IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received October 2, 2021, accepted October 15, 2021, date of publication October 18, 2021, date of current version October 27, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3121291

ARAP-SG: Anonymous and Reliable Authentication Protocol for Smart Grids

MUHAMMAD TANVEER[1], ABD ULLAH KHAN[2], (Member, IEEE), HABIB SHAH[3], AHMED ALKHAYYAT[4], (Member, IEEE), SHEHZAD ASHRAF CHAUDHRY[5], AND MUSHEER AHMAD[6]
[1]Faculty of Computer Science and Engineering, GIK Institute of Engineering Sciences and Technology, Topi 23640, Pakistan
[2]School of Electrical Engineering and Computer Science, National University of Sciences and Technology, Islamabad 44000, Pakistan
[3]Department of Computer Science, College of Computer Science, King Khalid University, Abha 62529, Saudi Arabia
[4]Department of Computer Technical Engineering, College of Technical Engineering, Islamic University, Najaf 54001, Iraq
[5]Department of Computer Engineering, Faculty of Engineering and Architecture, Istanbul Gelisim University, 34310 Istanbul, Turkey
[6]Department of Computer Engineering, Jamia Millia Islamia, New Delhi 110025, India

Corresponding author: Abd Ullah Khan (akhan.dphd17seecs@seecs.edu.pk)

This work was supported by the Deanship of Scientific Research at King Khalid University and titled Advanced Computational Methods for Solving Complex Computer Science and Mathematical Engineering Problems under Grant RGP.2/365/42.

ABSTRACT Internet of Things-enabled smart grid (SG) technology provides ample advantages to traditional power grids. In an SG system, the smart meter (SM) is the critical component that collects the power usage information related to users and delivers the accumulated vital information to the central service provider (CSP) via the Internet. The information is exposed to numerous pernicious security threats. Consequently, it is crucial to preserve the integrity of the communication between SMs and CSP for the smooth running of the SG system. Authentication protocol effectively enables SM and CSP to communicate securely by establishing a secure channel. Therefore, this paper presents an anonymous and reliable authentication protocol for SG (ARAP-SG) to enable secure and reliable information exchange between SM and CSP. The proposed ARAP-SG uses the hash function, elliptic curve cryptography, and symmetric encryption to complete the authentication phase. Consequently, ARAP-SG guarantees reliable information exchange during the authentication phase while conserving the anonymity of both SP and SM. Additionally, ARAP-SG authorizes CSP and SM to construct a session key (SK) after accomplishing the authentication phase for undecipherable information exchange in the future. We utilize the random oracle model to corroborate the security of the constructed SK in ARAP-SG. Moreover, by effectuating informal security analysis, it is manifested that ARAP-SG is proficient in thwarting covert security attacks. Furthermore, Scyther-based analysis is conducted to manifest that ARAP-SG is secure. Finally, through a comparative analysis with relevant authentication protocols, it is explained and shown that ARAP-SG entails 25.5-56.76% and 7.69-49.47% low computational and communication overheads, respectively, with improved security properties.

INDEX TERMS Authenticated encryption, security, privacy, authentication, smart Grid, AEAD.

I. INTRODUCTION

The advent of the Internet of things (IoT) enabled communication paradigm and advancement in the embedded system design to expand the cyber-physical system (CPS) employment in practical applications [1], [2]. A CPS is the synthesis of the cyber system, the physical system, and the communication technology. The cyber system accomplishes comprehensive computational operations on the data acquired from the physical IoT devices, deciphers the data, and originates control operations and actions in real-time. IoT-enabled smart grid (SG) CPS is the emerging CPS comprising resource-constricted IoT devices interconnected through standard communication mechanisms for exchanging information. The SG system comprises the smart meters (SMs), equipped with a communication module, sensing capabilities, actuation unit, storage unit, power resources, and central service provider (CPS). CSP stores the information received from the different IoT devices, such as SMs deployed in the SG system. CSP uses the collected data to

The associate editor coordinating the review of this manuscript and approving it for publication was Mouloud Denai.

generate billing information and predict consumer behavior. SM is the critical component of the SG system, collects the vital information associated with electricity usage by the consumer and transmits the collected sensitive information to CSP. SM and CSP use cellular communication technology (5G/4G) to exchange information. Consequently, the information thus exchanged is exposed to several security threats [3]. After commandeering sensitive information communication over the public communication channel, the attacker can use the captured information to effectuate various unauthorized actions. Thus, reliable and secure communication mechanisms are paramount for the productive and streamlined operation of the SG CPS. Therefore, an access control (AC) protocol effectively facilitates secure communication in the SG system. The AC protocol establishes a session key (SK) for encrypted communication after accomplishing the mutual authentication (MA) between SMs and CSP [4], [5].

II. RELATED WORK

In the existing literature, many authentication protocols are devised to enable secure and reliable communication in the SG system. However, most authentication protocols cannot impede different security attacks, making them unsuitable for the SG system. In this direction, the authors in [6] proposed an authentication protocol for the SG system by employing the elliptic curve cryptography (ECC), Exclusive-OR, and the secure hash algorithm (SHA). However, the authentication protocol presented in [6] is unable to provide resistance against the device capture attack. The authors in [7] presented an SHA, Exclusive-OR, and ECC-based authentication protocol for the SG system, which is incapable of restraining the de-synchronization (D-Syn) attack and does not ensure SM's anonymity. The authentication protocol presented by authors in [7] is incapable of thwarting D-Syn attack. The authors in [8] proposed an efficient authentication protocol based on physical unclonable function (PUF) and SHA, which can secure the information exchange between SM and CSP. An AEAD, ASCON-hash, and ECC-based authentication protocol for the smart grid system is presented in [9]. The protocol proposed in [9] can provide the resistance against the physical capture attack.

An ECC and SHA-based authentication protocol is presented in [10], [11] for the SG system, which is unable to impede the MITMD and impersonation attacks. In addition, the protocol proposed in [10], [11] does not render the anonymity and un-traceablity functionalities. The authors in [12] propounded an SHA, ECC, and Exclusive-OR based authentication protocol, which cannot resist D-Syn attack. The authentication protocol presented by the authors in [13] is unable to impede MITMD and impersonation attacks. In addition the protocol presented in [13] does not render the anonymity feature. The authentication scheme presented in [14] is prone to ESL, MITMD, SM physical capture attack attacks and unable to render un-traceablity and anonymity functionalities. The access control protocol presented in [15] cannot resist D-Syn attack. The authentication scheme presented in [16] cannot resist denial-of service (Do's), MITMD, replay, and ESL attacks and does not ensure the SM anonymity, as demonstrated in [17]. An authenticated encryption with associative data (AEAD) authentication scheme is resented in [18]. The scheme proposed in [19] cannot resist the D-Syn and PI attacks. Similarly, an AEAD based authentication scheme proposed in [20] for the smart home environment. The scheme presented in [21] lacks the SK verification mechanism and cannot ensure anonymity. The authors in [22] proposed an AEAD, SHA, and ECC-based authentication scheme, which lacks the feature of SK verification mechanism.

The authentication scheme proposed in [23] prone to PI, ESL attacks and does not ensure anonymity of SM. An ECC and SHA-based authentication scheme proposed in [24] to ensure privacy preserving communication the SG system. The authentication scheme rendered in [25] cannot resist MITMD, impersonation, replay, and SM capture attacks. An SHA and ECC based authentication scheme is provided in [26], which is unable to resist impersonation and ESL attacks and does not ensure anonymity feature. The authentication scheme presented in [10] is vulnerable to replay and does not render SM anonymity. An authentication scheme for the SG system is proposed in [27], which is proved to be insecure against various attack in [28]. A lightweight authentication scheme for the SG system is proposed in [29]. Yu *et al*. [30] designed an authentication scheme for the smart grid environment, which is proved to be insecure against DoS and replay attacks in [31]. In addition, the authentication scheme presented in [31] is unable to render resistance against D-Syn attack.

A. RESEARCH CONTRIBUTION

Several authentication protocols have been devised to ensure secure and reliable communication in the SG system in the existing literature, as evinced in Section II. But most of them are not proficient enough to ensure confidentiality, the integrity of the communicated information in the SG system. Thus, ensuring the integrity and confidentiality of the exchanged information has become a crucial issue that has increasingly captured the attention of the research community. The paper has the following main contributions.

1) We present an anonymous and reliable authentication protocol for the SG, ARAP-SG, based on ECC, Exclusive-OR, hash function "BLAKE", and symmetric encryption algorithm "AES-CBC-256". The proposed ARAP-SG provides the functionality of MA and enables SM and CSP to communicate securely after establishing an SK. Moreover, ARAP-SG renders the data uploading and new SM addition phase. Furthermore, in ARAP-SG, CSP can update its long-term secret without requiring a complicated mechanism. Additionally, ARAP-SG renders the phase to upload the collected data to the storage module of CSP.

2) Random oracle model (ROM) and Scyther-based security formal validation are conducted for ARAP-SG that explicate that ARAP-SG is secure and can resist various security risks. In addition to this, the information security analysis explicates that ARAP-SG is resilient against replay, MITMD, and impersonation attacks. In addition, ARAP-SG employs PUF to ensure the security against the SM physical capture attack.
3) We use the python-based cryptographic library ''PyCrypto'' to evaluate the execution time of various cryptographic primitives on resource constricted platform ''Raspberry Pi-3''. Meticulous comparative analysis explicates that ARAP-SG requires 25.5-56.76% and 7.69-49.47% low computational and communication'' costs than state-of-the-art AKE protocols with enhanced security characteristics and features.

The remainder of the article is constructed as follows. The network and threat models are discussed in Section III. The proposed ARAP-SG is elaborated in Section IV. ARAP-SG protocol is analyzed formally and informally in Section V. The efficiency of ARAP-SG is evaluated in SectionVI. The paper ends with concluding remarks in Section VII.

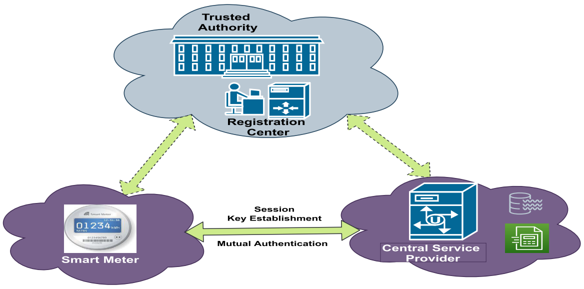


FIGURE 1. IoT-enabled SG system.

TABLE 1. List of notations used in ARAP-SG.

Notation	Description
CSP_z	z^{th} central service provider
SM_y	y^{th} smart meter
ID_{CSP_z}	Real identity (128 bits) of CSP_z
PID_y	Temporary parameter (128 bits) associated with SM_y
P	Denotes the generation point on the elliptic curve
SEC_{CSP_z}, PUB_{CSP_z}	Secret and public key pair for CSP_z
SEC_{SM_y}, SM_{SM_y}	Secret and public key pair for SM_y
TM_a, TM_b	Timestamps used in ARAP-SG
$TAD\, TRC$	Allowed time delay and receiving time of a particular message
K_2	Secret parameter or key associated with SM_y, which is used in decryption process
IV	Denotes the initialization vectors used in the encryption and encryption process
CH_y	Challenge parameter associated with SM_y
$PUF(\cdot)$	Physical unclonable function generates the parameters $K_1 = K_3$ by taking CH_y as the input
K_1, K_3	Secret parameters or keys, generated using PUF
Kr_2, Kr_3	Secret keys used in the encryption and decryption process
$E_k(meg), D_k(ct)$	AES-based encryption of message meg and decryption of ciphertext ct using the secret-key
CT, PT	Denote the ciphertext and plaintext
RN_a, RN_b	Random numbers used in the construction of session key
$Auth6 \overset{?}{=} Auth5$	Checks if both the authentication parameter are same
$H(.)$	Hash-function
$\oplus, \|$	Exclusive-OR, concatenation, respectively

III. SYSTEM MODELS

A. AUTHENTICATION MODEL

Fig. 1 represents the application scenarios for the SG system and can be considered as the authentication or network model in the proposed ARAP-SG. The network model comprises trusted authority (TA), smart meter ($SM_y|y = 1, 2, \cdots, W$), where W denotes the number of SM_y deployed in the SG system, and central service provider ($CSP_z|z = 1, 2, \cdots, T$), where T signifies the number CSP_z deployed in the SG system. TA is responsible for registering SM_y and CSP_z via registration center (RC). CSP_z is deployed in the SG system to store the information received from all SM_ys deployed in the SG system. In addition, CSP_z stores the sensitive information associated with SM_y used during the authentication phase. SM_y is responsible for collecting the electricity usage information and dispatch the collected information to CSP_z via the public communication channel (3G/4G/5G). CSP_z and SM_y exchange the information using the wireless channel, which is susceptible to various security threats. Therefore, a secure and reliable authentication protocol is imperative for the SG system to enable CSP_z and SM_y to establish an SK, which is used in accomplishing the encrypted communication after performing MA. Moreover, Table 1 summarizes the notations utilized in the proposed ARAP-SG protocol.

B. ADVERSARIAL MODEL

DY model is considered as the most accordant threat model in the designing of authentication schemes. For the proposed ARAP-SG, we consider the DY models as the threat model with the following capabilities.

1) The adversary $\mathcal{A}$, after commandeering the communicated message in the SG environment, can accomplish various operations, such that it can modify the message content, can delete the expropriated message, and can reconstruct the captured message using randomly generated parameters. After performing any of the aforementioned malicious activity, $\mathcal{A}$ can re-transmit the modified message.
2) SM_y are not the trusted devices as they are deployed in the unattended SG environment. $\mathcal{A}$ can capture a SM_y and can procure the secret credentials loaded in the memory of SM_y.
3) CSP_z are usually placed in the locking system and cannot be captured by $\mathcal{A}$ physically. In addition, RC is the fully trusted authority in the SG system.
4) Finally, we consider the CK-adversary model, which is commonly used in designing ''key-exchange protocols.'' According to the CK-adversary model, $\mathcal{A}$ can accomplish similar functions as accomplished in the DY model as mentioned earlier, and can also reveal the secreted parameters, such as ''secret keys,'' ''session states,'' and ''session keys.''

IV. THE PROPOSED ARAP-SG PROTOCOL

In this section, we present the ARAP-SG protocol for the SG system. It is imperative to perceive that we essentially focus on the mutual authentication between SM_y and CSP_z followed by the SK's establishment. Once both the SM_y and CSP_z successfully set up an SK during the authenticated key exchange phase, then SM_y can securely transmit the accumulated data towards CSP_z through the public internet. ARAP-SG protocol comprises the trailing phases.

A. SYSTEM SETUP PHASE

The ECC-based cryptosystem is extensively employed to devise AKE protocols. ECC utilizes the trailing formula:

$$Y^2 = X^2 + aX + b \mod p \quad a, b \in F_p, \tag{1}$$

where F_p represents the finite filed over the prime numbers p. ECC-based cryptosystem over F_p is consider to be secure if the condition $4a^3 + 27b^2 \neq 0$ holds. RC selects P as the base point or generation point on F_p. In addition to this, RC picks identity ID_{CSP_z} and long-term secret key SEC_{CSP_z} for CSP_z. Moreover, RC computes the public key for CSP_z as $PUB_{CSP_z} = SEC_{CSP_z} \cdot P$. RC loads the credentials $\{SEC_{CSP_z}, PUB_{CSP_z}, ID_{CSP_z}, P\}$ in the database (DB) of CSP_z. Finally, CSP_z makes PUB_{CSP_z} and P as the public parameter in the SG system.

B. SM REGISTRATION PHASE

In the SM registration (SREG) phase, RC deploys an SM after loading the secret parameters in the memory of the SM in the SG system. RC needs to effectuate the following essential steps to register an SM.

1) STEP SREG-1

SM_y sends the enrollment or registration request message to RC. RC after getting the registration request sends a challenge CH_y to SM_y via a secure channel. SM_y on getting CH_y from RC, generates a response $K1$ as $K1 = PUF(CH_y)$ and sends $\{K1, CH_y\}$ to RC.

Remark 1: To render the physical security, we assume that SM_y is provided with a robust Physical Unclonable Function (PUF). PUF takes challenge CH_y as the input and generates response K, which can be expressed by the expression $K = PUF(CH_y)$. For a particular input challenge, PUF produces an identical response each time. In addition, for two distinct input challenges, PUF produces distinct output responses.

2) STEP SREG-2

RC upon receiving $\{K1, CH_y\}$, picks unique searching identity PID_y and "key" $K2$ and computes $U_1 = E_{(K2\|ID_{CSP_z})}\{K1, CH_y\}$ by using AES-CBC-256 encryption/decryption algorithm. Finally, RC sends the list of parameters $\{K2, PID_y\}$ to SM_y via a secure channel and stores the credentials $\{PID_y, U_1\}$ in the database of CSP_z.

Remark 2: Advanced encryption standard with cipher block chaining (AES-CBC-256) mode is used for the encryption and decryption process. Here "256" denotes the secret key size used in the encryption and decryption process. The encryption and decryption process of AES-CBC-256 can be defined by $CT = E_k\{(IV), PT\}$ and $PT = D_k\{(IV), CT\}$, respectively, where CT, PT, k, and IV denote ciphertext, plaintext, key, and initialization vector, respectively.

3) STEP SREG-3

After receiving the credentials $\{K2, PID_y\}$ from RC, SM_y computes $Auth1 = H(K2 \| PID_y \| K1)$ and $U_2 = E_{K1}\{K2, PID_y\}$. Finally, SM_y stores the credentials $\{CH_y, U_2, Auth1\}$ in its own memory.

C. AKE PHASE

In this phase, SM_y and CSP_z achieve MA and then establish a secret SK for the encrypted communication in future. Following steps are executed to accomplish the AKE phase.

1) STEP AKE-1

SM_y extracts the stored challenge parameter CH_y from its own memory and computes

$$K3 = PUF(CH_y), \tag{2}$$
$$(PID_y \| K2) = D_{K3}\{U_2\}, \tag{3}$$
$$Auth2 = H(K2 \| PID_y \| K3). \tag{4}$$

In addition, SM_y checks $Auth1 \overset{?}{=} Auth2$. If it is true, SM_y continues the AKE process. Otherwise, SM_y stops further execution of the AKE phase. Moreover, SM_y selects RN_a, timestamps TM_a, secret key SEC_y, and computes

$$PUB_{SM_y} = (SEC_y \cdot P), \tag{5}$$
$$SECK_1 = (SEC_y \cdot PUB_{CSP_z}), \tag{6}$$
$$U3 = (K2 \| PID_y) \oplus H(TM_a \| SECK_1), \tag{7}$$
$$IV_1 = H(K2 \| PID_y \| TM_a), \tag{8}$$
$$CT3 = E_{K3}\{(IV_1), RN_a\}, \tag{9}$$
$$Auth3 = H(RN_a \| SECK_1 \| K2 \| PID_y), \tag{10}$$

Finally, SM_y fabricates the message $M_{SM_y} : \{TM_a, U3, CT3, Auth3, PUB_{SM_y}\}$ and dispatches it to CSP_z through the public channel.

2) STEP AKE-2

CSP_z on getting M_{SM_y} from SM_y, ensures the freshness of M_{SM_y} by corroborating the condition $TAD \geq |TRC - TM_a|$, where TAD, TRC, and TM_a represent the allowed time delay, M_{SM_y} received time, and M_{SM_y} received time, respectively. Moreover, CSP_z performs the following computation

$$SECK_2 = (SEC_{CSP_z} \cdot PUB_{SM_y}), \tag{11}$$
$$(K2 \| PID_y) = U3 \oplus H(TM_a \| SECK_2), \tag{12}$$

where $SECK_2$ is the shared secret, generated using ECC. Moreover, after procuring the parameters $(K2 \| PID_y)$, CSP_z checks if PID_y exists in its database. If found, CSP_z retrieves the parameter $\{U_1\}$ associated with PID_y. In addition to this, CSP_z calculates

$$(K1, CH_y) = D_{(K2\|ID_{CSP_z})}\{U_1\} \tag{13}$$
$$IV_2 = H(K2 \| PID_y \| TM_a), \tag{14}$$
$$RN_a = D_{K2}\{(IV_2), CT3\}, \tag{15}$$
$$Auth4 = H(RN_a \| SECK_2 \| K2 \| PID_y), \tag{16}$$

Smart Meter SM_y	**Service Provider** CSP_z
$\{CH_y, U_2, Auth1\}$	$\{PID_y, U_1\}$
picks SEC_{SM_y}, RN_1, and TM_a, retrieves CH_y and computes, $K3 = PUF(CH_y)$, $(PID_y \parallel K2) = D_{K3}\{CT1\}$, $Auth2 = H(K2 \parallel PID_y \parallel K3)$, $Auth1 \overset{?}{=} Auth2$, if so, picks RN_a, TM_a, computes $PUB_{SM_y} = (SEC_y \cdot P)$, $SECK_1 = (SEC_y \cdot PUB_{CSP_z})$, $U3 = (K2 \parallel PID_y) \oplus H(TM_a \parallel SECK_1)$, $IV_1 = H(K2 \parallel PID_y \parallel TM_a)$, $CT3 = E_{K3}\{(IV_1), RN_a\}$, $Auth3 = H(RN_a \parallel SECK_1 \parallel K2 \parallel PID_y)$, $\xrightarrow[SM_y \rightarrow CSP_z]{\{TM_a,\ U3,\ CT3,\ Auth3,\ PUB_{SM_y}\}}$.	
	validates $TAD \geq \lvert TRC - TM_a \rvert$, if holds, $SECK_2 = (SEC_{CSP_z} \cdot PUB_{SM_y})$, $(K2 \parallel PID_y) = U3 \oplus H(TM_a \parallel SECK_2)$, retrieves $\{U_1\}$ associated with PID_y, $(K1, CH_y) = D_{(K2 \parallel ID_{CSP_z})}\{U_1\}$, $IV_2 = H(K2 \parallel PID_y \parallel TM_a)$, $RN_a = D_{K2}\{(IV_2), CT3\}$, $Auth4 = H(RN_a \parallel SECK_2 \parallel K2 \parallel PID_y)$, checks $Auth4 \overset{?}{=} Auth3$, if so, selects TM_b, RN_b, and computes $Kr = H(RN_a \parallel TM_b \parallel SECK_2 \parallel K1)$, $IV_3 = (RN_a \oplus K2)$, $CT4 = E_{Kr}\{(IV_3), RN_b, ID_{CSP_z}\}$, $SK_{CSP_z} = H(RN_a \parallel RN_b \parallel SECK_2 \parallel ID_{CSP_z} \parallel TM_a \parallel TM_b \parallel PID_y)$, $Auth5 = H(SK_{CSP_z} \parallel RN_b \parallel Kr \parallel K_3 \parallel RN_a)$, $\xleftarrow[CSP_z \rightarrow SM_y]{\{TM_b,\ CT4,\ Auth5\}}$.
checks $TAD \geq \lvert TRC - TM_b \rvert$, if holds, $Kr2 = H(RN_a \parallel TM_b \parallel SECK_2 \parallel K3)$, $IV_4 = (RN_a \oplus K2)$, $(RN_b, ID_{CSP_z}) = D_{Kr2}\{(IV_4), CT4\}$, $SK_{SM_y} = H(RN_a \parallel RN_b \parallel SECK_1 \parallel ID_{CSP_z} \parallel TM_a \parallel TM_b \parallel PID_y)$, $Auth6 = H(SK_{SM_y} \parallel RN_b \parallel Kr2 \parallel K_3 \parallel RN_a)$, checks $Auth6 \overset{?}{=} Auth5$, SM_y after validating the condition considers that both session keys established at SM_y and CSP_z are similar.	
$SK_{SM_y}(= SK_{CSP_z}) = H(RN_a \parallel RN_b \parallel SECK_2 \parallel ID_{CSP_z} \parallel TM_a \parallel TM_b \parallel PID_y)$	

FIGURE 2. ARAP-SG's SK establishment phase.

where $SECK_2$, $(K2 \parallel PID_y)$, IV_2, RN_a, and $Auth4$ represent the shared secret parameter generated using ECC point multiplication, pair of secret parameters (plaintext) from the decryption process, initialization vector, plaintext generated from the decryption process, and authentication parameter generated. In addition, CSP_z checks the trailing condition

$$Auth4 \overset{?}{=} Auth3. \tag{17}$$

If the condition is corroborated, CSP_z contemplates the received M_{SM_y} as the authentic message. CSP_z after corroborating the validity of M_{SM_y}, selects TM_b, RN_b, and computes

$$Kr = H(RN_a \parallel TM_b \parallel SECK_2 \parallel K1), \tag{18}$$

$$IV_3 = (RN_a \oplus K2), \tag{19}$$

$$CT4 = E_{Kr}\{(IV_3), RN_b, ID_{CSP_z}\}, \tag{20}$$

$$SK_{CSP_z} = H(RN_a \parallel RN_b \parallel SECK_2 \parallel ID_{CSP_z} \parallel TM_a \parallel TM_b \parallel PID_y), \tag{21}$$

$$Auth5 = H(SK_{CSP_z} \parallel RN_b \parallel Kr \parallel K_1 \parallel RN_a), \tag{22}$$

where Kr, $CT4$, SK_{CSP_z}, and $Auth5$ denote secret key for the encrypting RN_b, and ID_{CSP_z}, ciphertext generated by using AES-CBC-256, secret session key for accomplishing the encrypted communication, and authentication parameter, which will be validated at SM. Finally, CSP_z constructs the message M_{CSP_z} :$\{TM_b, CT4, Auth5\}$ and transmits M_{CSP_z} to SM_y through an open channel.

3) STEP AKE-3

SM_y after getting the response message M_{CSP_z} from CSP_z, ensures the freshness of M_{CSP_z} by corroborating the condition $TAD \geq |TRC - TM_b|$, where TAD, TRC, and TM_b represent the allowed time delay, M_{CSP_z} received time, and M_{CSP_z} received time, respectively.

$$Kr2 = H(RN_a \parallel TM_b \parallel SECK_2 \parallel K3), \tag{23}$$

$$IV_4 = (RN_a \oplus K2), \tag{24}$$

$$(RN_b, ID_{CSP_z}) = D_{Kr2}\{(IV_4), CT4\}, \tag{25}$$

$$SK_{SM_y} = H(RN_a \parallel RN_b \parallel SECK_2 \parallel ID_{CSP_z} \parallel TM_a \parallel TM_b \parallel PID_y), \tag{26}$$

$$Auth6 = H(SK_{SM_y} \parallel RN_b \parallel Kr \parallel K_3 \parallel RN_a), \tag{27}$$

where $Kr2$, SK_{SM_y}, and $Auth6$ denote secret key used in the decryption process to get RN_b and ID_{CSP_z}, which is performed using AES-CBC-256, secret session key employed to achieve the indecipherable communication, and authentication parameter. Finally, to corroborate authenticity of the received message M_{CSP_z}, SM_y checks the condition

$$Auth6 \overset{?}{=} Auth5. \tag{28}$$

If the condition is corroborated, SM_y considers M_{CSP_z} as the authentic massage. In addition, SM_y after validating the condition considers that both session keys established at SM_y and CSP_z are similar. The proposed ARAP-SG is recapitulated in Fig. 2.

D. NEW SM ADDITION PHASE

In new SM addition (NSA) phase, RC adds a new SM_y^{new} the SG environment by executing the trailing steps.

1) STEP NSA-1

SM_y^{new} dispatches the registration message to RC. RC on getting message, sends a challenge CH_y to SM_y via a secure channel. Moreover, SM_y^{new} on procuring CH_y^{new} from RC, determines the response $K1^{new}$ by $K1^{new} = PUF(CH_y^{new})$ and transmits $\{K1^{new}, CH_y^{new}\}$ to RC via secure channel.

2) STEP NSA-2

RC upon procuring the parameters $\{K1^{new}, CH_y^{new}\}$, picks PID_y^{new} and "key" $K2^{new}$ and calculates $U_1^{new} = E_{(K2^{new} \| ID_{CSP_z})}\{K1^{new}, CH_y^{new}\}$. Finally, RC sends the list of parameters $\{K2^{new}, PID_y^{new}\}$ to SM_y^{new} via a secure channel and stores the credentials $\{PID_y^{new}, U_1^{new}\}$ in the database of CSP_z.

3) STEP NSA-3

After obtaining the credentials $\{K2^{new}, PID_y^{new}\}$ from RC, SM_y^{new} determines $Auth1^{new} = H(K2 \parallel PID_y^{new} \parallel K1^{new})$ and $U_2^{new} = E_{K1^{new}}\{K2^{new}, PID_y^{new}\}$. Finally, SM_y^{new} stores the credentials $\{CH_y^{new}, U_2^{new}, Auth1^{new}\}$ in its own memory.

E. DATA STORE PHASE

In this phase, SM_y uploads the collected data to data collection module of CSP_z. Data store (DS) phase comprises the following steps.

1) STEP DS-1

After collecting the data (DT), SM_y needs to send the collected data to CSP_z for further analysis. For this purpose, SM_y selects R_6, R_7, and computes $PUB_{SM_y} = R_7 \cdot P$ and

$$U_7 = (PID_y \parallel R_6) \oplus H(R_7 \cdot PUB_{CSP_z}), \tag{29}$$

$$K_7 = H(R_7 \cdot PUB_{CSP_z} \parallel SK_{SM_y}), \tag{30}$$

$$CT_7 = E_{K_7}\{(IV_7 = R_6), DT\}. \tag{31}$$

Finally, SM_y contrives a message MD_1 :$\{U_7, CT_7, PUB_{SM_y}, R_6\}$ and sends it to CSP_z data storage module.

2) STEP DS-2

CSP_z after getting the message MD_1, computes

$$(PID_y \parallel R_6) = U_8 \oplus H(SEC_{CSP_z} \cdot PUB_{SM_y}), \tag{32}$$

$$K_9 = (SEC_{CSP_z} \cdot PUB_{SM_y} \parallel SK_{CSP_z}), \tag{33}$$

$$DT = D_{K_9}\{(IV_8 = R_6), CT\}. \tag{34}$$

Finally, CSP_z stores the data DT against PID_y in its data store module.

V. SECURITY EVALUATION

In this section, we evaluate the security of the proposed ARAP-SG by conducting formal and informal analyses.

A. INFORMAL SECURITY EVALUATION

The non-mathematical security validation demonstrates that the proposed ARAP-SG thwarts various well-known attacks.

1) PRIVILEGED INSIDER ATTACK

Under this attack, a legitimate user can access the information stored in the database of CSP_z. By using these information, $\mathcal{A}$ can effectuate various attack on behalf of a specific SM_y. However, in the proposed ARAP-SG, CSP_z stores the sensitive information, associated with SM_y in encrypted form. Thus, to decrypt sensitive information, $\mathcal{A}$ needs long term secret key of CSP_z, which is known only to CSP_z and $\mathcal{A}$ cannot get this secret key. Therefore, without knowing the secret key of CSP_z, $\mathcal{A}$ cannot obtain any sensitive information to effectuate various attacks. Thus, ARAP-SG can resist privilege insider attack.

2) REPLAY ATTACK

In the proposed ARAP-SG, there are two messages, such as M_{SM_y} : $\{TM_a, U3, CT3, Auth3, PUB_{SM_y}\}$ and M_{CSP_z} : $\{TM_b, CT4, Auth5\}$ are exchanged to accomplish the AKE process. $\mathcal{A}$ can extract valuable information from a particulars entity of the SG system by replaying the captured messages. However, each transmitted message to accomplish the AKE phase incorporates the latest timestamps and new random numbers. In addition, CSP_z and SM_y check the condition $TAD \geq |TRC - TM_a|$ and $TAD \geq |TRC - TM_b|$ for M_{SM_y} and M_{CSP_z} to ensure the freshness of the received message. Thus, ARAP-SG can resist replay attack.

3) DoS ATTACK

DoS attack enables $\mathcal{A}$ to overwhelm the processing resources by sending to many AKE messages to CSP_z on behalf of some SM_y. However, in the proposed ARAP-SG, before sending an AKE request message to CSP_y, SM_y needs to achieve the local authentication by performing the computation $K3 = PUF(CH_y)$, $(PID_y \parallel K2) = D_{K3}\ \{CT1\}$, and $Auth2 = H(K2 \parallel PID_y \parallel K3)$. Local authentication will be successfully if the $Auth1 \overset{?}{=} Auth2$ is corroborated. However, without accomplishing the above computation, $\mathcal{A}$ cannot generate a valid AKE request message. Thus, ARAP-SG can thwart DoS attack.

4) IMPERSONATION ATTACK

According to adversarial model described in the Section III-B, $\mathcal{A}$ can capture M_{SM_y} : $\{TM_a, U3, CT3, Auth3, PUB_{SM_y}\}$ and M_{CSP_z} :$\{TM_b, CT4, Auth5\}$. After expropriating the captured messages, $\mathcal{A}$ attempts to impersonate as a legitimate SM_y and CSP_z. To impersonate as legitimate SM_y, $\mathcal{A}$ needs to construct valid M_{SM_y}. However, $\mathcal{A}$ cannot construct as valid message without knowing the secret parameter related to SM_y. Similarly, $\mathcal{A}$ cannot fabricate licit message M_{CSP_z} without knowing the secret credentials related to CSP_z. Thus, ARAP-SG is resistant to the impersonation attacks.

5) ANONYMITY AND UNTRACEABLITY

Suppose that $\mathcal{A}$ captures the messages M_{SM_y} : $\{TM_a, U3, CT3, Auth3, PUB_{SM_y}\}$ and M_{CSP_z} :$\{TM_b, CT4, Auth5\}$ and strives to get actual identities PID_y and ID_{CSP_z} of SM_y and CSP_z, respectively. The real identifies of SM_y and CSP_z are protected using the hash function and encryption algorithm. Thus, $\mathcal{A}$ is unable to extricate the real identities of SM_y and CSP_z. In addition the communicated message are dynamic and $\mathcal{A}$ canot establish correlation between the messages expropriated from two different AKE sessions. Hence, ARAP-SG ensure the anonymity and untraceablity features.

6) SM CAPTURE ATTACK

After capturing SM_y deployed in SG environment, $\mathcal{A}$ can extricate the sensitive information, such as $\{CH_y, U_2, Auth1\}$ from the memory of SM_y. However, the information stored in the memory of SM_y are in encrypted form, which are encrypted using the secret key generated by PUF function. In addition, all SM_y store unique secret credentials.

7) MITMD ATTACK

To effectuate a MITMD attack, $\mathcal{A}$ requires to produce a legitimate AKE request or response message. After capturing $M_{SM_y} : \{TM_a, U3, CT3, Auth3, PUB_{SM_y}\}$, $\mathcal{A}$ can generate a modified AKE request message,i.e, $M'_{SM_y} : \{TM'_a, U3', CT3', Auth3', PUB'_{SM_y}\}$. However, $\mathcal{A}$ cannot fabricate an authentic message without knowing the credentials $\{SEC_{CSP_z}, K1/K2, PID_{SM_y}\}$. Similarly, after capturing M_{CSP_z} :$\{TM_b, CT4, Auth5\}$, $\mathcal{A}$ cannot generate a modified message M'_{CSP_z} :$\{TM'_b, CT4', Auth5'\}$ without knowing the secret credentials associated with CSP_z. Hence, ARAP-SG can thwart MITMD attack.

8) ESL ATTACK

In ARAP-SG, the session key $SK_{SM_y}(= SK_{CSP_z}) = H(RN_a \parallel RN_b \parallel SECK_2 \parallel ID_{CSP_z} \parallel TM_a \parallel TM_b \parallel PID_y)$ is constructed by using the both the long-term secret (LOS) and ephemeral secret (EPS) credentials. Therefore, to construct a licit SK, $\mathcal{A}$ needs to compromise both LOS and EPS. However, it is infeasible for $\mathcal{A}$ to extricate both the LOS and EPS at the same time. Thus, ARAP-SG can resist the ESL attack.

9) ADAPTABLE CSP SECRET KEY UPDATE

ARAP-SG enables the CSP_z to update its long-term secret key SEC_{CSP_z} without requiring any complex mechanism. RC selects new $SEC^n_{CSP_z}$ and computes the new public key as $PUB^n_{CSP_z} = SEC^n_{CSP_z} \cdot P$. After generating the new parameters, such as $SEC^n_{CSP_z}$ and $PUB^n_{CSP_z}$ and loads these credentials in the database of CSP_z. Finally, CSP_z broadcasts the $PUB^n_{CSP_z}$ in the SG environment and all the SM_y stores the $PUB^n_{CSP_z}$ in the memory.

B. SECURITY EVALUATION USING RANDOM ORACLE MODEL

The devised ARAP-SG is investigated through ROM to verify the semantic security and determine that ARAP-SG fulfills the required and satisfactory SK security. We initially elaborate on the ROM of the designed ARAP-SG and then explain the SK security of the propounded scheme in Theorem 1. According to the ROM model of the devised ARAP-SG, the p^{th} instance of a participant $\mathcal{G}$ is designated as $\mathcal{G}_t$. Smart meter SM_y and central service provider CSP_z are defined as the entities $\mathcal{G}_{SM_y}$ and $\mathcal{G}_{CSP_z}$, and their p_1^{th}, and p_2^{th} instances are defined as $\mathcal{G}^{p1}_{SM_y}$ and $\mathcal{G}^{p2}_{CSP_z}$, respectively. In addition, collision-avoidance hash operation H(.) is represented as a random oracle HSH, available to all participants in the ROM. Moreover, the ROM incorporates a set of queries presented in Table 2 employed by $\mathcal{A}$ in designing an attack.

TABLE 2. ROM queries.

Query	Purpose
$Execute(\mathcal{G}^{p2}_{SM_y}, \mathcal{G}^{p3}_{CSP_j})$	$\mathcal{A}$ by accomplishing this query can commandeer all messages dispatched between SM_y and CSP_j.
$CorruptSM(\mathcal{G}^{p1}_{SM_y})$	$\mathcal{A}$ by executing this query, through PA attacks, extricate the secret parameters from SM_y's memory.
$Test(\mathcal{G}^{p1})$	$\mathcal{A}$ by accomplishing this query makes an SK request to $\mathcal{G}^{p1}$, i.e. if the requested SK is accurate or probabilistic output, procured by flipping a coin 'C.'
$Reveal(\mathcal{G}^{p1})$	$\mathcal{A}$ by accomplishing this query reveals the SK, constructed between $\mathcal{G}^{p1}$ and its associate entity.
$Send(\mathcal{G}^{p1}, MES)$	$\mathcal{A}$ by effectuating this query can effectuate an active attack by dispatching a message MES to $\mathcal{G}^{p1}$, $\mathcal{G}^{p1}$ generates a response message MES accordingly.

Definition 1: $Adv^{ECDLP}_{\mathcal{A}}(plt)$ denotes $\mathcal{A}$'s advantage in polynomial time (plt) to procure the secret key from the public of the network entity. However, the advantage of $\mathcal{A}$ in extracting SEC_{CSP_z} from the $PUB_{CSP_z} = SEC_{CSP_z} \cdot P$ is trivial and contemplated to as elliptic curve discrete logarithm problem (ECDLP).

Definition 2: The encryption algorithm is IND-CPA secure in single/multiple eavesdropper setting and $Adv^{IND-CPA}_{SE,\Omega}(l)$ or $Adv^{IND-CPA}_{ME,\Omega}(l)$ is trivial for $\mathcal{A}$ in polynomial time (plt). Here, Ω denotes an encryption algorithm (AES-CBC-256).

Theorem 1: Let $Adv^{ARAP-SG}_{\mathcal{A}}(plt)$ be $\mathcal{A}$'s advantage, executing in plt to breach the security of the SK constructed during the AKE phase of the proposed ARAP-SG. Assume HQU^2, HPF^2, $|HSH|$, $|PUF|$, $Adv^{IND-CPA}_{\mathcal{A}}(plt)$, and $Adv^{ECDLP}_{\mathcal{A}}(plt)$ represent the hash queries, PUF queries, hash output space, PUF output rage space, $\mathcal{A}$'s in breaking the security of AES-CBC-256, and $\mathcal{A}$'s in breaking the security of ECC algorithm, respectively. Then,

$$Adv^{ARAP-SG}_{\mathcal{A}}(plt) \leq \frac{HQU^2}{|HSH|} + \frac{HPF^2}{|PUF|} + 2.Adv^{IND-CPA}_{\mathcal{A}}(plt) + Adv^{ECDLP}_{\mathcal{A}}(plt). \tag{35}$$

Proof: To prove the Theorem 1, we describe five games $Game_0$, $Game_1$, $Game_2$, $Game_3$, and $Game_4$ including an event SC, where $\mathcal{A}$ guesses the bit B correctly. Moreover, we describe $\mathcal{A}$'s advantage in winning the game ($Game_0 - Game_4$) as $Adv_{\mathcal{A}} = PB[SC]$. The games $Game_0$, $Game_1$, $Game_2$, $Game_3$, and $Game_4$ are explained in details as follows.

$Game_0$:

$$Adv^{ARAP-SG}_{\mathcal{A}}(plt) = |2.PB[SC0] - 1|. \tag{36}$$

$Game_1$: $\mathcal{A}$ effectuates an active attack by executing $Execute$ and $Test$ queries, which are defined in Table 2. By using $Execute$ query, $\mathcal{A}$ can capture the communicated messages, such as $M_{SM_y} : \{TM_a, U3, CT3, Auth3, PUB_{SM_y}\}$

and M_{CSP_z} :$\{TM_b, CT4, Auth5\}$ during the AKE process. In addition, by using *Test*, $\mathcal{A}$ can determine the guessed session key is real key or a random number. However, in the proposed ARAP-SG, the session key is generated as $SK_{SM_y}(= SK_{CSP_z}) = H(RN_a \parallel RN_b \parallel SECK_2 \parallel ID_{CSP_z} \parallel TM_a \parallel TM_b \parallel PID_y)$, which is the synthesis of both LOS and EPS. Thus, to break the security of $SK_{SM_y}(= SK_{CSP_z})$, $\mathcal{A}$ needs to both LOS and EPS. In addition, from the captured messages, $\mathcal{A}$ canot derive sensitive credentials, which are used to construct SK. So, $\mathcal{A}$ cannot win the game only by capturing the communicated messages. Therefore, under eavesdropping attack both $Game_0$ and $Game_1$ remain indistinguishable. Thus, we can get

$$PB[SC0] = PB[SC1]. \tag{37}$$

$Game_2$: $\mathcal{A}$ launches an active attacks, by performing an *HSH* queries. In the proposed ARAP-SG, SM_y sends a response message $M_{SM_y} : \{TM_a, U3, CT3, Auth3, PUB_{SM_y}\}$ to CSP_z, where the parameter $U3 = (K2 \parallel PID_y) \oplus H(TM_a \parallel SECK_1)$ is protected by collision resistant hash function. Thus, $\mathcal{A}$ cannot find any collision while executing *HSH* queries. Therefore, by birthday paradox, we get

$$|PB[SC1] - PB[SC2]| \leq \frac{HQU^2}{2|HSH|}. \tag{38}$$

$Game_3$: After capturing the smart meter and executing $CorruptSM(\mathcal{G}^{p1}_{SM_y})$, $\mathcal{A}$ can extricate the sensitive information, such as $\{CH_y, U_2, Auth1\}$, which are stored in the encrypted form in the memory of SM_y. Thus, to procure the secret information, $\mathcal{A}$ need to perform PUF queries. However, PUF generates a unique response against a unique challenge. Therefore, $\mathcal{A}$ cannot find any collision, while executing the PUF queries. Hence, we get

$$|PB[SC3] - PB[SC2]| \leq \frac{HPF^2}{2|PUF|}. \tag{39}$$

$Game_4$: This is the last game wherein $\mathcal{A}$ by eavesdropping the request and response messages, such as M_{SM_y} : $\{TM_a, U3, CT3, Auth3, PUB_{SM_y}\}$ and M_{CSP_z} :$\{TM_b, CT4, Auth5\}$ tries to construct the session key. However, the parameters $CT3$ and $CT4$ of message M_{SM_y} and M_{CSP_z}, respectively are protected by encryption algorithm (AES-CBC-256). AES-CBC-256 in secure against the chosen plaintext attack (Definition 2). In addition, $\mathcal{A}$ cannot extract the long-term secret key of CSP_z from the parameter PUB_{SM_y} (Definition 1). From the Definition (1) and Definition (2), we get

$$|PB[SC3] - PB[SC4]| \leq Adv_{\mathcal{A}}^{IND-CPA}(plt) + Adv_{\mathcal{A}}^{ECDLP}(plt). \tag{40}$$

Besides, $\mathcal{A}'$s in presuming the consequence of the flipped coin B, by accomplishing the games $Game_x | x \in [0, 4]$,is as follows

$$PB[SC4] = 1/2. \tag{41}$$

From (36) and (37), we get

$$Adv_{\mathcal{A}}^{ARAP-SG}(plt) = |2.PB[SC0] - \frac{1}{2}|. \tag{42}$$

From (42), we get

$$\frac{1}{2}.Adv_{\mathcal{A}}^{ARAP-SG}(plt) = |PB[SC0] - \frac{1}{2}|. \tag{43}$$

By using (41) and (43), we obtain

$$\frac{1}{2}.Adv_{\mathcal{A}}^{ARAP-SG}(plt) = |PB[SC1] - PB[SC4]| \tag{44}$$

By using triangular inequality, we get

$$\begin{aligned} &|PB[SC1] - PB[SC4]| \\ &\quad \leq |PB[SC1] - PB[SC2]| + |PB[SC2] - PB[SC4]| \\ &\quad \leq |PB[SC1] - PB[SC2]| + |PB[SC2] - PB[SC3]| \\ &\qquad + |PB[SC3] - PB[SC4]|. \end{aligned} \tag{45}$$

By using (38), (39), (40), and (45), we get

$$\begin{aligned} Adv_{\mathcal{A}}^{ARAP-SG}(plt) \leq{}& \frac{HQU^2}{|HSH|} + \frac{HPF^2}{|PUF|} \\ &+ 2.Adv_{\mathcal{A}}^{IND-CPA}(plt) + Adv_{\mathcal{A}}^{ECDLP}(plt). \end{aligned} \tag{46}$$

□

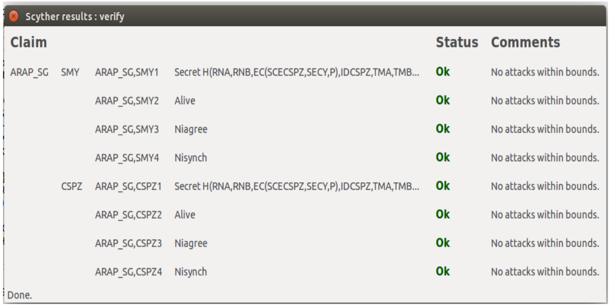
C. SCYTHER-BASED ANALYSIS

Scyther is a software tool used to validate the resiliency of the proposed security protocol against various security attacks. In addition, Scyther explicates the security vulnerability in the tested security protocol. Thus, we employed the Scyther tool to validate the security of the proposed ARAP-SG. Scyther uses the security protocol description language (SPDL) for the implementation of security protocol. SPDL is a python-like language. We coded ARAP-SG using the SPDL language.

In the SPDL script, we have defined two roles, such as SMY and CSPZ. Each role has some manually defined claims and some automatically generated roles. Manually specified claim for SMY is $claim(SMY, Secret, SEK)$ and CSPZ is $claim(CSPZ, Secret, SEK)$, which are validated by the Scyther, as shown in Fig. 3. Moreover, the claims for the role SMY, such as $claim(SMY, Alive)$, $claim(SMY, Nisynch)$, and $claim(SMY, Niagree)$ are validated by Scyther. Similarly, same type of claims are also validated by Scyther for role CSPZ, as demonstrated in Fig. 3.

VI. RESULTS AND DISCUSSION

We compare the proposed ARAP-SG with the relevant AKE schemes, such as Ashraf *et al.* [6], Dariush *et al.* [10], Vangala *et al.* [15], Bera *et al.* [7], Jangirala *et al.* [13], Garg *et al.* [32], and Odelu *et al.* [33] devised for the SG system. We consider performance metrics, such as the computational and communication costs, to evaluate the efficacy of ARAP-SG and the relevant security schemes.



Claim				Status	Comments
ARAP_SG	SMY	ARAP_SG,SMY1	Secret H(RNA,RNB,EC(SCECSPZ,SECY,P),IDCSPZ,TMA,TMB...	Ok	No attacks within bounds.
		ARAP_SG,SMY2	Alive	Ok	No attacks within bounds.
		ARAP_SG,SMY3	Niagree	Ok	No attacks within bounds.
		ARAP_SG,SMY4	Nisynch	Ok	No attacks within bounds.
	CSPZ	ARAP_SG,CSPZ1	Secret H(RNA,RNB,EC(SCECSPZ,SECY,P),IDCSPZ,TMA,TMB...	Ok	No attacks within bounds.
		ARAP_SG,CSPZ2	Alive	Ok	No attacks within bounds.
		ARAP_SG,CSPZ3	Niagree	Ok	No attacks within bounds.
		ARAP_SG,CSPZ4	Nisynch	Ok	No attacks within bounds.

Done.

FIGURE 3. Security evaluation using Scyther.

TABLE 3. Estimated time for different cryptographic primitives.

Notation	Computational cost (P1)	Computational cost (P2)
T_{ha}	0.3421 ms	0.311/0.343
T_{enc}	0.550 ms	0.150 ms
T_{ecc}	2.94 ms	0.72 ms
T_{eca}	0.135 ms	0.0235 ms
T_{bh}	0.301 ms	0.0401 ms
T_{bp}	8.123 ms	4.42 ms
T_{exp}	1.42 ms	0.042 ms
T_{pf}	0.59 μs	-

To simulate SM_y, we used the platform "Ubuntu LTS-16.4, Raspberry Pi-3 with "Ubuntu LTS-16.4", Quad-Core @1.2 Ghz, and 1-GB of RAM". Similarly, system "Core-i5" with processor @2.6 Ghz, operating system "Ubuntu LTS-16.4" and 4-GB of RAM is used to simulate CSP_z. In addition, Python-based library "PyCrypto" to determine the computational costs of various cryptographic primitives. All the computational costs of different primitives is given in Table 3.

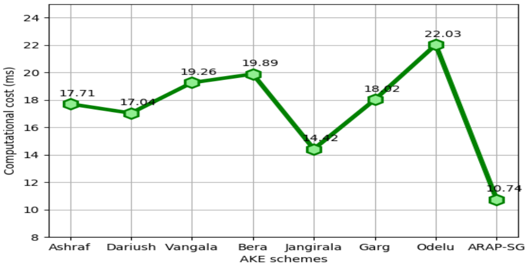


FIGURE 4. Computational cost required to complete the AKE phase.

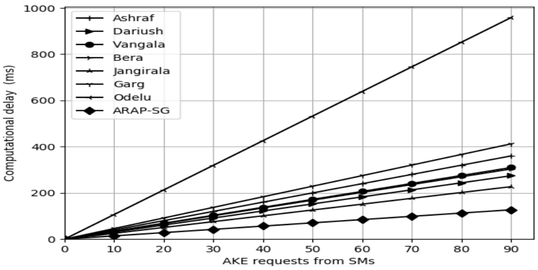


FIGURE 5. *CSP_z* computational cost with increasing the number of users.

A. COMPUTATIONAL COST

We denote computational time of "ECC point multiplication", "ECC point addition", "bi-linear paring", "modular exponentiation", "PUF", "hash function BLAKE", and "hash function SHA-160" by T_{ecc}, T_{eca}, T_{bp}, T_{bh}, T_{exp}, T_{pf}, and T_{sh}. To determine the computational cost, we use the computational complexities of various cryptographic primitives presented in Table 3. The computational cost at SM_y, CSP_z and total computational cost is given in Table 4. The Computational at SM_y is 9.3 ms, which is 32.17%, 33.57%, 41.14%, 43.64%, 30.6%, 18.42%, and 17.7% lower than Ashraf *et al.* [6], Dariush *et al.* [10], Vangala *et al.* [15], Bera *et al.* [7], Jangirala *et al.* [13], Garg *et al.* [32], and Odelu *et al.* [33], respectively. In addition, the computational cost at CSP_z is 1.4 ms, which is 64.1%, 53.95%, 58.82%, 58.46%, 44%, 70.83%, and 86.79% lower than the state-of-the-art AKE schemes. ARAP-SG's estimated total computational cost is 12 ms, which is 39.36%, 36.97%, 44.24%, 46%, 25.52%, 42.93%, 51.25%, and 56.76% lower than the state-of-the-art AKE schemes. CSP_z is the main component of the SG system, which keeps the sensitive information associated with SM_y and is responsible for verifying the authenticity of SM_y. Therefore, it is imperative to reduce the computational cost at CSP_z when a large number of SM_y send AKE messages to CSP_z. Fig. 5 shows the relationship between the number of users and computational cost.

B. SECURITY FEATURES

This subsection renders the comparative analysis of the security features of ARAP-SG and the other related AKE schemes. The analysis of the security features are presented in Table 5. The scheme of Ashraf *et al.* [6] cannot withstand the device capture attack. The scheme of Ashraf *et al.* cannot ensure the secure certificate computation. Dariush *et al.* [10] susceptible to MITMD eavesdropping, information leakage, and impersonation attacks. Additionally, the scheme Dariush *et al.* cannot provide unlinkability and anonymity features, Vangala *et al.* [15] susceptible to de-synchronization attack, Bera *et al.* [7] susceptible to de-synchronization attack and does not render the certificate anonymity which leads to the traceablity of the smart meter, Jangirala *et al.* [13] susceptible to MITMD eavesdropping, information leakage, and impersonation attacks. Additionally, the scheme Jangirala *et al.* cannot provide unlinkability and anonymity features, Garg *et al.* [32] unable to impede device impersonation attack, and Odelu *et al.* [33] susceptible to MITMD eavesdropping, information leakage, and impersonation attacks. Additionally, the scheme Odelu *et al.* cannot provide unlinkability and anonymity features. However, the scheme of ARAP-SG is unable to resist the aforementioned security threats and renders enhanced security features.

C. COMMUNICATION COST

The communication cost refers to number message exchanged to accomplish the AKE phase. Reducing the communication cost is salient objective of the devised AKE scheme. In the proposed ARAP-SG, two AKE messages

TABLE 4. An analysis of the computational cost.

AKE Scheme	SM_y Side	CSP_z Side	Total Time
Ashraf *et al.* [6]	$4T_{ha} + 4T_{ecc} + 2T_{eca} \approx 13.71\ ms$	$4T_{ha} + 5T_{ecc} \approx 3.9\ ms$	$8T_{ha} + 9T_{ecc} + 2T_{eca} \approx 17.71\ ms$
Dariush *et al.* [10]	$5T_{ha} + 5T_{ecc} + T_{eca} \approx 14\ ms$	$T_{ha} + 4T_{ecc} + T_{eca} \approx 3.04\ ms$	$9T_{ha} + 9T_{ecc} + 2T_{eca} \approx 17.04\ ms$
Vangala *et al.* [15]	$9T_{ha} + 4T_{ecc} + 2T_{eca} \approx 15.8\ ms$	$9T_{ha} + 4T_{ecc} + 2T_{eca} \approx 3.4\ ms$	$18T_{ha} + 8T_{ecc} + 4T_{eca} \approx 19.26\ ms$
Bera *et al.* [7]	$11T_{ha} + 4T_{ecc} + T_{eca} \approx 16.5\ ms$	$11T_{ha} + 4T_{ecc} + T_{eca} \approx 3.37\ ms$	$11T_{ha} + 8T_{ecc} + 2T_{eca} \approx 19.89\ ms$
Jangirala *et al.* [13]	$16T_{ha} + 5T_{ecc} + 2T_{eca} \approx 11.9\ ms$	$11T_{ha} + 3T_{ecc} + T_{eca} \approx 2.5\ ms$	$35T_{ha} + 11T_{ecc} + 4T_{eca} + T_B \approx 14.42\ ms$
Garg *et al.* [32]	$7T_{ha} + 3T_{ecc} + T_{eca} \approx 13.4\ ms$	$7T_{ha} + 3T_{ecc} + T_{eca} \approx 4.8\ ms$	$14T_{ha} + 6T_{ecc} + 2T_{eca} \approx 18.82\ ms$
Odelu *et al.* [33]	$6T_{ha} + 2T_{ecc} + T_{eca} + T_{exp} \approx 11.3\ ms$	$6T_{ha} + 2T_{ecc} + T_{eca} + T_{exp} + T_{bp} \approx 10.6\ ms$	$12T_{ha} + 4T_{ecc} + 2T_{eca} + 2T_{exp} + T_{bp} \approx 22.03\ ms$
ARAP-SG	$6T_{bh} + 3T_{enc} + 2T_{ecc} + T_{pf} \approx 9.3\ ms$	$6T_{bh} + T_{ecc} + 3T_{enc} \approx 1.4\ ms$	$12T_{bh} + 3T_{ecc} + 6T_{enc} \approx 10.74\ ms$

TABLE 5. An analysis of the security features.

AKE Scheme	SF1	SF2	SF3	SF4	SF5	SF6	SF7	SF8	SF9	SF10	SF11	SF12
Ashraf *et al.* [6]	✓	×	✓	×	✓	✓	✓	✓	✓	✓	✓	×
Dariush [10]	×	✓	✓	✓	✓	✓	✓	✓	✓	×	✓	×
Vangala *et al.* [15]	✓	✓	×	✓	✓	✓	✓	✓	✓	✓	✓	-
Bera *et al.* [7]	✓	✓	×	✓	✓	✓	✓	✓	×	✓	✓	×
Jangirala *et al.* [13]	×	✓	✓	✓	✓	×	✓	✓	×	×	✓	×
Garg *et al.* [32]	✓	✓	✓	✓	✓	×	✓	✓	✓	✓	✓	×
Odelu *et al.* [33]	×	✓	✓	✓	✓	✓	✓	✓	×	×	✓	×
ARAP-SG	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

Note: SF1: MITMD attack, SF2: SM/Device capture attack, SF3: Replay attack, SF4: Secure certificate computation, SF5: MA, SF6: SM/IoT node impersonation attack, SF7: Eavesdropping attack , SF8: DoS, SF9: SM anonymity, SF10: Untraceablity, SF11: New SM addition phase, SF12: DS phase, ✓: Signifies available feature; × : indicates the feature not available

TABLE 6. An analysis of the communication cost.

AKE Scheme	Transmitted Message to Accomplish the AKE Phase	Total
Ashraf *et al.* [6]	$SM_y \xrightarrow{1152} CSP_z \xrightarrow{512} CSP_z$	**1664 bits**
Dariush *et al.* [10]	$SM_y \xrightarrow{2016} CSP_z \xrightarrow{512} SM_y$	**2528 bits**
Vangala *et al.* [15]	$SM_y \xrightarrow{928} CSP_z \xrightarrow{1088} SM_yCSP_z \xrightarrow{288} CSP_z$	**2304 bits**
Bera *et al.* [7]	$SM_y \xrightarrow{1184} CSP_z \xrightarrow{1280} CSP_z \xrightarrow{288} SM_y \xrightarrow{288} CSP_z$	**3040 bits**
Jangirala *et al.* [13]	$SM_y \xrightarrow{352} CSP_z \xrightarrow{832} CSP_z \xrightarrow{672} SM_y$	**1856 bits**
Garg *et al.* [32]	$SM_y \xrightarrow{864} CSP_z \xrightarrow{928} SM_y$	**1792 bits**
Odelu *et al.* [33]	$SM_y \xrightarrow{1088} CSP_z \xrightarrow{672} SM_y \xrightarrow{160} CSP_z$	**1920 bits**
ARAP-SG	$SM_y \xrightarrow{992} CSP_z \xrightarrow{544} SM_y$	**1536 bits**

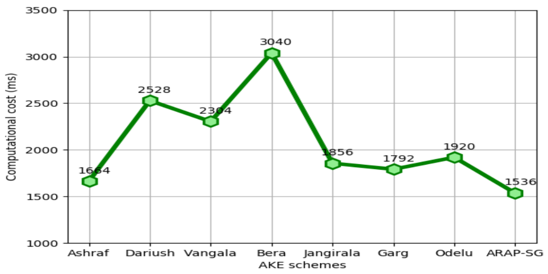


FIGURE 6. Communication cost needed to accomplish the AKE phase.

are exchange, such as M_{SM_y} : $\{TM_a, U3, CT3, Auth3, PUB_{SM_y}\}$ of size 864 bits and M_{CSP_z} :$\{TM_b, CT4, Auth5\}$ of size 544 bits. Total estimated communication cost is $\{992 + 544\} = 1536$ bits. The scheme of Ashraf *et al*. [6], Dariush *et al*. [10], Vangala *et al*. [15], Bera *et al*. [7], Jangirala *et al*. [13], Garg *et al*. [32], and Odelu *et al*. [33] require 1664 bits, 2528 bits, 2304 bits, 3040 bits, 1856 bits, 1792 bits, 1920 bits, and 3552 bits, respectively, which are 7.69%, 39.24%, 33.33%, 49.47%, 17.24%, 14.29%, and 20% higher than ARAP-SG. Table 6 and Fig. 6 present the comparative analysis of communication of ARAP-SG and the relevant AKE schemes. ARAP-SG incurs less communication cost than the related security scheme devised for the SG system.

VII. CONCLUSION

IoT devices in the SG environment transmit sensitive information to central server through an open channel. The channel is exposed to various security threats including information modification, which can potentially disrupt the streamlined operation of the SG system. To protect the integrity of information communicated between SM and CSP in SG system, we have introduced an ECC-based secure AKE protocol in this paper, called ARAP-SG. ARAP-SG enables CSP and SM to establish an SK after accomplishing the mutual authentication. We conducted the ROM-based and Scyther-based formal analysis to explicate that the ARAP-SG is secure. In addition, the informal security analysis confirms that ARAP-SG can withstand various security threats that can degrade the smooth operation of the SG system. Finally, ARAP-SG is contrasted with relevant AKE protocol to show that ARAP-SG requires fewer resources while rendering improved security functionalities.

ACKNOWLEDGMENT

The authors would like to thank King Khalid University of Saudi Arabia for supporting this research under the grant number R.G.P. 1/365/42.

REFERENCES

[1] P. Kumar, Y. Lin, G. Bai, A. Paverd, J. S. Dong, and A. Martin, "Smart grid metering networks: A survey on security, privacy and open research issues," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 3, pp. 2886–2927, 3rd Quart., 2019.
[2] Z. El Mrabet, N. Kaabouch, H. El Ghazi, and H. El Ghazi, "Cyber-security in smart grid: Survey and challenges," *Comput. Elect. Eng.*, vol. 67, pp. 469–482, Apr. 2018.
[3] M. Z. Gunduz and R. Das, "Cyber-security on smart grid: Threats and potential solutions," *Comput. Netw.*, vol. 169, Mar. 2020, Art. no. 107094.
[4] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao, "A survey on Internet of Things: Architecture, enabling technologies, security and privacy, and applications," *IEEE Internet Things J.*, vol. 4, no. 5, pp. 1125–1142, Oct. 2017.
[5] M. B. Mollah, J. Zhao, D. Niyato, K.-Y. Lam, X. Zhang, A. M. Y. M. Ghias, L. H. Koh, and L. Yang, "Blockchain for future smart grid: A comprehensive survey," *IEEE Internet Things J.*, vol. 8, no. 1, pp. 18–43, Jan. 2021.
[6] 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.
[7] B. Bera, S. Saha, A. K. Das, and A. V. Vasilakos, "Designing blockchain-based access control protocol in IoT-enabled smart-grid system," *IEEE Internet Things J.*, vol. 8, no. 7, pp. 5744–5761, Apr. 2021.
[8] H. M. S. Badar, S. Qadri, S. Shamshad, M. F. Ayub, K. Mahmood, and N. Kumar, "An identity based authentication protocol for smart grid environment using physical uncloneable function," *IEEE Trans. Smart Grid*, vol. 12, no. 5, pp. 4426–4434, Sep. 2021.
[9] M. Tanveer, A. U. Khan, N. Kumar, A. Naushad, and S. A. Chaudhry, "A robust access control protocol for the smart grid systems," *IEEE Internet Things J.*, early access, Sep. 17, 2021, doi: 10.1109/JIOT.2021.3113469.
[10] D. Abbasinezhad-Mood and M. Nikooghadam, "An anonymous ECC-based self-certified key distribution scheme for the smart grid," *IEEE Trans. Ind. Electron.*, vol. 65, no. 10, pp. 7996–8004, Oct. 2018.

[11] D. Abbasinezhad-Mood, A. Ostad-Sharif, M. Nikooghadam, and S. M. Mazinani, "A secure and efficient key establishment scheme for communications of smart meters and service providers in smart grid," *IEEE Trans. Ind. Informat.*, vol. 16, no. 3, pp. 1495–1502, Mar. 2020.

[12] A. K. Das, B. Bera, S. Saha, N. Kumar, I. You, and H.-C. Chao, "AI-envisioned blockchain-enabled signature-based key management scheme for industrial cyber-physical systems," *IEEE Internet Things J.*, early access, Sep. 1, 2021, doi: 10.1109/JIOT.2021.3109314.

[13] J. Srinivas, A. K. Das, X. Li, M. K. Khan, and M. Jo, "Designing anonymous signature-based authenticated key exchange scheme for Internet of Things-enabled smart grid systems," *IEEE Trans. Ind. Informat.*, vol. 17, no. 7, pp. 4425–4436, Jul. 2021.

[14] D. Wu and C. Zhou, "Fault-tolerant and scalable key management for smart grid," *IEEE Trans. Smart Grid*, vol. 2, no. 2, pp. 375–381, Jun. 2011.

[15] A. Vangala, A. K. Sutrala, A. K. Das, and M. Jo, "Smart contract-based blockchain-envisioned authentication scheme for smart farming," *IEEE Internet Things J.*, vol. 8, no. 13, pp. 10792–10806, Jul. 2021.

[16] X. Li, F. Wu, S. Kumari, L. Xu, A. K. Sangaiah, and K.-K.-R. Choo, "A provably secure and anonymous message authentication scheme for smart grids," *J. Parallel Distrib. Comput.*, vol. 132, pp. 242–249, Oct. 2019.

[17] L. Wu, J. Wang, S. Zeadally, and D. He, "Anonymous and efficient message authentication scheme for smart grid," *Secur. Commun. Netw.*, vol. 2019, p. 12, May 2019.

[18] M. Tanveer, G. Abbas, Z. H. Abbas, M. Waqas, F. Muhammad, and S. Kim, "S6AE: Securing 6LoWPAN using authenticated encryption scheme," *Sensors*, vol. 20, no. 9, p. 2707, May 2020.

[19] M. Tanveer, G. Abbas, and Z. H. Abbas, "LAS-6LE: A lightweight authentication scheme for 6LoWPAN environments," in *Proc. 14th Int. Conf. Open Source Syst. Technol. (ICOSST)*, Dec. 2020, pp. 1–6.

[20] M. Tanveer, A. H. Zahid, M. Ahmad, A. Baz, and H. Alhakami, "LAKE-IoD: Lightweight authenticated key exchange protocol for the Internet of drone environment," *IEEE Access*, vol. 8, pp. 155645–155659, 2020.

[21] M. Tanveer, G. Abbas, Z. H. Abbas, M. Bilal, A. Mukherjee, and K. S. Kwak, "LAKE-6SH: Lightweight user authenticated key exchange for 6LoWPAN-based smart Homes," *IEEE Internet Things J.*, early access, Jun. 3, 2021, doi: 10.1109/JIOT.2021.3085595.

[22] M. Tanveer, A. U. Khan, N. Kumar, and M. M. Hassan, "RAMP-IoD: A robust authenticated key management protocol for the Internet of Drones," *IEEE Internet Things J.*, early access, Jun. 4, 2021, doi: 10.1109/JIOT.2021.3084946.

[23] 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.

[24] 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, Nov. 2019, Art. no. e4137.

[25] 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 Generat. Comput. Syst.*, vol. 81, pp. 557–565, Apr. 2018.

[26] 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.

[27] A. A. Khan, V. Kumar, M. Ahmad, S. Rana, and D. Mishra, "PALK: Password-based anonymous lightweight key agreement framework for smart grid," *Int. J. Electr. Power Energy Syst.*, vol. 121, Oct. 2020, Art. no. 106121.

[28] S. A. Chaudhry, "Correcting 'PALK: Password-based anonymous lightweight key agreement framework for smart grid,'" *Int. J. Electr. Power Energy Syst.*, vol. 125, Feb. 2021, Art. no. 106529.

[29] A. A. Khan, V. Kumar, M. Ahmad, and S. Rana, "LAKAF: Lightweight authentication and key agreement framework for smart grid network," *J. Syst. Archit.*, vol. 116, Jun. 2021, Art. no. 102053.

[30] S. Yu, K. Park, J. Lee, Y. Park, Y. Park, S. Lee, and B. Chung, "Privacy-preserving lightweight authentication protocol for demand response management in smart grid environment," *Appl. Sci.*, vol. 10, no. 5, p. 1758, Mar. 2020.

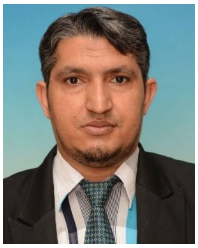
[31] A. Irshad, S. A. Chaudhry, M. Alazab, A. Kanwal, M. Sultan Zia, and Y. B. Zikria, "A secure demand response management authentication scheme for smart grid," *Sustain. Energy Technol. Assessments*, vol. 48, Dec. 2021, Art. no. 101571.

[32] S. Grag, K. Kaur, G. Kaddoum, and K.-K. R. Choo, "Toward secure and provable authentication for Internet of Things: Realizing industry 4.0," *IEEE Internet Things J.*, vol. 7, no. 5, pp. 4598–4606, May 2020.

[33] 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.

MUHAMMAD TANVEER received the B.S. degree in electronics from GCU Lahore, Pakistan, and the M.S. degree in computer science from the Institute of Management of Sciences (IMS), Lahore, in 2017. He is currently pursuing the Ph.D. degree with the Faculty of Computer Sciences and Engineering. His current research interests include remote user authentication, cyber security, security and privacy, cryptography, the Internet of Things, 6LoWPAN, and the Internet of Drone.

ABD ULLAH KHAN (Member, IEEE) received the B.S. degree (Hons.) in telecommunication from UST Bannu, in 2013, the M.S. degree in electrical engineering from COMSATS University Islamabad, in 2016, and the Ph.D. degree from the GIK Institute of Engineering sciences and Technology, Pakistan, in 2021. Part of his Ph.D. degree is from the National University of Sciences and Technology, Islamabad. He is currently working as an Assistant Professor with the National University of Science and Technology (NUST), Pakistan. He is an Active Member of the Telecommunications and Networking Research Center, GIK Institute, Pakistan, and the High Speed Networks Laboratory, NCTU, Taiwan. His research interests include resource allocation and management in wireless networks, artificial intelligence, and network security. He was a recipient of the prestigious scholarship of Higher Education Commission of Pakistan for M.S. and Ph.D. He is an Active Reviewer of IEEE Networks, IEEE Internet of Things Journal, IEEE Systems Journal, IEEE Access, and *Computer Communications*.



HABIB SHAH received the Ph.D. degree from the Faculty of Computer Science and Information Technology, University Tun Hussein Onn Malaysia, in 2013. He is currently an Assistant Professor with the Department of Computer Science, College of Computer Science, King Khalid University, Saudi Arabia. He has successfully published more than 40 articles in various international SCI and Scopus journals and conference proceedings. His research interests include artificial intelligence, learning algorithms, data mining techniques, time series analysis, and numerical optimization. He is a member of an editorial board, a guest editor, and acts as a reviewer for various journals and conferences as well. He has also served as a program committee member and a co-organizer for numerous international conferences/workshops. He is also working on three research projects of KKU and KSA.

AHMED ALKHAYYAT (Member, IEEE) received the B.Sc. degree in electrical engineering from Al Kufa University, Najaf, Iraq, in 2007, the M.Sc. degree from the Dehradun Institute of Technology, Dehradun, India, in 2010, and the Ph.D. degree from Cankaya University, Ankara, Turkey, in 2015. He is currently the Dean of International Relationship and a Manager of the word ranking with Islamic University, Najaf. His research interests include the IoT in the health-care systems, SDN, network coding, cognitive radio, efficient-energy routing algorithms, and efficient-energy MAC protocol in cooperative wireless networks and wireless body area networks, as well as cross-layer designing for self-organized networks. He contributed in organizing a several IEEE conferences, workshop, and special sessions. To serve his community, he acted as a reviewer for several journals and conferences.

SHEHZAD ASHRAF CHAUDHRY received the master's and Ph.D. degrees (Hons.).

He is currently an Associate Professor with the Department of Computer Engineering, Faculty of Engineering and Architecture, Istanbul Gelisim University, Istanbul, Turkey. Before this, he worked as an Associate Professor of computer science with the University of Sialkot, and International Islamic University, Islamabad, Pakistan. He was awarded gold medal for achieving maximum distinction of 4/4 CGPA in his master's. He is working in the field of information and communication security, he has published extensively in prestigious venues, such as *IEEE Communication Standards Magazine*, IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, IEEE INTERNET OF THINGS JOURNAL, IEEE TRANSACTIONS ON INDUSTRY APPLICATIONS, IEEE TRANSACTIONS ON RELIABILITY, *ACM Transactions on Internet Technology*, *Sustainable Cities and Society* (Elsevier), *FGCS*, *IJEPES*, and *Computer Networks*. Over 125 publications and with an H-index of 31, i-10 index of 66, and accumulate impact factor of 260+, he has published more than 100 SCI/E indexed manuscripts and has been cited 2800+ times. He has also supervised more than 40 graduate students in their research. In 2018, considering his research, Pakistan Council for Science and Technology granted him the Prestigious Research Productivity Award, while affirming him among Top Productive Computer Scientist in Pakistan. Recently, he is listed among Top 2% Computer Scientists across the world in Stanford University's report. His current research interests include lightweight cryptography, elliptic/hyper elliptic curve cryptography, multimedia security, e-payment systems, MANETs, SIP authentication, smart grid security, IP multimedia subsystems, and next generation networks. He occasionally writes on issues of higher education in Pakistan.

MUSHEER AHMAD received the B.Tech. and M.Tech. degrees from the Department of Computer Engineering, Aligarh Muslim University, India, in 2004 and 2008, respectively, and the Ph.D. degree in chaos-based cryptography from the Department of Computer Engineering, Jamia Millia Islamia, New Delhi, India. From 2007 to 2010, he worked with the Department of Computer Engineering, Aligarh Muslim University. Since 2011, he has been working as an Assistant Professor with the Department of Computer Engineering, Jamia Millia Islamia. He has published over 85 research papers in international reputed refereed journals and conference proceedings of the IEEE/Springer/Elsevier. He has more than 1600 citations of his research works with an H-index of 24. His research interests include multimedia security, chaos-based cryptography, cryptanalysis, machine learning for security, image processing, and optimization techniques. He has served as a reviewer and a technical program committee member of many international conferences. He has also served as referee of some renowned journals, such as *Information Sciences*, *Signal Processing*, *Journal of Information Security and Applications*, IEEE JOURNAL OF SELECTED AREAS IN COMMUNICATIONS, IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS FOR VIDEO TECHNOLOGY, IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, IEEE TRANSACTIONS ON PATTERN ANALYSIS AND MACHINE INTELLIGENCE, IEEE TRANSACTIONS ON NEURAL NETWORKS AND LEARNING SYSTEMS, IEEE TRANSACTIONS ON NANOBIOSCIENCE, IEEE MULTIMEDIA, IEEE ACCESS, *Wireless Personal Communications*, *Neural Computing and Applications*, *International Journal of Bifurcation and Chaos*, *Chaos Solitons & Fractals*, *Physica A*, *Signal Processing: Image Communication*, *Neurocomputing*, *IET Information Security*, *IET Image Processing, Security and Communication Networks*, *Optik, Optics and Laser Technology*, *Complexity*, *Computers in Biology and Medicine*, *Computational and Applied Mathematics*, and *Concurrency and Computation*.

• • •