Jestr

Journal of Engineering Science and Technology Review 15 (4) (2022) 82 - 89

Research Article

JOURNAL OF
Engineering Science and Technology Review

www.jestr.org

A Secure and Efficient Identity based Proxy Signcryption Scheme for Smart Grid Network

Rachana Patil*,[1] and Yogesh H. Patil[2]

[1]*Pimpri Chinchwad College of Engineering, Pune, Maharashtra, India*
[2]*D. Y. Patil Institute of Technology, Pimpri, Pune, Maharashtra, India*

Received 2 May 2022; Accepted 18 August 2022

Abstract

A smart grid is a modern network system that configures variety of equipment based on Internet of Things and such equipment while working with smart grid systems produces huge amounts of data. As a result the data requires confidentiality and access control. To secure the data access, the proxy signcryption scheme is the most suitable option. In this work we proposed an identity based proxy signcryption scheme for smart grid (IDPSC-SG). The proposed scheme can provide the advantages of both, the proxy signature and proxy signcryption using single algorithm. The comprehensive security study of the proposed scheme shows that, IDPSC-SG can achieve the security requirements of IND-IDPSC-SG-CCA2. Furthermore it also achieve the existential unforgeability against adaptive chosen messages attack (EUF-CMA). The formal verification using AVISPA tool shows that IDPSC-SG is safe under OFMC and CL-Atse. Moreover, extensive performance evaluation indicates its efficiency with respect to computation time.

Keywords: Proxy Signcryption, Smart Grid System, Identity based cryptography, Proxy signature, Bilinear pairing

1. Introduction

The various network protocols are used to establish communication between different devices, those are involved in functionality of complex smart grid systems. The complexity of the smart grid system encourages the main concern over its data security [1]. The data coming from individual devices need to be gathered in an organised manner and translated between protocols, but due to insecure data translation of network protocols, this gathering of data may lead to leaking or mishandling by unauthorized entities [2-5]. Additionally, most commercial network protocols like Profibus, Modbus, which are used in smart grid, are intended for data communication purposes only and their data is not securely handled. This insecurity in network protocols promotes a fertile environment for attackers [6,7]. Although few of the network protocols are secure, they have compatibility issues with other existing protocols.

Apart from network protocol issues, hardware establishment and some supporting software's including operating system may lead to a way for attackers. The operating system developed for the automation industry may not ensure data security [8]. Many physical devices are outdated, have a lack of memory space and analog in operation, and may not be compatible with upgraded versions of software which are secure. For e.g. LCD display circuits have limited memory space and may not be able to perform some computational operations, as they are intended for customized functions and so they are unable to cope up with software which provides data security, which may lead to data theft.

For smart grids, to protect the data, an easy approach or specific configuration may not be sufficient. To prevent cyber-attacks on smart grid data, we are supposed to implement data security in a more stringent way by bringing the numerous security techniques together [9,10]. This approach has some advantages like tackling the system's weakness, identifying the various cyber-attacks[11], implementing the suitable defense system and classifying the individuals participating.

2. Security challenges in the smart grid

Smart grid systems are very susceptible to cyber-attacks and data violations. This section focuses on different cyber security challenges.

Connectivity: the numerous devices like measuring instruments or actuators of smart grid systems are integrated in a systematic manner to perform their individual functions effectively through the communication network. The smart grid system comprises remote locations and spread over a wide area, leading to demand for stricter measures against cyber-attacks and data violations by unauthorized persons [12,13]. Failing to data security in communication links, leads to malfunctioning of field devices or damage of instruments and may be disastrous if the smart grid is implemented for highly explosive applications like nuclear power plant or chemical-petrochemical industries.

Trust: The large area scope of the smart grid system and its long-distance connectivity to integrate it makes the end users' trust doubtful. Some end users may not always follow the guidelines and protocols laid down by the smart grid system. For e.g the end user may tamper with the electrical power meter which is used to record electrical power consumption and is an integral part of smart grid system. The tampering of meters internally may cause wrong readings, hence wrong billing and may damage the complete billing software system of smart grid [14].

Consumers privacy: To safeguard the consumers or end

*E-mail address: rachana.patil@pccoepune.org

ISSN: 1791-2377 © 2022 School of Science, IHU. All rights reserved.
doi:10.25103/jestr.154.12

users privacy is the prime aspect of any system and applicable to smart grid and needs to be committed for shielding and preserving consumers data. For instance, the inclusion of smart meters with smart grid makes the involvement of consumers personal information and smart grid systems regular correspondence with consumers make its data at risk[15]. The service provider may interfere with the end users personal information, which is already collected during configuring smart grid system. The service provider may share the end users data with a telemarketing -advertising agency and it is data violation. To prevent this the end users data must be shielded securely and must not handled by any unauthorized personals.

Software vulnerabilities: any software is prone to an ample range of cyber threats. Smart grid systems consist of simple software technology due to cost factor and are susceptible to malware attacks and malicious updates. These softwares must be updated periodically to maintain the faithful operations of smart grid with required patching of known malware attacks or malicious updates [16,17]. The patching process is a little bit complex for smart grid like applications and may slow down its performance or sometimes may need to reboot-restart the system which hampers the routine operations of smart grid.

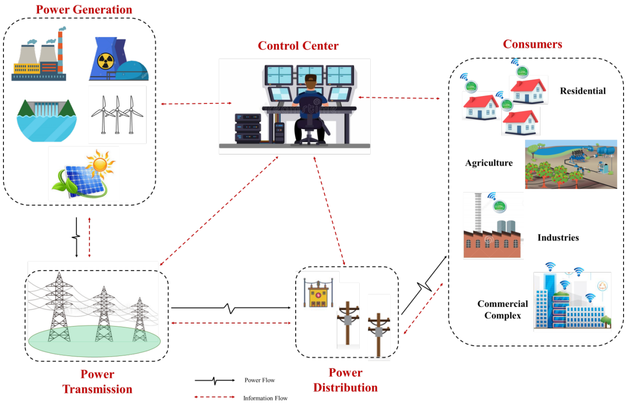


Fig.1. Generic illustration of Smart Grid system.

3. Related Work

The Identity (ID)-based Signcryption (IBS) method proposed by authors of [18], that takes a exclusive identification number accessible from each device which is handled by the authority holding a master key and can produce a unique secret key. Though the proposed method doesn't required exclusive arrangement for each device, it needs protected communication path to distribute secrete key between key generating servers and smart grid system. Authors of [19], presented identity-based signcryption with data aggregation for SG system. The pseudonym methodology can be used to check the user, as it protects data while communicating and minimizes the computational cost also. But the system is affected by key escrow problem and has communication bandwidth issues.

The data between end users and data creators can be protected by developing Elliptic Curve based signcryption using certificate less free pairing system as presented by [20], the system rectifies the certificates related issues and key escrow problem. Safe multicast communication system using attribute based signcryption system is proposed by [21]. It assures about data secrecy, complicity resistance, messages validation. The computational cost of SG system is more due to use of Bilinear Pairing for implementation. Signcrypted text can be developed by aggregate signcryption technique in which signcryption of multiple messages is combined as proposed by [22], masked random numbers are added to users data for signcryption, then building gateways develops multiple signcrypted messages and the same is pass on to control center.

In smart grid pull and push based secure multicast communication is possible by cipher text policy attribute based signcryption system as presented by [23], the proposed system supports privacy and essentials for data authentication and prevents any collusion attacks but due to use of bilinear pairing (BP) the communication bandwidth and computational speed reduces.

To minimize the computational efforts and achieve lighter pairing, ciphere text policy attribute based signcryption is proposed by aythors of [24], the signcryption working of end user can be subcontracted by transferring cipher text to simple cipher with the help of storage center and the overall system is effective with reduced computation while designcryption. However the use of bilinear pairing affects the systems performance for inadequate resources.

Protected communication between field devices and central server is implemented by heterogeneous signcryption system as proposed by authors of [25], IBC services are used by field devices PKI services facilitates for central server. The system supports data authorization, privacy, non repudiation and ciphertext secrecy. But the proposed system has to bear issues of certificate management and KEP. The smart grid operators and electrical power suppliers can establish secret communication with end users using multi-authority attribute based signcryption system as presented by authors of [26], though the system is short of forward secrecy, it provides non repudiation, data secrecy and authorization. To rectify the privacy leakage problems in smart meters, [27] promotes signcryption system without certificate. This system provides security to end users personal information and reduces the rate of data transmission via data concentrator with aggregation, but it affects due to PPKDP.

4. Preliminaries

The foundation and fundamental principles of bilinear pairing, assumption of complexity, nomenclature, and the mathematical formulation of the identity-based proxy signcryption scheme for smart grid environment[28,29] will be discussed in this segment.Table 1 lists the notations that were utilized in this work.

4.1. Bilinear Pairing

Let $\mathbb{G}$, $\mathbb{G}_T$ be a multiplicative cyclic group of prime order "P" and g, h be some elements of group$\mathbb{G}$. The map Ψ: $\mathbb{G}$ X $\mathbb{G}\rightarrow\mathbb{G}_T$isan acceptable map if the subsequent conditions stand true:

Ψ is bilinear, i.e for all a, b $\in_R \mathbb{Z}_p{}^*$, $\forall y \in_R \mathbb{G}$, Ψ maps as

$$\Psi\ (g.y,h) = \Psi(g,h).\Psi(y,h),$$

$$\Psi(g,h.y) = \ \Psi(g,h).$$

$$\Psi(g,y),\ \Psi(g^a,h^b) = \Psi\ (g,h)^{ab}$$

Ψ is non-degenerate, i. e. Ψ (g, g) $\neq 1_{\mathbb{G}T}$

$\Psi(g, h)$ is efficiently computable.

5. Formal model of proposed Identity based Proxy Signcryption for Smart Grid (IDPSC-SG) scheme

The IDPSC-SG Scheme is divided into seven algorithms as follows.

1. Setup Algorithm: - This algorithm is accountable for generating public parameters which are openly accessible to all the participating entities and master secret which is a secret of the trusted third party.
2. Key Extraction Algorithm: - Every individual user sends his/her unique identity IDa to the trusted third party. The secret key for the user Sa = $\mathcal{H}1$ (IDa) is generated and returned via the secret channel.
3. Warrant generation and Delegation Algorithm:-The original signer shall make a warrant w which contains the information about the type of delegation and time of delegation; it also defines the type of documents to be signcrypted by proxy signcryptor. This algorithm is accountable for generating the signing warrantSw and delegating it to proxy signer.
4. Warrant Verification Algorithm:-This algorithm is accountable for the verification of signing warrant received from original signer. If the warrant is verified correctly then the proxy signer executes the next algorithm.
5. Proxy Secret key Generation Algorithm:- The proxy signer generates the proxy secret key by using received warrant and his own private key. This key will further be used by proxy signer to generate signcrypted messages on behalf of original signer.
6. Proxy SigncryptionAlgorithm:-This algorithm takes the message to be sent M, proxy signers identity IDp, proxy Signers private key Sp = $\mathcal{H}1$ (IDp) identity of receiver IDr and public parameters as input and generates the signcrypted message and send to the receiver via a secure channel.
7. UnsigncryptionAlgorithm:- This algorithm takes received signcrypted message, receivers private key Sr = $\mathcal{H}1$ (IDr) and the identity of both sender and receiver IDp, IDr and generates the original message M if the signcrypted message has not tampered else it returns ⊥.

5.1. Security Definition

The proposed IDPSC-SG scheme must satisfy confidentiality and unforgeability of original message. Let us consider that there exist an adversary$\mathcal{A}_d$ for the proposed scheme and ℂh is a challenger. For indistinguishability againstadaptive chosen cipher text attack (IND-CCA2) the following interaction between adversary$\mathcal{A}_d$ and challenger ℂh.

Definition 1: If adversary$\mathcal{A}_d$ with no polynomial time and having non-negligible advantage win the following game , then the proposed scheme IDPSC-SG can achieve the security requirements of IND-IDPSC-SG-CCA2.

Initial: The challenger ℂhexecutes the setup algorithm to get the public parameters and a master secret ϑ.Then ℂhsends the public parameters to adversary$\mathcal{A}_d$ and keeps ϑ with itself.

Phase 1: Adversary$\mathcal{A}_d$ executes the following queries which are interdependent.

1. Key Extractionquery:-Adversary$\mathcal{A}_d$ selects the unique identity as ID. The challenger ℂh runs key extraction algorithm and returns the SID to Adversary$\mathcal{A}_d$.
2. Warrant generation and Delegationquery:-The adversary $\mathcal{A}_d$ sends the request for signing warrant. The challenger ℂhreturns the warrant w and signing warrant Sw.
3. Warrant Verificationquery:-The adversary $\mathcal{A}_d$ verifies the signing warrant received from challenger ℂh.
4. Proxy Secret key Generationquery:-The adversary $\mathcal{A}_d$selects two identities IDa and IDb. The challenger ℂhexecutes Warrant generation and Delegation query to get Sw. Then it executes Proxy Secret key Generation query for identity IDb and returns PSK_{OP} to adversary $\mathcal{A}_d$.
5. Proxy Signcryptionquery:-The adversary $\mathcal{A}_d$ selects message m and the identities IDa , IDb and IDc . The challenger ℂh executes Key Extraction and Warrant generation and Delegation to get secret keys of Sa, Sb and the signing warrant Sw , then executes Proxy Secret key Generation to get PSK_{OP}. Finally the challenger ℂhruns Proxy Signcryption and sends the signcrypted ciphertext σ to $\mathcal{A}_d$.
6. Unsigncryptionquery:-The adversary $\mathcal{A}_d$ selects the signcrypted ciphertext σ and the identities IDa , IDb and IDc. The challenger ℂh runs Key Extraction algorithm to get the Sc, then executes Unsigncryption algorithm and sends result to $\mathcal{A}_d$.

Challenge: The adversary $\mathcal{A}_d$ wishes to be challenged on the two messages M_0 , M_1 and identities ID_i , ID_j. In the first stage $\mathcal{A}_d$cannot query for secret key of any of the identity. The challenger $ℂ_h$produces the random bit Ь $\in_R$ {0,1}for which the $\sigma = signcrypt(M_b, S_b, ID_C)$ and sends to $\mathcal{A}_d$.

Phase 2: The adversary $\mathcal{A}_d$ executes the queries like phase 1. Except Key Extraction query for identities ID_i ,ID_j and unsigncrypted text for σ.

Guess: The adversary $\mathcal{A}_d$produces he random bit Ь' $\in_R$ {0,1}. If Ь= Ь' the adversary $\mathcal{A}_d$ wins the game. We have following advantage of $\mathcal{A}_d$

$$\text{Adv}\ (\mathcal{A}_d) = \left|Pr[\text{Ь} = \text{Ь}'] - \tfrac{1}{2}\right|$$

Definition 2: The proposed scheme IDPSC-SG can achieve the existential unforgeability against adaptive chosen messages attack (EUF-CMA)iFadversary$\mathcal{A}_d$ with no polynomial time and having non-negligible advantage in the following game.

Initial: The challenger $ℂ_h$executes the setup algorithm to get the public parameters and a master secret ϑ.Then ℂhsends the public parameters to adversary$\mathcal{A}_d$. Then $\mathcal{A}_d$ performs polynomial limited number of queries like in IND-IDPSC-SG-CCA2.Finally, adversary$\mathcal{A}_d$ generates (σ, IDi, IDj), In phase 2 the private key for IDi was not asked and the adversary$\mathcal{A}_d$ wins the game if the output of Unsigncryption(σ, Si, IDj) is not ⊥.

5.2. Proposed IDPSC-SG Algorithm

5.2.1. Setup Algorithm

Input:- Security parameters λ

Output:-public system parameters

1. Let $\mathbb{G}$, $\mathbb{G}$T be a multiplicative cyclic group of prime order p
2. g is generator of $\mathbb{G}$
3. Identity of each participating entities is represented as IDi
4. Bilinear map Ψ:$\mathbb{G}$ X $\mathbb{G}$→$\mathbb{G}$T

5. $\mathscr{H}1:\{0,1\}^* \to \mathbb{G}$, $\mathscr{H}2:\{0,1\}^* \to \mathbb{Z}_{p^*}$, $\mathscr{H}3: \mathbb{G}_T \to \{0,1\}^{\ell}$,
6. $\mathscr{H}4:\{0,1\}^{\ell} X\mathbb{G}_T \to \mathbb{Z}_{p^*}$
7. Select $\vartheta \in_R \mathbb{Z}_p$, where ϑ is a master secret
8. Master Public key $M_{Pub} = \vartheta * g$
9. Select symmetric key algorithm (EK(), DK())
10. The PKG publish the public system parameters as {$\mathbb{G}$, $\mathbb{G}$T, Ψ,ℓ ,M_{Pub},$\mathscr{H}1$, $\mathscr{H}2$, $\mathscr{H}3$, $\mathscr{H}4$,EK(), DK()}, The$\vartheta$is kept secret, where ℓ is bit length of message.

Table 1. Symbols used in proposed scheme.

Symbol	Definition
$\mathbb{G}$, $\mathbb{G}_T$	multiplicative cyclic group of prime order p
p	Order of group / a very large prime number
g	Generator of group g
id_i	Identity of user i
S_a	The secret key of user A
H_1, H_2, H_3, H_4	One-way cryptographic hash function
Ψ	Admissible bilinear map
$\mathbb{Z}_p$	Set of elements {0, 1, ……., p-1}
$\vartheta \in_R \mathbb{Z}_p$	Element ϑrandomly selected from $\mathbb{Z}_p$
M_{Pub}	Master Public key
ℓ	Bit length of message
S_w	Signcrypting warrant
w	Message warrent
PSK_{OP}	proxy secret key
σ	signcrypted ciphertext
⊥	Error symbol

5.2.2. Key Extraction Algorithm

Input: - Identity of Participating entities ID_i

Output: - Public and secret keys for ID_i

1. The Public key of user A with identity ID_a is $P_a = \mathscr{H}_1$ (ID_a)
2. The Secret key of user A with identity ID_a is $S_a = \vartheta * P_a$

5.2.3. Warrant generation and Delegation Algorithm

Input: - public system parameters, S_o,w

Output: - Signcrypting warrant S_w

The original signer shall make a warrant w which contains the information about the type of delegation and time of delegation; it also defines the type of documents to be signcrypted by proxy signcryptor.

By using warrant w the original signer generatessigncrypting warrant S_w by using original signer's private key$\boldsymbol{S_o}$.

1. Select $\alpha \in_R \mathbb{Z}_{p^*}$
2. V=$\alpha * g$
3. $\delta = \mathscr{H}_2\,(w,$V)
4. $S_w = \alpha * M_{Pub} + \delta * S_o$

The original signer sends (S_w, V, w) to proxy signcryptor.

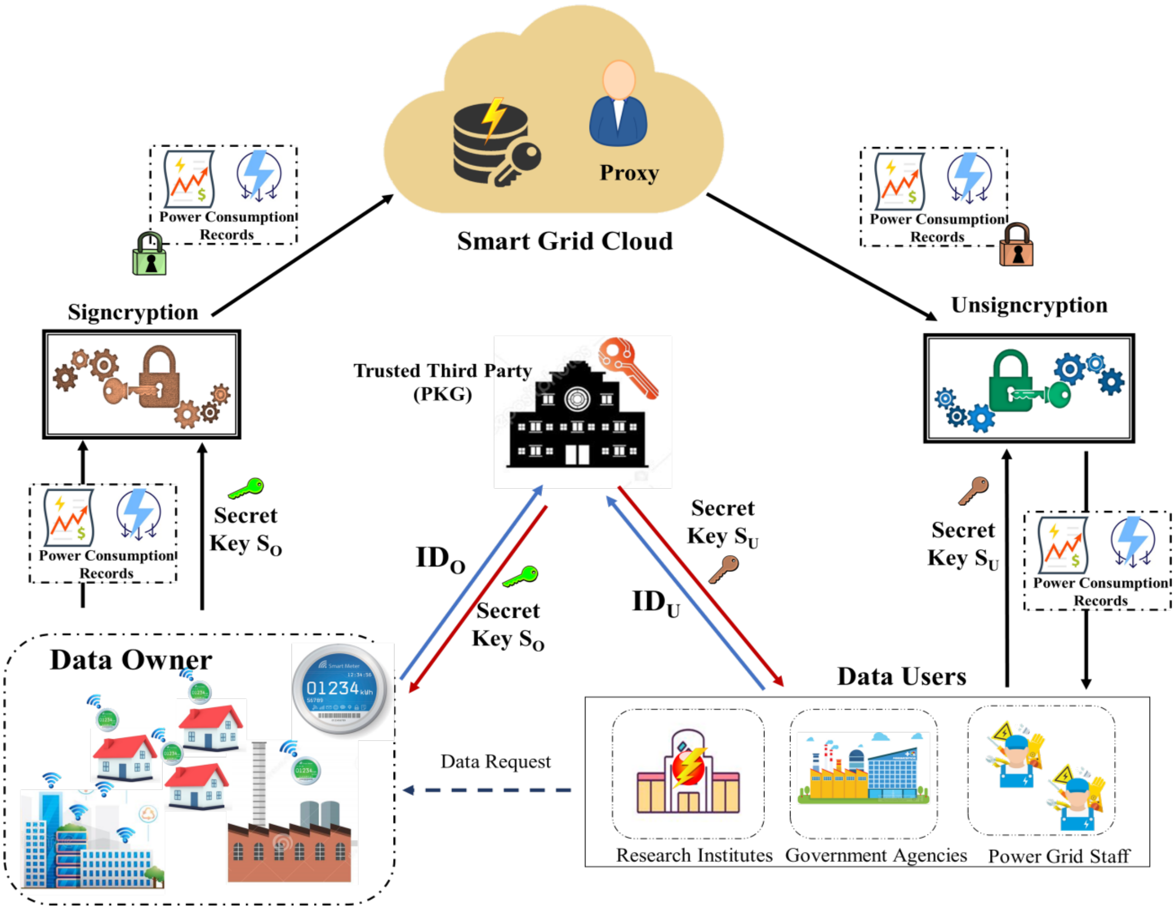


Fig. 2. The system model for the proposed Identity based Proxy Signcryption for Smart Grid (IDPSC-SG).

5.2.4. Warrant Verification Algorithm

Input: -(S_w, V, w)

Output: - Accept or reject the signing warrant

1. $\delta^{`} = \mathscr{H}_2\,(w,$V)
2. The proxy signer verifies the received delegation by computing

$$\Psi\ (g,\ S_w) = \Psi(M_{Pub}, \delta^{`} * S_o + V) \tag{1}$$

Verification of Eq(1)

$\Psi\ (g,\ S_w) = \Psi(M_{Pub}, \delta^{`} * S_o + V)$

$= \Psi(M_{Pub}, \delta^{`} * \vartheta * P_o + V)$

$= \Psi(\vartheta * g\ , \delta^{`} * \vartheta * P_o + V)$

$= \Psi(\vartheta * g\ , \delta^{`} * \vartheta * P_o + \alpha * g)$

$= \Psi(g\ , \delta^{`} * \vartheta * P_o + \vartheta * \alpha * g)$

$= \Psi(g\ , \delta^{`} * S_o + \alpha * M_{Pub})$

$= \Psi\ (g,\ S_w)$

5.2.5. Proxy Secret key Generation Algorithm

If warrant is verified in previous step, the proxy signcryptor can generate proxy secret key as follows.

$PSK_{OP} = \ \delta * S_p + S_w$

5.2.6. Proxy Signcryption Algorithm

Input: -Public system parameters, m, P_r,S_p, PSK_{OP},w

Output: - Signcrypted message σ

1. Select $\alpha^{`} \in_R \mathbb{Z}_{p^*}$
2. $P_r = \mathscr{H}_1\ (ID_r)$
3. $\acute{K}_1 = \Psi\ (g, M_{Pub})^{\alpha^{`}}$
4. $\acute{K}_2 = \mathscr{H}_3\ (\Psi(M_{Pub}, P_r)^{\alpha^{`}})$
5. $\sigma_1 = E_{\acute{K}_2}(m)$
6. $\sigma_2 = \mathscr{H}_4(\sigma_1, \acute{K}_1)$
7. $\sigma_3\ = \alpha^{`} M_{Pub} - (\sigma_2 * S_p + PSK_{OP})$
8. $\sigma = (\sigma_1, \sigma_2, \sigma_3, w)$

The proxy signcryptor uploads the signcrypted ciphertext σ on cloud.

5.2.6. UnsigncryptionAlgorithm

Input: -Public system parameters, S_r , σ

Output: - Original message m or ⊥

The receiver with identity ID_r will download the signcrypted ciphertext σ from cloud and perform the following operations to compute the original message m.

1. $P_o = \mathscr{H}_1\ (ID_o)$
2. $P_p = \mathscr{H}_1\ (ID_p)$
3. $\grave{\acute{K}}_1 = \Psi(g,\sigma_3)\ \Psi\big(M_{Pub}, P_p\big)^{(\delta+\sigma_2)}\Psi(M_{Pub}, \delta P_o + V)$
4. $\grave{\acute{K}}_2 = \mathscr{H}_3(\Psi(\sigma_3, P_r)\Psi\big(P_p, S_r\big)^{(\delta+\sigma_2)}\Psi(\delta P_o + V, S_r))$
5. The receiver with Identity ID_r will then decrypt the cipher text by using $\grave{\acute{K}}_2$ as follows
   m= $D_{\grave{\acute{K}}_2}(\sigma_1)$

The decrypted message m is accepted only if following condition holds

$\sigma_2 = \mathscr{H}_4(\sigma_1, \grave{\acute{K}}_1)$ otherwise it returns ⊥

6. Security Analysis

Theorem 1: In the proposed Identity based proxy signcryption scheme, any signcrypted message generated by Proxy signer P can be unsignrypted successfully by receiver R with a legitimate private key, i.e., the proposed scheme is consistent.

Proof: To verify the confidentiality and authenticity of the received signcrypted message, the receiver R computes $\grave{\acute{K}}_2$ by using its own private key S_r.

$\grave{\acute{K}}_2 = \mathscr{H}_3\Big(\Psi(\sigma_3, P_r)\Psi\big(P_p, S_r\big)^{(\delta+\sigma_2)}\Psi(\delta P_o + V, S_r)\Big)$

$= \mathscr{H}_3\big(\Psi(\sigma_3, P_r)\Psi\big(\sigma_2 S_p, P_r\big)\Psi(\delta S_p + \delta S_o + \alpha M_{Pub}, P_r)\big)$
$= \mathscr{H}_3\big(\Psi(\sigma_3, P_r)\Psi\big(\sigma_2 S_p, P_r\big)\Psi(PSK_{OP}, P_r)\big)$

$= \mathscr{H}_3\Big(\Psi(\alpha^{`} M_{Pub} - \sigma_2 S_p - PSK_{OP}, P_r)\Psi\big(\sigma_2 S_{p+}\, PSK_{OP}, P_r\big)\Big)$

$= \mathscr{H}_3\Big(\Psi(M_{Pub}, P_r)^{\alpha^{`}}\Big)$

$= \grave{\acute{K}}_2$

Theorem 2: The proposed scheme IDPSC-SG is secure against IND-IDPSC-SG-CCA2, if there exist an adversary$\mathcal{A}_d$ which has a non-negligible advantage that can (ε , t) breaks DBDH and asking q_{EK} key extraction queries, q_{PSK} proxy secret key generation queries, q_{SC} signcryption queries, q_{USC} unsigncryption queries and q_{Hi} queries to oracles Hi (i= 1, 2,3,4), then we can have following advantage of algorithm 𝔹 in DBDH problem.

$$\text{Adv}\ (\mathfrak{B})^{DBDH} \geq 2\left(\frac{\varepsilon - q_{USC}/2^{\lambda-1}}{q_{H1}^4}\right)$$

$$t \approx t + O(q_{PSK} + q_{SC} + q_{USC})t_{\varphi}$$

Where t_{φ} is time to execute one pairing operation.

Theorem 3: The proposed scheme IDPSC-SGis secure against EUF-IDPSC-SG-CMA, if no polynomial time adversary $\mathcal{A}_d$ can break CDH with non negligible advantage.

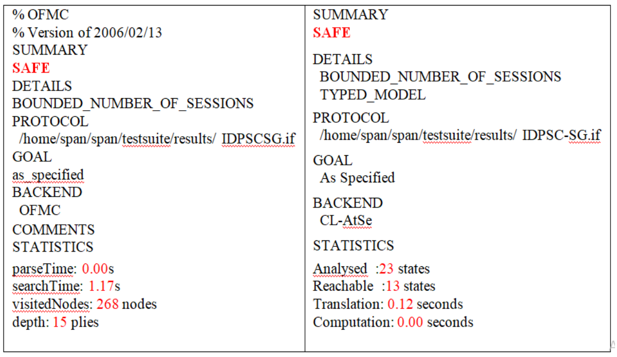
$$\epsilon\ \geq\ \frac{10(q_{SC}+1)(q_{SC}+q_{H3})q_{H1}}{(2^{\lambda}-1)}$$

$$t \leq 120686 * q_{H1} * q_{H3}\frac{t+O(q_{PSK}+q_{SC}+q_{USC}q_{H3}*)t_{\varphi}}{\Psi\left(1-\frac{1}{2\lambda}\right)}$$

6.1. Simulation study using AVISPA

In this section, the security analysis of the proposed IDPSC-SG scheme. We use the well-known AVISPA tool [30,31] to discuss the security proof and demonstrate that the proposed scheme is not susceptible to replay and man-in - the-middle attack. It should be noted that for any security protocol, AVISPA only handles replay and man-in - the-middle threats against an attacker.

The HLPSL code is written for the proposed scheme with the different roles like original signer, proxy signer and trusted third party. This code is then executed using SPAN and AVISPA with the backends OFMC and CL-AtSe. We can see that no attacks were discovered by OFMC. In other words, for a limited number of sessions as specified in the role of the environment, the stated security goals were achieved. The proposed protocol is also executed with CL-AtSe backend for bounded number of sessions. The output shows that the protocol is safe under CL-AtSe also. The software resources such as Oracle VM Virtual Box and Security protocol animator (SPAN) are used.The output of AVISPA is shown in Fig3.



```
% OFMC
% Version of 2006/02/13
SUMMARY
SAFE
DETAILS
BOUNDED_NUMBER_OF_SESSIONS
PROTOCOL
 /home/span/span/testsuite/results/ IDPSCSG.if
GOAL
as_specified
BACKEND
 OFMC
COMMENTS
STATISTICS
parseTime: 0.00s
searchTime: 1.17s
visitedNodes: 268 nodes
depth: 15 plies
```

```
SUMMARY
SAFE
DETAILS
 BOUNDED_NUMBER_OF_SESSIONS
 TYPED_MODEL
PROTOCOL
 /home/span/span/testsuite/results/ IDPSC-SG.if
GOAL
 As Specified
BACKEND
 CL-AtSe
STATISTICS
Analysed  :23 states
Reachable  :13 states
Translation: 0.12 seconds
Computation: 0.00 seconds
```

Fig. 3. AVISPA Output

6.2. Performance analysis

we have done the comparison of our proposed IDPSC-SG scheme with the eisting proxy signcryption schemes based on pairing, which include X.X.Li et al.[32], S S Duan et al.[33], X X Tian et al.[34], S.X. Chen et al.[35], Y. Ming et al.[36], H. Yu et al. [37],Caixue Zhou et al.[38], Yu H et al.[39]. The comparison outcomes are listed in Table 2. We define some notations as follows:

ℙ :- Pairing operation.

𝕄:- Scalar multiplication operation

𝔼:- exponentiation operation

The time required to perform the cryptographic operations [34] are 32.7 ms for pairing operation, 13.1 ms for multiplication operation and 2.24 ms for each exponentiation operation.

To assess the computing efficiency of the various systems, we employ a simple technique. For example the scheme proposed by X. X. Li [32] requires 12P, 8M and 7E operations. Therefore the total time required for this scheme is 512.88ms. In similar way the operation time required for each scheme is calculated and listed in Table 2.Hence it can be seen from Table 2, that the proposed approach outperforms the alternative schemes describe in [32-39]. The comparison of computational costs in terms of time in milliseconds (ms) for each phase of the IDPSC schemes is shown graphically in fig. 4.

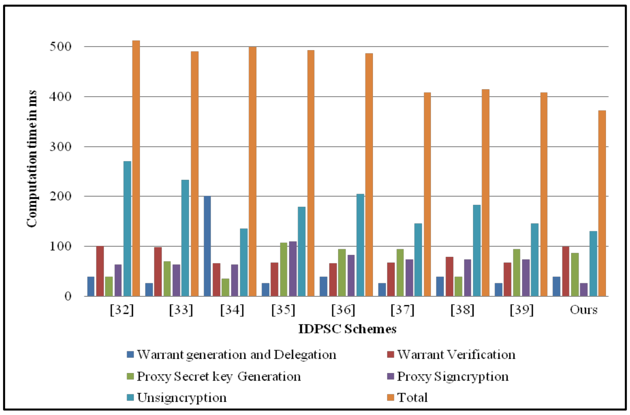


Fig. 4. Comparison of computation cost of alternative schemes with proposed IDPSC-SG Scheme.

Table 2. Comparison of various IDPSC Schemes

Scheme	Warrant generation and Delegation	Warrant Verification	Proxy Secret key Generation	Proxy Signcryption	Unsigncryption	Total	Time (milliseconds)
X. X. Li [32]	3 𝕄	3ℙ+𝔼	3 𝕄	ℙ+2 𝕄 +2𝔼	8ℙ+4𝔼	12 ℙ +8M+7 𝔼	512.88
S S Duan [33]	2𝕄	3ℙ	2ℙ+2𝔼	ℙ+2𝕄+2𝔼	7ℙ+2𝔼	13 ℙ +4 𝕄 +6 𝔼	490.94
X X Tian [34]	4ℙ+5𝕄+2 𝔼	2ℙ	1ℙ+1𝔼	ℙ+2𝕄+2𝔼	4ℙ+2𝔼	12 ℙ+7 𝕄+7 𝔼	499.78
S.X. Chen [35]	2𝕄	2ℙ+1𝔼	3𝕄 + 2ℙ + 1𝔼	3𝕄 + 2ℙ + 2𝔼	1𝕄 + 5ℙ + 1𝔼	11 ℙ+9 𝕄+7 𝔼	493.28
Y. Ming [36]	3𝕄	2ℙ	2𝕄 + 2ℙ + 1𝔼	1𝕄 + 2ℙ + 2𝔼	4𝔼 + 6ℙ	12 ℙ+6 𝕄+7 𝔼	486.68
H. Yu [37]	2𝕄	2ℙ+1𝔼	2𝕄 + 2ℙ + 1𝔼	3𝕄 + 1ℙ + 1𝔼	1𝕄 + 4ℙ + 1𝔼	9 ℙ+8 𝕄+4𝔼	408.06
Caixue Zhou [38]	3𝕄	2ℙ+𝕄	3𝕄	ℙ+3𝕄+𝔼	4ℙ+4𝕄	7 ℙ+14 𝕄+1𝔼	414.54
Yu H [39]	2𝕄	2ℙ+1𝔼	2𝕄 + 2ℙ + 1𝔼	1ℙ+1𝔼+3𝕄	4ℙ+1𝔼+1 𝕄	9 ℙ+8 𝕄+4𝔼	408.06
Ours	3𝕄	1𝕄+2ℙ	2𝕄 + 2ℙ	2𝕄	2𝕄 + 4ℙ	8 ℙ+10 𝕄	392.6

7. Conclusion

Energy service providers (ESP) make appropriate configuration of smart grid systems to communicate the power consumption and its related information in the form of statements to consumers at periodic intervals. It is quite possible to identify the type of electrical appliances that the user has, its location, and operating patterns, by studying power consumption statements. The security and safety of such data while acquisition and communication is at risk. So it's important to secure ESP's right of entry to consumers' statements. In this work, we have identified the need for securely sharing the usage data of electricity users with the help of a cloud-based environment. This article illustrates an identity based proxy signcryption technique that is both efficient and secure. The proposed scheme is exposed to be CCA2 sheltered, assuming that the decision BDH assumption is hard. It is also demonstrated that the projected IBSC system is unforgeable under the CDH problem's consideration. The widely used AVISPA tool is used to do a security evaluation, which includes formal security verification, and the results reveal that our proposed system is significantly immune to adversary attacks. In addition to these advantages, the proposed method is significantly more efficient in terms of computing cost when compared to the relevant existing techniques. As a result, in the smart grid environment, the suggested provably secure IDPSC-SG technique is more appropriate.

References

1. El Mrabet, Z., Kaabouch, N., El Ghazi, H. and El Ghazi, H., 2018. Cyber-security in smart grid: Survey and challenges. *Computers & Electrical Engineering*, *67*, pp.469-482.
2. Mohammadpourfard, M., Weng, Y., Pechenizkiy, M., Tajdinian, M. and Mohammadi-Ivatloo, B., 2020. Ensuring cybersecurity of smart grid against data integrity attacks under concept drift. *International Journal of Electrical Power & Energy Systems*, *119*, p.105947.
3. Gunduz, M.Z. and Das, R., 2020. Cyber-security on smart grid: Threats and potential solutions. *Computer networks*, *169*, p.107094.
4. Patil, R.Y. and Ranjanikar, M.A., 2022. A New Network Forensic Investigation Process Model. In *Mobile Computing and Sustainable Informatics* (pp. 139-146). Springer, Singapore.
5. Nguyen, T.N., Liu, B.H., Nguyen, N.P. and Chou, J.T., 2020, June. Cyber security of smart grid: attacks and defenses. In *ICC 2020-2020 IEEE International Conference on Communications (ICC)* (pp. 1-6). IEEE.
6. Ouaissa, M. and Ouaissa, M., 2020, September. Cyber Security Issues for IoT based Smart Grid Infrastructure. In *IOP Conference Series: Materials Science and Engineering* (Vol. 937, No. 1, p. 012001). IOP Publishing.
7. Bhole, D., Mote, A. and Patil, R., 2016. A new security protocol using hybrid cryptography algorithms. *International Journal of Computer Sciences and Engineering*, *4*(2), pp.18-22.
8. Ferrag, M.A., Babaghayou, M. and Yazici, M.A., 2020. Cyber security for fog-based smart grid SCADA systems: Solutions and challenges. *Journal of Information Security and Applications*, *52*, p.102500.
9. Leszczyna, R., 2018. Standards on cyber security assessment of smart grid. *International Journal of Critical Infrastructure Protection*, *22*, pp.70-89.
10. He, D., Chan, S. and Guizani, M., 2017. Cyber security analysis and protection of wireless sensor networks for smart grid monitoring. *IEEE Wireless Communications*, *24*(6), pp.98-103.
11. Patil, R.Y. and Ragha, L., 2011, December. A rate limiting mechanism for defending against flooding based distributed denial of service attack. In *2011 World Congress on Information and Communication Technologies* (pp. 182-186). IEEE.
12. Patil, N. and Patil, R., 2018, January. Achieving Flatness: with Video Captcha, Location Tracking, Selecting the Honeywords. In *2018 International Conference on Smart City and Emerging Technology (ICSCET)* (pp. 1-6). IEEE.
13. Pour, M.M., Anzalchi, A. and Sarwat, A., 2017, March. A review on cyber security issues and mitigation methods in smart grid systems. In *SoutheastCon 2017* (pp. 1-4). IEEE.
14. Kimani, K., Oduol, V. and Langat, K., 2019. Cyber security challenges for IoT-based smart grid networks. *International Journal of Critical Infrastructure Protection*, *25*, pp.36-49.
15. Khan, F.A., Asif, M., Ahmad, A., Alharbi, M. and Aljuaid, H., 2020. Blockchain technology, improvement suggestions, security challenges on smart grid and its application in healthcare for sustainable development. *Sustainable Cities and Society*, *55*, p.102018.
16. Otuoze, A.O., Mustafa, M.W. and Larik, R.M., 2018. Smart grids security challenges: Classification by sources of threats. *Journal of Electrical Systems and Information Technology*, *5*(3), pp.468-483.
17. Sha, K., Wei, W., Yang, T.A., Wang, Z. and Shi, W., 2018. On security challenges and open issues in Internet of Things. *Future Generation Computer Systems*, *83*, pp.326-337.
18. So, H.K.H., Kwok, S.H., Lam, E.Y. and Lui, K.S., 2010, October. Zero-configuration identity-based signcryption scheme for smart grid. In *2010 first IEEE international conference on smart grid communications* (pp. 321-326). IEEE.
19. Chen, J. and Zhang, Y.Y., 2014. The scheme of identity-based aggregation signcryption in smart grid. In *Advanced Materials Research* (Vol. 960, pp. 832-835). Trans Tech Publications Ltd.
20. Alishahi, S., Seyyedi, S.M., Yaghmaee, M.H. and Alishahi, M., 2004. Preserving integrity and privacy of data in smart grid communications. In *Proc. CIRED Workshop-Rome* (pp. 11-12).
21. Hu, C., Cheng, X., Tian, Z., Yu, J., Akkaya, K. and Sun, L., 2015, October. An attribute-based signcryption scheme to secure attribute-defined multicast communications. In *International Conference on Security and Privacy in Communication Systems* (pp. 418-437). Springer, Cham.
22. Chen, J. and Ren, X., 2016, October. A privacy protection scheme based on certificateless aggregate signcryption and masking random number in smart grid. In *The 4th International Conference on Mechanical Materials and Manufacturing Engineering (IC3ME2016), Shenzhen, China* (pp. 10-13).
23. Hu, C., Yu, J., Cheng, X., Tian, Z. and Sun, L., 2018, February. CP_ABSC: An attribute-based signcryption scheme to secure multicast communications in smart grids. In *Mathematical foundations of computer science* (Vol. 1, No. 1).
24. Sedaghat, S.M., Ameri, M.H., Delavar, M., Mohajeri, J. and Aref, M.R., 2018. An efficient and secure attribute-based signcryp-tion scheme for smart grid applications. *Scientia Iranica, Cryptol. ePrint Arch., Tech. Rep*, *263*, p.2018.
25. Jin, C., Chen, G., Yu, C., Shan, J., Zhao, J. and Jin, Y., 2018. An efficient heterogeneous signcryption for smart grid. *PloS one*, *13*(12), p.e0208311.
26. Wan, C., Phoha, V.V., Pei, B. and Chen, C., 2017. Securing dynamic microgrid partition in the smart grid. *International Journal of Distributed Sensor Networks*, *13*(5), p.1550147717711136.
27. Baoyi, W., Li, L., Shaomin, Z. and Jing, H., 2019. Research on privacy protection scheme based on certificateless aggregation signcryption in AMI. *Internet of Things (IoT) and Engineering Applications*, *4*(1), pp.7-12.
28. K.G. Paterson, ID-based signatures from pairings on elliptic curves, IEEE Commun. Lett. 38 (18) (2002) 1025–1026. 19.
29. Yu Y, Yang B, Sun Y, Zhu S. Identity based signcryption scheme without random oracles. Comput Stand Interfaces 2009;31(1):56–62.
30. Yogesh, P.R., 2020. Formal verification of secure evidence collection protocol using BAN logic and AVISPA. *Procedia*

Computer Science, *167*, pp.1334-1344.

31. Patil, R.Y. and Devane, S.R., 2019. Network Forensic Investigation Protocol to Identify True Origin of Cyber Crime. *Journal of King Saud University-Computer and Information Sciences*.
32. Li, X. and Chen, K., 2004, September. Identity based proxy-signcryption scheme from pairings. In *IEEE International Conference onServices Computing, 2004.(SCC 2004). Proceedings. 2004* (pp. 494-497). IEEE.
33. Duan, S., Cao, Z. and Zhou, Y., 2005, December. Secure delegation-by-warrant ID-based proxy signcryption scheme. In *International Conference on Computational and Information Science* (pp. 445-450). Springer, Berlin, Heidelberg.
34. Tian, X.X., Xu, J.P., Li, H.J., Peng, Y. and Zhang, A.Q., 2009, November. Secure ID-based proxy signcryption scheme with designated proxy signcrypter. In *2009 International Conference on Multimedia Information Networking and Security* (Vol. 1, pp. 351-355). IEEE.
35. Chen, S.X., Zhou, S.X., Yao, X.F. and Li, F.W., 2011. Efficient identity-based proxy signcryption scheme. *Jisuanji Yingyong Yanjiu*, *28*(7), pp.2694-2696.
36. Yang, M.I.N.G., Jie, F.E.N.G. and Qijun, H.U., 2014. Secure identity-based proxy signcryption scheme in standard model. *Journal of Computer Applications*, p.10.
37. Yu, H., Wang, Z., Li, J. and Gao, X., 2018. Identity-based proxy signcryption protocol with universal composability. *Security and Communication Networks*, *2018*.
38. Zhou, C., Zhang, Y. and Wang, L., 2018. A Provable Secure Identity-based Generalized Proxy Signcryption Scheme. *Int. J. Netw. Secur.*, *20*(6), pp.1183-1193.
39. Yu, H., Wang, Z., Li, J. and Gao, X., 2018. Identity-based proxy signcryption protocol with universal composability. *Security and Communication Networks*, *2018*.