A Privacy Enhanced Authentication Scheme for Securing Smart Grid Infrastructure

Shehzad Ashraf Chaudhry, Jamel Nebhan, Khalid Yahya, and Fadi Al-Turjman

***Abstract*—The rapid advancements in smart grid (SG) technology extend a large number of applications including vehicle charging, smart buildings, and smart cities through the efficient use of advanced communication architecture. However, the underlying public channel leads these services to be vulnerable to many threats. Recently, some security schemes were proposed to counter these threats. However, the insecurities of some of these schemes against key compromise impersonation (KCI) and related attacks or compromise on efficiency calls for a secure and efficient authentication scheme for SG infrastructure. A new scheme to secure SG communication is presented in this article to provide a direct device-to-device authentication among smart meter and neighborhood area network gateway. Designed specifically to resists KCI and related attacks, the proposed scheme is more secure and completes the authentication procedure by using the least communication cost as compared with related schemes, which is evident through security and efficiency comparisons.**

***Index Terms*—Key compromise impersonation attack (KCIA), smart city security, smart home environment, smart grid (SG) authentication.**

I. Introduction

THE smart grid (SG) technology provides an enhancement to the conventional electrical grid with the information and communication technologies (ICT) enabled bilateral communication among the utility center, sensors, and consumers. The conventional electrical grids were prone to many accidental blackouts and failures. For example, nearly 73 000 customers were without power in Manhattan, New York, on 13 July 2019, followed by a similar kind of massive breakdown on the same date in 1977. In the wake of such adverse upsets, SG systems have been evolved. The SG aims to incorporate the diversified nature of energy resources, reduce the carbon footprint, and load balancing of power production and consumption, detection, and dealing with power contingencies, and achieving a sustainable power dispensing system. The ICT-led advancements have facilitated the SG systems to become an integral part of the Internet of Things community. After the enhanced ICT-based automation and distributed intelligence, the operations in SG systems have become more efficient, secure, stable, and reliable, and has led to many advanced applications such as renewable energy integration, vehicle-to-grid services, automatic voltage regulation, demand response (DR) management, etc. This next-generation power system has evolved from centralized administration to decentralized power generation and distribution with the use of integrated communication, computing, and advanced sensing technology. As a result, this decentralized management of SG through advanced technology provides better control over the real-time power demands that are beneficial for consumers as well as power generation and distribution centers. Even though there are many advantages of SGs, their strong reliance on networking and communication systems makes them inherently susceptible to several threats such as forgery attacks, replay attacks, impersonation, and man-in-the-middle attacks. For instance, the ICT-enabled smart meters (SMs) as being used for power management of SG-based demand and supply, raise many security concerns [1]. For addressing such concerns, there must be a robust communication architecture enabling privacy as well as secure interactions [2], [3]. Thus, the SG-specific authenticated key agreement protocols have become critical for ensuring security in smart metering infrastructure with demonstrated security properties including anonymity, mutual authentication, forward key secrecy, session key security to dispense smooth power-related services in the SG system.

A. Motivations

The real advantage of the SG can be experienced in case the security and privacy of the communicating entities are ensured. Most of the literature depicts that many of the current authentication schemes based on elliptic curve cryptography (ECC) operations face the challenges of not providing sufficient anonymity to SM,or cannot resist key compromise impersonation (KCI) and related attacks. Moreover, some of these schemes bear high computational and communication overheads. Therein, the

Manuscript received May 30, 2021; revised August 7, 2021; accepted October 6, 2021. Date of publication October 14, 2021; date of current version April 13, 2022. Paper no. TII-21-2267. *(Corresponding author: Shehzad Ashraf Chaudhry.)*

Shehzad Ashraf Chaudhry is with the Department of Computer Engineering, Istanbul Gelisim University, Istanbul 34310, Turkey (e-mail: ashraf.shehzad.ch@gmail.com).

Jamel Nebhan is with Prince Sattem bin Abdulaziz University, Al Kharj 11942, Saudi Arabia (e-mail: j.nebhen@psau.edu.sa).

Khalid Yahya is with the Department of Mechatronics Engineering, Istanbul Gelisim University, Istanbul 41380, Turkey (e-mail: koyahya@gelisim.edu.tr).

Fadi Al-Turjman is with the Artificial Intelligence Department, Research Center for AI and IoT, Near East University, Marsin 10, Turkey (e-mail: fadi.alturjman@neu.edu.tr).

Color versions of one or more figures in this article are available at https://doi.org/10.1109/TII.2021.3119685.

Digital Object Identifier 10.1109/TII.2021.3119685

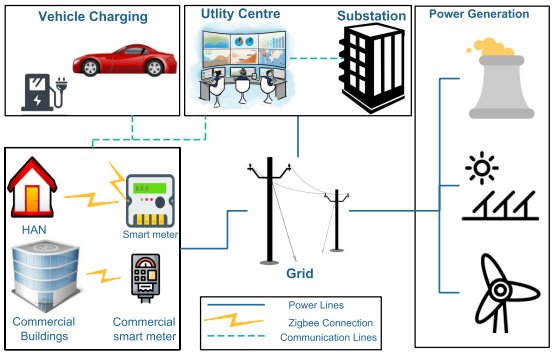

Fig. 1. SG Infrastructure.

SG environment needs more efficient and secure authentication protocols for practical implementations.

B. Contributions

The salient points of our contribution to this article are given as follows.

1) We propose an efficient authentication protocol that not only ensures mutual authentication but also enables to establish trust between the participants, i.e., SM and NAN gateway.
2) We performed rigorous testing to verify the security properties of the contributed model by using formal and informal analysis.
3) The obtained results depict the contributed protocol might resist various known attacks and could be well implemented in SG systems because of not only secure features but it is also efficient and saves energy due to less computational and communicative overheads.

C. System Model

Fig. 1 depicts the employed system model, where the SMs transport the related metering data to the utility center through an NAN gateway employing both secure as well as an insecure communication network. The SM utilizes an insecure channel to communicate the message toward the NAN gateway, which in turn acting as a middle-ware that forwards the message to the utility center using a secure channel. The prime focus of is this study is to establish a reliable communication link between the SM and NAN gateway by utilizing the secure authentication algorithms on an insecure open channel. A trusted third party, certificate authority (CA) registers the legal NAN gateways and all SMs and then publishes the respective cryptographic parameters for verification. The involved steps in registering the entities and then establishing the mutual key agreement between them are portrayed in Section III.

D. Attack Model

The common extended Canetti–Krawczyk (CK) (eCK) model [4] with a strong adversary is adopted. The eCk model also encompasses the key compromise attack (KCI), in addition to common capabilities under CK and DY models as shown in the following.

1) An adversary $\mathcal{U}_{\text{av}}$ may intercept the communication on the public channel between NAN gateway and SMs.
2) $\mathcal{U}_{\text{av}}$ may replay, hold, or alter the relayed contents among the legal participants. Moreover, the former may also insert newly constructed messages into the system to impersonate the legal entities.
3) $\mathcal{U}_{\text{av}}$ may attempt to forge the messages by impersonating on the behalf of a legal NAN gateway or SM.
4) The channel between the NAN gateway and utility center is assumed to be secure. However, $\mathcal{U}_{\text{av}}$ may attempt to intrude into the insecure communication between SMs and NAN gateway.
5) The timing clocks of the communicating entities, such as NAN gateway and SMs are duly synchronized.
6) $\mathcal{U}_{\text{av}}$ is allowed us to have access to the private key of one of the participants for impersonating it on behalf of the other devices. Precisely, the attacker is allowed us to launch a KCI attack as per the eCK model [5].

TABLE I
NOTATION GUIDE

Symbols	Representations
SM_i, CA	Smart Meter, Certificate Authority
NAN_j	Neighbourhood area network gateway
I_{sm}, I_{nan}	identities of SM, NAN
T_{sm}, T_{nan}	Timestamps recorded at SM, NAN
d_{sm}, d_{nan}	Private keys of SM, NAN
Q_{sm}, Q_{nan}	Public keys of SM, NAN
$H_1(.)$, $H_2(.)$	Two Hash functions

E. Article Organization

The rest of this article is organized as follows. Section II briefly explains the related work and the weaknesses of the existing works. Table I provides the notation guide. We present the proposed scheme in Section III. The Sections IV and V brief the security analysis of the proposed scheme and its comparisons with the existing schemes using efficiency and security as the metrics. Finally, Section VI concludes this article.

II. RELATED WORK

To address the privacy and security concerns of SG infrastructure, many authentication protocols have been demonstrated in a few years. For instance, to maintain and balance the power demands in SGs, Gope and Sikdar [6] designed a spatial data aggregation protocol by utilizing low-cost hash and XOR operations. Afterward, Mood and Nikooghadam [7] presented a Chebyshev chaotic-maps-based authentication protocol to secure the SGs. Similarly, Odelu *et al.* [8] demonstrated an efficient authentication protocol for SGs. Nevertheless, Wu *et al.* [9] discovered that the protocol [8] does not provide privacy to the user, and also it bears high computational cost due to costly pairing operations. Later, another secure authentication protocol in advanced metering infrastructure by Mustapa *et al.* [10] was designed with the use of ring oscillator physical unclonable functions. Abdallah and Shen [11] presented a lightweight as well as anonymous

data-aggregation protocol for SGs. In the same context, Jo *et al.* [12] suggested two anonymous and lightweight authentication protocols to tackle physical device stolen attacks in SGs. Recently, Kumar *et al.* [13] presented a lightweight authentication protocol by employing hybrid cryptography, for ensuring the mutual authenticity, anonymity, integrity, and secure establishment of the session key. Likewise, Mood and Nikooghadam [14] designed another privacy-preserving ECC-based key agreement protocol Later, Wu *et al.*[9] claimed that the scheme [14] does not preserve the privacy of the user. Thereafter, Mohammadali *et al.* [15] presented an identity-based authentication scheme employing ECC. Later, Mahmood *et al.* [16] put forward an authentication protocol with ECC-based operations to secure the message interactions between consumers and utility centers. Nevertheless, Mood and Nikooghadam claimed that the protocol [16] does not support forward secrecy and is also prone to many attacks under the CK attack model. Chaudhry *et al.* also proposed two ECC-based authentication schemes [5], [17]. Likewise, Kumar *et al.* [18] proposed a DR authentication scheme, and Mahmood *et al.* proposed two pairings and/or ECC-based schemes for the SG [19], [20]. However, it was proved in [21] that the scheme of Kumar *et al.* [18] is prey to incorrect authentication procedure, and in [22], it was argued that Mahmood *et al.* [20] are insecure against various attacks. The scheme proposed in [17] does not provide a direct device-to-device authentication.

Recently, Garg *et al.* [23] presented an authentication scheme for SG environment and claimed the security of their scheme. However, the scheme of Garg *et al.* has weaknesses against key compromise impersonation attacks (KCIA) and it does not provide SM anonymity and forward secrecy, as proved in the following.

1) In Garg *et al.*'s scheme the SM sends $\{I_{\text{sm}}, T_{\text{sm}}, r_{\text{sm}}, R_{\text{sm}}\}$ tuple in the request message. I_{sm} in the request message is the original smart user identity. The transmission of the original I_{sm} in the request message nullifies Garg *et al.*'s claim to provide SM anonymity.

2) In Garg *et al.*'s scheme if the secret key d_{nan} of NAN_j is compromised, then using the public parameters (public keys of the participants) and parameters sent over public channel, i.e., $\{I_{\text{sm}}, T_{\text{sm}}, r_{\text{sm}}, R_{\text{sm}}\}$ and $\{T_{\text{nan}}, r_{\text{nan}}, R_{\text{nan}}, \text{Auth}_{\text{nan}}\}$, the attacker can easily compute session key of any session by computing $d = H_1(R_{\text{sm}}, R_{\text{nan}}, Q_{\text{sm}}, Q_{\text{nan}}, T_{\text{sm}}, T_{\text{nan}})$, $e = H_1(R_{\text{nan}}, R_{\text{sm}}, Q_{\text{sm}}, Q_{\text{nan}}, T_{\text{sm}}, T_{\text{nan}})$, $s_{\text{nan}} = r_{\text{nan}} + ed_{\text{nan}} \mod q$ and $\phi_{\text{nan}} = s_{\text{nan}}(R_{\text{sm}} + dQ_{\text{sm}})$. The adversary can then compute the session key $\text{SK} = \text{kdf}(\phi_{\text{sm}}||T_{\text{sm}}||T_{\text{nan}})$ using these parameters. Hence, Garg *et al.*'s scheme has no provision of forward secrecy.

3) Using a KCI attack, an active attacker with knowledge of the private key of an entity (either SM or NAN) can impersonate him, as any other entity of the system. Let $\mathcal{A}$ be an attacker in Garg *et al.*'s protocol with access to the private key d_{nan} of NAN_j and $\mathcal{A}$ wants to impersonate on behalf of the SM with identity I_{sm}. $\mathcal{A}$ initiates the KCI and the following steps are executed between NAN_j and $\mathcal{A}$.

1) $\mathcal{A}$ selects $r_a \in Z_p^*$ randomly and current timestamp T_a. $\mathcal{A}$ now computes $R_a = r_a P$ and sends request message consisting of tuple $\{I_{\text{sm}}, T_a, r_a, R_a\}$ to NAN_j gateway.
2) On receiving request, NAN_j gateway validates freshness of T_a and belonging of R_a in finite field G. As both are valid because, T_a is freshly generated and R_a is also correctly computed using ra. Therefore, NAN_j selects $r_{\text{nan}} \in Z_p^*$, T_{nan} and computes: $R_{\text{nan}} = r_{\text{nan}}P$, $d = H_1(R_a, R_{\text{nan}}, Q_a, Q_{\text{nan}}, T_a, T_{\text{nan}})$, $e = H_1(R_{\text{nan}}, R_a, Q_a, Q_{\text{nan}}, T_a, T_{\text{nan}})s_{\text{nan}} = r_{\text{nan}} + ed_{\text{nan}} \mod q$, $\phi_{\text{nan}} = s_{\text{nan}}(R_a + dQ_{\text{sm}})$, $\text{Auth}_{\text{nan}} = H_2(\phi_{\text{nan}}||T_a||d_{\text{nan}}R_{\text{nan}})$. Now NAN_j sends $\{T_{\text{nan}}, r_{\text{nan}}, R_{\text{nan}}, \text{Auth}_{\text{nan}}\}$ to SM_i.
3) $\mathcal{A}$ intercepts the message and computes: $d = H_1(R_a, R_{\text{nan}}, Q_a, Q_{\text{nan}}, T_a, T_{\text{nan}})$, $e = H_1(R_{\text{nan}}, R_a, Q_a, Q_{\text{nan}}, T_a, T_{\text{nan}})$, $s_a = r_{\text{nan}} + ed_{\text{nan}} \mod q$, $\phi_a = s_{\text{nan}}(R_a + dQ_{\text{sm}})$, $\text{Auth}_a = H_2(\phi_a||T_{\text{nan}}||d_aR_a)$, $\text{SK} = \text{kdf}(\phi_a||T_a||T_{\text{nan}})$. Finally, $\mathcal{A}$ sends Auth_a to NAN_j.
4) NAN_j on receiving the response, checks

$$\text{Auth}_a \stackrel{?}{=} H_2(\phi_a||T_{\text{nan}}||d_{\text{sm}}R_a). \tag{1}$$

If (1) holds, NAN_j computes session key using (kdf) the same key derivation function as

$$\text{SK} = \text{kdf}(\phi_{\text{sm}}||T_{\text{sm}}||T_{\text{nan}}). \tag{2}$$

In (1), the attacker with the private key of NAN_j got itself falsely authenticated on behalf of SM_i with identity I_{sm} and in (2), the same has shared session key SK with the counterpart NAN_j. Hence, Garg *et al.*'s scheme is vulnerable to KCI attack.

III. Proposed Scheme

A brief explanation of the different phases of the proposed scheme is solicited in this section. The proposed scheme is designed carefully to resist KCIA and related attacks. The following sections explain the proposed procedures.

A. System Initialization Phase

To complete the initialization, the CA selects an elliptic curve $E_p(a, b)$, a public point $P \in E_p(a, b)$ and two oneway hash functions $H_1(.)$, $H_2(.)$ and announces all the system parameters publicly.

B. Registration Phase

All SMs and NANs register with the system for future communications. For completion of this phase, an SM chooses and sends its identity I_{sm} to CA and CA after verifying the uniqueness of the identity selects a private key d_{sm} and computes a public key $Q_{\text{sm}} = d_{\text{sm}}P$ and installs both the keys on SM through a secure channel. Similarly, this step is repeated for all SMs and NANs.

C. Authentication Phase

The authentication phase in Garg *et al.*'s scheme is initiated by an SM_i and following steps as illustrated in Fig. 2 are performed between SM_i and NAN_j gateway to complete this phase.

PA 1: SM_i selects a random number $r_{\text{sm}} \in Z_p^*$ and current timestamp T_{sm}. SM_i using the its own private key d_{sm} and public key Q_{nan} of the NAN_j computes: $R_{\text{sm}} = r_{\text{sm}}P$ and $K_{\text{sm}} = r_{\text{sm}}Q_{\text{nan}} =$

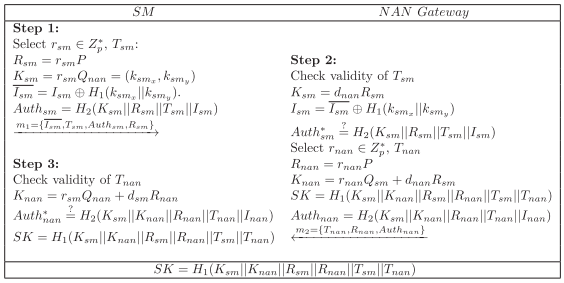

Fig. 2. Proposed procedure.

$(k_{\text{sm}_x}, k_{\text{sm}_y})$. Now SM_i computes dynamic identity $\overline{I_{\text{sm}}} = I_{\text{sm}} \oplus H_1(k_{\text{sm}_x}||k_{\text{sm}_y})$ and the authenticator $\text{Auth}_{\text{sm}} = H_2(K_{\text{sm}}||R_{\text{sm}}||T_{\text{sm}}||I_{\text{sm}})$. The SM_i now sends request message consisting of tuple $m_1 = \{\overline{I_{\text{sm}}}, T_{\text{sm}}, \text{Auth}_{\text{sm}}, R_{\text{sm}}\}$ to NAN_j gateway.

PA 2: On receiving request, NAN_j gateway validates freshness of T_{sm} and if the delay between T_{sm} and current timestamp at NAN is within the tolerable delay, the NAN_j using its private key d_{nan} computes $K_{\text{sm}} = d_{\text{nan}}R_{\text{sm}}$ and extract SM_is identity $I_{\text{sm}} = \overline{I_{\text{sm}}} \oplus H_1(k_{\text{sm}_x}||k_{\text{sm}_y})$. NAN_j then validates the equality $\text{Auth}^*_{\text{sm}} \stackrel{?}{=} H_2(K_{\text{sm}}||R_{\text{sm}}||T_{\text{sm}}||I_{\text{sm}})$. On successful verification, NAN_j selects a random number $r_{\text{nan}} \in Z_p^*$ and current time stamp T_{nan}. The NAN_j further computes $R_{\text{nan}} = r_{\text{nan}}P$, $K_{\text{nan}} = r_{\text{nan}}Q_{\text{sm}} + d_{\text{nan}}R_{\text{sm}}$, and session key $\text{SK} = H_1(K_{\text{sm}}||K_{\text{nan}}||R_{\text{sm}}||R_{\text{nan}}||T_{\text{sm}}||T_{\text{nan}})$. The NAN_j further computes the authenticator $\text{Auth}_{\text{nan}} = H_2(K_{\text{sm}}||K_{\text{nan}}||R_{\text{nan}}||T_{\text{nan}}||I_{\text{nan}})$ and sends $m_2 = \{T_{\text{nan}}, R_{\text{nan}}, \text{Auth}_{\text{nan}}\}$ to SM_i.

PA 3: SM_i on receiving the reply, validates freshness of T_{nan} and if the delay between T_{nan} and current timestamp at NAN is within the tolerable delay, th, computes $K_{\text{nan}} = r_{\text{sm}}Q_{\text{nan}} + d_{\text{sm}}R_{\text{nan}}$. Now SM_i checks the equality $\text{Auth}^*_{\text{nan}} \stackrel{?}{=} H_2(K_{\text{sm}}||K_{\text{nan}}||R_{\text{nan}}||T_{\text{nan}}||I_{\text{nan}})$, if it succeeds, the SM SM_i further computes the session key $\text{SK} = H_1(K_{\text{sm}}||K_{\text{nan}}||R_{\text{sm}}||R_{\text{nan}}||T_{\text{sm}}||T_{\text{nan}})$.

IV. Security Analysis

In this section, the formal security analysis along with a discussion on attack resilience of the proposed scheme is carried out.

A. Formal Security Analysis

For formal security analysis, we implement the commonly used real-or-random (ROR) model adopted from [24]. Under the ROR model, an adversary $\mathcal{U}_{\text{av}}$ connects with P^a, the ath instance of an executing participants (e.g., in our secure and lightweight authentication protocol for SG (SAP), it can be a legal SM, an NAN_s, or CA. Thus, these participants are $P^{a_1}_{\text{SM}}$, $P^{a_2}_{\text{NAN}_s}$, and $P^{a_3}_{\text{CA}}$ as the a_1^{th}, a_2^{th}, and a_3^{th} of SM, NAN_s, and CA, respectively. Furthermore, the ROR model assumes following different queries to resemble an attack.

1) *Send(P^a, M):* Modeled as an active attack, where $\mathcal{U}_{\text{av}}$ can dispatch a message M to an instance P^a, and also P_a replies accordingly.
2) *Reveal(P^a):* Execution of this query allows us to reveal current session key SK between P^a and its partner to $\mathcal{U}_{\text{av}}$.
3) *Test* (P^a)*:* A requests P_a for the session key SK and P_a replies probabilistically an outcome of a flipped unbiased coin d.
4) *Execute($P^{a_1}_{\text{SM}}$, $P^{a_2}_{\text{NAN}_s}$):* It enables $\mathcal{U}_{\text{av}}$ to eavesdrop the messages communicated among SM and NAN_s.

In Theorem 1, the SK security of SAP under the ROR model is proved using above queries.

Theorem 1. Suppose a polynomial time $\mathcal{U}_{\text{av}}$ Execute in time t against the presented protocol (SAP). If q^r_{send}, q^r_h, x and H represents the number of send queries, the number of h-queries, the range-space of $h(.)$. $\mathcal{U}_{\text{av}}$s advantage in explode SAP's semantic security to accomplish the SK between SM and NAN_s can approximate as

$$\text{Advs}^{\mathcal{U}_{\text{av}}}_{\text{SAP}}(t) \leq \frac{q^{r^2}_h}{H}. \tag{3}$$

Proof. In this article, proof is used in a similar manner that illustrated in [25]. We describe the four games mentioned below, say GM_k, $k \epsilon [0, 3]$. If W_k represents an event, therefore, $\mathcal{U}_{\text{av}}$ can imagine the random bit b in GM_k accurately, $\mathcal{U}_{\text{av}}$s advantage in winning this game will be denoted and defined by $\text{Advs}^{\mathcal{U}_{\text{av}},\text{GM}_k}_{\text{SAP}} = \Pr[W_k]$, where $\Pr[W_k]$ is an event W_ks probability. GM_0 (G_0): The real attack performed by $\mathcal{U}_{\text{av}}$ against SAP in the ROR model corresponds to GM_0. The bit c is picked up randomly at the starting of GM_0. Hence, we have

$$\text{Advs}^{\mathcal{U}_{\text{av}}}_{\text{SAP}}(t) = \left|2.\text{Advs}^{\mathcal{U}_{\text{av}},\text{GM}_0}_{\text{SAP}} - 1\right|. \tag{4}$$

GM_1: In this game, an eavesdropping attack is modeled in which $\mathcal{U}_{\text{av}}$ can intercept all the communicated messages $m_1 = \{\overline{I_{\text{sm}}}, T_{\text{sm}}, \text{Auth}_{\text{sm}}, R_{\text{sm}}\}$ and $m_2 = \{T_{\text{nan}}, R_{\text{nan}}, \text{Auth}_{\text{nan}}\}$ during the login and authentication stage which executing SAP using the Execute-query listed earlier. Afterward, $\mathcal{U}_{\text{av}}$ runs the test and reveals queries to scrutinize whether the extracted session key SK is real. The session-key established between legal SM and accessed NAN_s is $\text{SK} = H_1(K_{\text{sm}}||K_{\text{nan}}||R_{\text{sm}}||R_{\text{nan}}||T_{\text{sm}}||T_{\text{nan}})$. To computes SK, $\mathcal{U}_{\text{av}}$ needs the secrets $(R_{\text{sm}}, \text{Auth}_{\text{nan}}, R_{\text{nan}}$ and long-term secret (d_{nan}) which knows to $\mathcal{U}_{\text{av}}$. Therefore, just by eaves-dropping the messages m_1 and m_2 the winning chance of GM_1 by $\mathcal{U}_{\text{av}}$ is not at all increased. Leveraging the indistinguishably of GM_0 and GM_1, it follows that

$$\text{Advs}^{\mathcal{U}_{\text{av}},\text{GM}_1}_{\text{SAP}} = \text{Advs}^{\mathcal{U}_{\text{av}},\text{GM}_0}_{\text{SAP}}. \tag{5}$$

GM_2: It is the adversary's last action. The simulations of the Send and H queries are involved in this game to model it as an active attack. From the exchanged messages m_1 and m_2 all SM_j $(j = 1, 2, 3, ..9)$, are safeguarded by the collision-resistant $h(.)$. The random numbers, id-participants, secret credentials, and timestamps are included by SM_j, there will be no collusion when $\mathcal{U}_{\text{av}}$ executes the H and Send queries. The games GM_1 and GM_2 are identical except the involvement of execution of the H

and Send queries in GM_2. The following results are achieved by the output of birthday paradox

$$\left|\text{Advs}_{\text{SAP}}^{\mathcal{U}_{\text{av}},\text{GM}_1} - \text{Advs}_{\text{SAP}}^{\mathcal{U}_{\text{av}},\text{GM}_2}\right| \leq \frac{q_h^{r^2}}{2|H|}. \quad (6)$$

Since all the queries are executed by $\mathcal{U}_{\text{av}}$, it only remains to predict the bit c to win the game once the Test query is simulated, and hence, we have $\text{Advs}_{\text{SAP}}^{\mathcal{U}_{\text{av}},\text{GM}_2} = \frac{1}{2}$. Simplifying the equations and using the triangular-inequality, the following is attained:

$$\frac{1}{2}.\text{Advs}_{\text{SAP}}^{\mathcal{U}_{\text{av}}}(t) = |\text{Advs}_{\text{SAP}}^{\mathcal{U}_{\text{av}},\text{GM}_0} - \frac{1}{2}| = \text{Advs}_{\text{SAP}}^{\mathcal{U}_{\text{av}},\text{GM}_1} - \text{Advs}_{\text{SAP}}^{\mathcal{U}_{\text{av}},\text{GM}_2} \leq |\text{Advs}_{\text{SAP}}^{\mathcal{U}_{\text{av}},\text{GM}_1} - \text{Advs}_{\text{SAP}}^{\mathcal{U}_{\text{av}},\text{GM}_2}| + |\text{Advs}_{\text{SAP}}^{\mathcal{U}_{\text{av}},\text{GM}_2} - \text{Advs}_{\text{SAP}}^{\mathcal{U}_{\text{av}},\text{GM}_2}| \leq \frac{q_h^{r^2}}{H}.$$

Hence, it follows that $\text{Advs}_{\text{SAP}}^{\mathcal{U}_{\text{av}}}(t) \leq \frac{q_h^{r^2}}{H}$.

B. Validation Through ProVerif

We apply the automated verification tool ProVerif to validate the contributed scheme on the authentication benchmarks set by this formal verification tool. This automated verifying tool works on the principles of pi-calculus, which may be categorized into three sections declaration, processes, and main/events. The numeric constant/variable parameters and private/public channels are modeled by equations and constructors; whereas, the processes are defined as per the specifications of the steps depicted in Section III and Fig. 2. We applied two queries to check the initiation and termination of SM and NAN processes and another query to verify the noncompromise of a session key. The queries yield the following results.

1. RESULT inj − event(endNAN _ GW (id)) ==> inj − event(beginNAN _ GW (id)) is true.

2. RESULT inj − event(endSmart _ M (id _2513)) ==> inj− event(beginSmart _ M (id_2513)) is true.

3. RESULT not attacker (SK[]) is true.

The results (1) and (2) indicate evidently that both processes started and terminated with success, and result (3) shows that the constructed session key is hidden from the attacker during the mutual authentication phase.

C. Discussion on Attack Resilience

The following sections explain the attack resilience of the proposed scheme against different attacks.

1) Supports Mutual Authentication: After the successful execution of the protocol, the agreed session key $\text{SK} = H_1(K_{\text{sm}}||K_{\text{nan}}||R_{\text{sm}}||R_{\text{nan}}||T_{\text{sm}}||T_{\text{nan}})$ between these participants remains confidential. The adversary cannot construct a crucial factor of this session key SK, i.e., K_{sm} or K_{nan}, until it gets access to either of the private keys of legitimate participants. After verifying $\text{Auth}_{\text{nan}}^* \stackrel{?}{=} H_2(K_{\text{sm}}||K_{\text{nan}}||R_{\text{nan}}||T_{\text{nan}}||I_{\text{nan}})$, the SM certifies the received tokens and authenticity of NAN gateway. This is because it beholds that the computation of Auth_{nan} token requires K_{nan} parameter, which is computed as $K_{\text{nan}} = r_{\text{nan}}Q_{\text{sm}} + d_{\text{nan}}R_{\text{sm}}$ and engages the public key Q_{nan} of legal NAN gateway. Hence, this assures Auth_{nan} can never be computed by any intermediate adversary. Likewise, the NAN gateway verifies the authenticity of SM after computing $K_{\text{sm}} = d_{\text{nan}}R_{\text{sm}}$ and verifying the equation $\text{Auth}_{\text{sm}}^* \stackrel{?}{=} H_2(K_{\text{sm}}||R_{\text{sm}}||T_{\text{sm}}||I_{\text{sm}})$. Hence, the proposed scheme supports mutual authentication.

2) Resistance to Replay Attack: In proposed scheme, the respective timestamp $\{T_{\text{sm}}, T_{\text{nan}}\}$ and nonces $\{R_{\text{sm}}, R_{\text{nan}}\}$ are included in both request and reply messages. In case, the attacker inserts new timestamps into the message then it will invalidate the message verification of $\text{Auth}_{\text{sm}}^*$ and $\text{Auth}_{\text{nan}}^*$ parameters on both ends. Hence, the intercepted tokens will not be beneficial for the attacker in launching a replay attack.

3) Resistance to Impersonation Attack: To initiate a successful impersonation attack, the adversary requires access to the private key information, i.e., d_{sm} and d_{nan} of SM or NAN gateway, respectively. In the absence of such secret credentials, it would not be possible for the adversary to compute the legal tokens Auth_{sm} and Auth_{nan} and masquerade legitimate members. Besides, it is computationally intractable due to ECDLP hardness to recover those private secret credentials (d_{sm} and d_{nan}) from the publicly available public keys, i.e., Q_{sm} and Q_{nan}. Therefore, our scheme can comfortably withstand SM and NAN gateway impersonation attacks.

4) Adherence to Anonymity: In proposed scheme, the SM does not submit its identity I_{sm} in plain text on an insecure channel rather it encapsulates the SM's identity as a function of XOR in ($\overline{I_{\text{sm}}}$), i.e., $\overline{I_{\text{sm}}} = I_{\text{sm}} \oplus H_1(k_{\text{sm}_x}||k_{\text{sm}_y})$. Now, the adversary first needs to compute $H_1(k_{\text{sm}_x}||k_{\text{sm}_y})$ before recovering the identity I_{sm} from $\overline{I_{\text{sm}}}$ while $H_1(k_{\text{sm}_x}||k_{\text{sm}_y})$ can only be computed using the private key of SM. Same argument is applied to identity of NAN. Thus, our scheme adheres to the requirement of the anonymity feature.

5) Resistance to Eavesdropping Attacks: If an adversary can eavesdrop on the authentication tokens from an insecure channel, it could go for misusing those contents to impersonate any legal participant by either modifying or replaying those messages. In case, an adversary sniffs the channel between NAN gateway and SM, i.e., the former accesses the communication messages $m_1 = \{\overline{I_{\text{sm}}}, T_{\text{sm}}, \text{Auth}_{\text{sm}}, R_{\text{sm}}\}$ and $m_2 = \{T_{\text{nan}}, R_{\text{nan}}, \text{Auth}_{\text{nan}}\}$, then the adversary may not be able to decipher any critical information. This is due to the fact the authentication tokens $\text{Auth}_{\text{sm}} = H_2(K_{\text{sm}}||R_{\text{sm}}||T_{\text{sm}}||I_{\text{sm}})$ and $\text{Auth}_{\text{nan}} = H_2(K_{\text{sm}}||K_{\text{nan}}||R_{\text{nan}}||T_{\text{nan}}||I_{\text{nan}})$ are generated primarily to ensure freshness due to timestamps. Second, these messages or tokens utilize K_{sm} and K_{nan} parameters, which can only be computed with the use of private keys of respective legal participants Hence, the contributed scheme is protected from eavesdropping threats.

6) Resistance to KCI Attack: Assume that the private key of the SM is accidentally revealed to the adversary without the knowledge of SM, then to effectively impersonate as an NAN gateway, the adversary must have access to the NAN gateway's private key d_{nan} for constructing a valid message $m_2 = \{T_{\text{nan}}, R_{\text{nan}}, \text{Auth}_{\text{nan}}\}$. Similarly, $K_{\text{nan}} = r_{\text{nan}}Q_{\text{sm}} + d_{\text{nan}}R_{\text{sm}}$ cannot be computed without d_{nan}. Likewise, upon the revelation of the NAN gateway's private key, the attacker

must have access to the SM's private d_{sm}, to construct a legal $m_1 = \{\overline{I_{\text{sm}}}, T_{\text{sm}}, \text{Auth}_{\text{sm}}, R_{\text{sm}}\}$. Moreover, on reception of $m_2 = \{T_{\text{nan}}, R_{\text{nan}}, \text{Auth}_{\text{nan}}\}$, the attacker needs private key d_{sm} of the SM to compute $K_{\text{nan}} = r_{\text{sm}} Q_{\text{nan}} + d_{\text{sm}} R_{\text{nan}}$. Hence, our scheme is immune to a KCIA.

7) Supports Perfect Forward Secrecy: Our proposed scheme is compliant to perfect forward secrecy since upon the revelation of any of the private keys, either d_{sm} or d_{nan} of respective participants, the adversary may not compute previous session keys. Since, to compute the session keys of previous sessions, the adversary must compromise the short-term secrets, (R_{sm} or R_{nan}) as well in addition to compromising the long term private keys. Hence, our scheme supports perfect forward secrecy.

8) Resistance to Ephemeral Secrets Leakage Attack: As is previously mentioned the adversary must approach both long-term secrets as well as short-term nonces to compute previous session keys. That is if the adversary can succeed in approaching the short term secrets (R_{sm} or R_{nan}), it must have access to long term private keys d_{sm} or d_{nan} as well for computing the legal session keys as established between SM and NAN gateway.

9) Resistance to a Physical Attack on SM: In the proposed scheme, the SM memory contains only three secret parameters, i.e., $\{I_{\text{sm}}, d_{\text{sm}}, Q_{\text{sm}} = d_{\text{sm}} P\}$, where I_{sm} is the identity and $\{d_{\text{sm}}, Q_{\text{sm}}\}$ are the private/public key pair of the SM. In case, an attacker gets physical access to the memory of SM and reveals the $\{I_{\text{sm}}, d_{\text{sm}}, Q_{\text{sm}} = d_{\text{sm}} P\}$, it would not have any impact on all noncompromised SMs, because each SM has a different identity and key pair and all these keys pair are independent to each other. Hence, the proposed scheme resists physical attacks on SM memory.

10) Resistance to Known Session Key Threat: The proposed scheme provides mutual authentication and in each round of authentication, both participants construct the session key based on long-term private keys as well as session-specific random parameters. Therefore, even if one session key is compromised it does not affect the security of feature or past session keys.

V. Comparisons

In this section, the performance and security comparisons are presented. For comparison purposes, the related latest schemes [8], [13], [17], [18], [20], [23], [26], [27] are considered.

A. Computation Cost

In this section, the running time of proposed and competing schemes presented in [8], [13], [17], [18], [20], [23], [26], and [27] is computed. For computation time comparisons, we performed an experiment using two Pi3-B+ devices with Cortex-A53(ARMv8) 64-bits SoC-1.4 GHz processor to replicate an SM and an NAN. Both Pi3-B+ are equipped with 1-GB LPDDR2 SDRAM. The notations and running times of different operations as per our experiment are given in Table II.

Referring to Table III proposed scheme completes authentication between entities of SG infrastructure in ≈ 24.708 ms, which is quite reasonable and is better than schemes presented in [8], [20], and [26], while running time of the proposed scheme is greater than the schemes presented in [13], [17], [18], [23], and [27].

TABLE II
Running Time of Basic Operations

Notations	T_h	T_{se}	T_{ea}	T_{em}	T_{ex}	T_{pe}
Running Time	0.006	0.013	0.018	4.107	6.143	12.52

T_h: Hash; T_{se}: Symmetric encryption; T_{ea}: ECC Point addition; T_{em}: ECC Point multiplication; T_{ex}: Modular Exponentiation; T_{pe}: Bilinear Pairing.

TABLE III
Computational Cost Analysis

Scheme	Cost	Running time
[20]	$4T_{em} + 2T_{ex} + 3T_{pb} + 7T_h$	$\approx 66.316\ ms$
[17]	$2T_{em} + 20T_h$	$\approx 8.334\ ms$
[27]	$5T_{em} + 2T_{se} + 18T_h$	$\approx 20.669\ ms$
[8]	$7T_{em} + 2T_{ex} + 2T_{pb} + 10T_h$	$\approx 66.135\ ms$
[26]	$5T_{em} + 2T_{ex} + 2T_{pb} + 12T_h$	$\approx 57.933\ ms$
[13]	$6T_{em} + 13T_h + 12T_{se}$	$\approx 24.876\ ms$
[18]	$4T_{em} + 12T_h$	$\approx 16.5\ ms$
[23]	$6T_{em} + 2T_{ea} + 10T_h$	$\approx 24.738\ ms$
Our	$8T_{em} + 2T_{ea} + 8T_h$	$\approx 32.94\ ms$

TABLE IV
Communication Cost Analysis

Trans.↓	Our	[23]	[18]	[13]	[26]	[8]	[27]	[17]	[20]
Bits	1024	1504	1376	2368	1408	1920	2080	1536	1340
Msgs.	2	3	3	3	3	3	3	3	3

B. Communication Cost

The comparative communication costs are computed keeping in view the common assumptions regarding the exchanged parameters sizes, which are taken as follows: the standard size of selected SHA $-$ 1 as the hash function used in this article is 160 b, the sizes of ECC point and RSA are considered 320 and 1024 bits, respectively; whereas, size of both identity and random numbers is fixed at 160 bits and all timestamps are considered to be 32 bits long. To complete normal procedure of authentication, two message exchanges are performed in proposed scheme: 1) $m_1 = \{\overline{I_{\text{sm}}}, T_{\text{sm}}, \text{Auth}_{\text{sm}}, R_{\text{sm}}\}$ initiated by SM_i and received by NAN_j, while 2) $m_2 = \{T_{\text{nan}}, R_{\text{nan}}, \text{Auth}_{\text{nan}}\}$ is a reply message from NAN_j and is received by SM_i. The size in bits of m_1 is $\{160 + 32 + 160 + 320\} = 672$; whereas, bit size of m_2 is $\{32 + 160 + 160\} = 352$. Therefore, total communication cost of the proposed scheme is $672 + 352 = 1024$ bits. Referring Table IV, proposed scheme has least communication cost as compared with the related schemes [8], [13], [17], [18], [20], [23], [26], [27]. Moreover, proposed scheme completes the process by exchanging only two messages.

C. Security Parameters

The comparison of security parameters accomplished by our and schemes proposed in [8], [13], [17], [18], [20], [23], [26], and [27] is shown in Table V. The scheme of Garg *et al.* [23] is vulnerable to the KCI attack as well as it does not provide SM anonymity and forward secrecy. The scheme presented in [17] and [18] are having an incorrect procedure and could not complete the normal authentication process. The schemes presented in [17] and [27] do not support direct meter to NAN gateway authentication; while scheme proposed in [26] does not

TABLE V
SECURITY FEATURES

	Our	[23]	[18]	[13]	[26]	[8]	[27]	[17]	[20]
$\mathcal{A}_{s1}$	✓	✗	✓	✓	✓	✓	✓	✓	✓
$\mathcal{A}_{s2}$	✓	✓	✗	✓	✓	✓	✓	✗	✓
$\mathcal{A}_{s3}$	✓	✓	✓	✓	✓	✓	✗	✗	✓
$\mathcal{A}_{s4}$	✓	✓	✓	✓	✓	✗	✓	✓	✗
$\mathcal{A}_{s5}$	✓	✓	✓	✓	✓	✗	✓	✓	✓
$\mathcal{A}_{s6}$	✓	✓	✓	✓	✗	✓	✓	✓	✓
$\mathcal{A}_{s7}$	✓	✓	✓	✓	✗	✓	✓	✓	✓
$\mathcal{A}_{s8}$	✓	✓	✓	✓	✗	✓	✓	✓	✓
$\mathcal{A}_{s9}$	✓	✓	✓	✓	✓	✓	✓	✓	✓
$\mathcal{A}_{s10}$	✓	✓	✓	✗	✓	✓	✓	✓	✗
$\mathcal{A}_{s11}$	✓	✗	✓	✓	✓	✓	✓	✓	✓
$\mathcal{A}_{s12}$	✓	✗	✓	✗	✓	✓	✓	✓	✓
$\mathcal{A}_{s13}$	✓	✓	✓	✗	✓	✓	✓	✓	✓

Note: $\mathcal{A}_{s1}$: Resist KCI; $\mathcal{A}_{s2}$: Correctness; $\mathcal{A}_{s3}$:D2D Direct communication; $\mathcal{A}_{s4}$: Resist impersonation; $\mathcal{A}_{s5}$:Resists MIM; $\mathcal{A}_{s6}$: Resists privileged insider; $\mathcal{A}_{s7}$: Session key security; $\mathcal{A}_{s8}$: Dynamic node addition; $\mathcal{A}_{s9}$: Resists replay; $\mathcal{A}_{s10}$: Resist ephemeral secret leakage; $\mathcal{A}_{s11}$:Perfect forward secrecy; $\mathcal{A}_{s12}$: User anonymity; $\mathcal{A}_{s13}$: Resist stolen verifier; $\surd$: Secure or extends; ✗:Does not provide.

provide dynamic node addition, the security of the session key and resistance against privileged insider. The scheme proposed in [8] does not provide resistance against impersonation and man-in-the-middle attack. The scheme presented in [13] does not provide user anonymity/untraceability and cannot resist ephemeral secret Leakage and stolen verifier attacks. Only the proposed provides required security features.

VI. CONCLUSION

In this article, using the elliptic curve and symmetric key operators, an authentication scheme for the SG was presented. The proposed scheme helps in the establishment of a secure channel among the entities of the SG. The security of the proposed scheme is analyzed thoroughly to show its' resistance against the known attacks. The security comparisons have shown that except for the proposed scheme, the related schemes are having weaknesses against some attacks; whereas, the performance comparisons have shown that the proposed scheme takes less computation power as compared with some of the related schemes; whereas, the proposed scheme has the least communication cost. The security strength and better performance make the proposed scheme a good candidate for deployment in real-world SG networks.

REFERENCES

[1] N. Kumar, K. Kaur, S. C. Misra, and R. Iqbal, "An intelligent rfidenabled authentication scheme for Healthcare applications in vehicular mobile cloud," *Peer-Peer Netw. Appl.*, vol. 9, no. 5, pp. 824–840, 2016.

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

[3] J. Wang, L. Wu, K.-K. R. Choo, and D. He, "Blockchain-based anonymous authentication with key management for smart grid edge computing infrastructure," *IEEE Trans. Ind. Informat.*, vol. 16, no. 3, pp. 1984–1992, Mar. 2020.

[4] B. LaMacchia, K. Lauter, and A. Mityagin, "Stronger security of authenticated key exchange," in *Proc. Int. Conf. Provable Secur.*, 2007, pp. 1–16.

[5] S. A. Chaudhry, H. Alhakami, A. Baz, and F. Al-Turjman, "Securing demand response management: A certificate-based access control in smart grid edge computing infrastructure," *IEEE Access*, vol. 8, pp. 101235–101243, 2020.

[6] P. Gope and B. Sikdar, "Lightweight and privacy-friendly spatial data aggregation for secure power supply and demand management in smart grids," *IEEE Trans. Informat.*, vol. 14, no. 6, pp. 1554–1566, Jun. 2019.

[7] D. Abbasinezhad-Mood and M. Nikooghadam, "Efficient anonymous password-authenticated key exchange protocol to read isolated smart meters by utilization of extended Chebyshev chaotic maps," *IEEE Trans. Ind. Informat.*, vol. 14, no. 11, pp. 4815–4828, Nov. 2018.

[8] V. Odelu, A. K. Das, M. Wazid, and M. Conti, "Provably secure authenticated key agreement scheme for smart grid," *IEEE Trans. Smart Grid*, vol. 9, no. 3, pp. 1900–1910, May 2018.

[9] F. Wu, L. Xu, X. Li, S. Kumari, M. Karuppiah, and M. S. Obaidat, "A lightweight and provably secure key agreement systemfor a smart gridwith elliptic curve cryptography," *IEEE Syst. J.*, vol. 13, no. 3, pp. 2830–2838, Sep. 2019.

[10] M. Mustapa, M. Y. Niamat, A. P. D. Nath, and M. Alam, "Hardwareoriented authentication for advanced metering infrastructure," *IEEE Trans. Smart Grid*, vol. 9, no. 2, pp. 1261–1270, Mar. 2018.

[11] A. Abdallah and X. S. Shen, "A lightweight lattice-based homomorphic privacy-preserving data aggregation scheme for smart grid," *IEEE Trans. Smart Grid*, vol. 9, no. 1, pp. 396–405, Jan. 2018.

[12] H. J. Jo, I. S. Kim, and D. H. Lee, "Efficient and privacy-preserving metering protocols for smart grid systems," *IEEE Trans. Smart Grid*, vol. 7, no. 3, pp. 1732–1742, May 2016.

[13] P. Kumar, A. Gurtov, M. Sain, A. Martin, and P. H. Ha, "Lightweight authentication and key agreement for smart metering in smart energy networks," *IEEE Trans. Smart Grid*, vol. 10, no. 4, pp. 4349–4359, Jul. 2019.

[14] D. Abbasinezhad-Mood and M. Nikooghadam, "An anonymous eccbased self-certified key distribution scheme for the smart grid," *IEEE Trans. Ind. Electron.*, vol. 65, no. 10, pp. 7996–8004, Oct. 2018.

[15] A. Mohammadali, M. S. Haghighi, M. H. Tadayon, and A. MohammadiNodooshan, "A novel identity-based key establishment method for advanced metering infrastructure in smart grid," *IEEE Trans. Smart Grid*, vol. 9, no. 4, pp. 2834–2842, Jul. 2018.

[16] K. Mahmood, S. A. Chaudhry, H. Naqvi, S. Kumari, X. Li, and A. K. Sangaiah, "An elliptic curve cryptography based lightweight authentication scheme for smart grid communication," *Future Gener. Comput. Syst.*, vol. 81, pp. 557–565, 2018.

[17] S. Challa *et al.*, "Design and analysis of authenticated key agreement scheme in cloud-assisted cyber-physical systems," *Future Gener. Comput. Syst.*, vol. 108, pp. 1267–1286, 2018.

[18] N. Kumar, G. S. Aujla, A. K. Das, and M. Conti, "Eccauth: A secure authentication protocol for demand response management in a smart grid system," *IEEE Trans. Ind. Informat.*, vol. 15, no. 12, pp. 6572–6582, Dec. 2019.

[19] K. Mahmood, J. Arshad, S. A. Chaudhry, and S. Kumari, "An enhanced anonymous identity-based key agreement protocol for smart grid advanced metering infrastructure," *Int. J. Commun. Syst.*, vol. 32, no. 16, 2019, Art. no. e4137.

[20] K. Mahmood *et al.*, "Pairing based anonymous and secure key agreement protocol for smart grid edge computing infrastructure," *Future Gener. Comput. Syst.*, vol. 88, pp. 491–500, 2018.

[21] S. A. Chaudhry, K. Yahya, and F. Al-Turjman, "Correctness of an authentication scheme for managing demand response in smart grid," in *Smart-Grid in IoT-Enabled Spaces*, 1st ed., CRC Press, 2020, pp. 223–231.

[22] X.-C. Liang, T.-Y. Wu, Y.-Q. Lee, C.-M. Chen, and J.-H. Yeh, "Cryptanalysis of a pairing-based anonymous key agreement scheme for smart grid," in *Advances in Intelligent Information Hiding and Multimedia Signal Processing*. Berlin, Germany: Springer, 2020, pp. 125–131.

[23] S. Garg, K. Kaur, G. Kaddoum, J. J. Rodrigues, and M. Guizani, "Secure and lightweight authentication scheme for smart metering infrastructure in smart grid," *IEEE Trans. Ind. Informat.*, vol. 16, no. 5, pp. 3548–3557, May 2020, doi: 10.1109/TII.2019.2944880.

[24] M. Abdalla, P. Fouque, and D. Pointcheval, "Password-based authenticated key exchange in the three-party setting," *IEE Proc. Inf. Secur.*, vol. 153, no. 1, pp. 27–39, 2006.

[25] S. Roy, A. K. Das, S. Chatterjee, N. Kumar, S. Chattopadhyay, and J. J. Rodrigues, "Provably secure fine-grained data access control over multiple cloud servers in mobile cloud computing based healthcare applications," *IEEE Trans. Ind. Informat.*, vol. 15, no. 1, pp. 457–468, Jan. 2018.

[26] J.-L. Tsai and N.-W. Lo, "Secure anonymous key distribution scheme for smart grid," *IEEE Trans. Smart Grid*, vol. 7, no. 2, pp. 906–914, Mar. 2016.

[27] S. A. Chaudhry, T. Shon, F. Al-Turjman, and M. H. Alsharif, "Correcting design flaws: An improved and cloud assisted key agreement scheme in cyber physical systems," *Comput. Commun.*, vol. 153, pp. 527–537, 2020.