International Journal of Computing and Digital Systems
ISSN (2210-142X)
Int. J. Com. Dig. Sys. 10, No.1 (Jan-2021)

http://dx.doi.org/10.12785/ijcds/100115

An Efficient Privacy Protection Scheme for the Smart Meter in Electrical Distribution System

Rakhi Yadav[1] and Yogendra Kumar[2]

[1,2]*Department,of Electrical Engineering, MANIT Bhopal, India*

Received 28 Apr. 2020, Revised 30 Jul. 2020, Accepted 28 Aug. 2020, Published 1 Jan. 2021

Abstract: Nowadays, smart meters are being used for measuring power consumption at the consumer end. These smart meters send the energy consumption data to the control center of the service provider at regular intervals. However, the power consumption data may contain certain information of the user that may disclose consumer's privacy, like the usage pattern. Smart meters may also suffer from numerous physical and cyber-attacks because the smart meter terminal works as a part of open and public infrastructure. Therefore, the authenticity of smart meters is under concern. To address the problem mentioned above, we have proposed here a privacy protection scheme for a smart meter, which requires less computational time as compared to the existing related schemes. Moreover, this scheme scrutinizes the trustworthiness of the smart meter before sending the power consumption information to the service provider. The privacy protection and trustworthiness of the smart meter have been proved in theory. Performance analysis shows that the proposed scheme has higher computational efficiency than other existing literatures.

Keywords: Smart Meter, Privacy Protection, Ring Signcryption, Trusted Computing, Secret Sharing

1. INTRODUCTION

At present, government, industrial, and academic institutions all over the world are very keen about smart grids due to their high efficiency and reliability. The smart meters are beneficial for both consumers and energy suppliers to make the grid intelligent by monitoring the billing detail of the electricity consumption regularly of all different consumers [1]. Due to smart meters, bidirectional communication between power control centers is possible. Real-time information received from smart meters, improves the reliability and efficiency of the whole power system. Intruders may collect sensitive information about the habits and hobbies of the users by analyzing the real-time message sent by the smart meter, which raises serious privacy issues [2,3,4]. In addition to this, electricity distribution systems are also suffering from network attacks. Mostly, network attacks are seen at the terminals of the network [5,6]. Physical attack is also possible on the terminals (smart meters) of the network, which can affect the accessing of the sensitive data and keys. Unauthorized modification in the hardware also comes under the definition of physical attack. Electricity theft is also occurring due to tempering in the control logic of terminals and modified application code, which are running in the smart meters [7,8]. Therefore, the security of smart meters is a prime concern.

Moreover, smart meters are not immune to cyber-attacks as sensitive information is recorded and transmitted in the form of electricity bills. The concerns, as mentioned above and threats, clearly state the ineffective monitoring methods existing currently. Hence, smart meters are not being trusted. The current scheme of the paper could solve both the privacy protection of the smart meters used in the smart grid and the trustworthiness of smart meters.

Many research studies have been published to address some of the above-mentioned issues. J. Ni et al. [9] and R. Lu et al. [10] have proposed the privacy protection scheme by blurring the data. While some researchers have proposed to add noise in power consumption information prior to sending it to the control center using a data aggregation method. Hence, the control center receives this fuzzy data of the power consumption and privacy of the user is preserved. Another privacy protection approach is based on user's identity [11,12]. This method uses the cryptography-based approach, such as ring signcryption, in which the anonymous user identity is made instead of the real user to protect user's privacy.

In both, the discussed above approaches, trusted smart meters are used. As stated earlier, smart meters can

E-mail: yadavrakhi.87@gmail.com, ykmact@yahoo.co.in

be tempered either via physical or network attacks making them unreliable in the distribution system, which may affect the credibility of the power system. The solution to this problem is given by Karopoulos et al. [8], who designed and evaluated a trusted computing environment. This environment is used for the smart meters in which sensitive data, applications, and keys can be stored. J. Zhao et al. [13] have proposed another privacy scheme which is based on the trusted cryptography module (TCM) for sending the real-time electricity bills. The main drawback of the above scheme is the inability to verify the trustworthiness of the smart meter in real-time.

To address the above issues, we have proposed an efficient privacy protection scheme for smart meter in the electric distribution system, which can also verify the trustworthiness of the smart meter in real-time. The proposed scheme uses the idea of identity-based ring signcryption and visual secret sharing. The advantages of the proposed scheme over the existed related works exclude the need of certificates for attestation. Furthermore, it is independent of the number of ring members. Performance analysis has been done on the basis of computation cost, which shows that the proposed scheme has higher computational efficiency than other existed works.

The rest part of the paper is organized as follows. Section 2 describes the idea of trusted computing. Section 3 gives the details of the proposed scheme and the implementation of the scheme is given in section 4. Section 5 analyzes the proposed work based on security and performance. Section 6 concludes the proposed work and future research directions.

2. TRUSTED COMPUTING

The role of trusted computing (TC) is to check the trustworthiness of the smart meter. A group of companies (IBM and HP) known as trusted computing group has the technical manuals which are required for the information of hardware, software and the network architecture for TC. The basic component of TC is a Trusted Platform Module (TPM). TPM is a small System on Chip (SoC) that supports security functions [14]. The entities which may vary the integrity of the platform are measured by TPM with the help of the integrity measurement mechanism. The measurement event is recorded into the Stored Measurement Log (SML) and the measured values are stored in a Platform Configuration Register (PCR). During the inquiries of the entities, TPM reports the PCR values. TPM uses a unique Endorsement Key (EK) for its identity and it provides data security through the access authorization. This can be done by seal and un-seal operations. In seal operation, data encrypts and stores with user-specified PCR measured values. When PCR group values are the same as the sealed values, then the un-seal operation is successfully done.

In the case of remote access, the server requires the verification of the visitor which is trusted. TPM and remote certification protocols are used to verify the information of the platform's identity and platform's configuration were proposed by Trusted Computing Group (TCG), providing hardware-based credible evidence for entities in the network. TCG is a trusted computing organizational group of different companies such as IBM, HP. These companies have formulated the main technical manual for trusted computing which has necessary information of software, hardware, network architecture and terminal. The attestation of the configuration state of the platform is done by several methods like binary attestation, attribute-based attestation, etc. The binary-based attestation may expose the configuration information of the platform and makes the platform vulnerable to attacks. Poritz et al. [15] and A. R. Sadeghi and C. Stuble [16] have introduced attribute-based attestation. This type of attestation requires security attribute verification and does not need to provide specific configuration information. Dongjun L. and Jun Z. [17] have proposed an efficient anonymous remote attestation protocol that combines both the binary attestation and attribute-based attestation. The idea of a ring signature is applied with this protocol to achieve the attestation of the platform's identity and the status of integrity at the same time.

3. PROPOSED SCHEME

The System model of the proposed scheme is divided into two parts, one is the security model and another is system architecture. The details of the model are described as follows-

A. Security model

In the proposed security model, all the involved entities are trusted but curious. So, entities cannot attack actively, but user's behavior can be deduced from the data. We consider the external attack in this security model. There are two types of attacks. The first type, the intruder tries to attack on the smart meter to destroy the smart grid. It can be done by physical and network attacks. In physical attack, attacker tempers the smart meter by powerful magnets. It is not a smart way of the attack. Another possibility is the network attack, in which intruder places the malicious code in the network which is very dangerous. In this type of attack, key and data can be easily destroyed or modified.

B. System architecture

Our proposed scheme basically has five subparts. Their functions and roles for the smoother operation have been described as follows:

- Service provider (SP): Distributes electricity to the consumers.
- Trusted authority (TA): To verify the security aspects of smart meters.
- Smart meter M_i: Measures the energy consumption and sends to the concerned regional gateway.
- Regional gateway (RG): Collects energy consumption in that locality then it ensures the reliability by checking that message is correct or not sent by the meter, it also checks the reliability of that particular meter.
- Control center (CC): By using real-time information, it makes desirable decisions.

The proposed model is shown in figure 1.

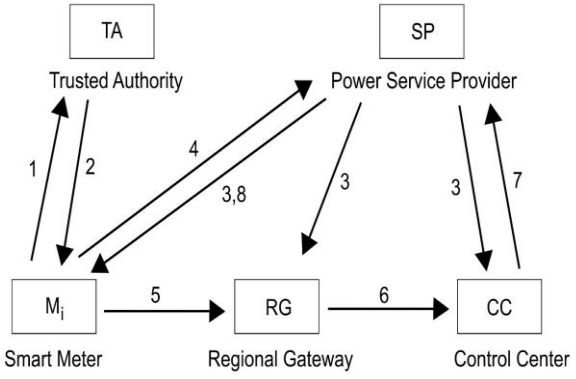

Figure 1. System Architecture

The concept of TPM module has been introduced in this proposed model. So, every smart meter has one TPM module. We have used an offline process for setting the security attributes for all smart meters. The prerequisite of every smart meter installation must be satisfied to have already defined security attributes by TA. Therefore, every authenticated smart meter would have a partial private key and set of the attribute value, produced, sealed, and bounded by TA. Then, prior to signcryption, seal measurement values and measured current PCR values would be compared by the smart meters. Equality of these two values shows that the configuration state of the smart meters has not been manipulated and this ensures the trustworthiness of meter because sealed partial private key can only be achieved by reliable meters [18].

When smart meter gets all the keys then it completes ring signcryption operation on energy consumption data by using the visual secret sharing approach (VSS) [19]. This VSS approach helps to preserve the true identity of consumers because RG does not restore plain text information for the verification of the validity of signcrypted messages. This helps to improve the security at the time of data transmission. CC, also can obtain the information of user's power consumption without knowing the true identity of users. The only service provider has the right to know the true identity of the users according to the user's pseudo-identity but cannot find the details of user's power consumption. Hence, the privacy of the user will be protected.

The assumption of the following symbols which are used in our paper- y_i is the partial secret key which is generated by TA for smart meter, x_i is another partial secret key which is generated by M_i and P is the security attribute set defined by trusted authority [18]; TPM_{Mi} is a TPM module which is installed on M_i; $V_{PCR\text{-}Mi}$is the PCR values of M_i; d_i is the pseudo-identity of the smart meter; $\{m||d_i\}(x_i, y_i)$ is asigncrypt the information.

The working procedure of the proposed work has been described by figure 1. Total eight steps shown in this figure are being discussed one by one as follows:

1) In first step, M_i requests TA for attribute property verification.

2) In step 2, trusted authority verifies the property of attribute set value of the smart meter corresponding to the request. Then, TA generates the partial secret key y_i for the smart meter only after fulfilling the verification criteria by the M_i. This y_i is binded with the PCR value $V_{PCR\text{-}Mi}$, and this is encrypted by ER public key. This bundle along with W is sent to the M_i, where W is another attribute set of values.

3) In step 3, the service provider provides partial secret keys for M_i, RG and CC and SP also provides a pseudo-identity d_i for M_i corresponding to I_i.

4) The M_i provides partial secret keys x_i and y_i to SP in step 4.

5) In step 5, the TPM_{Mi} calculates the current PCR value; this value is compared with V_{PCR-Mi}, if both values are the same, then performs the signcryption process. After this successful verification, smart meter gets the partial secret key y_i. Smart meter concatenates the power consumption information m and d_i, and applies all the partial secret keys on this concatenated information which is known as C. This C is combined with a verification code V_0 and sends it to the RG.

6) In step 6, signcrypted information is verified by regional gateway. Successful verification shows that message is valid and smart meter is trusted. The RG sends the cipher text to CC only after trustworthiness of the M_i.

7) In step 7, control center applies the secret key on the received message which is sent by RG and restore the message. Then, CC can analyze the fine grain data of the power consumption and calculates the electricity bill. This bill along with d_i is sent to the SP.

8) Service provider calculates real identity of the users on the basis of the d_i and sends the electricity bill to the real user in the last step 8.

4. IMPLEMENTATION PROCESS

We have observed that the trusted center has authority to generates all the keys which are used in Anonymous Attestation from Attribute-Based Ring Signature (AA-ABRS) [17]. Therefore, there is a possibility that if any trusted center itself is malicious then it may impersonate and can pass the verification easily which can be the serious cause of security concern. This type of security issue may pose a serious threat to the distribution system. Dongjun L. and Jun Z. [17] have introduced another privacy scheme which also creates large computational overhead due to the application of bilinear pairing in the verification phase. To overcome the above problem, the signcryption process has been improved.

To address the above mentioned issues, we have proposed a privacy-preserving scheme for smart meter in the electric distribution systems. It has better computational efficiency than other existed schemes [12, 17, 18, 20, 21, 22, 23]. Initially, the TA produces a partial key for smart meters and another part of key is generated by smart meters and service providers. Only a trusted, smart meter can achieve all the keys. These three keys form a complete signcryption key. The signcryption operation is performed only after the generation of all the keys. In this scheme, RG can verify the integrity of the signcrypted message without restoring the power consumption information, which shows that the proposed scheme is more secure.

The proposed work has been implemented in the following steps: Initialize parameters, attributes authentication, signcryption, verification, and measurement of energy consumption. Table I shows the list of used symbols.

A. *Initialize Parameters*

- First of all, we initialize trusted authority and service provider then SP generates the master key (*s)* and calculates a public key y=sP, where *P* is a security attribute set defined by TA. Trusted authority creates a secret key $s' \in Zq*$ and calculates the corresponding public key $P_{TA} = s'P$. P_{TA} remains open for public and secret key kept as secret. TA also generates a set of random number *W*. Smart meter has only some security attributes which are related to authentication. *W* and *P* are mapped with a function *f*, where *f* is a one to one mapping function.
- The SP issues partial keys for M_i, RG, and CC. Assume I_b and P_{kb} as the identity and partial private keys of RG, respectively. Then RG sends I_b and P_{kb} to SP. Similarly, CC sends I_c and P_{kc} to SP and M_i sends the partial keys x_i and y_i to SP. SP calculates the partial key $K_1=(x_i \oplus s)$ and $K_2=(y_i \oplus s)$. Then, SP returns K_1 to RG and K_2 to CC.

TABLE I. List of symbols

List of symbols	Description
M_i	Smart meter
P	security attribute set
x_i *and* y_i	Partial secret keys used by smart meter
C	Chipper text
K_1 *and* K_2	Partial secret keys used by regional gateway and control center respectively
d_i	pseudo-identity
m	power consumption information
L	$m \| d_i$
T_x	Computation time of XOR operation
T_b	Computation time of bilinear operation
T_e	Computation time of exponential operation
T_m	Computation time of multiplication operation
V_0	Verification code
P_{kb}	Partial private key of regional gateway
P_{kc}	Partial private key of control center
I_a	Identity of smart meter
I_b	Identity of regional gateway
I_c	Identity of control center
∂	Signcrypted cipher text
T_{2dnf}	Computation time of 2-DNF Formulas Cryptosystem Decryption
s	Master key of service provider

B. *Attributes authentication*

The verification process of the authenticity of smart meter M_i is done in three steps which are shown in figure 2. Verification procedure is being explained below-

- Smart meter uses the public key of trusted authority to encode V_{PCR-Mi}. TPM measures the metric log SML corresponding to the PCRs and for identity of the TPM used an EK certificate. The encoded message is sent to the trusted authority.
- Trusted authority decrypts the message by using private key s` and verify the certificate. After successful verification, TA calculates the standard values of V_{PCR} on the basis of the SML. If the calculated V_{PCR} value is same as the V_{PCR-Mi} then the smart meter is trusted.
- After verification of attribute in P of the smart meter, TA randomly generates the partial key y_i. Trusted authority encodes the $\{V_{PCR-Mi}, y_i\}$ by using EK public key and sends it to the smart meter. This message is decrypted by the TPM_{Mi}

and the encrypted key y_i is received by M_i if and only if the current PCR values are equal to the encrypted PCR value.

- Smart meter sends the identity I_a to the SP and SP returns the pseudo-id d_a corresponding to the I_a along with partial secret key P_{kb}.

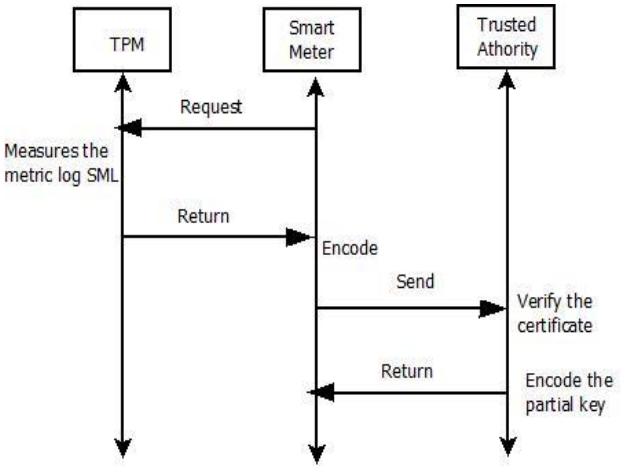

Figure 2. The process of meter's attribute authentication

C. Signcryption

After successfully attribute authentication by TA, smart meter receives the keys from TA and SP. After receiving these keys M_i generates another partial private key x_i and perform the signcryption by using these keys. It is assumed that the identity of M_i is I_a and pseudo-identity is d_a. Suppose L is the concatenation of the power consumption information m and pseudo-id d_a.

- Randomly, select partial secret key x_i, then concatenate the m with d_a and make as L, the size of the keys and L are same.
- M_i Send x_i and y_i to the Service Provider.
- Calculate cipher text: $C= L \oplus x_i \oplus y_i$.
- Calculate verification code: $V_0= C \oplus P_{kb}$.
- Output the signcrypted cipher text $\partial = (C, V_0)$ to the regional gateway (I_b).

D. Verification

In the verification phase, verification of the signcrypted message is done by the regional gateway and generate the cipher text C' for next level authentication which is sent to the control center. Regional gateway receives the signcrypted message ∂ (C, V_0) and calculate the authentication value (E), by following way: $E = V_0 \oplus P_{kb}$, Where P_{kb} is the partial key of region gateway. If(E==C) is true, then the signcrypted information is not tempered and M_i is trustworthy. After successful verification, calculate the cipher text value (C') for the next level authentication. The value of C' is calculated as: $C'= C \oplus K_1$ and it is sent to the control center.

E. Measurement of energy consumption

After successful verification of the integrity of the message by RG, RG sends the C*'* to the control center. Control center calculate *L*', $L'= C' \oplus K_2$, where $L'=L$. Control center analyses the fine grain data of the power consumption and calculates the electricity bill corresponding to the pseudo-id. This electricity bill is sent to the SP along with pseudo-id d_a. The service provider generates the real identity of the users by:
$I_a= d_a \oplus s$. Finally, SP sends this bill to the real user.

5. SCHEME ANALYSIS

The proposed approach verifies the trustworthiness of the smart meter via trusted computing and verifies the integrity of the message via visual secret sharing-based ring signcryption. The benefits of the approach are as follows-

- Attribute certificates are not required for remote anonymous verification.
- RG assures the trustworthiness of smart meters before receiving power consumption message.
- The proposed work checks the trustworthiness of the smart meters by doing one XOR operation.
- The Control center analyses the power consumption without knowing the user's identity.
- The signcryption process requires less computation cost compared to other existing approaches.

Analysis of the proposed work is based on the security and performance parameter.

A. Security analysis

Theorem 1: Signcrypted information is authenticated
Proof. Regional gateway receives the signcrypted information (C, V_0) sent by smart meter. To check the authentication of the information by comparing V with C, if V and C are equal then the message is authenticated otherwise not. The value of V is calculated as-
$V=V_0 \oplus P_{kb}$
$V =C \oplus P_{kb} \oplus P_{kb}$
$V= C$
The verifier value V is equal to C showing that the received cipher text (C) is not tempered, it means that the message is authenticated.
After successful verification of the message integrity, C' can be calculated as-

$C'=C\oplus K_1$ and it is sent to the control center for next level authentication. When CC receives the C', it calculates *L*' and the resultant of *L* is the electricity consumption corresponding to pseudo code.

$L'=C'\oplus K_2$
$=C\oplus K_1 \oplus K_2$
$=C\oplus s\oplus x_i\oplus s\oplus y_i$
$= C\oplus x_i\oplus y_i\oplus s\oplus s$
$= C\oplus x_i\oplus y_i$
$=L\oplus x_i\oplus y_i\oplus x_i\oplus y_i$
$=L\oplus x_i\oplus x_i\oplus y_i\oplus y_i$
$=L$
$=m||d_a$

Control center calculates the fine grain data corresponding to the electricity consumption and calculates the electricity bill. This electricity bill is sent to the service provider corresponding to pseudo-id without knowing the real identity of the users. Thus, our scheme is correct.

Theorem 2: Proposed scheme checks the trustworthiness of the smart meter before signcryption.

Proof. According to the security model, physical or network attacks are possible on the smart meter which affect the smart grid system. To overcome this type of problem, we check the trustworthiness of the smart meter before signcryption. It can be done by attribute authentication process which is performed by TPM. TPM verifies the sealed PCR values with generated PCR value; if the verification is successful, then the smart meter is able to get the partial secret key y_i provided by the trusted authority. After retrieving the y_i, the smart meter generates other parts of the secret key for the signcryption purpose.

B. Performance analysis

Theorem 3: The proposed privacy-preserving scheme requires less computation cost compared to other existed schemes.

Proof. In the existing state of the art, identity or attribute-based ring signcryption is used for privacy preservation. The identity-based approaches depend on the number of the ring members due to which overheads occur, and the attributes based approaches use the bilinear pairing (T_b), scalar multiplication (T_m) and exponentiation (T_e). Hence, the computing time is increased in this approach, but our proposed scheme does not depend on the ring members and also does not use bilinear pairing. Therefore, in our approach, computation time is reduced, which makes the system more efficient than the other existed schemes. The verification process of the trustworthiness of the smart meter is the same as given in reference [18] except the partial key generation for the smart meter, and ring signcryption is done by using the concept of visual secret sharing. In the proposed scheme, only 8 XOR (T_x) operations are required for the ring signcryption, which is efficient than T_b, T_m, T_e and T_{2dnf} (2-DNF Formulas Cryptosystem Decryption) operations. Hence, it takes less computation time as compared to the other existing works [12, 17, 18, 20, 21, 22, 23, 24, 25].

The AA-ABRS scheme [17] uses the 1026 bits for the signature whenever the proposed scheme has used 512 bits. In the proposed scheme 256 bits are used for the pseudo-id (d_a) and 256 bits for the power consumption information *m*. The concatenation of *m* and d_a is used as a secret message of the size 512 bits. The key size is also 512 bits long. The computing cost of the proposed work has been compared with other existing works, which is shown in tables II and III.

TABLE II. Comparison of computational complexity among [17], [18] and proposed scheme

Approaches	**Signcryption phase**	**Verification phase**	**No. of bits required**
Dongiun [17]	$5T_m$	$2T_b + T_e$	1026
Zhang [18]	$14T_m$	$7T_m$	640
Proposed scheme	$6T_x$	$2T_x$	512

TABLE III. Comparison between the proposed scheme and related state of the art

Approaches	**Computing cost**	**Depend on the number of ring members**	**Type of Cryptography used for Signcryption**
Zhang [12]	$(n+12)T_m$	Yes	Public Cryptography
Sharma [20]	$(2n+3)T_m$	Yes	Public Cryptography
Yu [21]	$(3n+1)T_m+2T_e$	Yes	Public Cryptography
Liu [22]	$(n+4)T_m+7T_e$	Yes	Public Cryptography
Qiz [23]	$4T_b+(2n+3)T_m$	Yes	Public Cryptography
Fan [24]	$3nT_m + (3n+1)T_e+ T_{2dnf}$	Yes	Public Cryptography
Wang [25]	$3T_b + 3T_m + 6T_e$	No	Public Cryptography
Proposed scheme	$8T_x$	No	Visual Secret Sharing

This scheme reduces the two bilinear pairings and one exponential operation by only 2 XOR operations in the verification phase, which is shown in table 1. In table 2, it can be seen that the proposed scheme requires only 8 XOR operations compared to other existed approaches, which are dependent on the bilinear pairing, exponential, and multiplication operations. Moreover, the computation cost of the proposed scheme is independent of the number of ring members. So, there is no efficient bottleneck caused by the number of ring members.

S. Zhang et al. [18] have stated that the bilinear logarithm, scalar multiplication and exponential operations require 8.419 ms, 0.392 ms and 0.996 ms respectively in the 2.40 GHz CPU, 8 GB RAM and windows 7 environment while Chun-I Fan et al. [24] have stated that 2-DNF Formulas Cryptosystem requires 1.06 ms in the 3 GHz Pentium IV system. On the basis of above statement, we can say that multiplication operator is more efficient operator than bilinear and exponential operators. From table 2 and 3, it is clear that among all the existing literatures, ref [18] is better than other ref [12, 17, 20, 21, 22, 23, 24, 25] for $n \geq 9$. S. Zhang et al. [18] have used only 21 times multiplication operations.

Proposed scheme has used only 8 times XOR operations for both signcryption and verification phases. Exclusive-OR operator requires approx. 1.83ms and multiplication operator needs approx. 1.24ms in 2.4 GHz CPU, 2 GB RAM, Windows 7. The total time required for 8 times XOR operations is 14.64ms while the total time required for 21 times multiplication operations is 26.04ms.

On the basis of above performance analysis, we can conclude that scheme of [18] is better than other schemes [12, 17, 20, 21, 22, 23, 24, 25] whereas scheme [18] has used 21 times multiplication operations. So, it is clear that the proposed scheme is more efficient than other existed literatures [12, 17, 18, 20, 21, 22, 23, 24, 25] because it uses only 8 times XOR operations which is more efficient than the 21 times of multiplication operations

Figures 3 & 4 deduces that the proposed work requires less computation cost as compared to the existing works [12, 17, 18, 20, 21, 22, 23, 24, 25]. The proposed scheme has used the visual cryptography technique instead of public cryptography, which is simple and easy to implement than public cryptography.

6. CONCLUSIONS

The scheme proposed in this paper is an efficient privacy-protection scheme for smart meter in the electrical distribution system. It can verify the trustworthiness of the smart meter before sending the power consumption information to the service provider. Apart from this, the privacy of the user remains preserved during all data exchanges between the smart meter and the service provider. The proposed scheme satisfies all the security requirements and it requires less computation time for signcryption and verification compared to other existing approaches. The performance analysis based on the computation time shows the effectiveness of the proposed work.

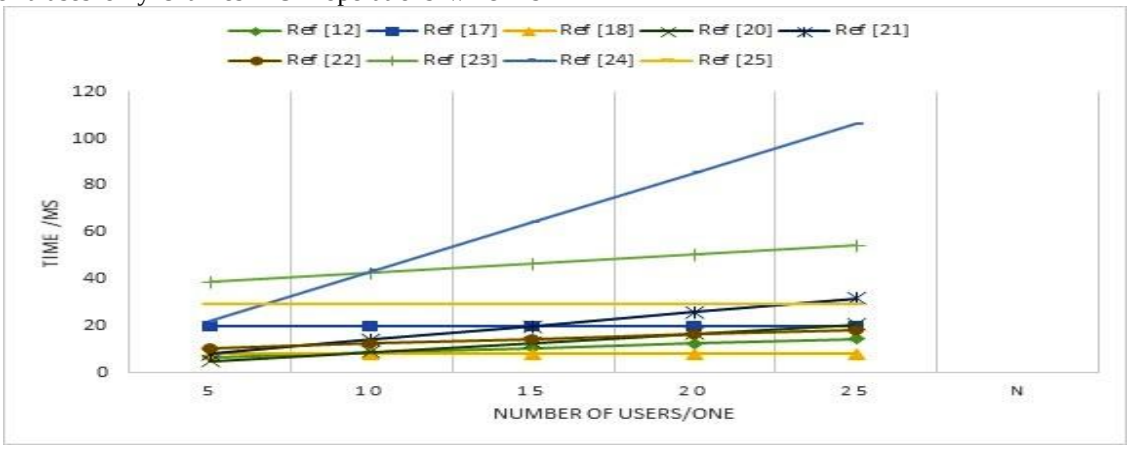

Figure 3. Comparison of computational time among different literature

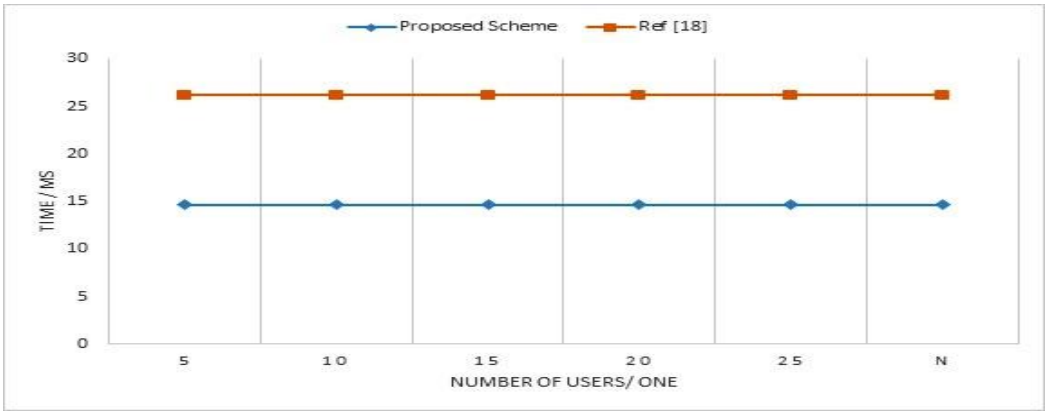

Figure 4. Comparison of computational time between proposed scheme and [18]

REFERENCES:

[1] Brown R. E. Impact of smart grid on distribution system design. Power and energy society general meeting: conversion and delivery of electrical energy in the century. 2008, pp. 1–4.

[2] Yang L, Chen X, Zhang J, Poor HV. Optimal privacy-preserving energy management for smart meters. IEEE INFOCOM. 2014, pp. 513–21.

[3] Rubio JE, Alcaraz C, Lopez J. Recommender system for privacy-preserving solutions in smart metering. Pervasive Mobile Comput 2017.

[4] Liu J, Xiao Y, Li S, Liang W, Chen CLP. Cyber security and privacy issues in smart grids. IEEE Commun Surv Tutorials 2012.

[5] Zhang S, Wang Z, Wang B. Terminal integrity detection scheme of electricity information acquisition system based on trusted computing. Electr Power Automat Equip 2017.

[6] Greveler U, Glösekötter P, Justus B, Loehr D. Multimedia content identification through smart meter power usage profiles. Computers, 2012, pp.1–8.

[7] Gao K, Wang Z, Ningyu AN, Zhao B. Construction of the immune system of cyber security for electric power supervise and control system based on trusted computing. Adv. Eng. Sci. 2017.

[8] Karopoulos G, Xenakis C, Tennina S, Evangelopoulos S. Towards trusted metering in the smart grid. IEEE international workshop on computer aided modeling and design of communication links and networks. 2017, pp. 65–74.

[9] Ni J, Zhang K, Alharbi K, Lin X, Zhang N, Shen X. Differentially private smart metering with fault tolerance and range-based filtering. IEEE Trans Smart Grid 2017.

[10] Lu R, Liang X, Li X, Lin X, Shen X. Eppa: an efficient and privacy-preserving aggregation scheme for secure smart grid communications. IEEE Trans Parallel Distrib Syst 2012.

[11] Chen Y, Martínez JF, Castillejo P, López L. An anonymous authentication and key establish scheme for smart grid: Fauth. Energies 2017.

[12] Zhang S, Zhao Y, Wang B. Certificateless ring signcryption scheme for preserving user privacy in smart grid. Automat Electr Power Syst 2018.

[13] Zhao J, Liu J, Qin Z, Ren K. Privacy protection scheme based on remote anonymous attestation for trusted smart meters. IEEE Trans Smart Grid 2016.

[14] Haldar V, Chandra D, Franz M. Semantic remote attestation: a virtual machine directed approach to trusted computing. In: Conference on virtual machine research and technology symposium; 2004. pp. 3–3.

[15] Poritz J, Schunter M, Herreweghen EV, Waidner M. Property attestation-scalable and privacy-friendly security assessment of peer computers. Bio-techniques, 2007; pp. 58–66.

[16] Sadeghi A. R., C. Stuble, Property-based attestation for computing platforms: caring about properties, not mechanisms. In: New security paradigms workshop, September 20–23, 2004, Nova Scotia, Canada, pp. 67–77.

[17] Dongjun L, Jun Z., Efficient anonymous attestation from attribute-based ring signature. Appl Res Comput 2012.

[18] S. Zhang, T. Zhang and B. Wang, A privacy protection scheme for smart meter that can verify terminals trustworthiness, Electrical Power and Energy Systems, 108 (2019), pp. 117-124.

[19] S. Shyu, Image encryption by random grids, Pattern Recognit., 40, (3), 2007, pp. 1014-1031.

[20] Sharma G, Bala S, Verma AK. Pairing-free certificateless ring signcryption (pf-clrsc) scheme for wireless sensor networks. Wireless Personal Commun 2015; pp. 1–17.

[21] Yu CM, Chen CY, Kuo SY, Chao HC.," Privacy-preserving power request in smart grid networks". IEEE Syst J 2014.

[22] Liu H, Ning H, Zhang Y, Xiong Q, Yang LT. Role-dependent privacy preservation for secure v2g networks in the smart grid. IEEE Trans Inform Forensics Secure, 2017.

[23] QiZ, Yang G, Ren X. Provably secure certificateless ring signcryption scheme, China Commun 2011; pp. 99–106.

[24] Chun-I Fan, Shi-Yuan Huang, and Yih-Loong Lai, Privacy Enhanced Data Aggregation Scheme Against Internal Attackers in Smart Grid, IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, 2013.

[25] Zhiwei Wang and HaoXie, Privacy-Preserving Meter Report Protocol of Isolated Smart Grid Devices, Wireless Communications and Mobile Computing, Wiley, 2017.

Rakhi Yadav has completed M. Tech. from MANIT Bhopal and currently pursuing Ph.D. from MANIT Bhopal. Her area of interest is smart grid, Electric distribution system and advanced metering infrastructure.

Yogendra Kumar has completed M. Tech. from MANIT, Bhopal and Ph.D. from IIT Roorkee. He is professor in Electrical Engineering Department, MANIT, Bhopal (M.P.). He also has been worked as HOD and dean (S&W). His area of interest is smart grid, electrical distribution system, neural network, fuzzy logic. He has published many research papers in reputed journals like IEEE transaction etc.