Renewable Energy and Power Quality Journal (RE&PQJ)
ISSN 2172-038 X, Volume No.22, September 2024

Application and Optimization of Multi-Factor Authentication and Biometric Technology in Power Grid Energy Network Access Control

Jiaxiao Meng[1, 2], Jinyan Du[1, 2], Zhihong Liang[1, 2], Chunyan Yang [1, 2], and Yixin Jiang[1, 2]

[1] Electric Power Research Institute
CSG
Guangzhou, Guangdong (China)
E-mail: **mengjx@csg.cn**

[2] Guangdong Provincial Key Laboratory of Power System Network Security
Guangzhou, Guangdong (China)
E-mail:**mengjx@csg.cn**

Abstract. With the sudden development in electronic and network technology, the power grid has emerged in several evolved nations and other areas with faster development. Energy storage can enhance the stability, resiliency and efficiency of the electric smart grid. The power grid transfers energy via bidirectional control of energy and information flow. In the power grid, a smart meter is an important component that is deployed on the user side to determine the consumption of energy regularly. However, the data about the usage of electricity leads to the leakage of the private information of the user, which threatens the privacy of the user. The attackers can change the in-transit message induce wrong information and sometimes cause disastrous action. Hence, it is important to assure data security and privacy of users by conducting authentication in power grid communication. An optimization technique named Puzzle Optimization Algorithm (POA) is designed for the efficient privacy-preserving aggregation approach with multi-factor authentication and a biometric scheme. Also, optimal key-based Elliptic Curve Cryptography (ECC) is used to encrypt the sensitive data that are securely stored. Authentication offers high security and texture analysis. In the registration phase, the privacy information of the person with their biometrics is the important feature point of the individual unique identification. Additionally, the designed approach is compared with other existing optimizations to analyse the functionality of the implemented technique. The simulation outcome defined that the suggested technique enhances user privacy and information security than other standard approaches.

Key words. Power Grid, Multi-Factor Authentication, Biometric Scheme.

1. Introduction

A. System View of Power Grid Energy Network Access Control

The smart grid is also known to be a revolutionary power delivery scheme with multiple characteristics such as integrating renewable and distributed energy, managing supply demand, and monitoring inflicted load and flow of electric power to consumers in an effective manner. In the future smart grid, it is expected that the demand response method starts the user to effectively utilize and pay for the needed power by minimizing or changing the usage at the time of peak hours to manage the supply balance demand in the power grid. Same way, the integration of renewable and distributed energy and monitoring of the dynamic load enables the high usage of sharing energy resources and efficient management of the power requirement in the system [1]. On the distribution end, a smart meter is deployed specifically in consumer premises like smart buildings, smart homes, etc. The smart meter maintained the customer's energy consumption profiles. Through the Neighborhood Area Network (NAN), the data value metering is transmitted to the “Utility Provider (UP)”. The smart meter is technically modeled to get the signal of demand response from the utility center that is provided with bidirectional communication. Moreover, the deployed smart meter communicates with the in-house to offer real-time energy consumption protocol to the consumer and provide several ways to maintain the energy utilization index [2].

In the system, there are different smart grid devices for gathering data on power consumption and offering the service of electricity management. The collected data are monitored by the utility center based on the demand response, load forecasting, power consumption, etc. The total electricity load consumption is compiled by the Utility Center (UC) after collecting it for taking measures to balance the limited capacity power load. However, the smart grid industrial field or remote home installed by the smart grid device, records and transmits the critical privacy concern. The electricity consumption report submitted by the smart grid device generally depends on the communication way to the utility centers. The smart grid device or smart metering is more relevant for the user for being at home other than giving importance to the readings. However, it is not a secure approach for such communication, because the information of a user from the device may be visible to the attackers. Therefore, the

authentication protocol is required for user privacy to be immune to the known attack [3].

To attain the system setting, the elliptic curve $E_q(\alpha,\beta)$ selected by the trusted authority over the finite field A_q with the base point $H \in E_q(\alpha,\beta)$ of large order. Here the huge prime number is denoted as q. The trusted authority chooses the y as private and selects the secure one-way function $h(\cdot)$ and publishes $\{E_q(\alpha,\beta), H, h(\cdot)\}$. The utility center registers each UC_k, and the trusted authority chooses the specific private key p_{sk} and ID_k, stored in the memory of the utility center. After the smart grid device SD_j registers, the trusted authority selects the unique ID_k and computes the certificate parameter, and stores it in the SD_j memory. The authentication phase is initiated by SD_j to maintain the secure section key UC_k to complete this phase [4]. The diagrammatic view of network access control in power grid energy is defined in Figure 1.

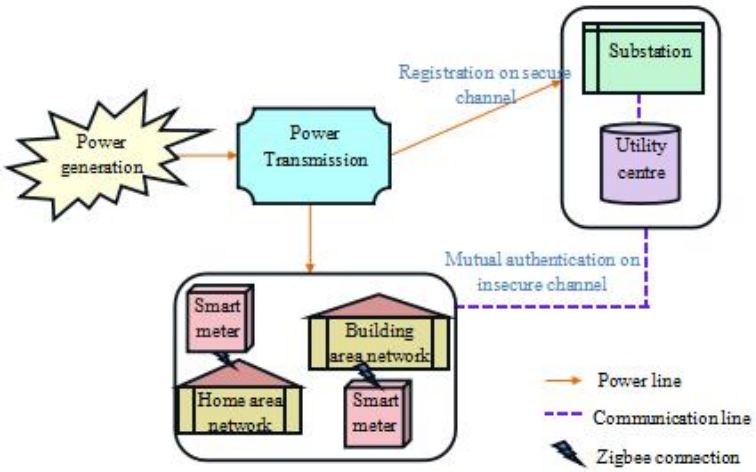


Figure 1. System Model of Power Grid Network

B. *Uses of Multi-factor Authentication with Biometric Technology*

All wireless networks are intrinsically insecure; therefore, it is important to adopt the authentication scheme and biometric approach for an effective smart grid. The importance of implementing biometric authentication in the smart grid is detailed as follows.

- Generally, smart home consumers are provided with a smart meter that gathers the energy consumption details and sends the details to the utility provider on a regular interval basis for billing and monitoring purposes. Therefore, securing the smart meter is very significant. Only an effective and secure authentication approach can guarantee the security of such smart devices [5].
- The attackers can easily modify the critical information if there is no authentication adopted in the smart grid network. Information like details about power usage, power utilization, erroneous billing, etc. can be threatened. Hence, it is important to construct an efficient authentication approach in the smart grid communication to secure the privacy of the information [6].
- When the operators remotely communicate with the control center, the authentication protocol is the initial step to authenticate the operator in the open network. This protocol mainly utilizes the biometric approach for effective authentication. This helps to control the forgery attacks and security threats happening in the network [7].
- The biometric system transfers the person's unique behavioral and physical characteristics into digital format and provides the result of information about the person's biometrics. This avoids the difficulties like users having to carry the authentication card or pass, remembering passwords risk of duplication and loss, etc [8].
- Multi-factor authentication allows the user to prove their authority by generating various steps using the attributes, which the user already knows. This process requires the user to pass on all the verification steps. After passing the multi-factor verification user's biometric information is verified. This helps to avoid unwanted threats, and enhance user privacy and secure information [9].

C. *Contributions*

Our contributions to the implemented work are detailed as follows:

- To develop an efficient and secure multi-factor authentication protocol in the power grid that not only ensures mutual authentication but also improves the trust between the participants using optimization-aided cryptography technique.
- To perform biometric verification in the power grid for the formal security analysis, which ensures the user's privacy by using the physical and behavioral characteristics of the individual for secure communication between the device and the utility center in the power grid.
- To design an optimization algorithm for generating the optimal key, which helps to encrypt the data using ECC to prevent unauthorized access of data tampering and protect the sensitive data in the power grid.
- To investigate the effectiveness of the suggested optimization model using multiple measures by comparing

the result with other existing approaches, which defines the effective function of the developed approach.

2. Description of the Earlier Models of Authentication for Grid Communications

Many researchers have developed multiple authentication and key exchange approaches to secure smart grid communication. Some of the approaches were demonstrated as follows. Gope [10] has established a multi-factor key authentication scheme to ensure the physical security of the smart meter. It helped to solve the issues raised in the security of the smart grid in a very quick manner. Khan *et al*. [11] have designed an authentication strategy based on ECC for smart grid communication using biometric technology. The proposed technology achieved less computation and communication costs. Mutlaq *et al*. [12] have recommended the smart card, ECC, and biometrics to design an authentication protocol. It performed strong session key negotiation and mutual authentication. Khan *et al*. [13] have introduced the key agreement strategy and lightweight authentication for smart grids to offer high security and privacy features. The designed model utilized the random oracle approach for formal security evaluation. Nicanfar *et al*. [14] have proposed an efficient scheme, which mutually authenticated a smart meter of a home area network by using an initial password. It minimized the process in the secure remote password scheme. Nyangaresi *et al*. [15] have developed the anonymous key agreement protocol to address the challenges in the existing technology. It was more effective in terms of computation and bandwidth requirement. Wazid *et al*. [16] have developed a new effective three-factor authentication method for a smart grid environment that utilizes cryptographic computation. Moreover, the developed model provided superior security for the smart meter, which helped the user effectively. Chaudhry *et al*. [17] have suggested a security approach to analyze the threat in the smart grid infrastructure. The suggested schemes ensured smart grid communication and provided a direct solution for the network structure. Byrne *et al*. [18] have implemented the optimization method and energy management system to effectively use energy storage to offer multiple grid services. The method helped to enhance the performance and cost of energy storage. Guan *et al*. [19] have introduced an effective data aggregation and privacy-preserving scheme to improve user privacy and electricity consumption status. Also, for fast authentication dloom filter method was adopted.

Guan *et al*. [20] have recommended the privacy-preserving aggregation technology, which was flexible and efficient for attaining data aggregation and data source authentication with high efficiency. Vijay and Indumathi [21] have provided a high-security IoT environment based on multi-factor authentication for texture analysis and to offer better information security. It had sufficient essential features for unique identification, which provided strong security. Sureshkumar *et al*. [22] have designed a novel mutually authenticated key protocol between the smart meter and service provider to initiate communication. It authenticated the smart meter for secure communication. Chen *et al*. [23] have initiated the key establishment and anonymous authentication approach by analyzing the recent authentication scheme in the smart grid. The suggested method was based on the key generation installed in the smart meter for user security. Xu *et al*. [24] have analyzed the basic network topology to enhance the communication robustness of the existing communication framework. The network connectivity problem was solved using the mathematical model to maintain the overall network reliability. Kumar *et al*. [25] have introduced the authentication protocol based on the ECC for preserving the demand response in the smart grid. The method established the secret section key among the utility center and smart grid device after the mutual authentication. Chen *et al*. [26] have suggested a secure mutual authentication scheme based on edge computing for use in a smart grid. It helped to resolve the issues in the security between the smart meter and the cloud center. Tanveer *et al*. [27] have presented a reliable and anonymous authentication for the smart grid to ensure reliable and secure information exchange between the central service provider and the smart meter. Alfakeeh *et al*. [28] have proposed a group authentication algorithm for preserving the demand response security in a smart grid. It offered a fine-grained access control feature to access the smart grid device. Wu *et al*. [29] have developed an authentication scheme based on the lightweight message, which attained mutual authentication in the smart grid environment. The developed protocol fulfills the lightweight requirement and security of the practical implementation of the smart grid.

From the review, the existing authentication scheme for smart grid networks was analyzed. But none of the earlier models provided all the security features, which were applicable in smart grid networks. Therefore, for the enhancement of the power grid energy system, optimization of multi-factor authentication and biometric technology was proposed in this work, which was detailed in the following.

3. Methodology

A. Proposed Model

The proposed security system in the power grid network utilizes the most effective ECC technique for the authentication process. Initially, the person's privacy data with their biometrics are collected and encrypted using the ECC. In the authentication phase, recognition is performed based on multiple factors like passwords, biometrics, and 'One Time Password (OTP)'. In this approach, the user is provided with essential parameters and keys by the trusted authority. In this way, the user of the smart grid encrypts the uploads and information to the server. The proposed approach is efficiently secure and fulfills the security requirement of the smart grid environment. Also, it offers better information security than the existing systems. The diagrammatic representation of the developed model is detailed in Figure 2.

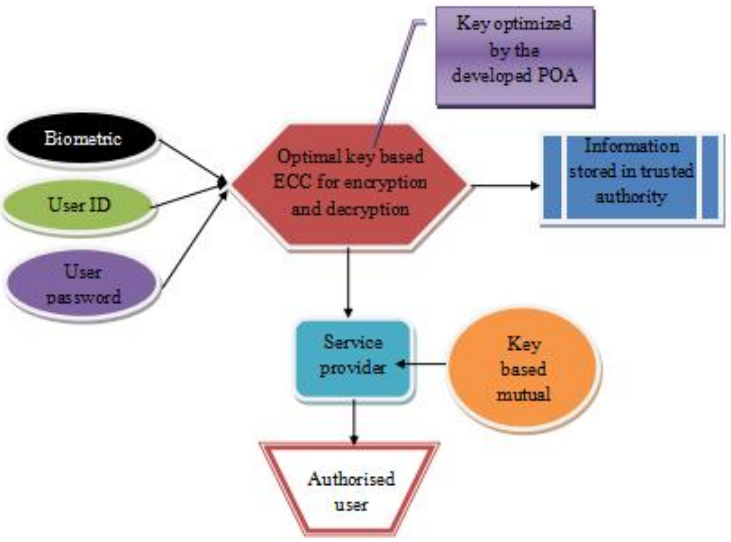


Figure 2. Architecture Diagram of the Proposed Model

B. Biometric Data

Biometric authentication is defined as the process of determining an identity based on the biometric trait which is used in a power grid network. The authentication techniques based on biometrics are classified in terms of behavioral and physiological methods. In the behavioral method, alterable biometric traits, which based on the user's behavior pattern. In the physiological method, body features like facial recognition, fingerprint, and retina identification. This type of biometric data is highly sensitive. The biometric system is generally designed to solve the matching problem based on live measurements of these characteristics. The person must provide the same biometric for new measurements upon authentication in the power grid system. The authentication scheme used AES to preserve the privacy of the user's biometric data gathered to authenticate the user of the smart grid system.

Generally, biometrics based on physiologic is more efficient than biometrics based on behavior in power grid systems. Moreover, behavioral biometrics is generally hard to steal by hackers. Most of the biometric systems rely on specific hardware for the collection of biometric data. This type of collected biometric data requires protection with the help of cryptography. Another way to save the biometric data is based on a strong encryption algorithm.

C. Heuristic Algorithm

Zeidabadi and Dehghani [30] is the population-based optimization, inspired by the process of solving the puzzle game. It is a game-based algorithm, in which members are known to be a puzzle in the population and the variables are determined from the piece of the puzzle. More points are attained by placing the better piece in the correct position, which helps to evaluate the range of the objective function. From the population, other members are guided to solve each puzzle, especially the best member.

In POA, each population member is a feasible solution to the optimization problem. The range of the problem variable is determined by each population member. The POA population is mathematically modeled using Eq. (1).

$$Z = \begin{bmatrix} Z_1 \\ \vdots \\ Z_j \\ \vdots \\ Z_N \end{bmatrix}_{N\times m} = \begin{bmatrix} z_{1,1} & \cdots & z_{1,k} & \cdots & z_{1,m} \\ \vdots & \ddots & \vdots & \iddots & \vdots \\ z_{j,1} & \cdots & z_{j,k} & \cdots & z_{j,m} \\ \vdots & \iddots & \vdots & \ddots & \vdots \\ z_{N,1} & \cdots & z_{N,k} & \cdots & z_{N,m} \end{bmatrix}_{N\times n} \quad (1)$$

Here the puzzle population is indicated as Z , Z_j is the j^{th} puzzle, the population number is represented as N , and the problem variable number is defined as m . The value of k^{th} variable in the j^{th} puzzle is indicated as $z_{j,k}$.

The value of the objective function is evaluated by solving an optimization problem for each member of the population. The objective function value simulated using Eq. (2)

$$H = \begin{bmatrix} h_1 \\ \vdots \\ h_j \\ \vdots \\ h_N \end{bmatrix}_{N\times 1} = \begin{bmatrix} H(Z_1) \\ \vdots \\ H(Z_j) \\ \vdots \\ H(Z_N) \end{bmatrix}_{N\times 1} \quad (2)$$

Here the obtained the objective function for the vector value is denoted as H , and j^{th} puzzle objective function value is represented as h_i . From the obtained objective function value, the best objective function value member is the population's best member. The best member is defined using Eq. (3).

$$Bm = Z_l, h_l = \min(H) \quad (3)$$

Here Bm is the best member and minimum objective function of l^{th} puzzle is defined as Z_l . There are two stages in updating the population members in POA. In the first stage, the updation is based on the guidance of the other member. In the second stage, the updation is based

on the puzzle piece suggested by other members. The first stage updation is modeled in Eq. (4) to (8).

$$Gm_j = Z_i, \quad i \in \{1,2,3,...,N\} \tag{4}$$

$$dz_{j,k} = \begin{cases} (Gm_{j,k} - I \times z_{j,k}), & H_g < H_j \\ (z_{j,k} - I \times Gm_{j,k}), & else \end{cases} \tag{5}$$

$$I = round(1 + rand) \tag{6}$$

$$Z_j^{new} = Z_j + r \times dZ_j \tag{7}$$

$$Z_j = \begin{cases} Z_j^{new}, & H_j^{new} < H_j \\ Z_j, & else \end{cases} \tag{8}$$

Here guiding member is indicated as Gm_j, the j^{th} puzzle k^{th} dimension guiding member is defined as $Gm_{j,k}$. Random number id represented as I. Z_j^{new} is the new status of j^{th} puzzle. H_j^{new} is the objective function value.

In the second stage, the status of each population member is updated using the suggested puzzle piece by other members of the population and it is defined using Eq. (9) to (11).

$$N_p = roun\left(0.5 \times \left(1 - \frac{t}{T}\right) \times N\right) \tag{9}$$

$$Z_{j,k_l}^{new} = Z_{g,k_l}, \begin{cases} g \in \{1,2,3,...,N\} \\ l \in \{1,2,3,...,N_q\} \\ k_l \in \{1,2,3,...,m\} \end{cases} \tag{10}$$

$$Z_j = \begin{cases} Z_j^{new}, & H_j^{new} < H_j \\ Z_j, & else \end{cases} \tag{11}$$

Here the suggested puzzle number is represented as N_p, the iteration counter, and the maximum iteration is defined as t and T. The obtained new value is indicated as Z_{j,k_l}^{new}. Once the population member gets updated to the first and second stages, an iteration of the algorithm is performed and a new population member is determined. The best optimal solution is obtained after the iteration is completed. The flow diagram for the POA is explained in Figure 3.

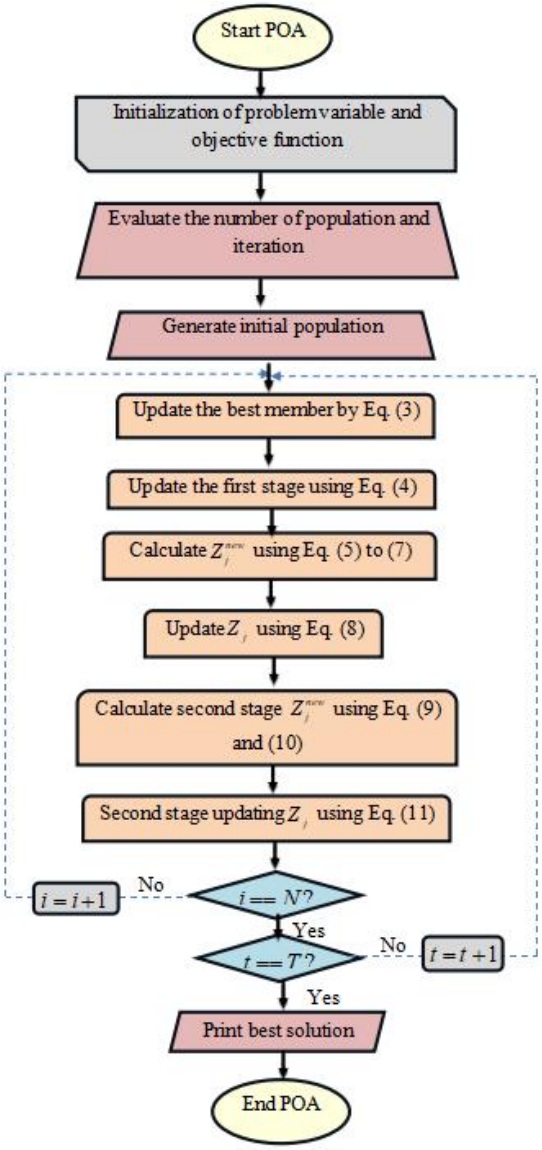


Figure 3. Flow Diagram for the Puzzle Optimization Algorithm

D. Optimal Key-based ECC

ECC is beneficial in enabling an effective protocol, which supports the device with multiple levels of technology that is significant in developing the smart grid system. The cryptosystem based on ECC is employed to device authenticated key exchange protocol. The training formula utilized by the ECC is defined in Eq. (12).

$$Z^2 = Y^2 + bY + c \quad \text{mod}\, q \;\; b,c \in G_q \tag{12}$$

Here the finite field over the prime number q indicated as G_q. The cryptosystem based on ECC over the G_q is known to be the secure condition $4b^3 + 27c^2 \neq 0$ holds. The registration center is selected Q as the generation or base point on G_q. Additionally, the identity and long-term secret key were taken by the registration center. Subsequently, the registration center computes the public key for a central service provider which is defined by $Pub_{csp} = \text{Sec}_{csp}.Q$. In the database, the registration center loads the credentials of the center service provider. The central service provider makes the Q as the public parameter in the smart grid system.

If the sender needs to encrypt the message Mr. The data is given by $Md = [lH, Mr + lMc]$ where l is the random value and the public key receiver is indicated as Mc, which is based on the private key receiver sC, $mC = sCH$. The data is decrypted by the receiver as $[Mr + lMc - sCLH]$. If $mC = sCH$, lMc and $lClH$ cancel each other and Mr be the message sent by the sender.

Optimal key generation: To further enhance the security system, the encrypted key is optimized by the POA in this approach. ECC-based encryption functions better for preserving data and therefore it is used in authentication applications to generate keys.

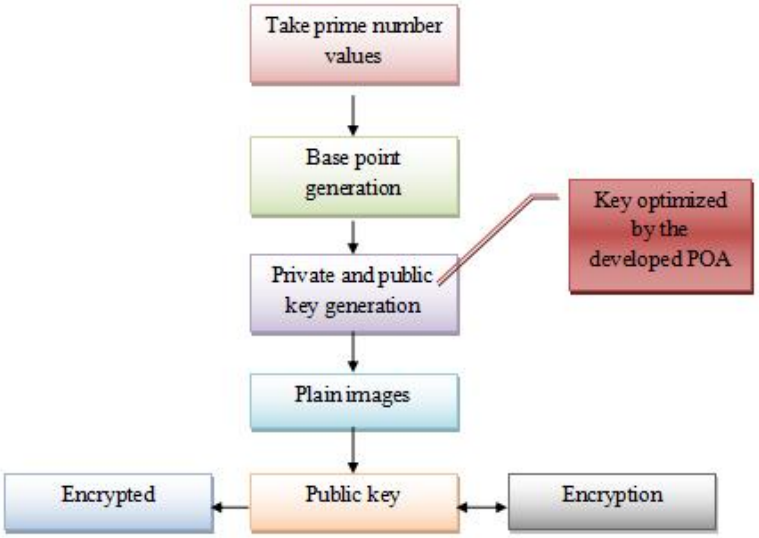


Figure 4. Illustration for Optimal Key-based ECC

E. Authentication Process

Among the user and service provider, the authentication strategy offered secure communication for privacy and security purposes in the power grid system. The existing authentication strategies are only known for identifying security attacks and are less efficient in computation. Different authentication strategies are designed to make safe transformations between the substation and smart meter, but these functions are not valid to stop general attacks like impersonation, user anonymity attacks, etc.

Hence, mutual authentication strategy based on ECC is designed for smart grid systems based on a biometric technique. With the help of a data storage system and legislative control, the transaction between the substation and the authorized station is secured. To secure the intermediate message between the smart device and substations, the authentication protocol is necessary in the power grid. In a smart grid, multiple devices share data with other devices. Authenticate the appliances, before exchanging the data between various types of appliances, to offer safe transformation with authorized users. In this way, it is essential for effective authentication in the smart grid environment. The efficient authentication structure can maintain privacy and security in the smart grid environment.

Before authentication, initialization and registration phases occurred. In the initialization phase, the secret key server for symmetric encryption and decryption. Both the keys are secure in the server. In the registration phase, the user tries to register with the ID. In this phase, the user inputs their biometric data and selects the random string and password.

After the registration phase, the user is able to communicate with the smart grid environment. In the authentication, the first step is the user login with ID, and imprint $C_v^{'}$, $QX_v^{'}$. Further, the user computes $\sigma_v^{'} = \text{Re}\, p(C_v^{'}, \theta_v^{'})$, $S_v^{'} \oplus \sigma_v^{'} S_5^{'} = i\left(JE_v^{'} \| QX_v^{'} \| S_v^{'}\right)$ and verifies $S_5^{'} = S_5$ if yes then, the user generates $v \in A_r^*$,

computes $T_1 = i(JE_v \| S_1 \| t_1)$, $JE_{v1} = JE_v \oplus (S_1 \oplus t_1)$ and sends $MA_{B1} = \{T_1, JE_{,v.1}, v.h, t_1\}$ to the server based on a reliable medium.

In the second step, on receiving N_{B1} , T verifies $t_2 - t_1 \le \Delta t$, if verification is successfully done then, T computes $JE_v^* = JE_{V1} \oplus (S_1 \oplus t_1)$, $T_1^8 = i(JE_V^* \| S_1 \| t_1)$ and verifies $T_1^* = T_1$. After that t generates the random number $t \in A_r^*$, computes $T_2 = i(JE_t \| S_3 \| t_2)$, session key $TL_{TV} = i\left(JE_V^* \| JE_T \| T_1^* \| T_2 \| S_3.h \| v.t.h \| y.h \| u_3\right)$, and computes $JE_{t1} = JE_t \oplus (S_3 \oplus u_3)$. Further T sends $MA_{B2} = \{T_2, JE_{,T.1}, th, , t_3\}$ towards the user.

In the third step, on receiving N_{B2} , the user verifies $t_4 - t_3 \le \Delta t$, if yes then, the user computes $JE_t^* = JE_{T1} \oplus (S_3 \oplus t_3)$, $T_2^* = i(JE_T^* \| S_3 \| t_3)$ and verifies $T_2^* = T_2$ if yes then sets its session key as $TL_{VT} = i\left(JE_V \| JE_T^* \| T_1 \| T_2^* \| S_3.h \| v.t.h \| QL_T \| u_3\right)$. The pseudocode of the login and authentication is explained in the following algorithm.

Login and Authentication Phase

User login $JE_V^{'}$, $QX_V^{'}$ and imprint $C_V^{'}$

User computes $\sigma_v^{'} = \mathrm{Re}\, p(C_v^{'}, \theta_v^{'})$, $S_v^{'} \oplus \sigma_v^{'} S_5^{'} = i\left(JE_v^{'} \| QX_v^{'} \| S_v^{'}\right)$

If $S_5^{'} = S_5$ then

The user selects the random number $v \in A_r^*$

User computer $T_1 = i(JE_v \| S_1 \| t_1)$, $JE_{v1} = JE_v \oplus (S_1 \oplus t_1)$

User send $MA_{B1} = \{T_1, JE_{,v.1}, v.h, t_1\}$ towards T

If $t_2 - t_1 \le \Delta t$ then

T computes $JE_v^* = JE_{V1} \oplus (S_1 \oplus t_1)$, $T_1^8 = i(JE_V^* \| S_1 \| t_1)$

If $T_1^* = T_1$ then

T generates $t \in A_r^*$

T computes $T_2 = i(JE_t \| S_3 \| t_2)$, $TL_{TV} = i\left(JE_V^* \| JE_T \| T_1^* \| T_2 \| S_3.h \| v.t.h \| y.h \| u_3\right)$, $JE_{t1} = JE_t \oplus (S_3 \oplus u_3)$

T sends $MA_{B2} = \{T_2, JE_{,T.1}, th, , t_3\}$ towards user

If $t_4 - t_3 \le \Delta t$ then

User computes $JE_t^* = JE_{T1} \oplus (S_3 \oplus t_3)$, $T_2^* = i(JE_T^* \| S_3 \| t_3)$

If $T_2^* = T_2$ then

User compute $TL_{VT} = i\left(JE_V \| JE_T^* \| T_1 \| T_2^* \| S_3.h \| v.t.h \| QL_T \| u_3\right)$

return (success)

else

return (failure)

end if

else

return (failure)

end if

else

return (failure)

end if

else

return (failure)

end if

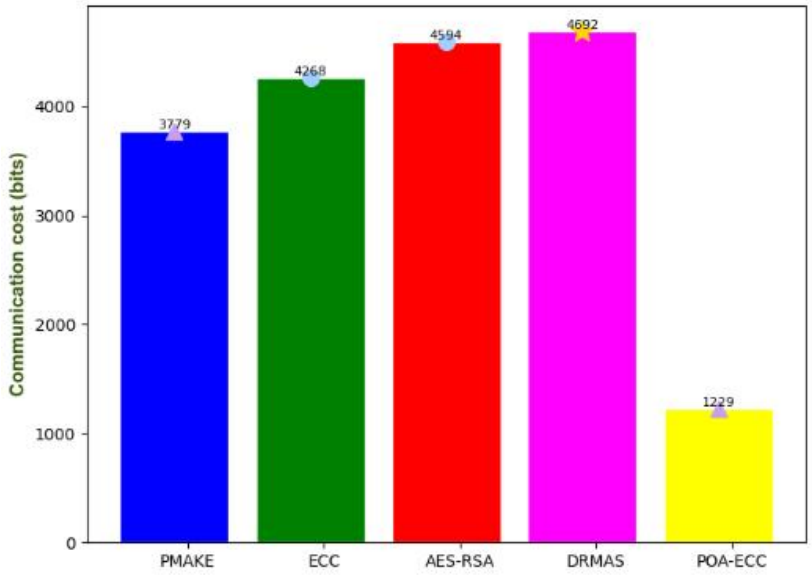
4. Result

A. Experimental Setup

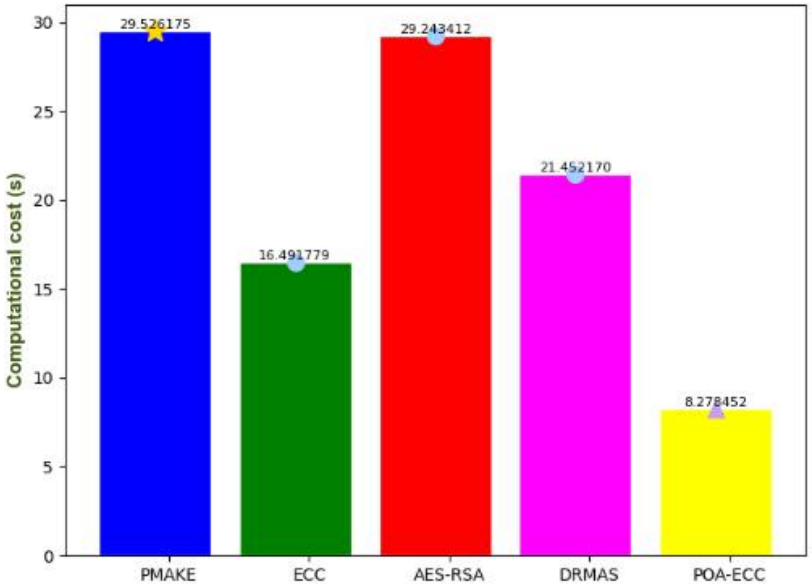
The suggested POA-ECC approach for multi-factor authentication and biometric technology in power grid energy networks compared with the existing approach was done to determine the function of the model. Various methods were used to calculate the execution. Other existing approach like Privacy-Aware Multi-Factor Authenticated Key Establishment scheme (PMAKE) [10], ECC [13], Advanced Encryption Standard Rivest-Shamir-Adleman (AES-RSA) [6], Demand Response Management (DRMAS) [4], Remote User Authentication Scheme for a Renewable Energy based Smart grid environment (TUAS-RESG) [16], Efficient Flexible Privacy-Preserving Aggregation Scheme (EFFECT) [20] and Anonymous and Reliable Authentication Protocol for Smart Grids (ARAP-SG) [27] were considered.

B. Cost Analysis for Proposed Approaches with Other Methods

Figures 5 and 6 define the cost function of the suggested approach compared with other existing models. Here the computation and communication cost are taken to estimate the cost function analysis. Different attributes are utilized to estimate the communication cost, which are ECC point, cryptographic hash function, random number generation, ECC encryption and decryption, identifiers, and time stamp. From the graph comparison, the developed model attains lower computation and communication costs than the existing approaches.

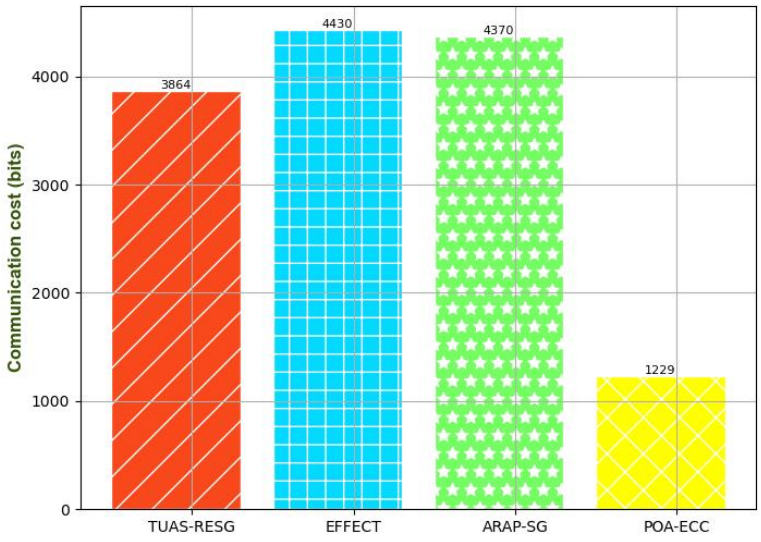


(a)

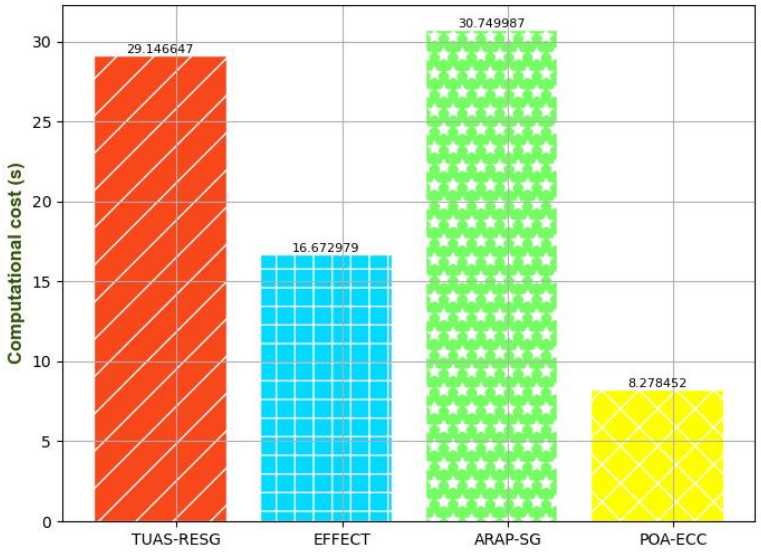


(b)

Figure 5. Cost Analysis of the Developed Method with other Methods in terms of "(a) Communication Cost, (b) Computation Cost"



(a)

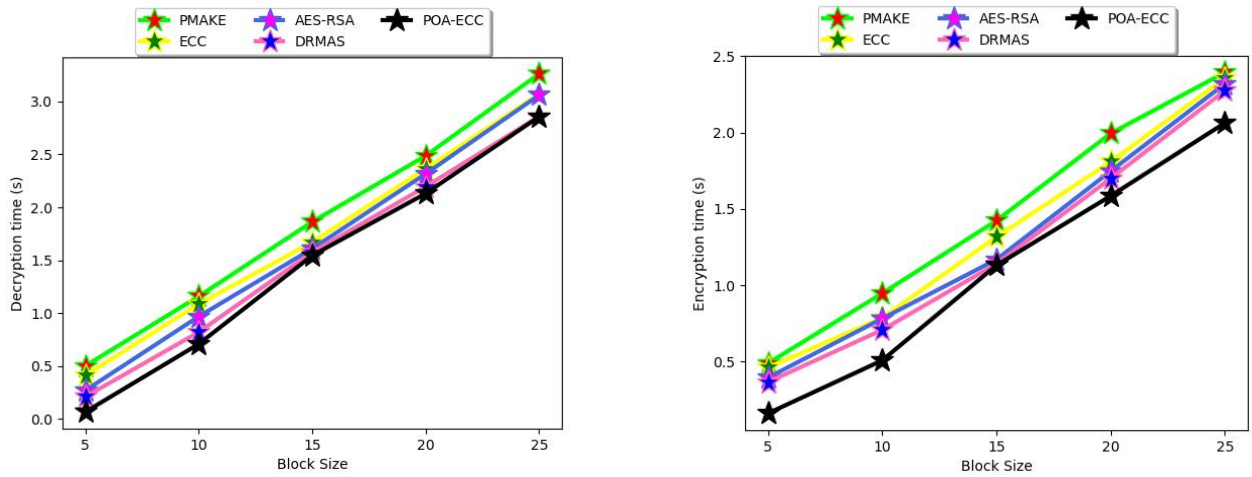


(b)

Figure 6. Cost Estimation of the Developed Method with other Methods in terms of "(a) Communication Cost, (b) Computation Cost"

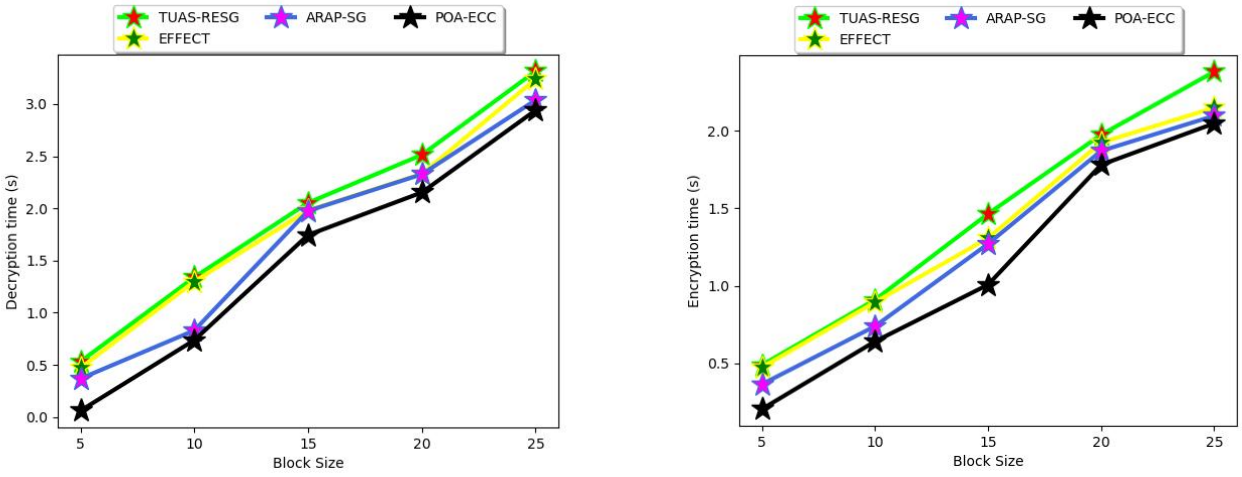
C. Comparison of Decryption and Encryption Time for the Suggested Method over Different Approaches

The run time of decryption and encryption performed for the suggested method is compared with various existing approaches in Figures 7 and 8. In the process of login and executing procedure, the time taken for the encryption and decryption is efficiently analyzed. From the outcome, it is revealed that the proposed model has taken maximum time for encryption and decryption compared to other approaches.



(a) (b)

Figure 7. Time Comparison of the Developed Method with Other Methods in terms of "(a) Decryption Time, (b) Encryption Time"

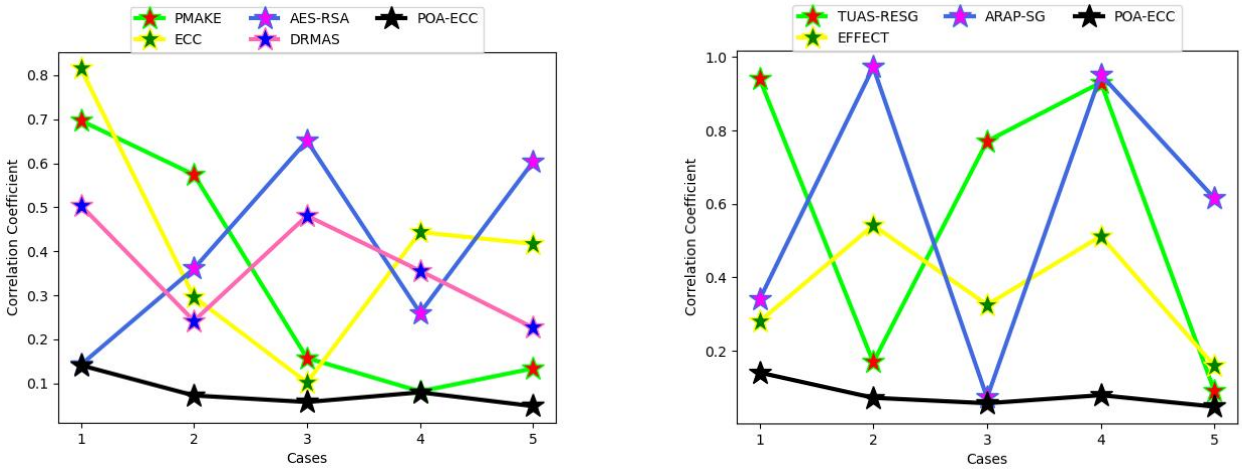


(a) (b)

Figure 8. Time Comparison of the Developed Method with other Methods in terms of "(a) Decryption Time, (b) Encryption Time"

D. Key Sensitivity Analysis of the Proposed Method Compared with Other Methods

Figure 9 defines the key sensitive analysis of the implemented technique against some of the existing approaches in terms of the correlation coefficient. Here the key sensitivity is performed based on attributes like user anonymity, message authentication, session key agreement, password information, replay attack, key freshness, and impersonation attack. It is clear from the comparative analysis that the implemented model has better function compared to other models for smart grid application.

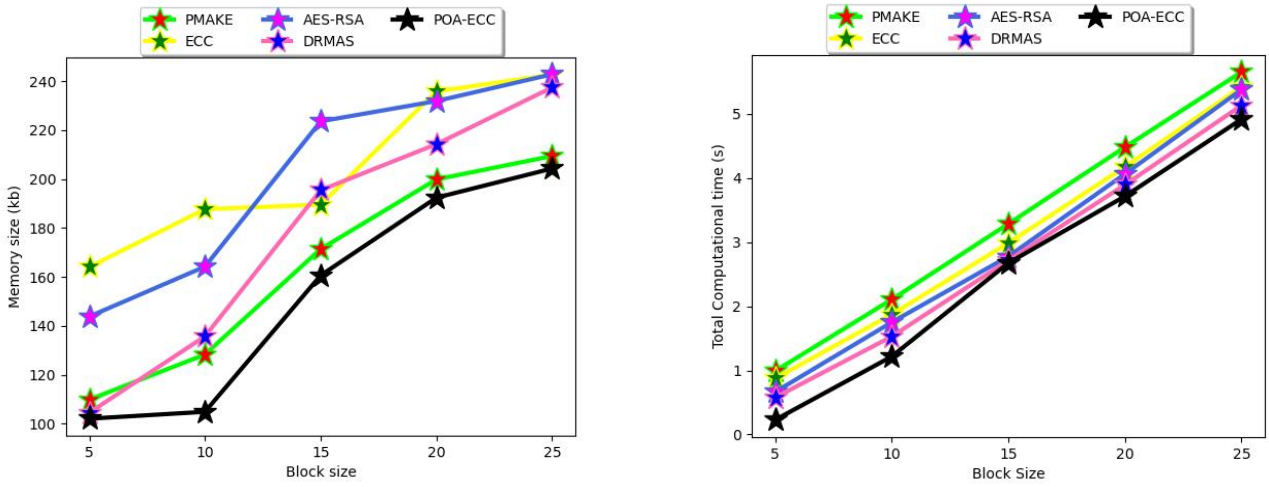


(a) (b)

Figure 9. Key Sensitivity Analysis of the Implemented Method Compared over Various Methods

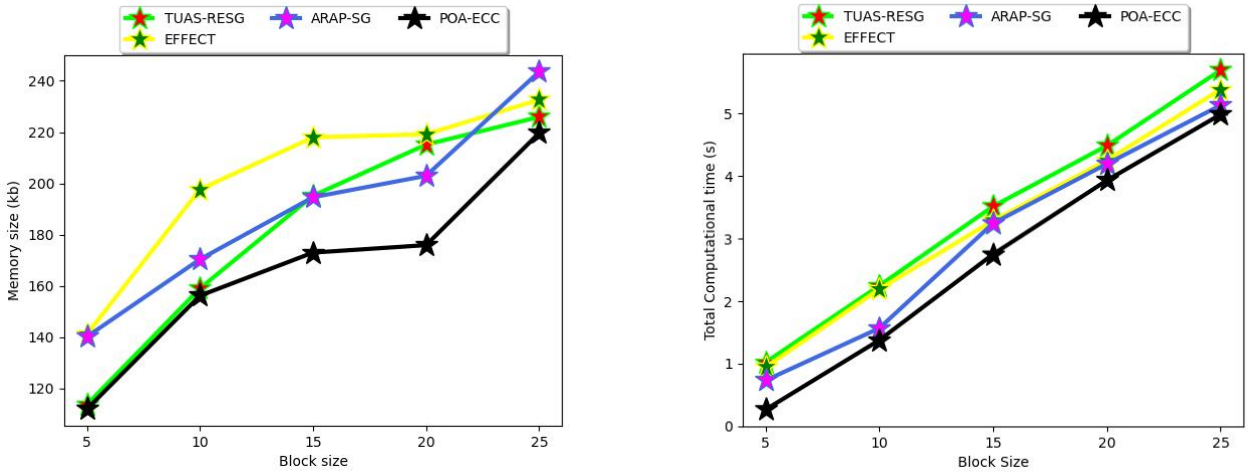
E. Performance Analysis of the Designed Model Compared with Other Models

To determine the functionality of the developed scheme, Figure 10 compares our implemented model concerning existing authentication approaches for smart grid communication. From the graph, it is clear that the overall memory required and total computation time of the designed scheme is less than the other. The designed approach takes significantly less computation time than the other existing models. Therefore, from the analysis, the proposed model has attained better memory size and computational time.



(a) (b)

Figure 10. Performance Estimation of the Introduced Model Compared with Other Existing Approaches in terms of "(a) Memory Size and (b) Total Computational Time"



(a) (b)

Figure 11. Performance Estimation of the Introduced Model Compared with Other Existing Approaches in terms of "(a) Memory Size and (b) Total Computational Time"

F. Comparison of Cost Analysis for the Developed Scheme Compared with Other Methods

Table 1 defines the computation and communication cost of the suggested scheme compared with other existing models. Here various attributes are taken to determine the communication and computational cost. From Table 1, the computation cost of the proposed approach decreased by 2.5% of PMAKE, 0.9% of ECC, 2.5% of AES-RSA, and 1.5% of DRMAS respectively. Similarly, the communication cost of the implemented technique was minimized by 2.1% of TUAS-RESG, 2.6% of EFFECT, and 2.5% of ARAP-SG respectively. From the analysis, it is noted that the implemented POA-ECC has the minimum computation and communication cost.

Table 1. Cost Analysis of the Implemented Scheme over Different Methods

Terms	Computational Cost	Communication cost
PMAKE [10]	29.52617526	3779
ECC [13]	16.4917789	4268
AES-RSA [6]	29.24341238	4594
DRMAS [4]	21.45217039	4692
TUAS-RESG [16]	29.14664668805216	3864
EFFECT [20]	16.67297877467616	4430
ARAP-SG [27]	30.749986914653693	4370
POA-ECC	8.278452029832607	1229

G. Key Sensitivity Analysis of the Proposed Method Compared over Various Approaches

Tables 2 and 3 define the comparison of the security attacks and features based on the developed method compared with other models. From the table, it is noted that the PMAKE model does not stand with MM, US, SA, IM, and PB. ECC does not stand with the US, ME, SA, IN, and PB. Similarly, AES-RSA does not give protection against SA, IN, US, and PB. Also, DRMAS does not provide password information. While comparing with the existing methods our proposed model stands with all the security property. Therefore, the result revealed that the developed model has more security properties than the existing approaches.

Table 2. Key Sensitive Analysis of the Proposed Scheme Compared over Different Methods

Security property	PMAKE [10]	ECC [13]	AES-RSA [6]	DRMAS [4]	POA-ECC
Replay attack (RS)	yes	yes	yes	yes	yes
User anonymity (US)	no	no	no	yes	yes
Key freshness (KF)	yes	yes	yes	yes	yes
Message authentication (ME)	yes	no	yes	yes	yes
Impersonation attack (IM)	no	yes	yes	yes	yes
Session key agreement (SA)	no	no	no	yes	yes
Insider attack (IN)	yes	no	no	yes	yes
Man-in-the-middle attack (MM)	no	yes	yes	yes	yes
Password-based (PB)	no	no	no	no	yes

Table 3. Key Sensitive Analysis of the Implemented Model Compared with Existing Approaches

Security property	TUAS-RESG [16]	EFFECT [20]	ARAP-SG [27]	POA-ECC
Replay attack (RS)	yes	yes	yes	yes
User anonymity (US)	no	no	yes	yes
Key freshness (KF)	yes	no	yes	yes
Message authentication (ME)	no	yes	no	yes
Impersonation attack (IM)	yes	yes	yes	yes
Session key agreement (SA)	yes	yes	yes	yes
Insider attack (IN)	no	no	yes	yes
Man-in-the-middle attack (MM)	yes	yes	yes	yes
Password-based (PB)	no	no	no	yes

5. Conclusion

In this work, an optimal key-ECC-based secure multi-factor authentication protocol for data management between the smart meter and utility center with the help of biometric technology was introduced in the power grid system. An optimization was implemented in the ECC key encryption that was associated with both security and integrity in the authentication phase of the smart grid. POA algorithm was implemented in the developed approach to optimize the key to enhance the security. The security of the implemented method proved that the approach withstands multiple types of attacks on the power grid. Also, the security property of the implemented technique compared with other existing protocols, showed that our implemented model was more secure in a smart grid environment. Moreover, the developed method was also effective in terms of secure communication and computation overhead. The analysis was carried out to determine the effectiveness of the authentication approach. From the findings, it was analyzed that the secure communication of the smart grid network was achieved by the optimal key-based ECC.

References

[1] N. Saxena and B. Choi, “State of the art authentication, access control, and secure integration in smart grid,” *Energies*, vol. 8, no. 10, pp. 11883-11915, Oct. 2015, doi: 10.3390/en81011883.

[2] M. S. Abdalzaher, M. M. Fouda, A. Emran, Z. M. Fadlullah, and M. I. Ibrahem, "A survey on key management and authentication approaches in smart metering systems," *Energies*, vol. 16, no. 5, p. 2355, 2023. Available: https://doi.org/10.3390/en16052355.

[3] A. Irshad, S. A. Chaudhry, M. Alazab, A. Kanwal, M. Sultan Zia, and Y. B. Zikria, “A secure demand response management authentication scheme for smart grid,” *Sustainable Energy Technol. Assess.*, vol. 48, p. 101571, Dec. 2021, doi: 10.1016/j.seta.2021.101571.

[4] S. A. Chaudhry, H. Alhakami, A. Baz, and F. Al-Turjman, “Securing demand response management: A certificate-based access control in smart grid edge computing infrastructure,” *IEEE Access*, vol. 8, pp. 101235-101243, 2020, doi: 10.1109/access.2020.2996093.

[5] N. Saxena, B. J. Choi, and R. Lu, “Authentication and authorization scheme for various user roles and devices in smart grid,” *IEEE Trans. Inf. Forensics Secur.*, vol. 11, no. 5, pp. 907-921, May 2016, doi: 10.1109/tifs.2015.2512525.

[6] K. Mahmood, S. Ashraf Chaudhry, H. Naqvi, T. Shon, and H. Farooq Ahmad, “A lightweight message authentication scheme for smart grid communications in power sector,” *Comput. Electr. Eng.*, vol. 52, pp. 114-124, May 2016, doi: 10.1016/j.compeleceng.2016.02.017.

[7] W. Yang *et al*., "A cancelable iris-and steganography-based user authentication system for the internet of things," *Sensors*, vol. 19, no. 13, p. 2985, 2019. [Online]. Available: https://doi.org/10.3390/s19132985.

[8] H. M. S. Badar, S. Qadri, S. Shamshad, M. F. Ayub, K. Mahmood, and N. Kumar, “An identity based authentication protocol for smart grid environment using physical uncloneable function,” *IEEE Trans. Smart Grid*, vol. 12, no. 5, pp. 4426-4434, Sep. 2021, doi: 10.1109/tsg.2021.3072244.

[9] S. Kim, H. J. Mun, and S. Hong, “Multi-factor authentication with randomly selected authentication methods with did on a random terminal,” *Appl. Sci.*, vol. 12, no. 5, p. 2301, Feb. 2022, doi: 10.3390/app12052301.

[10] P. Gope, “PMAKE: Privacy-aware multi-factor authenticated key establishment scheme for advance metering infrastructure in smart grid,” *Comput. Commun.*, vol. 152, pp. 338-344, Feb. 2020, doi: 10.1016/j.comcom.2019.12.042.

[11] A. A. Khan, V. Kumar, and M. Ahmad, “An elliptic curve cryptography based mutual authentication scheme for smart grid communications using biometric approach,” *J. King Saud Univ. Comput. Inf. Sci.*, vol. 34, no. 3, pp. 698-705, Mar. 2022, doi: 10.1016/j.jksuci.2019.04.013.

[12] K. A. A. Mutlaq *et al*., “Low complexity smart grid security protocol based on elliptic curve cryptography, biometrics and hamming distance,” *PLOS ONE*, vol. 19, no. 1, p. e0296781, Jan. 2024, doi: 10.1371/journal.pone.0296781.

[13] A. A. Khan, V. Kumar, M. Ahmad, and S. Rana, “LAKAF: Lightweight authentication and key agreement framework for smart grid network,” *J. Syst. Archit.*, vol. 116, p. 102053, Jun. 2021, doi: 10.1016/j.sysarc.2021.102053.

[14] H. Nicanfar, P. Jokar, K. Beznosov, and V. C. M. Leung, “Efficient authentication and key management mechanisms for smart grid communications,” *IEEE Syst. J.*, vol. 8, no. 2, pp. 629-640, Jun. 2014, doi: 10.1109/jsyst.2013.2260942.

[15] V. O. Nyangaresi, Z. A. Abduljabbar, S. H. A. Refish, M. A. AI Sibahee, E. W. Abood, and S. Lu, “Anonymous key agreement and mutual authentication protocol for smart grids,” in *Cognit. Radio Oriented Wireless Networks Wireless Internet*, 2022, pp. 325-340. doi: 10.1007/978-3-030-98002-3_24.

[16] S. Yu, K. Park, J. Lee, Y. Park, Y. Park, S. Lee, and B. Chung, "Privacy-preserving lightweight authentication protocol for demand response management in smart grid environment," *Applied Sciences*, vol. 10, no. 5, p. 1758, 2020. https://doi.org/10.3390/app10051758.

[17] D. Sadhukhan, S. Ray, M. S. Obaidat, and M. Dasgupta, "A secure and privacy preserving lightweight authentication

scheme for smart-grid communication using elliptic curve cryptography," *Journal of Systems Architecture*, vol. 114, p. 101938, 2021. [Online]. Available: https://doi.org/10.1016/j.sysarc.2021.101938.

[18] R. H. Byrne, T. A. Nguyen, D. A. Copp, B. R. Chalamala, and I. Gyuk, "Energy management and optimization methods for grid energy storage systems," *IEEE Access*, vol. 6, pp. 13231-13260, 2018, doi: 10.1109/access.2017.2741578.

[19] Z. Guan *et al*., "Privacy-preserving and efficient aggregation based on blockchain for power grid communications in smart communities," *IEEE Commun. Mag.*, vol. 56, no. 7, pp. 82-88, Jul. 2018, doi: 10.1109/mcom.2018.1700401.

[20] Z. Guan, Y. Zhang, L. Zhu, L. Wu, and S. Yu, "EFFECT: An efficient flexible privacy-preserving data aggregation scheme with authentication in smart grid," *Sci. China Inf. Sci.*, vol. 62, no. 3, Jan. 2019, doi: 10.1007/s11432-018-9451-y.

[21] M. Vijay and G. Indumathi, "A highly secure multi-factor authentication system using biometrics to enhance privacy in Internet of Things (IOT)," *Int. Res. J. Multidiscip. Technovation*, pp. 26-34, Nov. 2019, doi: 10.34256/irjmtcon4.

[22] V. Sureshkumar, S. Anandhi, R. Amin, N. Selvarajan, and R. Madhumathi, "Design of robust mutual authentication and key establishment security protocol for cloud-enabled smart grid communication," *IEEE Syst. J.*, vol. 15, no. 3, pp. 3565-3572, Sep. 2021, doi: 10.1109/jsyst.2020.3039402.

[23] Y. Chen, J. F. Martínez, P. Castillejo, and L. López, "An anonymous authentication and key establish scheme for smart grid: FAuth," *Energies*, vol. 10, no. 9, p. 1354, Sep. 2017, doi: 10.3390/en10091354.

[24] S. Xu, Y. Qian, and R. Qingyang Hu, "Reliable and resilient access network design for advanced metering infrastructures in smart grid," *IET Smart Grid*, vol. 1, no. 1, pp. 24-30, Apr. 2018, doi: 10.1049/iet-stg.2018.0008.

[25] L. Zhang, S. Tang, and H. Luo, "Elliptic curve cryptography-based authentication with identity protection for smart grids," *PloS One*, vol. 11, no. 3, p. e0151253, 2016. [Online]. Available: https://doi.org/10.1371/journal.pone.0151253.

[26] C. M. Chen, L. Chen, Y. Huang, S. Kumar, and J. M. T. Wu, "Lightweight authentication protocol in edge-based smart grid environment," *EURASIP J. Wireless Commun. Networking*, vol. 2021, no. 1, Mar. 2021, doi: 10.1186/s13638-021-01930-6.

[27] M. Tanveer, A. U. Khan, H. Shah, A. Alkhayyat, S. A. Chaudhry, and M. Ahmad, "ARAP-SG: Anonymous and reliable authentication protocol for smart grids," *IEEE Access*, vol. 9, pp. 143366-143377, 2021, doi: 10.1109/access.2021.3121291.

[28] A. S. Alfakeeh, S. Khan, and A. H. Al-Bayatti, "A multi-user, single-authentication protocol for smart grid architectures," *Sens.*, vol. 20, no. 6, p. 1581, Mar. 2020, doi: 10.3390/s20061581.

[29] L. Wu, J. Wang, S. Zeadally, and D. He, "Anonymous and efficient message authentication scheme for smart grid," *Secur. Commun. Netw.*, vol. 2019, pp. 1-12, May 2019, doi: 10.1155/2019/4836016.

[30] F. A. Zeidabadi and M. Dehghani, "POA: Puzzle optimization algorithm," *Int. J. Intell. Eng. Syst.*, vol. 15, no. 1, Feb. 2022, doi: 10.22266/ijies2022.0228.25.