Scientific Research Publishing

Energy and Power Engineering, 2020, 12, 53-62
https://www.scirp.org/journal/epe
ISSN Online: 1947-3818
ISSN Print: 1949-243X

Privacy Preservation of Smart Meters Based on Identity Authentication

Hongbo Hu, Xin Zhao, Yalian Wu, Mengbiao Huang, Ziqi Zhu, Qingyu Yang

College of Information Engineering, Xiangtan University, Xiangtan, China
Email: wyl@xtu.edu.cn

How to cite this paper: Hu, H.B., Zhao, X., Wu, Y.L., Huang, M.B., Zhu, Z.Q. and Yang, Q.Y. (2020) Privacy Preservation of Smart Meters Based on Identity Authentication. *Energy and Power Engineering*, **12**, 53-62.
https://doi.org/10.4236/epe.2020.124B006

Received: January 6, 2020
Accepted: April 7, 2020
Published: April 10, 2020

Abstract

Smart meters provide a lot of convenience for both power supply and consumption. Due to the frequent transmission of information, it brings great challenges to the privacy preservation of the user's household power consumption data in the smart grid. In order to achieve the anonymity of smart meters. A smart meter privacy preservation scheme based on identity authentication is proposed. The third-party certification authority is introduced in this scheme; it issues pseudonym certificates to realize the identity privacy preservation of smart meters. The masking technology with the Advanced Encryption Standard algorithm is used for data aggregation. The results show that our scheme reduces the computational cost and the communication overhead.

Keywords

Smart Meter, Identity Authentication, Privacy Preservation, Masking Technology

1. Introduction

Smart grid is the intelligence of the power grid. It is predicted to provide more stable and reliable power for power users [1]. The smart grid is the result of the transformation of the existing energy grid. Both customers and public utility companies have monitoring and control functions, and the ability to predict energy use [2]. With the development of science and technology as well as the deepening of related research, smart meters have become a key part between power supply enterprises and users, making them more closely linked and promoting the development of smart grid [3]. The European Union plans to replace at least 80$\% $ of its meters with smart meters by 2020 [4]. With the rapid development of smart meters, we should not only provide us with a convenient way of life, but also consider another issue, the privacy of users [5] [6]. The

smart meter data contains more private information of users. Once the attacker has mastered it, will cause the user's privacy to be leaked, thereby increasing the user's loss [7], which puts higher requirements on the security and accuracy of smart grid communications. However, without considering several security requirements, namely authentication, integrity, non-repudiation, access control, and privacy, it is not possible to deploy a smart grid widely [8]. Attackers modify the data in the electricity meter through network attacks or master the behavior patterns of the users by tracking measurement data, so transmitting secure and complete data with user privacy through the network is a certain challenge [9] [10].

Chim [11] implements user identity authentication by generating a signature using a hash information verification code, but this method cannot protect the user's identity privacy. Jeanno [12] uses a blind signature privacy preservation scheme to implement identity authentication while protecting user identity privacy However, this requires multiple verifications before signing, which increases computational overhead. Yu [13] used a ring signature privacy preservation scheme to achieve identity authentication and identity privacy preservation while avoiding a large number of signing credentials, but it was unable to prevent collusion between the key distribution center and the power company, requiring a lot of computation and communication overhead. Guan [14] guaranteed the anonymity and authenticity of the device by issuing certificates, authenticated the device, and effectively protected the user's identity and privacy. Carcia [15] uses a homomorphic encryption scheme, which enhances the privacy preservation strength, but also increases the computational overhead. Saxena [16] realized the effective authentication of the user's identity through a secure mutual authentication and authorization scheme, but did not consider the identity privacy of the user. Acs [17] adopted a privacy preservation scheme to achieve data aggregation and privacy preservation. The existing privacy preservation schemes have the problems of large computational cost and communication overhead, and the user's identity privacy cannot be effectively protected.

Therefore, we proposed a smart meter privacy preservation scheme based on identity authentication. The introduction of third-party certification agencies, trusted certification authority and local certification authority issued pseudonyms and pseudonym certificates to ensure the anonymity of smart meters and achieve for the protection of user identity privacy. The masking technology with the Advanced Encryption Standard algorithm [18] is used for data aggregation.

We have summarized the contributions of our article as follows:

- We have improved the system model. In this model, we adopt a third-party certification authority to authenticate the smart meter.
- The certification authority has realized the anonymity of smart meters by issuing a pseudonym certificate, which effectively protects the identity privacy of users.
- The masking technology with the Advanced Encryption Standard algorithm is used for data aggregation. The results show that our scheme reduces the

computational cost and the communication overhead.

2. Related Basis

2.1. Zero-Knowledge Proof

Zero-knowledge proof is that the prover can convince the verifier that a certain conclusion is correct without providing the verifier with any useful information. Let A be the entity that has certain information and wants to confirm this fact. Let V be the confirming entity. A protocol proves to V that A does hold certain information, but V cannot guess what the information is. In addition to knowing that A can confirm Except for one fact, no other knowledge can be obtained, saying that A achieved zero-knowledge proof [19].

2.2. Maintaining the Integrity of the Specifications

G_1, G_2 are addition cyclic groups whose order is q, G_T is a multiplication cyclic group whose order is q, g is a generator, which constitutes a bilinear map $G_1 \times G_1 \to G_T$. This assumption claims that given g^a, g^b, computing g^{ab} is computationally hard [20].

3. System Model and Attack Model

3.1. System Model

The description of these five components is as follows

1) Smart meter (SM): Smart meters are an important part of the smart grid. It increases the connection between users and power companies. Smart meters have added intelligent functions to traditional meters, and have also become a key part of the smart grid.

2) Aggregator (AG): The aggregator is an important part of the intermediate connection. The power data is collected from the smart meter end, and then the data is transmitted to the next level through the data aggregation technology. It is an important media component of a smart meter and control center.

3) Control Center (CC): The control center is equivalent to the brain, it will store the data collected by the smart meter in the future, and also process the data. It also has a role to provide guidance for the power supply process of power companies for the optimization of smart grid scheduling. The user's power is used for billing. Second, the user's power consumption data is analyzed to adjust the power accordingly.

4) Trusted Certificate Authority (TCA): The trusted certificate authority is an independent key and certificate management authority that generates various parameters and keys for the system.

5) Local Certificate Authorities (LCA): The trusted certificate authority is a management agency. Its main role is to issue certificates to other entities in the system and generate corresponding parameters. It is an independent third-party management agency.

As shown in **Figure 1**.

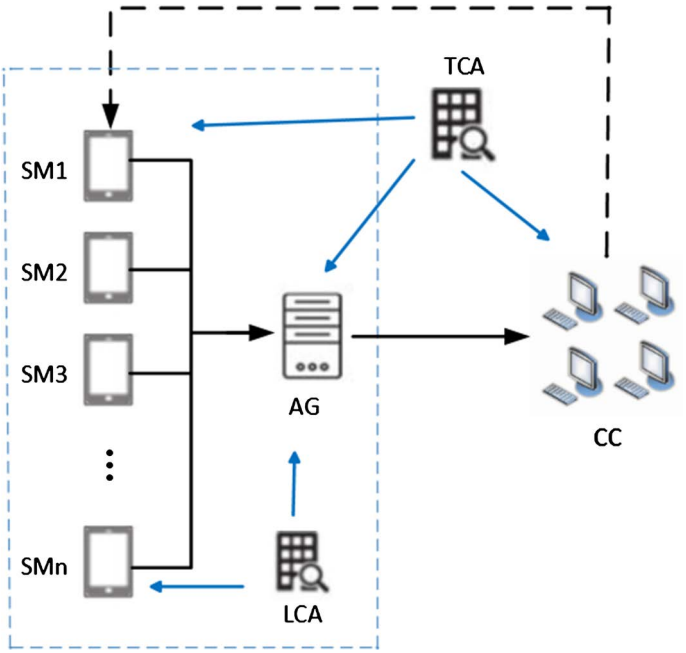

Figure 1. System model.

3.2. Attack Model

In our proposed privacy protection scheme, the attack model is an honest and curious model. We assume that the opponent is easy to attack the smart meter, and the sensitive power data can be obtained by the opponent through a legitimate device identity. The adversary conducts further tracking to obtain the user's true identity, so that the user's privacy is leaked. The aggregator and control center are honest but curious. They are trying to obtain sensitive data information. The communication channel between the aggregator and the data center may not be completely encrypted, and the adversary can eavesdrop to obtain valuable information. In addition, during the transmission process, the adversary may launch an active attack to destroy data integrity.

4. Scheme Description

Our scheme introduces a third-party certification authority; it issues pseudonym certificates to achieve smart meter identity privacy. The masking technology with the Advanced Encryption Standard algorithm is used for data aggregation.

4.1. System Initialization

When the SM receives a request from the CC to collect user power usage information, the initialization system process is completed by the LCA and TCA by generating the corresponding parameters p_0 q_0, calculates the public key (e, N_0), the private key is d, and sends it to the SM. The TCA randomly selects two large prime numbers p_1 and q_1, calculates the public key (β, N_1), and sends it to the LCA. The private key is α and sends it to the AG. After the relevant parameters are given, two prime numbers are selected by the TCA. These

two numbers are random. p_2, q_2, calculates (n, g), it is the public key. Sends it to the SM, and sends the private key to the CC, it is (λ, μ). Three one-way hash functions are defined by the TCA. $H_1 = \{0,1\}^* \to Z_N^*$, $H_2 = \{0,1\}^* \to Z_N^*$, $H_3 = \{0,1\}^* \to Z_N^*$.

4.2. Registration

1) SM registration

SM need to request a pseudonym to protect privacy. SM registration selects a number $r \in Z_N^*$ which is random, calculates $P = g^r$, then calculates the signature.

$$\delta_{SM} = H_1(P)^d \bmod N_0. \tag{1}$$

$$M_{SM} = H_2\left(P \| ID_{SM} \| r^d \bmod N_0 \| TS\right). \tag{2}$$

the certificate information is calculated according to the signature

$$Cr_{SM} = \frac{r}{\delta_{SM} M_{SM}} \bmod N_0. \tag{3}$$

and finally the smart meter sends a data request packet to the LCA.

$$SM \to LCA: \{M_{SM} \| Cr_{SM} \| ID_{SM} \| P \| TS\}. \tag{4}$$

The LCA receives the request message, which is sent by the SM, the LCA checks δ_{SM} through the public key e to verify M_{SM}. If

$$M_{SM} = H_2\left(P \| ID_{SM} \| Cr_{SM}{}^e \cdot H_1(P)^{M_{SM}} \bmod N_0\right). \tag{5}$$

$$Cr_{SM}{}^e \cdot H_1(P)^{M_{SM}} \bmod N_0 = \frac{r^e}{H_1(P)^{d \cdot e \cdot M_{SM}}} \cdot H_1(P)^{M_{SM}} = r^e \bmod N_0. \tag{6}$$

The LCA selects a random number $r_1 \in Z_N^*$, calculates $Q = g^{r_1}$, and then sends an encrypted response packet $Enc(P \| Q \| TS, Pub_{SM})$ to the smart meter, and calculates the pseudonym $Pseu_{SM} = P^{r_1} = g^{r \cdot r_1}$ of the smart meter, store and update the pseudonym, and then send the pseudonym to the TCA.

$$LCA \to SM: Enc\left(\{P \| Q \| TS\}, \mathrm{Pub}_{SM}\right). \tag{7}$$

The SM decrypts with the private key after receiving the response packet. If the P recovered is right, the SM calculates $P' = g^{r'}$ with a random number $r' \in Z_N^*$, r' satisfies $r' + r = 1 \bmod n$, The request packet is sent to the TCA, its role is to obtain a pseudonym certificate, which is used for secure communication.

$$SM \to TCA: Enc\left(\{P' \| Q \| TS\}, \mathrm{Pub}_{TCA}\right). \tag{8}$$

After the certificate request is received, the received message is decrypted by TCA, the pseudonym of the smart meter is verified, and the validity of the timestamp is verified. A random number is selected by TCA $r_2 \in Z_N^*$, calculates $I = g^{r_2}$, and generates a pseudonym certificate $Cerp_{SM} = P'^{r_2} = g^{r' \cdot r_2}$. Finally, the TCA stores and updates the pseudonym certificate, and sends the response

packet to the SM.

$$TCA \to SM : Enc\left(\left\{P' \| I \| TS\right\}, \mathrm{Pub}_{SM}\right). \tag{9}$$

The SM uses the private key for decryption. If the recovered P' is correct, its pseudonym certificate can be calculated.

2) AG registration

The AG selects a random number $r_3 \in Z_N^*$, calculates $L = g^{r_3}$, and then calculates the signature

$$\delta_{AG} = H_1\left(P\right)^{\alpha} \bmod N_0. \tag{10}$$

$$M_{AG} = H_2\left(L \| ID_{AG} \| r_3^{\alpha} \bmod N_0 \| TS\right). \tag{11}$$

Calculate this certificate information, it is calculated based on the signature

$$Cr_{AG} = \frac{r_3}{\delta_{AG} M_{AG}} \bmod N_0. \tag{12}$$

Finally, a data request message is sent, which is sent by the SM to the LCA.

$$AG \to LCA : \left\{M_{AG} \| Cr_{AG} \| ID_{AG} \| L \| TS\right\}. \tag{13}$$

The LCA receives the request message, which is sent by the SM, the LCA checks δ_{SM} through the public key β to verify M_{AG}. If

$$M_{AG} = H_2\left(L \| ID_{AG} \| {Cr_{AG}}^{\beta} \cdot H_1\left(L\right)^{M_{AG}} \bmod N_0\right). \tag{14}$$

then verify the identity of the AG. Then calculate $r_1' \in Z_N^*$, r_1' satisfies $r_1' + r_1 = 1 \bmod n$, calculate the new aggregator pseudonym.

$$Pseu_{AG} = L^{r_1'} = g^{r_1' \cdot r_2}. \tag{15}$$

and the LCA reports to the TCA send a pseudonym certificate request.

$$LCA \to TCA : Enc\left(\left\{L \| Pseu_{AG} \| TS\right\}, \mathrm{Pub}_{TCA}\right). \tag{16}$$

After the request packet is received, it is decrypted by the TCA and a number is selected, which is random $r_2' \in Z_N^*$, r_2' satisfies $r_2' + r_2 = 1 \bmod n$, calculates a pseudonym certificate

$$Cerp_{AG} = {Pseu_{AG}}^{r_2'} = g^{r_1' \cdot r_2' \cdot r_2}. \tag{17}$$

store and update, and send the response packet to the AG.

$$TCA \to AG : Enc\left(\left\{L \| Cerp_{AG} \| TS\right\}, \mathrm{Pub}_{AG}\right). \tag{18}$$

3) Data aggregation

The SM chooses based on its pseudonym, adds a masked random number to the collected electricity consumption data, encrypts the plaintext data (B) with the electricity consumption information of the user by using Advanced Encryption Standard algorithm to obtain the encrypted ciphertext data (C). $C = E\left(K, B\right)$, the SM calculates the message $\sigma = H_3(C) \bmod n$, and then sends the data packet to the AG.

$$SM \to AG : \left\{C \| \sigma \| Cerp_{SM} \| TS\right\}. \tag{19}$$

The decryption process is $B = D(K, C)$. AG gets total power usage data with CC shared key.

Encrypted data process:

$$C_1 = E(K, B_1) = (B_1 + x_{1,2} + x_{1,3} + \cdots + x_{1,t} + K_{1,AG} + K_{1,CC}) \bmod n. \quad (20)$$

$$C_2 = E(K, B_2) = (B_2 - x_{1,2} + x_{2,3} + \cdots + x_{2,t} + K_{2,AG} + K_{2,CC}) \bmod n. \quad (21)$$

$$C_3 = E(K, B_3) = (B_3 - x_{1,3} - x_{2,3} + \cdots + x_{3,t} + K_{3,AG} + K_{3,CC}) \bmod n. \quad (22)$$

$$\vdots$$

$$C_t = E(K, B_t) = (B_t - x_{1,t} - x_{2,t} - x_{3,t} + \cdots + K_{t,AG} + K_{t,CC}) \bmod n. \quad (23)$$

Decryption process:

$$B_{AG} = D(K, C) = (\sum_{i=1}^{t} C_i - \sum_{i=1}^{t} K_{i,AG}). \quad (24)$$

$$B_{CC} = (\sum_{i=1}^{t} C_i - \sum_{i=1}^{t} K_{i,AG} - \sum_{i=1}^{t} K_{i,CC}) = \sum_{i=1}^{t} B_i. \quad (25)$$

The CC gets the total electricity consumption data.

5. Performance Analysis

5.1. Security Analysis

In this section, we will analyze the proposed privacy protection scheme, analyze the security, and analyze the privacy protection. We will focus on analyzing how this solution achieves the anonymity of SM and the reasons why the identity of legitimate SM cannot be used fraudulently. In addition, through integrity checks, in our proposed privacy protection scheme, we can not only resist passive attacks but also active attacks. On this basis, we not only guarantee the anonymity of SM, but also its unforgeability.

1) When the LCA receives a registration request, the request is sent by the new local device, $M_{SM} = H_2(P \| ID_{SM} \| r^d \bmod N_0 \| TS)$ is a message with zero knowledge signature, and the smart meter uses its own private key d generates signature $\delta_{SM} = H_1(P)^d \bmod N_0$. The message is then used to generate certificate information Cr_{SM}. After receiving the request, the LCA uses its public key e to verify the true identity of the SM, without knowing the zero-knowledge-based certification protocol Specific signature δ_{SM}. Even if the opponent holds the private key d, it is difficult to find $x' \in Z_N^*$, so that $(x')^d = \delta_{SM}$, so the LCA can verify the identity of the device, and the signature will not be leaked, nor forged.

2) The LCA sends a response packet $Enc(P \| Q \| TS, Pub_{SM})$ to the SM. This response data packet is encrypted. It is encrypted by the SM using the public key. This data packet can only be correctly obtained by the SM, and the verification can only be performed by the SM. $P = g^r$ changed and generates its pseudonym $Pseu_{SM} = P^{r_1} = g^{r \cdot r_1}$. In addition, the parameter exchange used to generate pseudonyms is performed under the assumption of Diffie Hellman: given g^r, g^{r_1}, it is difficult to calculate $g^{r \cdot r_1}$, Even if the P, Q obtained, the pseudonym will not be calculated correctly by the opponent, so as to guarantee SM's pseudonym and make it unforgeable.

3) When a pseudonym certificate is generated, the TCA does not need to know the actual identity of the SM, and determines whether the user is legitimate by verifying the pseudonym. The process of generating a pseudonym certificate is similar to the pseudonym generation process, both of which are based on Diffie Hellman assumption. Therefore, the counterfeit certificate of the SM cannot be stolen and forged by the adversary.

4) SM can change the pseudonym, as well as the pseudonym certificate, which makes it difficult for adversaries to track it. In this way, the identity of the SM can be protected, and the opponent cannot know. In addition, because the generation of pseudonyms is related to multiple entities, the process of generating pseudonym certificates is the same. Our privacy protection scheme can reduce privacy leakage and protect the identity privacy of users, compared with a single pseudonym solution. During transmission, the integrity of the data is done by each entity verifying the message. One-way hash function $H_2 = \{0,1\}^* \to Z_N^*$, $H_3 = \{0,1\}^* \to Z_N^*$ is a random mapping. If the opponent modifies the data during the transmission of the data, it can also be detected, and the data receiver can verify the message for detection.

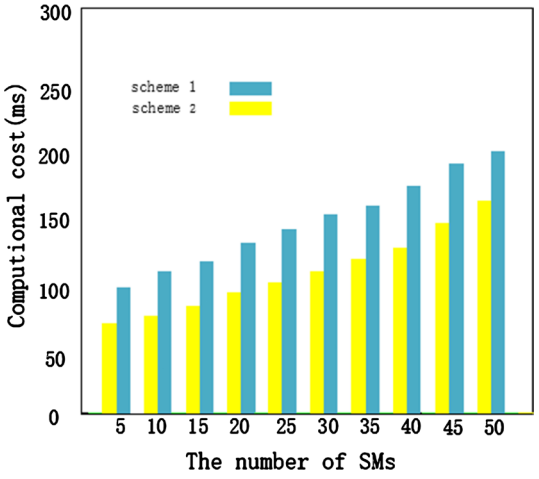

Figure 2. Comparison of computational cost.

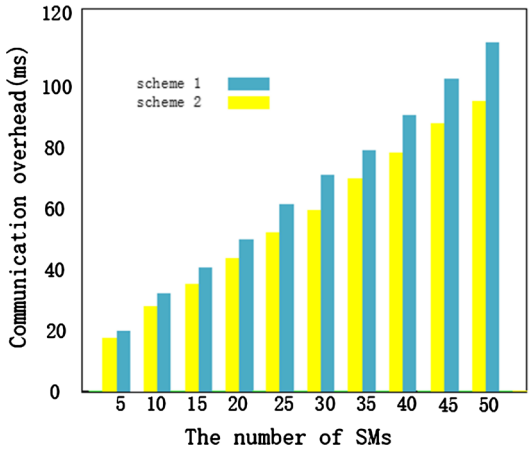

Figure 3. Comparison of communication overhead.

5.2. Computational Cost and Communication Overhead

Our experiments were performed on the matlab platform. 128-bit Advanced Encryption Standard is used, and the number of encryption rounds is 10. **Figure 2** illustrates the relationship between the computational cost and the number of SMs. **Figure 3** illustrates the relationship between the communication overhead and the number of SMs. The scheme 2 proposed in this paper is compared with the scheme 1 in the literature [14]. The results show that the scheme has less computational cost and communication overhead than the literature [14].

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

[1] Ferrag, M.A., Maglaras, L.A., Janicke, H., *et al.* (2018) A Systematic Review of Data Protection and Privacy Preservation Schemes for Smart Grid Communications. *Sustainable Cities and Society*, S2210670717308399.

[2] Farhangi, H. (2010) The Path of the Smart Grid. *IEEE Power and Energy Magazine*, **8**, 18-28.

[3] Chan, J.C.L. and Wong, D.S. (2015) A Survey on Security Assessment of Metering Infrastructure in Smart Grid Systems. *Proc. IEEE Southeast Con*, 1-4.

[4] Smartgrids and Meters (2015). http://ec.europa.eu/energy/en/topics/marketsand-consumers/smart-grids-and-meters

[5] Yu, S. (2017) Big Privacy: Challenges and Opportunities of Privacy Study in the Age of Big Data. *IEEE Access.*

[6] Mehmood, A., Natgunanathan, I., Xiang, Y., *et al.* (2016) Protection of Big Data Privacy. *IEEE Access*, **4**, 1821-1834.

[7] Karimi, B., Namboodiri, V. and Jadliwala, M. (2015) Scalable Meter Data Collection in Smart Grids through Message Concatenation. *IEEE Transactions on Smart Grid*, **6**, 1697-1706.

[8] Li, F., Luo, B. and Liu, P. (2011) Secure and Privacy-Preserving Information Aggregation for Smart Grids. *Int. J. Security and Networks*, **6**, 28-39.

[9] Saxena, N., Choi, B.J. and Grijalva, S. (2017) Secure and Privacy-Preserving Concentration of Metering Data in AMI Networks. *IEEE ICC.*

[10] Tan, X., Zheng, J., Zou, C., *et al.* (2016) Pseudonym-Based Privacy-Preserving Scheme for Data Collection in Smart Grid. *International Journal of Ad Hoc & Ubiquitous Computing*, **22**, 120-127.

[11] Chim, T., Yiu, S., Hui, L. and Li, V. (2011) PASS: Privacy-Preserving Authentication Scheme for Smart Grid Network. 2011 *IEEE International Conference on Smart Grid Communications* (*SmartGridComm*).

[12] Cheung, J.C.L., Chim, T.W., Yiu, S.M., *et al.* (2011) Credential-Based Privacy-Preserving Power Request Scheme for Smart Grid Network. *IEEE Global Telecommunications Conference.*

[13] Yu, C.M., Chen, C.Y., Kuo, S.Y., *et al.* (2014) Privacy-Preserving Power Request in Smart Grid Networks.

[14] Guan, Z., Zhang, Y. and Wu, L. APPA: An Anonymous and Privacy Preserving Data Aggregation Scheme for Fog-Enhanced IoT. *Journal of Network and Computer Applications.*

[15] Garcia and Jacobs, B. (2010) Privacy-Friendly Energy-Metering via Homomorphic Encryption.

[16] Saxena, N., Choi, B. and Lu, R. (2015) Authentication and Authorization Scheme for Various User-Roles and Devices in Smart Grid. *IEEE Transactions on Information Forensics and Security*, 1.

[17] Ács, G. and Castelluccia, C. (2011) I Have a DREAM! (DiffeRentially privatE smArt Metering).

[18] Riyaldhi, R. and Kurniawan, A. (2017) Improvement of Advanced Encryption Standard Algorithm with Shift Row and S.Box Modification Mapping in Mix Column. *Procedia Computer Science*, **116**, 401-407.

[19] Camenisch, J. and Stadler, M. (1997) Efficient Group Signature Schemes for Large Groups. *Annual International Cryptology Conference*, Springer, 410-424.

[20] Zhang, L., Liang, P. and Mu, Y. (2018) Improving Privacy-Preserving and Security for Decentralized Key-Policy Attributed-Based Encryption. *IEEE Access*, **6**, 12736-12745.