Symmetric Key Based Scheme for Verification Token Generation in Internet of Things Communication Environment

Keyan Abdul-Aziz Mutlaq[1,2], Vincent Omollo Nyangaresi[3], Mohd Adib Omar[1(✉)], and Zaid Ameen Abduljabbar[4]

[1] School of Computer Sciences, Universiti Sains Malaysia, USM, 11800 Gelugor, Penang, Malaysia
keyan.alsibahi@student.usm.my, keyan.alsibahi@uobasrah.edu.iq, adib@usm.my

[2] IT and Communications Center, University of Basrah, Basrah 61004, Iraq

[3] Faculty of Biological and Physical Sciences, Tom Mboya University College, Homabay, Kenya
vnyangaresi@tmuc.ac.ke

[4] Department of Computer Science, College of Education for Pure Sciences, University of Basrah, Basrah 61004, Iraq
zaid.ameen@uobasrah.edu.iq

Abstract. The traditional power grid systems are being replaced with smart grids so as to offer the required levels of flexibility, reliability, efficiency and dynamic power adjustments. However, security and privacy challenges are serious issues in smart grid environment due to a myriad of heterogeneous appliances that interconnect with the grid system. Consequently, many security and privacy preservation schemes have been developed based on techniques such as elliptic curve cryptography, blockchains, homomorphic encryption, public key certificates and bilinear pairing operations among others. However, these schemes have numerous performance and security constraints. In addition, some of these protocols require tamper proof devices which ride on unrealistic security assumptions. In this paper, a symmetric key based scheme for verification token generation is developed for internet of things communication environment. Extensive performance evaluation is executed in terms of computation, communication and space complexities. The results show that the proposed scheme has relatively low storage complexity, and the least computation and communication complexities. This renders it applicable in smart grid communication environment. In terms of security and privacy, a number of hypotheses are formulated and proofed to show that this scheme is secure under both the Dolev-Yao (DY) and the Canetti-Krawczyk threat models.

Keywords: Authentication · IoT · Key agreement · Pseudonymity · Time-stamping

J. Lin and Q. Tang (Eds.): AC3 2022, LNICST 448, pp. 46–64, 2022.
https://doi.org/10.1007/978-3-031-17081-2_4

1 Introduction

The smart grid (SG) integrates information and communication technology to the traditional power grids to offer intelligent services such as real-time electricity data management and end-to-end connectivity between consumers and utility service providers (USPs). This integration also achieves some levels of enhanced efficiency, flexibility and dependability in grid data processing [1]. As pointed out in [2], smart grids improve the power supply quality, reduce power consumption, and facilitate the support of new technologies such as electric vehicles. A typical smart grid comprises of smart meters (SMs), wireless access channels, energy resources and smart appliances [3]. Compared with the traditional electric power systems, smart grids are efficient in addressing economic, social and industrial challenges of the conventional power systems [4]. Essentially, the smart grid executes continuous monitoring of the power consumption and provides the required adjustments [5, 6].

In smart grids, the smart meter has two interfaces, with one monitoring power consumption while the other one provides the communicating gateway. As such, the smart meter offers power measurement, monitoring as well as control [7]. All the consumption information collected at the consumer side are regularly forwarded to the neighboring node, which can be a gateway, data collector, another smart meter or control center. This neighboring node continuously aggregates data from diverse smart meters until all consumer data from a particular area are collected. Afterwards, these consumption reports are forwarded to the utility service provider. Here, the USP deploys the received reports to evaluate the power supply and demand, and provide dynamic price or power supply adjustments [1]. As such, it is possible for the USP to utilize the smart grid to estimate energy consumption and formulate a stochastic pricing strategy [8]. Further, the SMs can provide power theft detection, power quality monitoring and on-demand reading [9].

Despite all the benefits that come with the deployment of smart grids, numerous security and privacy issues lurk in these grids [10]. For instance, the smart grid components can be physically captured and the communication pathways can be eavesdropped. As pointed out in [3], security threats are some of the challenges facing the integration of the power grid with information and communication technology. According to [11], malevolent command injection, eavesdropping, false data injection, private data theft, Man-In-The-Middle (MITM) and Denial of Service (DoS) attacks are serious issues in smart grids. In addition, authors in [12] identify privacy leaks as one of the factors that impede smart grid deployments. For instance, adversaries can analyze consumer power consumption reports and hence infer about home occupancy, consumer daily activities and lifestyle [1, 13].

According to [14], the interconnection among many smart grids and appliances offers a large surface from which attacks may be launched. In addition, the IP-based communication in smart grids produces high volumes of control and sensitive data which can be targeted by adversaries. The continued incorporation of new technologies further exposes the smart grids to new security threats [15]. Consequently, security and privacy have become major challenges in these grids. In particular, the preservation of confidentiality, integrity and availability is crucial in these networks [16]. As pointed out in [17] and [18], mutual authentications as well as secure communication between

the users and the USP are some of the key steps towards addressing cyber threats in this environment. In addition, encryption, network segmentation, firewalls, passwords and anti-malware programs may be deployed. However, all these techniques have their own challenges that limit their applicability in smart grids. For instance, the usage of low entropy passwords may be easily broken by polynomial time adversaries. As such, the design of ideal authentication and key agreement protocols for smart grids is challenging owing to the diverse security and privacy requirements among its components [7]. The specific contributions of this paper are as follows:

- A scheme that leverages on pseudonymity and time-stamping is developed to protect against replay and impersonation attacks.
- A session key is negotiated among the communicating entities to encipher the packets exchanged after successful authentication procedures.
- Extensive security analysis is carried out to show that the proposed scheme is secure under both the Dolev-Yao (DY) and the Canetti-Krawczyk threat models.
- Performance evaluation is executed to show that the proposed scheme has lower storage costs and the least computation and communication complexities.

The rest of this research article is structured as follows: Sect. 2 discusses related work while Sect. 3 elaborates the adopted system model for the proposed scheme. On the other hand, Sect. 4 executes security analysis and comparative evaluation of the proposed protocol. Finally, Sect. 5 concludes the paper and provides some future research directions.

2 Related Work

Many authentication and key agreement schemes have been presented in literature, although each of these schemes exhibits some security, privacy or performance weaknesses. For instance, the lightweight privacy protection scheme introduced in [19] incurs high communication and computation overheads. In addition, the transmission of secret credentials over the open wireless channels can lead to impersonation attacks. On the other hand, the scheme in [20] requires a fully trusted third party entity which is cumbersome to get in the real world [1]. A bilinear pairing based authentication and key agreement scheme has been developed in [21]. Although this protocol offers smart meter privacy and session key secrecy, it is susceptible to impersonation and traceability attacks [22]. In addition, the usage of pairing operations increases its computation costs [23]. Authors in [14] have presented a lightweight authorization protocol for smart grids. However, the identities of the communicating entities are sent in plain-text over insecure channels and hence they are susceptible to impersonation attacks [24]. In addition, it fails to offer user anonymity. An identity-based scheme is developed in [25], while Elliptic Curve Cryptography (ECC) based protocols are introduced in [24] and [26]. However, these protocols experience high computation overheads due to time consuming elliptic curve point multiplication operations [27]. An anonymous authentication protocol is developed in [28] for multi-granular energy management. However, this protocol has unrealistic requirement that the terminal device communicate directly with the control center [12]. Homomorphic encryption based schemes have been introduced in [8]

and [29–31] for data privacy protection. However, homomorphic encryption techniques have high computation overheads hence not ideal for smart meters [1]. Based on ECC, a lightweight authentication protocol for smart grids is developed in [32]. Unfortunately, this scheme does not offer user anonymity [33]. Although the message authentication scheme in [34] offers session key establishment, user anonymity and mutual authentication, it is susceptible to privileged insider attacks [14]. Moreover, it incurs high storage costs and fails to offer perfect forward key secrecy.

Schemes for electricity theft detection are presented in [35–37], while an ECC based lightweight authentication protocol is introduced in [15]. However, the protocol in [15] is vulnerable to attacks such as known session specific temporary information (KSSTI), server masquerading, privileged insider and impersonation [38]. In addition, it does not offer user anonymity, private key protection and is susceptible to de-synchronization attacks [32]. Although the scheme in [39] offers user and smart meter anonymity, it is vulnerable to session key leakage attacks [21] and has high computation costs due to bilinear operations [40, 41]. Similarly, the bilinear pairing based authentication protocols in [9] and [42] have high computation overheads [19]. Although the scheme in [43] offers error detection in smart grids, it fails to offer session key negotiation [15].

To enhance trust in smart grids, a blockchain based framework is presented in [44] for distributed trust, availability, data anonymity and integrity. However, blockchain introduces some computation and storage burdens to the smart meters [45]. Although the user authentication scheme in [46] provides data integrity and user anonymity, it incurs high communication and computation overheads. In addition, the deployment of static keys implies the protocol cannot offer perfect forward key secrecy [34]. A scheme that offers anonymous smart meter authentication to the USP is presented in [47]. Unfortunately, this scheme has challenges with the revocation of malicious anonymous users [12]. On the other hand, the authenticated key agreement protocol in [48] cannot thwart ephemeral secret leakage attacks. To protect against side-channeling attacks, a Physical Unclonable Function (PUF) based scheme is presented in [49], while a distributed authentication scheme is introduced in [50]. However, the protocol in [50] incurs high communication overheads.

A lightweight key sharing protocol is presented in [40], but is susceptible to KSSTI leakage and smart meter private key disclosure attacks [51]. Although the group signature based scheme in [52] offers user privacy and thwarts both replay and spamming attacks, it cannot revoke malicious user anonymity. On the other hand, the public key certificate based protocol in [53] requires high computation costs for certificate management [34, 54]. To provide smart grid security, a password-based anonymous authentication protocol is developed in [55]. Unfortunately, password based schemes are susceptible to brute force as well as dictionary attacks. Although the user authentication scheme in [56] has low communication and computation costs, it is vulnerable to privileged insider attacks. On the other hand, the cryptographic hash function based scheme in [57] deploys timestamps and hence is susceptible to de-synchronization attacks [19, 58]. To offer session key security, an ECC based protocol is developed in [59], while a two-phase authentication protocol is presented in [60]. However, the protocol in [60] is insecure [51].

Based on the discussion above, it is evident that most of the current smart grid security and privacy preservation protocols have numerous challenges that render them unsuitable for deployment in this environment. In this paper, a scheme that addresses some of these security, performance and privacy issues is developed.

3 System Model

In order to offer the required levels of privacy and security protection in smart grids, an efficient and provably secure message verification scheme is required. All the communicating entities must be properly authenticated so as to thwart any adversarial modification of energy consumption reports, privacy leaks, erroneous billing or power adjustments. In the proposed scheme, the major components include the smart meters that are installed at the customer premises, the Trusted Control Server (TCS), data aggregator (DA) and the Utility Service Provider (USP) as shown in Fig. 1. In this environment, the smart meters and the USP have to register at the TCS upon which they are issued with the relevant security tokens to enable them communicate securely.

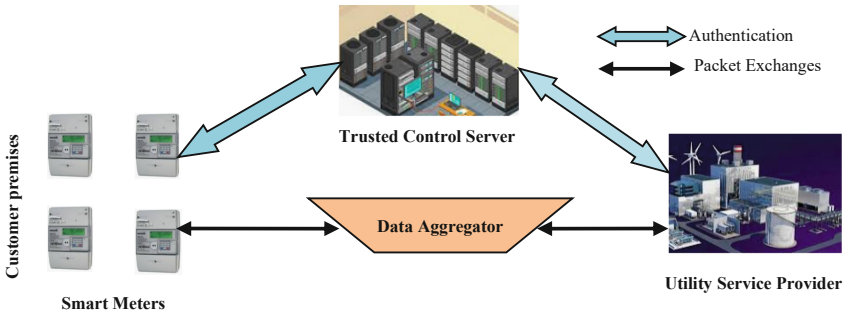

Fig.1. Network architecture

On the other hand, the data aggregator amalgamates energy consumption reports from various consumers before forwarding these reports to the USP. Table 1 presents the symbols deployed in this article, together with their brief descriptions.

The four major phases that make up the propose scheme include the system setup, registration, authentication and session key negotiation. The specifics of these phases are described in the sub-sections below.

3.1 System Setup Phase

During the system setup phase, the trusted control server generates its master key. In addition, other security parameters that will be utilized during message verification are also derived. This is a two-step procedure whose details are described below.

Step 1: To start off the system setup phase, the TCS randomly generates master key MK_T followed by the selection of SV_T as its secret value that is utilized in the derivation

Table 1. Symbols and their descriptions

Symbol	Description
MK_T	TCS master key
S_P	USP secret parameter
k	TCS public parameter
ID_S	Smart meter unique identity
$Rand_i$	Random number *i*
SV_T	TCS secret value
PN_U	USP pseudonym
PN_T	TCS pseudonym
PN_S	SM pseudonym
ID_T	TCS unique identity
T_{st_i}	Timestamp *i*
ΔT_{st}	Maximum allowed transmission delay
RM_i	Registration message *i*
AM_i	Authentication message *i*
SK_{SU}	Session key established between SM & USP
ID_U	USP unique identity
h(.)	Hashing operation
$\|\|$	Concatenation operation
$\oplus$	XOR operation

of other security parameters for the smart meter and the utility service provider. It also chooses *k* as its public security parameter.

Step 2: The TCS selects $h:\{0,1\}^* \rightarrow Z_k$ as the one-way hashing function that is used to encipher the exchanged security parameters during and after registration phase. Next, the TSC derives its unique identity ID_T that it utilizes to compute its pseudonym $PN_T = h(ID_T||SV_T)$. Finally, it saves $\{MK_T, SV_T\}$ in its database before publishing parameter set $\{k, PN_T, h(.)\}$.

3.2 Registration Phase

Before the smart meter and the utility service provider can establish any communication session, they need to register with the trusted control center. In this arrangement, the TCS acts as an intermediately between the smart meter and the utility service provider. It offers some of the services of typical gateway node in addition to the control functionality. This phase serves to assign the smart meter and the utility service provider some secret security parameters required to establish a secure channel between them.

3.2.1 Utility Service Provider Registration

To register itself to the TCS, the USP executes the 3 critical steps. The exact cryptographic operations carried out are discussed below.

Step 1: The USP randomly chooses ID_U and S_P as its unique identity and secret parameter respectively. Next, it uses secure channels to transmit registration request U_{RR} to the TCS, accompanied by its identity ID_U.
Step 2: On receiving the USP's registration request, the TCS derives USP's pseudonym $PN_U = h(ID_U||SV_T)$ and $H_1 = h(ID_U||MK_T)$. It then securely stores parameter set $\{ID_U, H_1, PN_U\}$ in its database before composing message $RM_1 = \{H_1, PN_U\}$ that is then sent over to the USP in registration response U_{RS} through some secure channels as shown in Fig. 2.
Step 3: After obtaining RM_1 from the TCS, the USP derives $H_2 = h(ID_U||S_P) \oplus H_1$, $PN_U{}^* = h(ID_U||S_P) \oplus PN_U$ and $PN_S = h(ID_U||SV_T)$. Lastly, it stores parameters $\{H_2, PN_U{}^*, PN_S\}$ in its database.

3.2.2 Smart Meter Registration

To usher in the smart meter registration, it first randomly chooses its identity that is then transmitted over to the TCS. In exchange, the TCS issues the smart meter with some secret key for use in the subsequent phase. This is a 3 step process as elaborated below.

Step 1: The smart meter chooses its unique identity ID_S that it then securely sends to the TCS in registration request S_{RR} over some trusted channels.
Step 2: Upon receiving this identity ID_S from the smart meter, the TCS computes $PN_S{}^* = h(ID_U||SV_T)$ and $H_3 = h(ID_S||MK_T)$. It then stores parameters $\{ID_S, H_3, PN_S{}^*\}$ in its database. Lastly, it composes message $RM_2 = \{H_3, PN_S{}^*\}$ that is transmitted in registration response S_{RS} to the smart meter over some trusted channels.

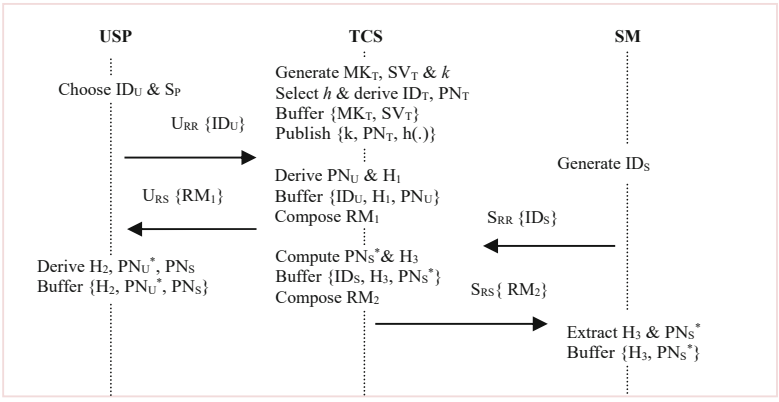

Fig. 2. System setup and registration

Step 3: After obtaining message RM_2, the smart meter extracts H_3 and $PN_S{}^*$ which it then stores securely in its memory.

3.3 Authentication and Session Key Negotiation Phase

After the successful registration of the smart meter and the utility service provider, these two entities need to negotiation a session key for secure communication between them. This phase is executed in 6 steps as discussed below.

Step 1: The USP initiates the authentication process by using its identity ID_U and secret parameter S_P to derive $PN_U = PN_U{}^* \oplus h(ID_U||S_P)$, $H_1 = H_2 \oplus h(ID_U||S_P)$. This is followed by the generation of random number $Rand_1 \in Z_k^*$ and the determination of the current timestamp, T_{st_1}. Using these values, the following parameters are computed:

$$Auth1 = h(PNT||T_{st_1}) \oplus PNU$$
$$Auth_2 = h(PN_U||PN_T||H_1) \oplus Rand_1$$
$$Auth3 = h(PNU||PNT||H1||Rand1) \oplus PNS$$
$$Auth_4 = h(PN_U||PN_S||PN_T||H_1||Rand_1)$$

Lastly, the USP constructs message $AM_1 = \{Auth_1, Auth_2, Auth_3, Auth_4)$ that is transmitted in authentication request U_{AR} to the TCS over public channels as shown in Fig. 3.

Step 2: Upon receiving AM_1 from the USP, the TCS establishes the current time T_{st_C} and checks if $T_{st_C} - T_{st_1} \leq \Delta T_{st}$. If this condition does not hold, the TCS rejects authentication message AM_1. However, if this condition holds, the TCS proceeds to compute $PN_U{}^{**} = Auth_1 \oplus h(PN_T||T_{st_1})$. Afterwards, it retrieves $H_1{}^*$ from its database that it deploys to derive the following security parameters:

$$Rand_1{}^* = Auth_2 \oplus h(PN_U{}^{**}||PN_T||H_1{}^*)$$
$$PN_S{}^* = Auth_3 \oplus h(PN_U{}^{**}||PN_T||H_1{}^*||Rand_1{}^*)$$
$$Auth_4{}^* = h(PN_U{}^{**}||PN_S{}^*||PN_T||H_1{}^*||Rand_1{}^*)$$

Step 3: The TCS then confirms whether $Auth_4{}^* \stackrel{?}{=} Auth_4$ such that the authentication request is rejected if these values are not identical. Otherwise, the TCS has authenticated the USP and hence proceeds to retrieve $H_3{}^*$ corresponding to $PN_S{}^*$ from its database. Next, the following parameters are computed:

$$Auth_5 = h(PN_S{}^*||H_3{}^*) \oplus Rand_1{}^*$$
$$Auth_6 = h(PN_S{*}||PN_T||H_3{*}||Rand_1{*}) \oplus PN_U{**}$$
$$Auth_7 = h(PN_U{}^{**}||PN_S{}^*||PN_T||H_3{}^*||Rand_1{}^*)$$

Finally, the TCS constructs message $AM_2 = \{Auth_5, Auth_6, Auth_7\}$ and sends it in authentication token S_{AT} to the smart meter over some public channels.

Step 4: On receiving message AM_2 from the TCS, the smart meter first derives the following parameters:

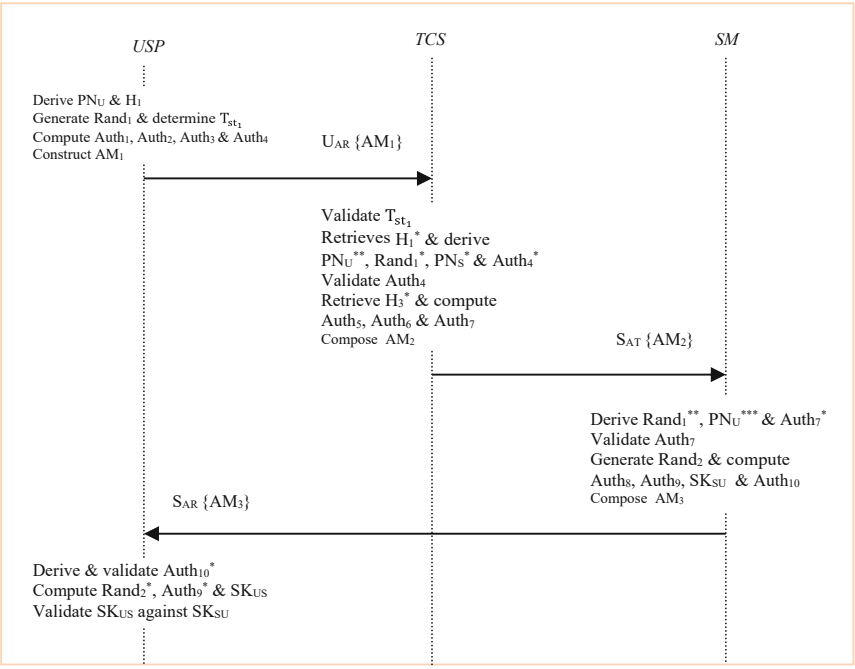

Fig. 3. Authentication and key negotiation

$$\text{Rand}_1^{**} = \text{Auth}_5 \oplus \text{h}(\text{PN}_\text{S}||\text{H}_3)$$
$$\text{PN}_\text{U}^{***} = \text{Auth}_6 \oplus \text{h}(\text{PN}_\text{S}||\text{PN}_\text{T}||\text{H}_3||\text{Rand}_1^{**})$$
$$\text{Auth}_7^{*} = \text{h}(\text{PN}_\text{U}^{***}||\text{PN}_\text{S}||\text{PN}_\text{T}||\text{H}_3||\text{Rand}_1^{**})$$

Step 5: The smart meter checks if $\text{Auth}_7^{*} \stackrel{?}{=} \text{Auth}_7$ such that the authentication request is reject when these two values are different. Otherwise, the smart meter has authenticated the TCS and proceeds to randomly select $\text{Rand}_2 \in Z_k^*$ that it utilizes to compute the following parameters:

$$\text{Auth8} = \text{h}(\text{PNS}||\text{PNU}^{***}||\text{Rand1}^{**}) \oplus \text{Rand2}$$
$$\text{Auth}_9 = \text{h}(\text{Rand}_1^{**}||\text{Rand}_2)$$
$$\text{SK}_\text{SU} = \text{h}(\text{PN}_\text{U}^{***}||\text{PN}_\text{S}||\text{PN}_\text{T}||\text{Auth}_9)$$
$$\text{Auth}_{10} = \text{h}(\text{PN}_\text{U}^{***}||\text{PN}_\text{S}||\text{PN}_\text{T}||\text{Rand}_1^{**}||\text{Rand}_2||\text{Auth}_9)$$

At the end, the smart meter composes message $\text{AM}_3 = \{\text{Auth}_8, \text{Auth}_{10}\}$ that is then sent in authentication response S_AR to the USP over public channels.

Step 6: Upon receiving AM_3 from the smart meter, the USP derives $\text{Auth}_{10}^{*} = \text{h}(\text{PN}_\text{U}||\text{PN}_\text{S}||\text{PN}_\text{T}||\text{Rand}_1||\text{Rand}_2^{*})$ before checking if $\text{Auth}_{10}^{*} \stackrel{?}{=} \text{Auth}_{10}$. Here, the authentication request is rejected when the two parameters are dissimilar. Otherwise, the smart meter is successfully authenticated. As such, the USP proceeds to derive the following parameters together with the session key SK_US:

$Rand_2^* = Auth_8 \oplus h(PN_S||PN_U||Rand_1)$
$Auth_9^* = h(Rand_1||Rand_2^*)$
$SK_{US} = h(PN_U||PN_S||PN_T||Auth_9^*)$

This is followed by the verification of whether $SK_{US} \stackrel{?}{=} SK_{SU}$. Here, the authentication request is rejected when the two session keys are dissimilar. Otherwise, the smart meter, TCS and the USP have successfully authenticated each other.

4 Comparative Analysis and Evaluation

This section presents the security analysis of the proposed protocol, based on some most common threat models. This is followed by the performance evaluation, which is executed in terms of computation, storage and communication overheads.

4.1 Security Evaluation

In this sub-section, we show that the proposed protocol is secure under both the Dolev-Yao (DY) model and the Canetti-Krawczyk model. These two security models are the most popular in appraising authentication protocols, and their assumptions are detailed in [6]. To achieve this, the following 10 hypotheses are formulated and proofed.

Hypothesis 1: The proposed scheme is robust against forgery attacks.

Proof: Suppose that an attacker is interested in modifying messages such as $Auth_4$, $Auth_7$ and $Auth_{10}$ exchanged during the authentication phase. Here, $Auth_4 = h(PN_U||PN_S||PN_T||H_1||Rand_1)$ and is sent from the USP towards the TCS, $Auth_7 = h(PN_U^{**}||PN_S^*||PN_T||H_3^*||Rand_1^*)$ and is sent from the TCS towards the SM while $Auth_{10} = h(PN_U^{***}||PN_S||PN_T||Rand_1^{**}||Rand_2||Auth_9)$ and is transmitted from the SM towards the USP. If this attack succeeds, then an adversary would have forged messages submitted by all the three communicating entities. However, message $Auth_4$ contains USP's secret key H_1 while $Auth_7$ contains the SM's secret key H_3^*. The validity of message $Auth_4$ and $Auth_7$ is confirmed through $Auth_4^* \stackrel{?}{=} Auth_4$ check at the TCS and $Auth_7^* \stackrel{?}{=} Auth_7$ check at the SM. As such, any forgery is easily detected. Regarding message $Auth_{10}$, it incorporates the USP's random number $Rand_1^{**}$ which is difficult to correctly guess. In addition, any forgery is easily detected at the USP by checking if $Auth_{10}^* \stackrel{?}{=} Auth_{10}$. Therefore, the proposed scheme is secure against forgery attacks.

Hypothesis 2: All the communicating entities are mutually authenticated in the proposed scheme.

Proof: Before the smart meter and the USP can exchange power consumption reports**,** they authenticate one another with the help of the TCS. This essentially serves to establish some trust levels between these communicating entities. In addition, the smart meter and the USP also authenticate the TCS. To start off, the USP derives $Auth_4 = h(PN_U||PN_S||PN_T||H_1||Rand_1)$ which is authenticated by the TCS in step 3 using the

re-computed $\text{Auth}_4{}^*$. Next, TCS computes $\text{Auth}_7 = \text{h}(\text{PN}_\text{U}{}^{**}||\text{PN}_\text{S}{}^*||\text{PN}_\text{T}||\text{H}_3{}^*||\text{Rand}_1{}^*)$ that is authenticated at the smart meter in step 5 using the re-computed $\text{Auth}_7{}^*$. Similarly, the smart meter computes $\text{Auth}_{10} = \text{h}(\text{PN}_\text{U}{}^{***}||\text{PN}_\text{S}||\text{PN}_\text{T}||\text{Rand}_1{}^{**}||\text{Rand}_2||\text{Auth}_9)$ that is authenticated at the USP using the re-computed $\text{Auth}_{10}{}^*$ in step 6. Evidently, the proposed scheme achieves mutual authentication among the USP, TCS and smart meter.

Hypothesis 3: The proposed scheme is resilient against known session key attacks.

Proof: Suppose that an attacker has captured the session keys such as $\text{SK}_\text{SU} = \text{h}(\text{PN}_\text{U}{}^{***}||\text{PN}_\text{S}||\text{PN}_\text{T}||\text{Auth}_9)$ or $\text{SK}_\text{US} = \text{h}(\text{PN}_\text{U}||\text{PN}_\text{S}||\text{PN}_\text{T}||\text{Auth}_9{}^*)$ that belong to a particular session. Here, $\text{Auth}_9 = \text{h}(\text{Rand}_1{}^{**}||\text{Rand}_2)$ and $\text{Auth}_9{}^* = \text{h}(\text{Rand}_1||\text{Rand}_2{}^*)$. The aim of the adversary is to utilize this current key to derive a valid session key for the next communication session. However, the session keys in this scheme are one-way hash values comprising of random numbers and the communicating entities' pseudonyms. Based on the collision-resistant property of the secure one-way hashing functions, an attacker is unable to parse these random numbers from the captured session keys. Consequently, an adversary cannot derive a valid session key devoid of these random numbers and pseudonyms PN_U, PN_S and PN_T. Therefore, this attack can never succeed against the proposed scheme.

Hypothesis 4: Anonymity of the communicating entities is upheld in this scheme.

Proof: In the proposed scheme, the identities of the smart meter, TCS and USP are ID_S, ID_T and ID_U respectively. All these unique identities are never transmitted in plain-text over public channels. For instance, the USP's identity is masked in pseudonym $\text{PN}_\text{U} = \text{h}(\text{ID}_\text{U}||\text{SV}_\text{T})$, which is in turn embedded in $\text{Auth}_1 = \text{h}(\text{PN}_\text{T}||\text{T}_{\text{st}_1}) \oplus \text{PN}_\text{U}$. In addition, ID_S is masked in $\text{H}_3 = \text{h}(\text{ID}_\text{S}||\text{MK}_\text{T})$ while ID_T is encapsulated in $\text{PN}_\text{T} = \text{h}(\text{ID}_\text{T}||\text{SV}_\text{T})$. Since it is computationally difficult to guess with high accuracy the deployed random numbers, an attacker is unable to derive the entities' real identities devoid of master keys MK_T and SV_T.

Hypothesis 5: Man-in-the-middle attacks are effectively thwarted in the proposed scheme.

Proof: In our scheme, the USP is authenticated by the TCS by checking whether $\text{Auth}_4{}^* \stackrel{?}{=} \text{Auth}_4$, while the TCS is authenticated by the smart meter by confirming if $\text{Auth}_7{}^* \stackrel{?}{=} \text{Auth}_7$. On the other hand, the smart meter is identified by the USP through Rand_1. Similarly, the smart meter is authenticated by the USP by checking if $\text{Auth}_{10}{}^* \stackrel{?}{=} \text{Auth}_{10}$. As such, any MitM attacks using these authentication messages are effectively curbed.

Hypothesis 6: The proposed scheme is robust against replay attacks.

Proof: In this scheme, the USP chooses random number $\text{Rand}_1 \in Z_k^*$ while the smart meter selects $\text{Rand}_2 \in Z_k^*$. Here, the USP incorporates Rand_1 in message $\text{Auth}_4 = \text{h}(\text{PN}_\text{U}||\text{PN}_\text{S}||\text{PN}_\text{T}||\text{H}_1||\text{Rand}_1)$, while the smart meter incorporates Rand_2 in message $\text{Auth}_{10} = \text{h}(\text{PN}_\text{U}{}^{***}||\text{PN}_\text{S}||\text{PN}_\text{T}||\text{Rand}_1{}^{**}||\text{Rand}_2||\text{Auth}_9)$. Since these random numbers

are one-time, the TCS, USP and smart meters can detect bogus replayed messages. In addition, upon receiving $AM_1 = \{Auth_1, Auth_2, Auth_3, Auth_4)$ from the USP, the TCS validates the freshness of the timestamp T_{st_1} incorporated in $Auth_1 = h(PN_T||T_{st_1}) \oplus PN_U$. As such, if AM_1 is replayed by an adversary, it will fail the freshness check $T_{st_C} - T_{st_1} \leq \Delta T_{st}$ executed at the TCS.

Hypothesis 7: The smart meter and the USP negotiate a session key in the proposed scheme.

Proof: In the proposed scheme, the USP authenticates the smart meter by validating $Auth_{10}{}^{*} = h(PN_U||PN_S||PN_T||Rand_1||Rand_2{}^{*})$ against $Auth_{10} = h(PN_U{}^{***}||PN_S||PN_T||Rand_1{}^{**}||Rand_2||Auth_9)$. On the other hand, the SM implicitly authenticates the USP by verifying $Auth_7{}^{*} = h(PN_U{}^{***}||PN_S||PN_T||H_3||Rand_1{}^{**})$ against $Auth_7 = h(PN_U{}^{**}||PN_S{}^{*}||PN_T||H_3{}^{*}||Rand_1{}^{*})$. By doing so, the two entities ensure that they possess valid random numbers $Rand_1$ and $Rand_2$ needed to derive the session key. After these checks, they derive session keys $SK_{SU} = h(PN_U{}^{***}||PN_S||PN_T||Auth_9)$ and $SK_{US} = h(PN_U||PN_S||PN_T||Auth_9{}^{*})$. These session key must be similar and as such, the USP checks if $SK_{US} \stackrel{?}{=} SK_{SU}$. Provided that these session keys match, any traffic exchanged between the SM and USP is enciphered using this session key.

Hypothesis 8: The proposed scheme is robust against impersonation attacks.

Proof: Suppose that an attacker has successfully physically captured the smart meter and has deployed power analysis techniques to extract the security parameters stored in its memory. Next, the adversary makes attempts to impersonate the USP and SM. To successfully impersonate the USP, the attacker derives $Auth_1{}^{adv} = h(PN_T||T_{st_1}) \oplus PN_U$ and $Auth_4{}^{adv} = h(PN_U||PN_S||PN_T||H_1{}^{adv}||Rand_1{}^{adv})$ and transmits them to the TCS. Here, $H_1{}^{adv}$ and $Rand_1{}^{adv}$ have been randomly chosen by the attacker. Upon receiving these two messages, the TCS first parses PN_U from $Auth_1{}^{adv}$ and retrieves corresponding secret key H_1 from its database. Thereafter, the TCS derives $Auth_4{}^{*} = h(PN_U{}^{**}||PN_S{}^{*}||PN_T||H_1{}^{*}||Rand_1{}^{*})$ and checks if $Auth_4{}^{*} \stackrel{?}{=} Auth_4{}^{adv}$. Since an adversary does not know the actual H_1, this verification will fail at the TCS. Suppose that now the attacker wants to impersonate the SM. This requires that message $Auth_{10} = h(PN_U{}^{***}||PN_S||PN_T||Rand_1{}^{**}||Rand_2||Auth_9)$ be derived and sent over to the USP. As such, the attacker randomly selects $Rand_1{}^{adv**}$ and $Rand_2{}^{adv}$ and computes $Auth_{10}{}^{adv} = h(PN_U{}^{***}||PN_S||PN_T||Rand_1{}^{adv**}||Rand_2{}^{adv}||Auth_9)$. Upon receiving $Auth_{10}{}^{adv}$, the USP computes $Auth_{10}{}^{*} = h(PN_U||PN_S||PN_T||Rand_1||Rand_2{}^{*})$ and checks if $Auth_{10}{}^{*} \stackrel{?}{=} Auth_{10}$. Since the adversary does not know the actual values of random numbers $Rand_1{}^{**}$and $Rand_2$, this verification will fail and hence the proposed scheme can distinguish legitimate and impersonated messages.

Hypothesis 9: Smart meter physical capture attacks are curbed in the proposed scheme.

Proof: The assumption made in these attacks is that an adversary has physically captured the smart meter and has extracted the stored security tokens such as $H_3 =$

$h(ID_S||MK_T)$, $PN_S^* = h(ID_U||SV_T)$ and $SK_{SU} = h(PN_U^{***}||PN_S||PN_T||Auth_9)$. Here, $Auth_9 = h(Rand_1^{**}||Rand_2)$. However, the master key MK_T and SV_T are both masked in one-way hashing function. As such, these two keys can never be derived from the captured parameters. In addition, the session key SK_{SU} incorporates pseudonyms and random numbers. Consequently, the session key for subsequent communication can never be derived using the captured tokens.

Hypothesis 10: The proposed scheme is robust against spoofing attacks.

Proof: Suppose that an attacker masquerades as the TCS and transmits message $Auth_7^{adv} = h(PN_U^{**}||PN_S^*||PN_T||H_3^{adv*}||Rand_1^*)$ to the smart meter. Here, H_3^{adv*} is the random parameter chosen by the attacker as the SM's secret key. Upon receiving message $Auth_7^{adv}$, the SM derives $Auth_7^* = h(PN_U^{***}||PN_S||PN_T||H_3||Rand_1^{**})$ using the real H_3. Afterwards, the SM checks whether $Auth_7^* \stackrel{?}{=} Auth_7^{adv}$. Since $H_3^{adv*} \neq H_3$, this validation fails and hence malicious TCS is easily detected.

4.2 Performance Evaluation

In this sub-section, the proposed scheme is evaluated using computation, storage and communication complexities. These metrics are selected based on their prevalence during authentication protocol evaluations.

4.2.1 Computation Complexity

To evaluate the computation complexity of the propose scheme, the execution time of the various cryptographic primitives are considered. To achieve this, the authentication and key agreement phase is used and the obtained values are compared with other related schemes. In the proposed scheme, the utility service provider executes 10 one-way hashing operations (T_H) while the smart meter executes 7 one-way hashing operations. On its part, the trusted control server carries out 7 one-way hashing operations. As such, a total of $24T_H$ operations are executed in this scheme during the authentication and key agreement phase. Based on the values in [19] and [21], bilinear pairing operations T_{BP}, ECC point addition T_{ECA}, hashing operation T_H, ECC scalar multiplication T_{ECM}, symmetric encryption T_{SE} and symmetric decryption T_{SD} take 3160000 ns, 13670 ns, 1599 ns, 270016 ns, 3910 ns and 4367 ns respectively. As such, the total computation complexity of the proposed scheme is 38376 ns as shown in Table 2.

As shown in Table 2, the protocol in [39] has the highest computation complexity followed by the protocols in [15, 26] and [25] respectively. On the other hand, the proposed scheme has the lowest computation complexity. Since most of the components in the smart grid have limited computation power, the proposed scheme is the most suitable for deployment in this scenario.

4.2.2 Communication Complexity

During the authentication and key agreement phase the messages exchanged in the proposed scheme include the following:

Table 2. Computation complexities

Scheme	Overheads (ns)
[15]	1371745
[25]	1361273
[26]	1382624
[39]	8234379
Proposed	38376

$AM_1 = \{Auth_1, Auth_2, Auth_3, Auth_4)$
$AM_2 = \{Auth_5, Auth_6, Auth_7\}$
$AM_3 = \{Auth_8, Auth_{10}\}$

Here, $Auth_1 = h(PN_T||T_{st_1}) \oplus PN_U$, $Auth_2 = h(PN_U||PN_T||H_1) \oplus Rand_1$, $Auth_3 = h(PN_U||PN_T||H_1||Rand_1) \oplus PN_S$, $Auth_4 = h(PN_U||PN_S||PN_T||H_1||Rand_1)$, $Auth_5 = h(PN_S{}^*||H_3{}^*) \oplus Rand_1{}^*$, $Auth_6 = h(PN_S{}^*||PN_T||H_3{}^*||Rand_1{}^*) \oplus PN_U{}^{**}$, $Auth_7 = h(PN_U{}^{**}||PN_S{}^*||PN_T||H_3{}^*||Rand_1{}^*)$, $Auth_8 = h(PN_S||PN_U{}^{***}||Rand_1{}^{**}) \oplus Rand_2$ and $Auth_{10} = h(PN_U{}^{***}||PN_S||PN_T||Rand_1{}^{**}||Rand_2||Auth_9)$. Using the values in [19] and [21], Advanced Encryption Standard (AES) encryption, hash value, EC point, AES decryption, and timestamps are 128 bits, 160 bits, 320 bits, 128 bits and 32 bits long respectively. As such, the total communication complexity of the proposed scheme is 1440 bits, which is equivalent to 180 bytes as shown in Table 3.

Table 3. Communication complexities

Scheme	Overheads (bytes)
[15]	248
[25]	240
[26]	263
[39]	200
Proposed	180

As shown in Fig. 4, the protocol in [26] has the highest communication complexity followed by the protocols in [15, 25] and [39] respectively.

On the other hand, the proposed scheme has the lowest communication complexity. Consequently, the proposed scheme is the most appropriate for deployment in smart grid environment due to its lowest bandwidth requirements.

4.2.3 Storage Complexities

In the proposed scheme, the USP stores parameters $\{H_2, PN_U{}^*, PN_S\}$ in its database. On its part, the smart meter stores $\{H_3, PN_S{}^*\}$ in its memory. Here, $H_3 = H_2 = PN_S{}^*$

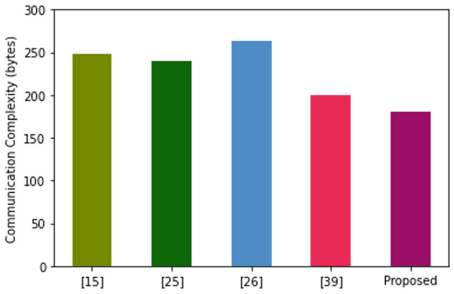

Fig. 4. Communication complexities

$= PN_U{}^* = PN_S = 160$ bits. Consequently, the overall storage cost of this scheme is 800 bits, which is equivalent to 100 bytes as shown in Table 4.

Table 4. Storage complexities

Scheme	Overheads (bytes)
[15]	60
[25]	100
[26]	160
[39]	160
Proposed	100

As shown in Fig. 5, the schemes in [26] and [39] have the highest space complexities followed by the proposed scheme and the protocol in [25] respectively. On the other hand, the protocol in [15] has the lowest space complexity.

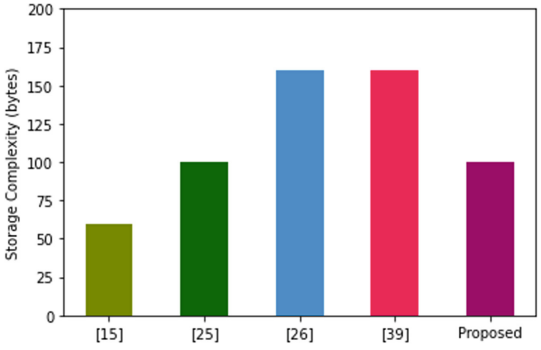

Fig. 5. Storage complexities

However, the scheme in [15] transmits identities of the communicating entities in plain-text over insecure channels, and hence it is susceptible to impersonation attacks. In addition, it fails to offer user anonymity. Consequently, the proposed scheme offers smart grid security and privacy at low computation, storage and communication costs.

5 Conclusion and Future Work

It is paramount that the signaling as well as energy consumption reports be protected from malicious modifications during their transmission over smart grid networks. In addition, eavesdropping of the smart meter collected data should be thwarted as it can potentially reveal the consumer lifestyle or home occupancy status. Although many protocols to address these issues have been presented over the recent past, a myriad of shortcomings are inherent in these schemes. Consequently, the attainment of perfect security and privacy protection at low computation, storage and communication complexities is still a mirage. The proposed scheme has been demonstrated to be secure under both the Dolev-Yao and the Canetti-Krawczyk threat models and hence potentially addresses majority of the security and privacy issues in the smart grids. In terms of performance, the proposed scheme has the least computation, and communication overheads. Since smart grid components such as smart meters are resource-constrained, the proposed scheme perfectly fits this application domain. Future work lies in the formal verification of the security features provided by the proposed scheme. There is also need for the deployment of the proposed scheme in a real smart grid environment so that its performance as well as security features can be validated.

References

1. Gai, N., Xue, K., Zhu, B., Yang, J., Liu, J., He, D.: An efficient data aggregation scheme with local differential privacy in smart grid. Digit. Commun. Netw. 1–10 (2022)
2. Desai, S., Alhadad, R., Chilamkurti, N., Mahmood, A.: A survey of privacy preserving schemes in IoE enabled smart grid advanced metering infrastructure. Clust. Comput. **22**(1), 43–69 (2019)
3. Tolba, A., Al-Makhadmeh, Z.: A cybersecurity user authentication approach for securing smart grid communications. Sustain. Energy Technol. Assess **46**, 101284 (2021)
4. Badra, M., Zeadally, S.: Lightweight and efficient privacy-preserving data aggregation approach for the Smart Grid. Ad Hoc Netw. **64**, 32–40 (2017)
5. Ferrag, M.A., Maglaras, L.A., Janicke, H., Jiang, J., Shu, L.: A systematic review of data protection and privacy preservation schemes for smart grid communications. Sustain. Cities Soc. **38**, 806–835 (2018)
6. Nyangaresi, V.O., Mohammad, Z.: Privacy preservation protocol for smart grid networks. In: 2021 International Telecommunications Conference (ITC-Egypt), pp. 1–4. IEEE (2021)
7. Luo, Y., Zheng, W.M., Chen, Y.C.: An anonymous authentication and key exchange protocol in smart grid. J. Netw. Intell. **6**(2), 206–215 (2021)
8. Liu, Y., Guo, W., Fan, C.I., Chang, L., Cheng, C.: A practical privacy-preserving data aggregation (3PDA) scheme for smart grid. IEEE Trans. Industr. Inf. **15**(3), 1767–1774 (2018)
9. Wu, T.Y., Lee, Y.Q., Chen, C.M., Tian, Y., Al-Nabhan, N.A.: An enhanced pairing-based authentication scheme for smart grid communications. J. Ambient Intell. Humaniz. Comput. 1–13 (2021)

10. Nyangaresi, V.O., Moundounga, A.R.A.: Secure data exchange scheme for smart grids. In: 2021 IEEE 6th International Forum on Research and Technology for Society and Industry (RTSI), pp. 312–316. IEEE (2021)
11. Ni, Z., Paul, S.: A multistage game in smart grid security: a reinforcement learning solution. IEEE Trans. Neural Netw. Learn. Syst. **30**(9), 2684–2695 (2019)
12. Kong, W., Shen, J., Vijayakumar, P., Cho, Y., Chang, V.: A practical group blind signature scheme for privacy protection in smart grid. J. Parallel Distrib. Comput. **136**, 29–39 (2020)
13. Nyangaresi, V.O., Alsamhi, S.H.: Towards secure traffic signaling in smart grids. In: 2021 3rd Global Power, Energy and Communication Conference (GPECOM), pp. 196–201. IEEE (2021)
14. Mahmood, K., Chaudhry, S.A., Naqvi, H., Shon, T., Ahmad, H.F.: A lightweight message authentication scheme for Smart Grid communications in power sector. Comput. Electr. Eng. **52**, 114–124 (2016)
15. Mahmood, K., Chaudhry, S.A., Naqvi, H., Kumari, S., Li, X., Sangaiah, A.K.: An elliptic curve cryptography based lightweight authentication scheme for smart grid communication. Futur. Gener. Comput. Syst. **81**, 557–565 (2018)
16. Hafizul Islam, S.K., Sabzinejad Farash, M., Biswas, G.P., Khurram Khan, M., Obaidat, M.S.: A pairing-free certificateless digital multisignature scheme using elliptic curve cryptography. Int. J. Comput. Math. **94**(1), 39–55 (2017)
17. Sadhukhan, D., Ray, S., Obaidat, M.S., Dasgupta, M.: A secure and privacy preserving lightweight authentication scheme for smart-grid communication using elliptic curve cryptography. J. Syst. Architect. **114**, 101938 (2021)
18. Nyangaresi, V.O., Rodrigues, A.J., Abeka, S.O.: ANN-FL secure handover protocol for 5G and beyond networks. In: Zitouni, R., Phokeer, A., Chavula, J., Elmokashfi, A., Gueye, A., Benamar, N. (eds.) AFRICOMM 2020. LNICSSITE, vol. 361, pp. 99–118. Springer, Cham (2021). https://doi.org/10.1007/978-3-030-70572-5_7
19. Zhang, L., Zhao, L., Yin, S., Chi, C.H., Liu, R., Zhang, Y.: A lightweight authentication scheme with privacy protection for smart grid communications. Futur. Gener. Comput. Syst. **100**, 770–778 (2019)
20. Jia, W., Zhu, H., Cao, Z., Dong, X., Xiao, C.: Human-factor aware privacy-preserving aggregation in smart grid. IEEE Syst. J. **8**(2), 598–607 (2013)
21. Odelu, V., Das, A.K., Wazid, M., Conti, M.: Provably secure authenticated key agreement scheme for smart grid. IEEE Trans. Smart Grid **9**(3), 1900–1910 (2016)
22. Chen, Y., Martínez, J.F., Castillejo, P., López, L.: An anonymous authentication and key establish scheme for smart grid: FAuth. Energies **10**(9), 1354 (2016)
23. Nyangaresi, V.O., Ogundoyin, S.O.: Certificate based authentication scheme for smart homes. In: 2021 3rd Global Power, Energy and Communication Conference (GPECOM), pp. 202–207. IEEE (2021)
24. Abbasinezhad-Mood, D., Nikooghadam, M.: An anonymous ECC-based self-certified key distribution scheme for the smart grid. IEEE Trans. Industr. Electron. **65**(10), 7996–8004 (2018)
25. Mohammadali, A., Haghighi, M.S., Tadayon, M.H., Mohammadi-Nodooshan, A.: A novel identity-based key establishment method for advanced metering infrastructure in smart grid. IEEE Trans. Smart Grid **9**(4), 2834–2842 (2016)
26. Kumar, N., Aujla, G.S., Das, A.K., Conti, M.: Eccauth: a secure authentication protocol for demand response management in a smart grid system. IEEE Trans. Industr. Inf. **15**(12), 6572–6582 (2019)
27. Zhang, L., Zhu, Y., Ren, W., Wang, Y., Choo, K.K.R., Xiong, N.N.: An energy-efficient authentication scheme based on Chebyshev chaotic map for smart grid environments. IEEE Internet Things J. **8**(23), 17120–17130 (2021)

28. Dimitriou, T., Karame, K.: Privacy-friendly tasking and trading of energy in smart grids. In: ACM Symposium on Applied Computing, vol. 21, no. 6, pp. 652–659 (2013)
29. Chen, L., Lu, R., Cao, Z.: PDAFT: A privacy-preserving data aggregation scheme with fault tolerance for smart grid communications. Peer-to-Peer Netw. Appl. **8**(6), 1122–1132 (2014). https://doi.org/10.1007/s12083-014-0255-5
30. Chim, T.W., Yiu, S.M., Li, V.O., Hui, L.C., Zhong, J.: PRGA: Privacy-preserving recording & gateway-assisted authentication of power usage information for smart grid. IEEE Trans. Dependable Secure Comput. **12**(1), 85–97 (2014)
31. Xue, K., et al.: PPSO: A privacy-preserving service outsourcing scheme for real-time pricing demand response in smart grid. IEEE Internet Things J. **6**(2), 2486–2496 (2018)
32. Abbasinezhad-Mood, D., Nikooghadam, M.: Design and hardware implementation of a security-enhanced elliptic curve cryptography based lightweight authentication scheme for smart grid communications. Futur. Gener. Comput. Syst. **84**, 47–57 (2018)
33. Wu, F., Xu, L., Li, X., Kumari, S., Karuppiah, M., Obaidat, M.S: A lightweight and provably secure key agreement system for a smart grid with elliptic curve cryptography. IEEE Syst. J. **13**(3), 2830–2838 (2018)
34. Zhang, L., Tang, S., Luo, H.: Elliptic curve cryptography-based authentication with identity protection for smart grids. PLoS One **11**(3), 151253 (2016)
35. Gao, Y., Foggo, B., Yu, N.: A physically inspired data-driven model for electricity theft detection with smart meter data. IEEE Trans. Industr. Inf. **15**(9), 5076–5088 (2019)
36. Yao, D., Wen, M., Liang, X., Fu, Z., Zhang, K., Yang, B.: Energy theft detection with energy privacy preservation in the smart grid. IEEE Internet Things J. **6**(5), 7659–7669 (2019)
37. Tao, J., Michailidis, G.: A statistical framework for detecting electricity theft activities in smart grid distribution networks. IEEE J. Sel. Areas Commun. **38**(1), 205–216 (2019)
38. Sadhukhan, D., Ray, S.: Cryptanalysis of an elliptic curve cryptography based lightweight authentication scheme for smart grid communication. In: 2018 4th International Conference on Recent Advances in Information Technology (RAIT), pp. 1–6. IEEE (2018)
39. Tsai, J.L., Lo, N.W.: Secure anonymous key distribution scheme for smart grid. IEEE Trans. Smart Grid **7**(2), 906–914 (2015)
40. He, D., Wang, H., Khan, M.K., Wang, L.: Lightweight anonymous key distribution scheme for smart grid using elliptic curve cryptography. IET Commun. **10**(14), 795–1802 (2016)
41. Nyangaresi, V.O.: Hardware assisted protocol for attacks prevention in ad hoc networks. In: Miraz, M.H., Southall, G., Ali, M., Ware, A., Soomro, S. (eds.) iCETiC 2021. LNICSSITE, vol. 395, pp. 3–20. Springer, Cham (2021). https://doi.org/10.1007/978-3-030-90016-8_1
42. Wan, Z., Wang, G., Yang, Y., Shi, S.: SKM: Scalable key management for advanced metering infrastructure in smart grids. IEEE Trans. Industr. Electron. **61**(12), 7055–7066 (2014)
43. Li, X., Wu, F., Kumari, S., Xu, L., Sangaiah, A.K., Choo, K.K.R.: A provably secure and anonymous message authentication scheme for smart grids. J. Parallel Distrib. Comput. **132**, 242–249 (2017)
44. Li, Y., Rahmani, R., Fouassier, N., Stenlund, P., Ouyang, K.: A blockchain-based architecture for stable and trustworthy smart grid. Proc. Comput. Sci. **155**, 410–416 (2019)
45. Nyangaresi, V.O.: Lightweight key agreement and authentication protocol for smart homes. In: 2021 IEEE AFRICON, pp. 1–6. IEEE (2021)
46. Li, H., Lin, X., Yang, H., Liang, X., Lu, R., Shen, X.: EPPDR: an efficient privacy-preserving demand response scheme with adaptive key evolution in smart grid. IEEE Trans. Parallel Distrib. Syst. **25**(8), 2053–2064 (2014)
47. Dimitriou, T., Karame, K.: Enabling anonymous authorization and rewarding in the smart grid. IEEE Trans. Dependable Secure Comput. **14**(5), 565–572 (2015)
48. Harishma, B., Patranabis, S., Chatterjee, U., Mukhopadhyay, D.: POSTER: authenticated key-exchange protocol for heterogeneous CPS. In: 2018 Asia Conference on Computer and Communications Security (ASIACCS), pp. 849–851, ACM, New York (2018)

49. Tahavori, M., Moazami, F.: Lightweight and secure PUF-based authenticated key agreement scheme for smart grid. Peer-to-Peer Netw. Appl. **13**(5), 1616–1628 (2020). https://doi.org/10.1007/s12083-020-00911-8
50. Gong, X., Hua, Q.S., Qian, L., Yu, D., Jin, H.: Communication efficient and privacy-preserving data aggregation without trusted authority. In: Proceedings of the 2018 IEEE Conference on Computer Communications (INFOCOM), pp. 1250–1258. IEEE (2018)
51. Abbasinezhad-Mood, D., Nikooghadam, M.: Efficient anonymous password-authenticated key exchange protocol to read isolated smart meters by utilization of extended Chebyshev chaotic maps. IEEE Trans. Industr. Inf. **14**(11), 4815–4828 (2018)
52. Jeske, T.: Privacy-preserving smart metering without a trusted-third party. In: Proceedings of the International Conference on Security and Cryptography, pp. 114–123. IEEE (2014)
53. Vaidya, B., Makrakis, D., Mouftah, H.T.: Efficient authentication mechanism for PEV charging infrastructure. In: 2011 IEEE International Conference on Communications (ICC), pp. 1–5. IEEE (2011)
54. Nyangaresi, V.O.: Provably secure protocol for 5G HetNets. In: 2021 IEEE International Conference on Microwaves, Antennas, Communications and Electronic Systems (COMCAS), pp. 17–22. IEEE (2021)
55. Khan, A.A., Kumar, V., Ahmad, M., Rana, S., Mishra, D.: PALK: password-based anonymous lightweight key agreement framework for smart grid. Int. J. Electr. Power Energy Syst. **121**, 106121 (2020)
56. Chen, Y., Martínez, J.F., Castillejo, P., López, L.: A privacy protection user authentication and key agreement scheme tailored for the internet of things environment: Priauth. Wirel. Commun. Mob. Comput. **5290579**, 1–17 (2017)
57. Kumar, P., Gurtov, A., Sain, M., Martin, A., Ha, P.H.: Lightweight authentication and key agreement for smart metering in smart energy networks. IEEE Trans. Smart Grid **10**(4), 4349–4359 (2018)
58. Nyangaresi, V.O., Rodrigues, A.J.: Efficient handover protocol for 5G and beyond networks. Comput. Secur. **113**, 102546 (2022)
59. Braeken, A., Kumar, P., Martin, A.: Efficient and provably secure key agreement for modern smart metering communications. Energies **11**(10), 2662 (2018)
60. Sha, K., Alatrash, N., Wang, Z.: A secure and efficient framework to read isolated smart grid devices. IEEE Trans. Smart Grid **8**(6), 2519–2531 (2017)