [4] and the computational Diffie Hellman problem (CDHP) [1]. We verified it using mathematical informal security analysis. Then, we implemented code for a proposed scheme in widely

accepted automated validation of internet security protocol and application (AVISPA) tool [6], and ProVerif tool [7] to check the correctness of informal security analysis and our claim of stronger security. The result of the analyses and comparison with existing schemes demonstrates that compared with existing schemes, the proposed scheme is more dominant, productive, secure against all actives, and passive attacks and achieve the goal of secure design. This rendering our scheme more effective and realistic for handling a huge number of authentication requests in SG-IoT environments and removed the existing weakness in recent schemes.

This paper is organized as follows. Section II presents the related state-of-the-art works, and existing weakness, mathematical preliminary used in the proposed scheme. The proposed ECC-based protocol is introduced in Section III. In Section IV, we present the cryptoanalysis of the proposed protocol by utilizing the informal security analysis, automated validation of internet security protocol and application (AVISPA) tool, and ProVerif tool. Furthermore, we present the performance and proficiency assessments of the proposed scheme using the PBC library in comparison with the existing schemes in Section V. Finally, in Section VI, we present the conclusions and future work.

II. RELATED WORK

1. ***Overview of Related Works***

Every smart meter (SM) sends daily consumption of usage of electricity to the service provider (SP) after every 15/30/60 minutes []. Therefore, the authentication scheme plays a major role in initiate efficient and secure communication between SM and SP. In this subsection, we selected recent IoT studies which are suitable to address this application scenario in SG. In 2019, Zhou et al. [8] study presented a lightweight authentication scheme, which secures against password guessing attack, insider attack, and user anonymity attack. Zhou et al. also claimed that their scheme is efficient against computational-limited smart devices. However, we found in our study that the Zhou et al. scheme has a high cost of communication, which weakens their aforementioned claim. Yu et al. [9] proposed a lightweight authentication scheme, which provided protection against replay attack, embedded device impersonation attack, forward secrecy, and user anonymity attack. Yu et al. also guaranteed secure mutual authentication and an efficient and ideal for realistic IoT-based solutions. However, we found that Yu et al. scheme has high communication costs. Xie et al. [10] enhanced Wang et al.'s [11] scheme (i.e., prone to key compromise impersonation (KCI) attack) and introduced a secure authentication scheme for the IoT application scenario like SG. However, Xie et al. scheme provide security at the cost of high communication and computation costs. Chatterjee et al. [12] proposed an ECC based, lightweight three-way authentication scheme. They also reported that their scheme provides security at less computation and communication overhead. However, we found that Chatterjee et al. scheme has high computation, communication, and storage cost, which weakens their claim. Yu et al. [13] introduced a secure authentication scheme for IoT applications scenario such as SG and claimed robust performance for devices. However, Yu et al. scheme have high computation and storage costs. Sengupta et al. [14] presented novel authentication scheme and claimed its realistic for IoT applications scenario like SG. However, Sengupta et al. scheme have higher communication and storage cost. Yang et al. [15] proposed an authentication scheme for information exchange in IoT communications. However, Yang et al. scheme suffer from high

communication and storage cost. Wang et al. [16] implemented an innovative authentication system and guaranteed optimum security capabilities with reasonable overheads for computation and communication. Wang et al., however, scheme high computation cost and communication, which weaken their aforementioned claim. Wazid et al. [17] presented a lightweight authentication scheme using fuzzy extractors and claimed enhanced security with a low computation and communication overhead. However, we noticed that the storage cost of the Wazid et al. scheme is very high.

***B. Weakness because of the high operational costs***

In the previous subsection, we studied various existing schemes, their essential lacking lightweight requirements for designing a secure authentication protocol in IoT based SG environments. In this subsection, we focus on problems that occur in embedded devices (i.e., SM) because of high operational (i.e., either high computation or communication or storage) cost are as follows:

**1) Intake of more memory:** The current system has high storage costs, which raises memory usage in low storage SM, impacting system efficiency (i.e., a low SM processor requires considerable time to execute large memory content) to some extent [18].

**2) High electric power intake:** The current scheme has high operatingcosts. Since the level of computing power consumption is directly proportional to the amount of energy, the system absorbs. Therefore, due to the high operating costs, the current scheme requires high machine computational power, which results in more electrical power consumption causes overheating and damaging of SM [19]. It increases the cost of maintenance.

**3) High Computing power intake:** The current system has high computing costs, indicating the enormous number of authentication requests generated (i.e., million or trillion) demanding massive processing power to execute the authentication request in low storage SM devices. Consequently, this results in a loss of SM efficiency [19].

**4) Increase traffic on communication channel:** The existing scheme has high transmission costs, implying the transition of high bit parameters in the channel. However, transferring several high bits into a real scenario for a huge number of authentications will greatly increase the burden on the medium of communication [19].

**5) Increase authentication response time:** Limited capacity SM uses more computing processing power due to high operational cost. Therefore, it increases the execution and response time for an authentication request, which is considered lost in a huge real-time scenario [19].

***C. Mathematical preliminary***

The detailed definition of ECC and the hash operation mentioned in [4]. The following property of ECC multiplication and *h()* we inherited in the proposed scheme:

**Property 1:** Elliptic Curve Discrete Logarithm Problem (ECDLP). Let n is a positive integer with two-point P, Q on the curve , such that Q=n.P. Therefore, to obtain n in polynomial time, even if P and Q are identified, is computationally infeasible for a large prime p [4].

**Property 2:** Computational Diffie Hellman Problem (CDHP). For, an a, b [1, n-1], given P, aP and bP, difficult to compute abP [1].

**Property 3:** Collision-Resistant One-Way Hash Function (*h*())

[4]. The hash function *h()* is collision resistant if it is hard to find two inputs that hash to the same output; that is, two inputs x and

y such that *h*(x) = *h*(y), and x ≠ y. (e.g., SHA-256) where function *h*() is one way invertible function.

TABLE I

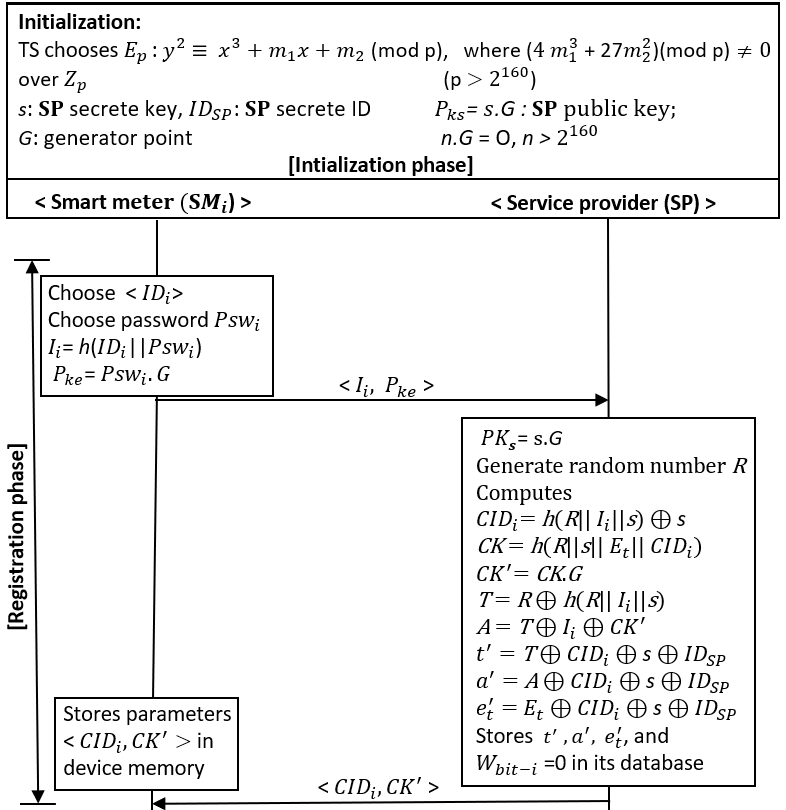
NOTATIONS GUIDE

|  |  |
| --- | --- |
| **Notations** | **Description** |
|  | Secret password of the smart meter (SM) |
|  | Public key of the SM |
|  | Public key of the service provider server (SP) |
|  | Hashed smart meter ID |
|  | Server-generated smart meter ID |
|  | Session cookie |
|  | Server private key |
|  | Server database table encryption key |
|  | Challenges |
|  | Ephemeral secretes |
|  | Expiration time of the cookie |
|  | Equations |
|  | Session key |
|  | Unique secrete Identity of server SP |
|  | Tamper Proof device storage table encryption   key |

III. PROPOSED ECC-BASED PRIVACY-PRESERVING AUTHENTICATION SCHEME

In the previous section, we analyzed that existing schemes were secure; however, fail to maintain lightweight because of the high

the operational cost involved. Therefore, to address this issue, in this section, we studied the existing research and optimized the efficient use of multiplication operations (.) (i.e., it includes ECDLP and CDHP), a hash function (h), concatenation (||), and an exclusive-or operation () and proposed lightweight, the secure authentication scheme for SM communication. The proposed scheme consists of the following two phases: the registration phase and the password-authentication phase, which includes the session-key-distribution phase. Note that we proposed a scheme for tamperproof SM (i.e., embedded devices) and the service provider (SP) based application [21]. The security of tamperproof SM ensures the owner of the devices unable to access any kind of data stored in SM. In addition, to launch an attack on successfully SM, an attacker needs special equipment whose cost even higher than SM; thus, an attacker cannot have economic incentives to mount an attack on tamperproof devices [21]. Therefore, tamperproof SM improves the security strength of the proposed protocol. The proposed scheme design is depicted in Figs. 1, and 2. We used different notations for the ease of explanation, which is listed in Table I. For proposed scheme security, we defined the ECC definition in the initial phase.

Fig. 1. Proposed ECC-based signup scheme

***A. Initialization phase***

Until beginning the registration process, SP chooses an elliptical curve equation : (mod p) over , where (p ) is the finite range of the group. SP selects two fields respectively and , where and must obey condition + 27. Let G be the base point with a prime order n (n ) and O be the point at infinity such that n×G=O. Then, SP chooses arbitrary nonce (s) as its secrete key [22].

***B. Registration phase***

In the beginning, to make a user legal, before selling a product to the owner, the company of device must register itself to the third trusted party through a secure channel. Fig. 1 shows the details of the registration phase, which are as follows:

***Step 1.*** Initially, the device registers an authenticated identity with a service provider (SP*)*; to that end, the SM chooses a password for computing hashed identity ) which will protected SM from a user or device anonymity attack.

***Step 2.*** Then sends the registration request < toSP through a trusted channel. Where = is a public key of , which ensure the security of by using the concept of ECDLP.

***Step 3.*** SPchecks whether has been registered. If has not been registered, SPselects a random number *R* and computes server-generated unique identity (=h(R||||s )s) for uniquely identifying The security of is well protected in SP by using ECDLP (). Then SP, compute a unique session cookie for The security of is protected in SP by using ECDLP (. Then SP computes challenge *T =Rh*(*R||||s* )hide it inside another challenge (*A=T*) using the and Finally, to protect the security of challenges *T* and *A,* SP hides them

inside it also hides expiration time () of the cookie inside . Subsequently, SPstores parameters <> on its server (SP) database sets the working bit as , and sends <,> to through a secure, trusted channel. The servers encrypt the table using their personal secret keys =. The security of key (is well protected by the concept of ECDLP and CDHP. The device also encrypts their table using their personal secret keys =. The security of key (is well protected by the concept of ECDLP. Note that during the registration process, before handover SM to their owner, the company performs the registration process through a secure channel (i.e., wolfSSL [23]). Once the device successfully registers to the SP, the company hand over the registered tamper proof [21] product to the owner. Then, every time while initiating communication with SP, owner device must authenticate to the SP through an open communication channel, and then after successful authentication, SM sends an encrypted message to the SP using their session key

***C. Authentication phase***

Initially, each registered participant client device requires to be

be authenticated with SP to start communication (See Fig. 2). Therefore, the authentication of the registered devices with SP proceeds as follows:

***Step 1***. : . The legitimately registered device randomly selects an ephemeral secret

and computes challenges using ECC point multiplication, hides inside and finally sends the challenge through a open channel. The security of inside both and is protected by the concept of ECDLP and CDHP.

***Step 2.*** :  After receiving the challenge, SP recomputes and extract parameters () from know parameter <> of the SP (i.e., it computes s, , h(R||||s )R=h(R||||s ), ), and then SP computes and checks whether If the deduction from both sides is unsuccessful, the session is terminated; otherwise, proceed to the further steps. Subsequently, SP randomly selects an ephemeral secret , and then compute challenges by using ECC point multiplication, hides inside, and finally sends challenges through an open channel. The security of inside < and > is protected by the concept of ECDLP and CDHP.

***Step 3***. Computation of the session key =: After receiving the challenges from SP, recomputes A= and checks whether . If the deduction from both sides is unsuccessful, the session is terminated; otherwise, proceed to the further steps. Subsequently, the computes the last challenge *()* using the session key and send challenges to SP through an open channel. After receiving the challenges, recomputes and checks whether *()*. If

the deduction from both the sides leads is unsuccessful, the session is terminated; otherwise, proceed to the further steps. Finally, after successful deduction on both the sides, the computes the session key ).....................................................................

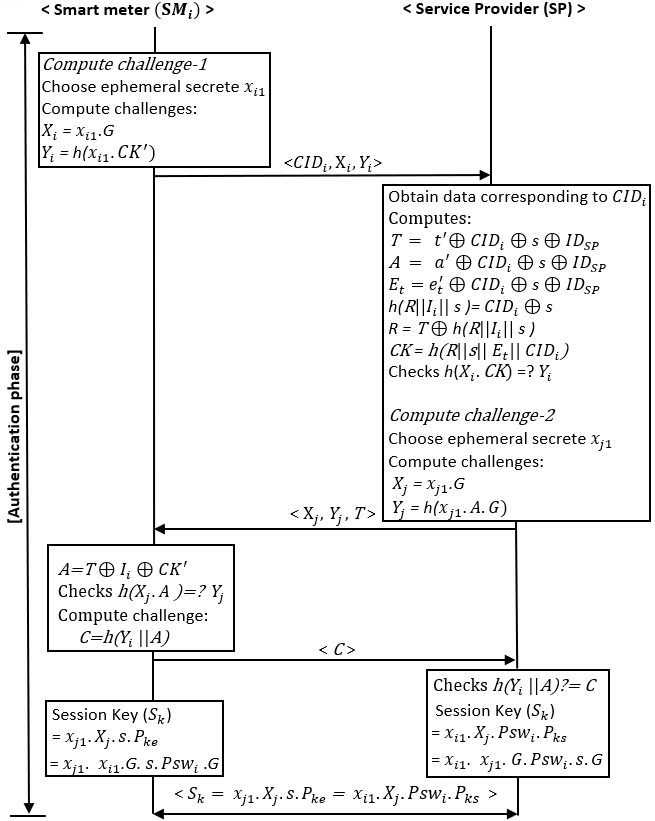


Fig. 2. Proposed ECC-based login scheme

***D. Password-change phase***

To change the password, the embedded devices first perform authentication and authorization and prove their genuineness. Note that communications are encrypted using a session key which ensures the security of the password change phase. The details of the password change are as follows:

***Step 1.*** : The authorized legitimated embedded device selects a new password and then recomputes the hashed identity and public key (=. Subsequently, it sends the updated <to SP through a channel by using the session key .

***Step 2***. : Furthermore, SP receive updated parameters < and repeat the same procedures as mentioned in the registration phase for an updated parameter. A detailed explanation is given in [].

IV. CRYPTOANALYSIS OF THE PROPOSED PROTOCOL

In this section, we analyze the security strength of the proposed scheme using informal security analysis (i.e., mathematical verification). Also, we verified the correctness of our mathematical explanation, by using AVISPA, and ProVerif simulation tool.

***B. Informal security analysis***

For ensuring the security of the proposed scheme, we used the collision-free one-way hash function and two hard problems: the ECDHP and CDHP*.* The proposed scheme is targeting optimized performance at a lower cost. Therefore, in this subsection, we present how the proposed scheme is secure against those known cryptographic attacks, which affect the performance of the authentication scheme as follows:

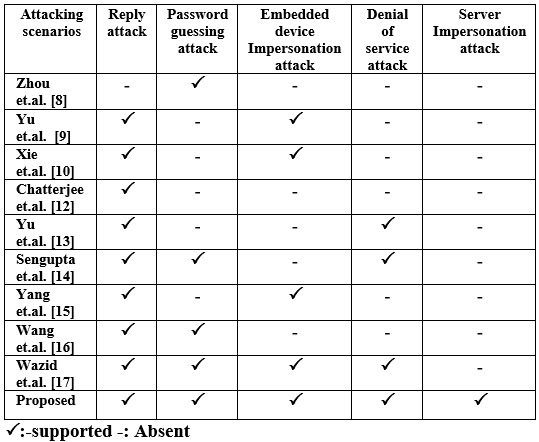
**1)** **Replay attacks**: In this attack, an adversary may impersonate a legitimate user by reusing the message obtained from a previous protocol run and transfer it to the SP. After receiving the log-in request, SP computes and verifies whether and sends back new challenges > to . However, after impersonating messages <> send to , the attacker would be unable to compute without knowing and . Notably, both and are neither sent through any messages over public channel nor can be acquired from the embedded device because of its tamper-proof design [21]. Thus, it cannot verify the challenge . Without the knowledge of the secret key of the device and server, the attacker cannot compute the valid session key ). Also, the security of the session key is well protected by ECDLP and CDHP. Therefore, it almost impossible to extract private key <> of the device, and the server in polynomial time. Hence, the proposed scheme is secure against replay attacks.

**2) DoS attacks**:To prevent the proposed scheme from DoS attack**,** the server (SP) terminatesthe login session if the number of incorrect attempts to enter reaches the maximum limit.However, the login request will be continued as soon as the correct is entered. Furthermore, in the login phase, assume

the adversary replaces message <with> by randomly selecting the elliptical curve point and sent it back to SP; however, the SP computes and compares the previous value with the received If SP finds a difference between both the values, it terminates the protocol with a failure message to the user. Therefore, the proposed scheme is secure for DoS attacks.

TABLE II

SECURITY ATTRIBUTES COMPARISON



The resource optimization of the SG system can be influenced by the success of a major attack (i.e., DOS and Replay attack) [24]. The proposed scheme is, however, protective against both attacks. Thus, it ensures the security of the performance of the proposed scheme. In addition, we have mentioned a couple of security attacks that can affect the performance of the authentication scheme at certain extent as follow:

**3) Password-guessing attacks**: In the proposed scheme, an embedded device password store in the form ofa password generator (i.e., public key )) and wrapped in the form of . Consequently, the attacker cannot guess the password without knowing and . Therefore, the proposed scheme maintains the security of the password by using ECDLP and a hash function (*h*()). Notably, of is neither sent through any messages over open public channel nor can be acquired from the embedded device because of its tamper-proof design (i.e., nor is it stored in the and SP). Therefore, the proposed scheme prevented the password-guessing attack.

**4) Server Impersonation attacks**: Assume the scenario, where the phase of authentication of is impersonated by an adversarial server. An adversarial server impersonates receives the parameters <, , > from Then adversary server randomly chooses parameters <, > and send it back to the

After receiving parameters <, >, the computes factor and check *h*( = ? . However, equivalence does come wrong. This is because of, an attacker randomly computes challenge *T* as and completely unaware about challenge A. In addition, attackers unable to compute a session key. This is due to attacker unable to extract private server key (s) or device password ( from past session key due to its security protected by ECDLP and CDHP. Further, the security of s is protected in server ) by ECDLP and CDHP. Therefore, the proposed scheme is secure against the server impersonation attack.

**5) Server database stolen attacks**: In this case, if an attacker makes a server database attack, however, an attacker is unsuccessful in breaking the table of the server database. Since the security of the server, the database is protected by an encryption keywhose security protected by ECDLP and CDHP. Therefore, an attacker unable to extract either s or from In addition, even if the attacker got s by any means, the attacker still unable to extract from . Further, if encryption key of the server is compromised by somehow, however, attacker unable to extract security parameter <> from <>. This is due to parameters security is still protected by and s. Therefore, the proposed scheme is preventive against the server database stolen attack.

**6) Embedded device Impersonation attacks** or **Key compromise impersonation attacks:** In this case, if an attacker impersonates toward server (SP) as real embedded devices by replaying the previous intercept message. However, an attacker still lacking secrete parameters <>. This is due to, that secrete parameter is protected due to tamper-proof design of In addition, of in and in is protected by hash function *h*() and ECDLP, respectively. Therefore, attacker unable to compute *A=T*

correctly without knowing parameters,. Result into incorrect deduction *h*(=? which leads to the termination of the session. Further, an attacker is unsuccessful in extracting from the past session key whose security is protected by ECDLP and CDHP. Therefore, an attacker unable to compute a session key for a current session without knowing Therefore, from the above reasons, an attacker fail to launch embedded device impersonation attacks on .

Finally, due to the page limit, we explain other security attacks (i.e., many logged-in users attack, forward secrecy, insider attack, known session-specific temporary information attack, user anonymity attack, and many others attacks) prevention mechanism for a proposed scheme in [25]. Then, we selected some security attributes (i.e., usually protect the security of an authentication protocol) for comparison. We compare those security attributes of some current schemes [8-10, 12-17] with those of the proposed scheme, as presented in Table II. The comparison demonstrates that the proposed scheme is free from all the shortcomings within the existing schemes.

***C. Formal security validation using AVISPA tool***

In this section, we perform the simulation of the proposed scheme

by utilizing the widely accepted AVISPA tool [6] and ensure that the proposed scheme is secure against both man-in-the-middle and replay attacks. The AVISPA tool is coded in one of the power languages (i.e., high-level protocol specification language (HLPSL)). We implemented the proposed scheme code on a SPAN Ubuntu 10.10 virtual machine [6] wit RAM=2048 GB. This experimental set up install on originally window 10 PC with an Intel Core i5-8500,6-core 3.10 GHz CPU provided by the service provider. The Avispa simulation used SPAN software to assess the security strength of the proposed protocol against both active and passive attacks using AVISPA toolset [6]. The detailed explanation and code implementation for embedded devices () and server (SP) for the proposed scheme found in [25]. Therefore, on the basis of analyzing the simulation result on the CL-AtSe and OFMC backend, we conclude that the proposed protocol is safe as follows:

**1)** **Replay attack**: For the replay-attack check, the CL-AtSe and OFMC backend confirm whether the genuine agents can execute the specified protocol by inquiring an inactive intruder. This

backend gives the interloper the information of some normal sessions among the genuine agents. The test outcomes appeared. Fig. 3 exhibit that our scheme is secure against the replay attack.

**2)** **Active and passive attack check**: The outline result for CL-AtSe and OFMC backend shows that the proposed scheme is SAFE, meaning that the proposed scheme is secure against all active and passive attacks [17].

**3)** **Dolev–Yao model check**: For performing the Dolev–Yao model check, the CL-AtSe, and OFMC backend additionally confirm whether there is any man-in-the-middle attack conceivable by an intruder. The outcomes in Fig. 3 show that our scheme satisfies the design properties and that it is additionally secure under this backend.

*D*. *Formal security validation using ProVerif tool*

ProVerif is widely accepted as an automatic cryptographic protocol verifier tool, in the symbolic model (so-called Dolev–Yao model) [8]. This protocol verifier depends on the portrayal of the protocol by Horn clauses. In this subsection, we implemented the proposed scheme code in the Proverif tool to test its correctness of mutual authentication. We perform this experiment on Intel Core i5-8500, 6-core 3.10 GHz CPU with window 10 operating system provided by a service provider. This simulation used ProVerif version 2.00 binary package [8] to stimulate the registration, mutual authentication, and session key agreement phase between an embedded device. The description of the ProVerif simulation tool for the proposed scheme can be found in [25]. Toward the end of the execution, three queries are executed to amend the correctness and secrecy of the proposed scheme. The consequences of the queries are shown in Fig. 4. The rightness of the proposed scheme is substantiated because the initial two queries are executed successfully, which indicate the successful beginning of initial interaction between devices and server, although its secrecy is affirmed because of an unsuccessful query (i.e., last query in queries section in Fig. 4) attack on the session key.

TABLE III

PRIMITIVE TIMING FOR CRYPTOGRAPHY OPERATION

|  |  |  |
| --- | --- | --- |
| **Operation** | **Terminology**  **(Executation time (ms))** | **Execution Time (ms)** |
| **Hash operation** |  | 0.039 |
| **ECC multiplication** |  | 0.110 |
| **Modular exponentiation** |  | 0.343 |
| **Pairing** |  | 0.992 |
| **Symmetric Encryption+Decruption** |  | 0.686 |

z

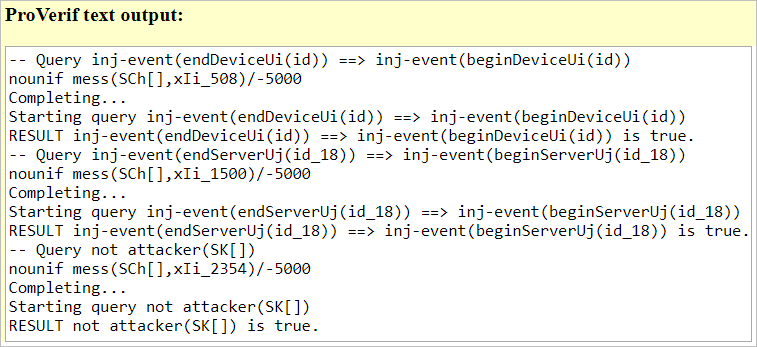


Fig. 4. Output of query execution

V. EVALUATION

In the previous section, we verified the security of our proposed

scheme by using the AVISPA tool. We also verified the mutual authentication and session-key agreement of the proposed scheme by using the ProVerif tool. In this section, we present how the proposed scheme is more efficient than the existing schemes in terms of computation, communication, and storage cost, based on performance analysis. Furthermore, we compared our proposed scheme with the recent schemes to evaluates its benefits.

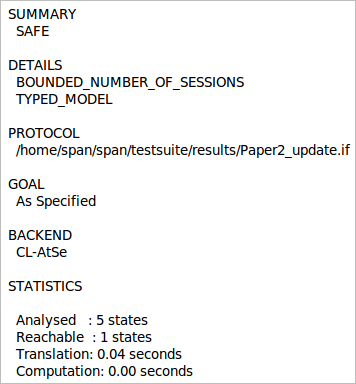
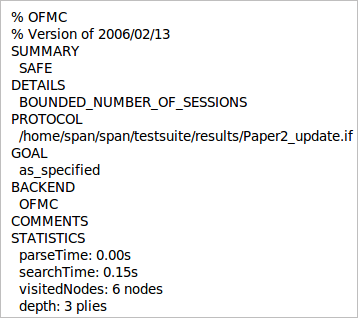
 

Fig. 3.Analysis result using the CL-AtSe and OFMC backend

*A. Performance Analysis*

In this section, we implemented the PBC library on embedded devices (SM) to calculate the primitive timing needed to measure the operational cost of the proposed scheme [5]. In the PBC library, we implemented a pairing operation on a curve = +x over the field for some prime q= 3mod4, where both and are the group of point belongs to the . We used the SHA-256 function to compute the cost of the general hash operation [26]. Our experimental set up consists of Ubuntu 12.04 virtual machine install on Intel Core i5-8500, 6-core 3.10 GHz CPU with window 10 operating system provided by a service provider. In the oracle environment virtual, we stimulated SM devices, and we set RAM to 256 MB and execution cap to 26 percent (i.e., it reflects a single-core 798 MHz CPU), which is not very far from a real SM configuration [27]. To calculate the primitive timing of different cryptography operations used in the proposed scheme, our simulation used pbc-0.5.14 library [5] and the GMP library [28]. Finally, we calculate and compare the operational cost of the proposed scheme using the PBC library to testify the performance of the proposed scheme. Table III summarizes the outcome of simulation performance analysis of PBC code, which we executed, along with terms used to describe different cryptographic operations.

**1) Computation cost:** Note that the computing costs of lightweight operations (i.e., XOR, concatenation, and comparison) were overlooked due to their inexpensive computation. At the authentication phase, a huge computing process is conducted. Hence, we measured the cost of the computation at the authentication phase. We computed the computation cost of some recent schemes along with the proposed scheme in Table IV. To compute cost, and we counted a number of and operational involved in the login phase where communication happens at the public open channel. Then, for each cryptography operation, we assigned the value we obtain in our PBC implementation (See Table III). From Table IV, it is clear that the computational costs of the schemes each proposed by Chatterjee et al., Yu et al., and Wang et al. scheme, and that of the proposed scheme are 11+13 = 1859, 1+6 = , 21+5 = , and 7+6 = , respectively. We evaluate that all computation cost value is in μs; however, this μs is the considerable maximum period when processing a

huge number of authentication requests (i.e., million and zillion) in a real-time scenario. We also computed the computation cost of some recent schemes. Comparing the computation costs of the existing schemes (see Table IV), the proposed scheme is more productive, by virtue of its lighter weight computation power, than the scheme recently proposed by existing schemes.

**2)** **Communication cost**: We used the parameter <q, r> each of the sizes <256, 224> bit during PBC library-based primitive timing calculation [10], and we choose this parameter since the suggested elliptic curve key length is 256 bit for NIST 2016-2030 [29] and for ECRYPR II 2031-2040 [30]. An ECC point therefore requires (128 + 128) =256 bits, where each parameter consumes 128 bits. The cost of other parameters for the communication element is described in Table V are , and. Thus, the communication cost is (640+640+128) = 1480 bits. Similarly, we computed the communication costs for the recent schemes and compared it with the proposed scheme. In comparison, we conclude that the communication cost of the proposed protocol

was less as compared to the existing scheme, as mentioned in Table IV.

**3) Storage cost**: Throughout this subsection, we measured the storage component cost dependent on the PBC library- applied on our machine, which meets NIST [29] and ECRYPR II [30] recommendations (See Table V). Table IV presents the computed storage cost of the components in the proposed scheme. To compute storage cost, we need to identify the number of components is stored in the embedded device's memory. In the proposed scheme, embedded device stores cookie, as well as pseudo-identity (i.e., ), thereby consuming 256 + 128 = 384 bits of memory (see Table IV). Likewise, we counted a number of components stored in their storage cost. Therefore, from Table V, we infer that the proposed scheme has a lower operational cost relative to other existing schemes. It also eliminated high operation costs weakness

TABLE V

COMMUNICATION COMPONENTS COST

|  |  |
| --- | --- |
| **Components** | **Size in bits** |
|  | 128 |
|  | 128 |
|  | 128 |
|  | 256 |
|  | (256+256+128) =640 |
|  | (256+256+128) =640 |
|  | (640+640+128) =1408 |

TABLE IV

COMPUTATION, COMMUNICATION AND STORAGE COST COMPARISON

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Schemes** | **Total cost ()** | **# of Messages** | **Communication   cost/bit** | **Storage cost/bit** |
| Zhou et. al. [16] | 36= 1404 | 4 | 3072 | 640 |
| Yu et. al. [17] | 34**=** 1326 | 4 | 2176 | 384 |
| Xie et. al. [18] | 9+7 = 1121 | 5 | 1792 | 384 |
| Chatterjee et. al. [20] | 11+13= 1859 | 4 | 2176 | 640 |
| Yu et. al. [21] | + 6 6= 3284 | 3 | 1408 | 768 |
| Sengupta et. al. [22] | 11+9= 1419 | 3 | 1408 | 640 |
| Yang et. al. [23] | 28 | 10 | 5376 | 512 |
| Wang et. al. [24] | 21+5= 4249 | 4 | 2304 | 768 |
| Wazid et. al. [25] | 34= 1326 | 3 | 1664 | 640 |
| **Proposed** | 7+6 = | **3** | **1408** | **384** |

in existing schemes as follow:

**1) Optimized intake of memory:** The proposed scheme has lower storage and computation costs compared to existing schemes implying that the proposed scheme is ideal to meet the real SM framework's needs for limited memory and low processing power.

**2) Optimized intake of electric power:** The amount of computing computer power consumption is directly proportional to the amount of energy the system uses [18]. Because the proposed scheme works in less computational power, it needs less energy and, therefore, it supports the efficient use of electricity, and avoided the chances of overheating and damaging of SM devices in SG environments.

**3) Optimized intake of computing power:** Because of the low execution cost (i.e., low cost = computation + communication + storage) of the proposed scheme relative to other existing schemes, the proposed scheme effectively help SM and SP to execute the request in small memory in more efficiently, which is significant contribution while handling a massive number of authentication requests in large industry scenario.

**4)** **Optimized intake and traffic on the communication channel:** Because of low communication costs, the proposed scheme transfers low bit messages over the communication channel, which is efficiently optimized the traffic over the communication channel.

**5) Optimized authentication response time:** The proposed scheme required less operational time to proceed with the authentication request due to low execution cost. Therefore, while governing the authentication requests of a huge scenario, the proposed scheme plays a huge role in executing authentication requests efficiently in quick response time.

VI. CONCLUSION AND FUTURE WORK

In this study, we examined numerous weaknesses (i.e., additional consumption of electric power, device memory, computing power, etc.) in recent authentication schemes due to failing to achieve the target of a lightweight, secure architecture, which considerably increase the authentication request response time. In addition, it increases overheating and damaging of the SM devices, which reduces its performance. To address this issue, we proposed a novel lightweight-computational authentication scheme. We confirmed our claim of lightweight security using widely accepted standard PBC, AVISPA, and ProVerif code implementation and mathematics formulation. The outcome of those confirms that in comparison to existing schemes, the proposed scheme lightweight in design and preventive against all kinds of active and passive attacks. This makes the proposed scheme reasonable and realistic for massive implementation scenarios based on industrial SG environments.

REFERENCES

1. Liu, J., Ren, A., Zhang, L., Sun, R., Du, X. and Guizani, M., 2019. A Novel Secure Authentication Scheme for Heterogeneous Internet of Thing. arXiv preprint arXiv:1902.03562.
2. Roy, S., Chatterjee, S., Das, A.K., Chattopadhyay, S., Kumari, S. and Jo, M., 2017. Chaotic map-based anonymous user authentication scheme with user biometrics and fuzzy extractor for crowdsourcing Internet of Things. IEEE Internet of Things Journal, 5(4), pp.2884-2895.
3. Yang, Y., Wu, L., Yin, G., Li, L. and Zhao, H., 2017. A survey on security and privacy issues in Internet-of-Things. IEEE Internet of Things Journal, 4(5), pp.1250-1258.
4. Dhillon, P.K. and Kalra, S., 2019. A secure multi-factor ECC based authentication scheme for Cloud-IoT based healthcare services. Journal of Ambient Intelligence and Smart Environments, 11(2), pp.149-164.
5. Pbc Library. Accessed: Mar. 16, 2020. [Online]. Available: <http://crypto.standford.edu/pbc/>
6. Avispa-project.org. (2020). *AVISPA Web Tool*. [online] Available at: http://www.avispa-project.org/web-interface/basic.php [[Accessed 16 Mar. 2020].
7. “Cryptographic Protocol Verifier in the Formal Model.” *ProVerif*, prosecco.gforge.inria.fr/personal/bblanche/proverif/.
8. Zhou, L., Li, X., Yeh, K.H., Su, C. and Chiu, W., 2019. Lightweight IoT-based authentication scheme in cloud computing circumstance. *Future Generation Computer Systems*, *91*, pp.244-251.
9. Yu, S., Park, K. and Park, Y., 2019. A Secure Lightweight Three-Factor Authentication Scheme for IoT in Cloud Computing Environment. *Sensors*, *19*(16), p.3598.
10. Xie, Z. and Jiang, L., 2020, January. An improved authentication scheme for the Internet of things. In IOP Conference Series: Materials Science and Engineering (Vol. 715, No. 1, p. 012031). IOP Publishing.
11. K.-H. Wang, C.-M. Chen, W. Fang, and T.-Y. Wu, “A secure authentication scheme for the internet of things,” Pervasive and Mobile Computing, vol. 42, pp. 15–26, 2017.
12. Chatterjee, S. and Samaddar, S.G., 2020. A robust lightweight ECC-based three-way authentication scheme for IoT in the cloud. In Smart Computing Paradigms: New Progresses and Challenges (pp. 101-111). Springer, Singapore.
13. Yu, Y., Hu, L. and Chu, J., 2020. A Secure Authentication and Key Agreement Scheme for IoT-Based Cloud Computing Environment. Symmetry, 12(1), p.150.
14. Sengupta, S., 2020. A Secured Biometric-Based Authentication Scheme in IoT-Based Patient Monitoring System. In Emerging Technology in Modelling and Graphics (pp. 501-518). Springer, Singapore.
15. Yang, S.K., Shiue, Y.M., Su, Z.Y., Liu, I.H. and Liu, C.G., 2020. An Authentication Information Exchange Scheme in WSN for IoT Applications. IEEE Access, 8, pp.9728-9738.
16. Wang, F., Xu, G., Xu, G., Wang, Y. and Peng, J., 2020. A Robust IoT-Based Three-Factor Authentication Scheme for Cloud Computing Resistant to Session Key Exposure. Wireless Communications and Mobile Computing, 2020.
17. Wazid, M., Das, A.K., Bhat, V. and Vasilakos, A.V., 2020. LAM-CIoT: Lightweight authentication mechanism in a cloud-based IoT environment. Journal of Network and Computer Applications, 150, p.102496.
18. Hester, R.E. and Harrison, R.M. eds., 2018. Energy Storage Options and Their Environmental Impact (Vol. 46). Royal Society of Chemistry.
19. Yu, W., Liang, F., He, X., Hatcher, W.G., Lu, C., Lin, J. and Yang, X., 2017. A survey on the edge computing for the Internet of Things. IEEE access, 6, pp.6900-6919.
20. Lo, J.W., Wu, C.Y. and Chiou, S.F., 2020. A Lightweight Authentication and Key Agreement Scheme for Telecare Medicine Information System. Journal of Internet Technology, 21(1), pp.263-272.
21. Kumari, S., Karuppiah, M., Das, A.K., Li, X., Wu, F. and Kumar, N., 2018. A secure authentication scheme based on elliptic curve cryptography for IoT and cloud servers. The Journal of Supercomputing, 74(12), pp.6428-6453.
22. Kalra, S. and Sood, S.K., 2015. Secure authentication scheme for IoT and cloud servers. Pervasive and Mobile Computing, 24, pp.210-223
23. wolfSSL. “WolfSSL Embedded SSL/TLS Library: Now Supporting TLS 1.3.” WolfSSL, www.wolfssl.com/.
24. Darwish, M., Ouda, A. and Capretz, L.F., 2017. Formal Analysis of an Authentication Protocol against External Cloud-Based Denial-of-Service (DoS) Attack. arXiv preprint arXiv:1711.09985.
25. Thakare, A., (2020). *AVISPA+ProVerif experiment*. [online] GitHub. Available at: < https://github.com/Abhijeet241093/Secure-and-Efficient-Authentication-Scheme-in-Industrial-IoT-Environments> [Accessed 6 April 2020].
26. Chen, Y., Martínez, J.F., Castillejo, P. and López, L., 2019. A bilinear map pairing based authentication scheme for smart grid communications: Pauth. IEEE Access, 7, pp.22633-22643.
27. Atmels Family of, Microchip. Atmel's Family of SM Devices. Accessed: Mar. 16, 2020. [Online]. Available: https://www.microchip.com/design-centers/smart-energy-products.
28. GMP source. Accessed: Mar. 16, 2020. [Online]. Library for Arbitrary Precision Arithmetic, Operating on Signed Integers, Rational Numbers, and Floating-Point Numbers. Available: https://gmplib.org/.
29. Recommendation for Key Management, Part 1: General, SP 800-57 Part 1 Rev. 4, NIST, Gaithersburg, MD, USA, Mar. 2020. [Online]. Available: https://www.keylength.com/en/compare/
30. Algorithms, Key Size and Protocols Report (2018), document H2020-ICT2014-Project 645421, D5.4, ECRYPT-CSA, Mar. 2020