IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received November 15, 2020, accepted December 11, 2020, date of publication December 21, 2020, date of current version January 7, 2021.

Digital Object Identifier 10.1109/ACCESS.2020.3046367

A Provably Secure Lightweight Subtree-Based Short Signature Scheme With Fuzzy User Data Sharing for Human-Centered IoT

CHANDRASHEKHAR MESHRAM[1], AHMED ALSANAD[2], JITENDRA V. TEMBHURNE[3], SHAILENDRA W. SHENDE[4], KAILASH WAMANRAO KALARE[5], SARITA GAJBHIYE MESHRAM[6,7], MUHAMMAD AZEEM AKBAR[8], AND ABDU GUMAEI[2]

[1]Department of Post Graduate Studies and Research in Mathematics, Jayawanti Haksar Government Post Graduation College of Chhindwara University, Betul 460001, India
[2]STC's Artificial Intelligence Chair, Department of Information Systems, College of Computer and Information Sciences, King Saud University, Riyadh 11451, Saudi Arabia
[3]Department of Computer Science and Engineering, Indian Institute of Information Technology, Nagpur 440006, India
[4]Department of Information Technology, Yeshwantrao Chavan College of Engineering, Nagpur 441110, India
[5]Department of Computer Science and Engineering, PDPM Indian Institute of Information Technology, Design, and Manufacturing, Jabalpur 482005, India
[6]Department for Management of Science and Technology Development, Ton Duc Thang University, Ho Chi Minh City 700000, Vietnam
[7]Faculty of Environment and Labour Safety, Ton Duc Thang University, Ho Chi Minh City 700000, Vietnam
[8]College of Computer Science and Technology, Nanjing University of Aeronautics and Astronautics, Nanjing 210023, China

Corresponding authors: Chandrashekhar Meshram (cs_meshram@rediffmail.com) and Ahmed Alsanad (aasanad@ksu.edu.sa)

The authors are grateful to the Deanship of Scientific Research, King Saud University for funding through Vice Deanship of Scientific Research Chairs.

ABSTRACT Internet of Things (IoT) is made up of various smart devices for the exchange of sensed data through online services. Direct contact with people through smart devices to define parameters for healthcare and send them to a centralized repository. At the time of data exchange, messages need to be secure between a source (sender) and target (receiver) in order to confront human malicious attacks. Various signature-based schemes are presented in the literature to provide secure communication. Smart apps, however, require lightweight activities by maintaining critical security strengths. The key challenge in signature-based methods is more incurred computational expense for signing and checking process involving large numbers. In this article, a new lightweight provably secure partial discrete logarithm (DL) based subtree-based short signature with fuzzy user data sharing for human-centered IoT systems is introduced and it's security analysis is demonstrated on random oracle (RO) model. The presented scheme provides assurance of better security than other standing short-signature schemes. For low-storage, low-computation environments and low-bandwidth communication, the presented new provably secure and lightweight subtree-based short-signature scheme is needed. The results demonstrate the strength of proposed scheme, as opposed to existing works.

INDEX TERMS Fuzzy user data sharing, IoT, identity-based signature scheme, partial discrete logarithm, probability security analysis, subtree.

I. INTRODUCTION

In the past, we had witnessed so much development in the security aspects related to numerous domains such as e-commerce, healthcare, IoT, industrial IoT, and cloud computing, etc. Variety of cryptographic algorithms are presented in various domains to satisfy the essential security needs by the users or organizations. Initially, public-key cryptography (PKC) was adopted to offer the security wherein public-key is shared amongst all the users. The message exchange is stared after the generation of key pairs (*encryption, signature*), the certificate request is submitted with identity proof to CA (certificate authority), and hence receive certificates signed by CA for authentication to exchange messages in

The associate editor coordinating the review of this manuscript and approving it for publication was Constantinos Marios Angelopoulos.

encrypted form. In these process lots of time is consumed and is vulnerable to attacks, also prohibiting the users to communicate. Due to this, new technique is invented to overcome the drawbacks of PKC by ID-based cryptography (IBC) [1]. In IBC, the user's unique identity serves the purpose of public-key without managing the certificates for authentication. Eventually, it was observed that the technique was not able to handle identity-based encryption (IBE). In [2] and [3] the realization and applicability of IBC is investigated and all the problems in [1] were resolved. However, this attracted the researchers to investigate and apply the IBC to provide security in wide range of domains.

Subsequently, IBC is employed for the technique of key distribution, digital signature, and identification of a user by using the DL [4]. The modular p (i.e. large prime) operations are utilized in aforementioned technique. User identification technique is applied for authenticating the user, the authenticity of a message is verified by digital signature, and to achieve secure communication amongst the users, key distribution scheme is applied. To realize the applicability of IBC, basically in key agreement, signature, and encryption schemes towards to provide the security and efficiency is systematically presented in [5]. However, identity of the user (e.g. email or MAC address) as a public-key is utilized, no public-key repository is maintained, and verification of signature and encryption of a message is performed by the sender, and receiver identity is offered by the IBC. Hence, ID-based cryptography is significantly efficient over the primitive PKC wherein key distribution is not seamless. Nevertheless, to provide security to grid, ID-based cryptography is used to address the problem of grid authentication [6] which is currently based on traditional PKI (public-key infrastructure). Private Key is generated using ID-based signature (IBS) at the time of grid authentication to avoid proxy key generation. However, the security scheme suffers from escrow problem of private key and heavy computation by private key generators (PKGs), and associations of PKGs. Furthermore, ID-based cryptosystem is presented [7] which utilizes integer factorization (IF) and generalized DL to offer more security in the implemented system. The system is strictly fulfilling an original concept of Shamir and no communication before the data exchange. Also, system requires fewer operations for encryption/decryption which proves the efficiency and the strength of system is lies in unsolvability of DL and IF.

Nevertheless, focus is shifting from IoT devices to human centered IoT (HC-IoT) devices where social and technical methods are applied to IoT [8]. The problems in HC-IoT is to design, deploy, and support various IoT components in the context of human interpretation and suitability to adapt the IoT ecosystem. Due to humanize IoT [9], [10] the challenge exist to provide security and privacy of data exchange amongst the IoT devices, specifically HC-IoT. Moreover, popularity of IoT is increasing over the period and hence to provide all essential IoT security measures such as confidentiality, security, privacy, and data protection need to be carefully handle [11], [12]. This motivates to investigate and present the security method in human centered IoT using the combination of best security techniques.

A. OUR CONTRIBUTION

From the literature, we identified that the current identity-based signature schemes built by using DL are not secure. In this paper, we recommend a provably secure IBSS protocol to resolve the problem of partial DL, where an improvement uses the variation in [13]. Specifically, we exhibit that in our protocol, it is difficult to solve partial DL problem. This paper presents a provably secure lightweight subtree-based short signature scheme (SSSS) utilizing partial DL with fuzzy user data sharing in HC-IoT targeting smart devices. It utilizes less comprehensive operations built on partial discrete logarithm to produce the credentials for security during verification and signing phase. The scheme is demonstrated with exemplary simple values obtained in the various steps to display proof of notion.

Also, we discussed security validation for SSS under EUF-ST-CMA i.e. existential unforgeability on adaptive chosen message/subtree attacks utilizing Forking Lemma [14] proposed in [15] in RO, which we suggest that our SSS protocol enhanced the security guarantees related to existing partial discrete logarithm-based signature sachems. The presented SSS is not utilizing pairings operations for achieving higher efficiency and direct execution. Also, it does not rely on the hardness of pairing-based cryptosystem. So, all the pairing operations are not needed in the protocol. This reduces an overheads of computation and communication, and coordination along with increased flexibility compared to current comprehensive operations based on real number in DSA-based schemes.

B. ROAD MAP OF THIS PAPER

The rest of this article is composed as takes after: Related work is discussed in Section 2. Section 3 highlights the related background and mathematical formulation for the proposal of security protocol. The proposed IBSS protocol is presented in Section 4 which utilizes partial DL. Security investigation and validations are presented in Section 5 related to proposed protocol. Section 6 illustrates the analysis of comparison of other similar recent schemes with the proposed schemes. Lastly, Section 7 concludes the article.

II. RELATED WORKS

Numerous method has been proposed on IBC to provide the probable security in various domains. In cryptography scheme, disclosure of private key leads to security threat and whole system will collapse. This is the major challenge to cryptography. So, key insulation with aggregate signature using IBC is introduced in [18] for mobile devices where bilinear pairing is utilized over elliptic curve environment. The exposure of a private key is easily handle without compromising the security over the time. Also, the scheme offers constant size signature verification efficiently for different signers with fixed pairing operations. Nevertheless, the usage of mobile devices is increasing day-by-day which leads to the problem of key exposure. To resolve this issue, integrated forward security in ID-based cryptography is presented in [17]. The integration of IF and DL is adopted to show the creation of new IBE scheme, and security verification is demonstrated on RO model. The key benefits of the scheme is to provide more security compare to existing schemes, small size public key, and less cost for computations. In [18], the problems of security in cloud storage is addressed where security is provided under PKI, and more computation cost incurred due to verification of certificates. The authors proposed identity-based auditing method based on IBC for data integrity in cloud storage and extended to support multi-user environment for batch auditing. The suitability of method allows to use in cloud storage with huge data as compared to [19]. Further, the security of e-health cloud environment is investigated to provide security over patient's health data. Different identity-based cryptography methods has been proposed by Wang *et al.* [20] to secure e-health system which uses IBE and ID-based proxy re-encryption techniques under the assumption of the bilinear group for cost-effective utilization of cloud. In [21], handover authentication method for mobile devices is described to offer secure and seamless mobility amongst different networks. The various privacy and security challenges are analyzed related to IBC and comparative study presented to list associated cost required for computation and communication. The authors claimed that the ID-based cryptography satisfy relevant privacy and security requirements.

Subsequently, breaking of security in [17] is investigated on the applicability of IBE and found that it is not using bilinear pairing [22]. Due to this, the scheme [17] is insecure and the secrete key can be retrieve by querying the system in polynomial time. Furthermore, revocable IBC is employed to resolve the problem of key revocation is reviewed systematically in [23] related to [24]–[28]. This study highlights the framework, assumption, mathematical modeling for the proposal of revocable IBC system, moreover in depth security analysis is presented to understand revocable IBC system.

Nevertheless, ID-based short signature is proposed [29] for wireless sensor network (WSN) for constrained resources which is the extension of [30]. The proposed offline/online signing method not required signer's private data, and generates required data using PKG as a trustworthy resource i.e. WSN's base node. To relax the burden on WSN, aggregate signing method for generation/verification of signature not utilizing bilinear pairing hence offline data can be reused. In [31], authors designed the secure IBE and ID-based signature methods over Cyclotomic Field. The ID-based signature is protective against existentially unforgeable attack and IBE is secure over chosen plaintext/identity attacks wherein the used key size was very short. This makes it is suitable to apply in IoT ecosystem.

Due to the popularity of IBC, the security scheme is introduced to overcome privacy and security threats in VANET (Vehicular Ad Hoc Network) while exchanging messages related to traffic [32]. This scheme avoids the possibility of malicious users to temper the message in the conversation between two vehicles. To ease the verification of messages in VANET, ID-based signature using elliptic curve and hash functions are adopted in communication in VANET. Additionally, verification of batch signature is supported for the authentication of numerous messages at a time. The security analysis of the scheme is validated on RO model. Eventually, IBC also investigated for key revocation as a prominent feature for cryptography approaches. A hierarchical IBE is proposed [33] to handle the functionality of key delegation which offers organization of cryptographic techniques in large scale. To diminish the lack of bilinear maps, lattice is adopted to avoid the use of property called as *key re-randomization*. In addition, hierarchical features are extracted by using level conversion keys which is independent of key re-randomization.

Recently, another ID-based signature for key revocation is discussed to support the revocation mechanism belongs to untrustworthy and conflicting users in IBC environment [34]. As per other revocable ID-based signature the security assumption are not robust which fails under quantum computing setting. Hence, more and more emphasis is given on lattice-based cryptosystem because it is prevalent against attacks under quantum computing setting. The lattice-based revocable ID-based signature structured in the binary tree is adopted to provide scalability and offload the work of PKG, which is the drawback in [35]. The system is protective against existentially unforgeable and proof of verification is shown on standard model.

The literature motivates to apply IBC for the proposal of new IBE and ID-based signature techniques. In this article, we target to propose new protocol for Human-Centered IoT systems using IBC environment.

III. BACKGROUD AND MATERIALS

Firstly, we will establish the notations to use in the presented protocol, specifically SSSS, utilizing partial DL for human-centered IoT systems for sharing data under fuzzy client environment. The security of the presented scheme in the community in which the signature is established will be reduction in complexity of partial DL problem. We quickly examine the definition.

A. NOTATIONS

A novel attempt is our SSSS that uses PDL under fuzzy client data sharing for Human-Centered IoT systems. The notations used for proposed SSSS are listed as follows.

To avoid ambiguity, $[c, d]$ correspond to $\{c, c+1, \ldots, d\}$, and $[c]$ for $[1, c]$. For every $\mathit{id} = (\mathit{id}_1, \mathit{id}_2, \ldots, \mathit{id}_{\mathfrak{k}})$, where id is an identity vector, let $S_{\mathit{id}} = \{\mathit{id}_1, \ldots, \mathit{id}_{\mathfrak{k}}\}$ denotes identities set (id). We describe $I_{\mathit{id}} = \{i : \mathit{id}_i \in S_{\mathit{id}}\}$ as the id position records in the model's tree structure. In tree-structured, ID-based cryptographic strategy, the probable receivers construct a subtree [36]–[39]. In the tree structure $\mathcal{id}$ and their receiver positions are inserted in to $\mathbb{T}$. Any authorize $\mathbb{T}$ necessarily cover the root (node) of the tree. Here, we observe the system is regulated via PKG. Similarly, $S_{\mathcal{id}}$ of $\mathbb{T}$, position indices of $\mathbb{T}$ are defined by $S_{\mathbb{T}} = \cup_{\mathcal{id}\in\mathbb{T}} S_{\mathcal{id}}$, $I_{\mathcal{id}} = \{i : \mathcal{id}_i \in S_{\mathbb{T}}\}$. By the similar token, it is possible to use the expression $Sup\,(\mathcal{id}) = \{(\mathcal{id}_1, \mathcal{id}_2, \ldots, \mathcal{id}_{k'}) : k' \le k\}$ to signify the superiority of $\mathcal{id} = (\mathcal{id}_1, \mathcal{id}_2, \ldots, \mathcal{id}_{k})$. The predicted recipients of Subtree $\mathbb{T}$ are defined as $Sup\,(\mathbb{T}) = \cup_{\mathcal{id}\in\mathbb{T}} Sup\,(\mathcal{id})$.

Now, let's understand how the symbolization fits with our current SSSS architecture using PDL for HC-IoT systems. The proposed SSSS promises applicants to ensure the sharing of data by a fuzzy entity while meeting the security measures, but experiences difficulties with efficiency in multiple receivers. Fig. 1 shows the users are placed in the tree. If $\mathrm{S}_{\mathcal{id}} = \{\mathrm{M}, \mathrm{R}\}$ and $\mathrm{I}_{\mathcal{id}} = \{2, 7\}$, to define a scheduled user with $\mathcal{id} = (\mathrm{M}, \mathrm{R})$. User generates $\mathrm{Sup}\,(\mathcal{id}) = \{(\mathrm{M}), (\mathrm{M}, \mathrm{R})\}$ as a set that includes both itself and its superiors. If data owner refers a message belongs to recipients in $\mathbb{T} = \{(\mathrm{L})\,(\mathrm{M}, \mathrm{R})\,(\mathrm{M}, \mathrm{S})$ a subtree. We can symbolize $\mathbb{T}$'s position indices and identity set as $\mathrm{I}_{\mathbb{T}} = \{1, 2, 7, 8\}$ and $\mathrm{S}_{\mathbb{T}} = \{\mathrm{L}, \mathrm{M}, \mathrm{R}, \mathrm{S}\}$. $\mathrm{Sup}\,(\mathbb{T}) = \{(\mathrm{L})\,(\mathrm{M})\,(\mathrm{M}, \mathrm{R})\,(\mathrm{M}, \mathrm{S})$ is labelled as $\mathbb{T}$'s superiors, which is user agreement need to satisfy by data owner and wishes to pass on.

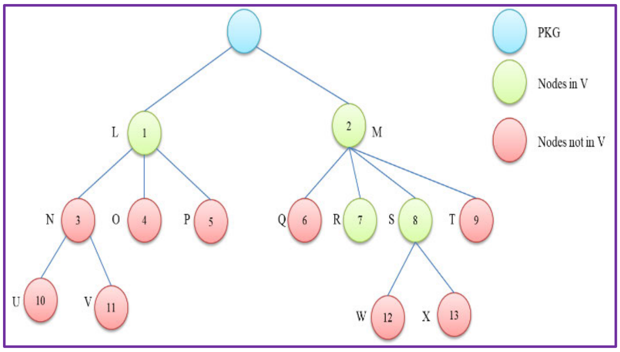


FIGURE 1. An illustration of SSSS structure.

B. PARTIAL DISCRETE LOGARITHM (PDL)

Let $\eta = q_1 p_1$ be an integer such that q_1 and p_1 are primes of $q_1 = 2q_1' + 1$ and $p_1 = 2p_1' + 1$ structure where q_1' and p_1' are primes as well. The arrangements of the prime ℓ length numbers are indicated by $S(\ell)$. A cyclic group G i.e. $\mathcal{G} = QR_{\eta^2}$ of η^2 i.e. quadratic residues modulo. We have got the command, $ord\,(\mathcal{G}) = \frac{\lambda(\eta^2)}{2} = q_1 q_1' p_1 p_1' = \frac{\eta\lambda(\eta)}{2}$, $\lambda\,(\eta) = 2q_1'p_1'$. Max order of an element is $\frac{\eta\lambda(\eta)}{2}$ within a group, and every element of order η is arranged as $\alpha = (1 + k\eta)$

Definition 1 (PDL): Let $g \in \mathcal{G}$ with max order, for directness, with assumption $g^{\lambda(\eta)}(mod\,\eta^2) = (1+\eta)\,(mod\,\eta^2)$, i.e. $k = 1$. Given g and $z = g^b(mod\,\eta^2)$ (where $b \in [1, ord\,(\mathcal{G})]$, PDL was defined by Paillier [40] as the computational problem of registration $b\,(mod\,\eta)$. We anticipate this issue to be challenging (without the modulus factorization), as the associated mistrust expresses.

Assumption 1 (PDL over $\mathbb{Z}^*_{\eta^2}$): A negligible function $negl()$ for increasing probabilistic polynomial time (PPT) algorithm A, so that suitably large l.

$$\Pr\left[\begin{array}{l} A\,(\eta, g, z) = a(mod\,\eta)|q, p \leftarrow SP\left(\frac{\ell}{2}\right); \\ \eta = qp;\ g \leftarrow \mathcal{G};\ a \leftarrow \left[1, ord\,(\mathcal{G})\right];\ z \leftarrow g^a(mod\,\eta^2) \end{array}\right] = negl(\ell)$$

C. MULTIPLE FORKING LEMMA

In this subsection, firstly we reproduce the algorithm of multiple forking [15] and then announce multiple forking lemma.

1) MULTIPLE-FORKING ALGORITHM

Considering fixed $\upsilon \epsilon \mathbb{Z}^+$ and set S with $|S| \ge 2$. Let randomized algorithm (Y) to return a triple $(\imath, \jmath, \varsigma)$ contains two integers $0 \le \jmath < \imath \le \delta$ and string ς on string x and exponents $s_1, \ldots, s_\delta \epsilon S$ Let $\eta \ge 1$ be an odd integer. Similar to Y and η, the multiple-forking algorithm $M_{Y,\eta}$ is defined as:

Algorithm 1 $M_{Y,\eta}$

```
Instate the effects of a vacant display [0, ..., $\eta$]
When casual, pick coins $\rho$ for Y
$s^0_1, \ldots, s^0_\delta \in \boldsymbol{S} : (\imath_0, \jmath_0, \varsigma_0) \leftarrow Y(x, s^0_1, \ldots, s^0_\delta : \rho)$ [Run 0]
if $(\imath_0 = 0 \vee \jmath_0 = 0)$ then
return (0, result)
end if
$s^1_{\imath_0}, \ldots, s^1_\delta \in \boldsymbol{S} : (\imath_1, \jmath_1, \varsigma_1) \leftarrow Y(x, s^0_1, \ldots, s^0_{\imath_0 - 1}, s^0_{\imath_0}, \ldots, s^1_\delta : \rho)$ [Run 1]
if $(\imath_0, \jmath_1) \ne (\imath_0, \jmath_1) \vee (s^1_{\imath_0} = s^0_{\imath_0})$ then
return (0, result)
end if
$i \leftarrow 2$
While $(i < \eta)$ do
$s^i_{\jmath_0}, \ldots, s^i_\delta \in S : (\imath_i, \jmath_i, \varsigma_i) \leftarrow Y(x, s^0_1, \ldots, s^0_i, s^0_{\imath_0}, \ldots, s^i_\delta : \rho)$ [Run $i$]
if $(\imath_i, \jmath_i) \ne (\imath_0, \jmath_0) \vee (s^i_{\jmath_0} = s^{i-1}_{\jmath_0})$ then
return (0, result)
end if
$s^{i+1}_{\imath_0}, \ldots, s^{i+1}_\delta \in S : (\imath_{i+1}, \jmath_{i+1}, \varsigma_{i+1}) \leftarrow Y(x, s^0_1, \ldots, s^0_i, s^0_{\jmath_0}, \ldots, s^0_{\imath_0 - 1}, s^{i+1}_{\imath_0}, \ldots, s^i_\delta : \rho)$ [Run $i + 1$]
if $(\imath_{i+1}, \jmath_{i+1}) \ne (i_0, \jmath_0) \vee (s^{i+1}_{\jmath_0} = s^i_{\jmath_0})$ then
return (0, result)
end if
$i \leftarrow i + 2$
end while
for $i := 0$ to $\eta$ do
results $[i] \leftarrow \varsigma_i$
end for
return (1, results)
```

Lemma 1 (Multiple-Forking [41]): Let, randomized algorithm ($\mathcal{G}_1$), does not contribution and returns any number. Let:

$$\begin{aligned}\xi'' &= \Pr[x \leftarrow \mathcal{G}_1 : s_1^0, \ldots, s_\delta^0 \in S;\\ (i_0, j_0, \varsigma_0) &\leftarrow Y(x, s_1^0, \ldots, s_\delta^0) | i_0 \geq 1 \wedge j_0 \geq 1]\end{aligned}$$

and

$$\xi' = \Pr[x \leftarrow \mathcal{G}_1 : (\text{result, results}) \leftarrow M_{Y,\eta}(x) | \text{result} = 1]$$

then

$$\xi' \geq \xi''(\frac{\xi''^{\eta}}{\delta^{2\eta}} - \frac{\eta}{|S|}) \tag{1}$$

IV. PROPOSED SSS FOR HUMAN-CENTERED IoT

Here, we proposed efficient subtree-based short signature scheme. In our presented SSS, the signing process at the signer and verification process at the verifier likes Alexa and John respectively is shown in Fig. 2. In order to sign the message, signer has to receive the private key from the PKG by sending its own public identity, this phase is called as *Extract*. Using the received private key and public identity, the signer generate signature ς of id on message m. The signed message is then transmitted through the secured channel to the verifier. Given a signature ς, a message m, an identity id and PKG public parameters, verifier outputs accept if ς is a valid signature on m for identity id, and outputs reject otherwise.

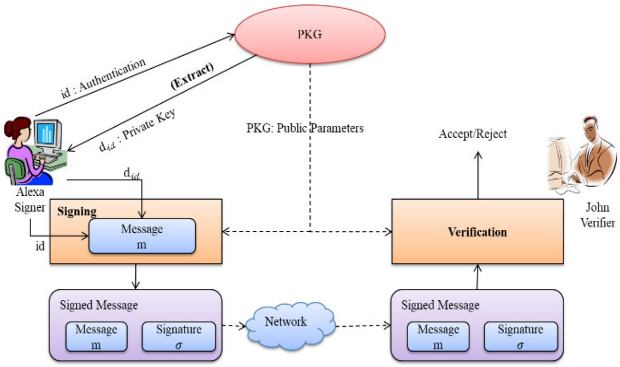


FIGURE 2. Structure of identity-based short signature scheme using subtree.

2) SSS SCHEME – SETUP, EXTRACT, SIGNATURE AND VERIFICATION PROCESSES

In this subsection, we will demonstrate the detailed working of the proposed scheme. This scheme consist of four major processes namely *Setup, Extract, Signing*, and *Verification.*

In the *Setup* process, Public Key Generator (PKG) on input various security parameter, public parameters are generated for the scheme, master public key (mpk) and master private key (msk). The PKG announces public parameters and retains the master key.

```
Setup

1. Select $\eta = q_1 p_1$ is an integer such that $q_1$ and $p_1$ are primes of $q_1 = 2q_1' + 1$ and $p_1 = 2p_1' + 1$, structures where $q_1'$ and $p_1'$ are both primes.
2. Let $G_{g,\eta} = \left\{g^0, g^1, \ldots, g^{ord(G)-1}\right\} \subseteq Z_{\eta^2}^*$, where g is a creator of $G_{g,\eta}$.
3. Pick an arbitrary number $x \xleftarrow{R} Z_{\eta^2}^*$ and set $y \leftarrow g^x \pmod{\eta^2}$.
4. Defines the one-way ($h_1$) and hash ($h_2$) functions i.e. $h_1:\{0,1\}^* * Z_{\eta^2}^* \rightarrow \{0,1\}^{\frac{k}{2}}$ and $h_2$: Sup $(\mathbb{T}) \rightarrow Z_{\eta^2}^*$
Master private key ($msk$) and master public key ($mpk$) are specified via x and $\{g, h_1, h_2, y\}$.
```

```
Pseudo Code I: Extract

For given entities identity $id \in$ Sup $(\mathbb{T})$, the PKG do the subsequent
1. Picks at an arbitrary number $\ell \xleftarrow{\mathcal{R}} Z_{\eta^2}^*$.
2. Compute $\mathcal{Y} \leftarrow g^{\ell} \pmod{\eta^2}$
3. Compute $w \leftarrow h_2(id, \mathcal{Y}) \pmod{\eta^2}$,
4. Compute $s \leftarrow (\ell - wx) \pmod{\eta^2}$.
The private key is given by $d_{id} \leftarrow (\mathcal{Y}, s) \pmod{\eta^2}$.
```

```
Pseudo Code II: Signing

The signer proceeds as follows for message $m \in \{0,1\}^*$ signing, utilizing $d_{id} \leftarrow (\mathcal{Y}, s) \pmod{\eta^2}$
1. Pick a random number $k \xleftarrow{R} Z_{\eta^2}^*$ and calculate $\mathcal{X} \leftarrow g^{k} \pmod{\eta^2}$.
2. Compute $u \leftarrow h_2(id, m, \mathcal{X})(mod\ \eta^2)$.
3. Compute $v \leftarrow (k - us)(mod\ \eta^2)$ and in addition to $t \leftarrow g^{v} \pmod{\eta^2}$.
The signature is specified by $\varsigma \leftarrow (\mathcal{X}, v, \mathcal{Y})\ (mod\ \eta^2)$ on $m$
```

```
Pseudo Code III: Verification

For the verification of $\varsigma = (\mathcal{X}, v, \mathcal{Y}) \pmod{\eta^2}$ signs on $m$:
1. Computes $t' \leftarrow \mathcal{X}\mathcal{Y}^{-u} y^{-uw}\ (mod\ \eta^2)$.
2. If $t = t'$ then it accepts signature; otherwise it is refused.
```

Given an identity $id \in$ Sup $(\mathbb{T})$ by the signer, PKG generates the private key d_{id} of id Initially PKG generate random number ℓ during the *Extract* process, and then computes $\mathcal{Y}$ in the function F1 using g and ℓ, as shown in step-2 of pseudo code-I. Hash function h_2 is applied over the identity id and $\mathcal{Y}$ to generate w. Next calculate s using w, x and ℓ in

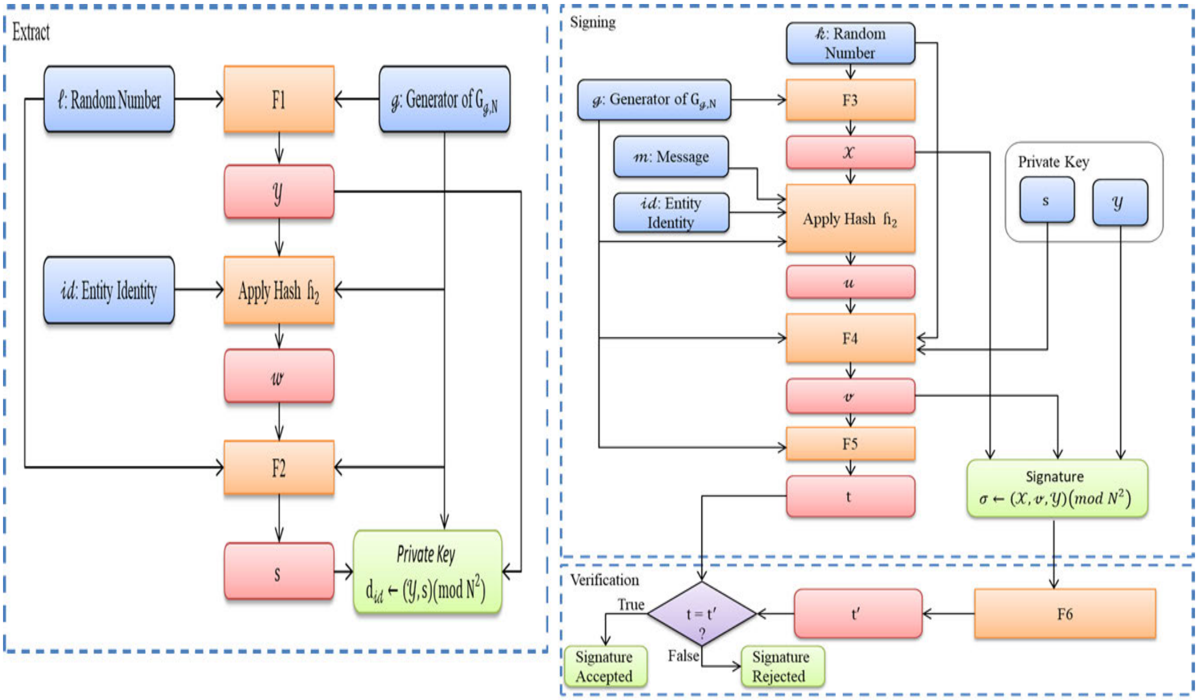


FIGURE 3. Working model of subtree-based short signature scheme.

function F2. Using $\mathcal{Y}$ and s it derives the private key d_{id} as shown in Fig. 3 and corresponding steps-3, 4, and 5 in pseudo code-I respectively.

In *Signing* process, to sign a message m using the private key d_{id} the signer picks the arbitrary number $\hbar$ and calculate $\mathcal{X}$ in function F3 using g and $\hbar$ as shown in step-1 of pseudo code-II. Then apply hash $\hbar_2$ over id, m and $\mathcal{X}$ to generate u. Then, compute v in function F4 using $\hbar$, u and s as well as t in function F5 using v and g according to the steps-2, and 3 in of pseudo code-II. Now, Alexa produces the digital signature. The signature on m is the triple $\varsigma = (\mathcal{X}, v, \mathcal{Y})\left(mod\ \eta^2\right)$ as illustrated in Fig. 3 and then forwarded the signed message to John.

During verification at receiver, John as verifier, verify a signature $\varsigma = (\mathcal{X}, v, \mathcal{Y})\left(mod\ \eta^2\right)$ on a message m for an identity id, the verifier computes t′ in function F6 using signature σ, and compare it with t as shown in Fig. 3. If the value of t is equal to t′ then acceptance of signature is confirmed; else signature is rejected.

V. SECURITY EXAMINATION AND DISCUSSION

We examine the security of the intended SSS scheme in this section using [42].

Theorem 5.1: A SSS scheme is $(t, \mathbb{i}_{\hbar_1}, \mathbb{i}_{\hbar_2}, \mathbb{i}_{\varepsilon}, \mathbb{i}_s, \epsilon)$*-secure in the logic of EUF-ST-CMA in RO model, assuming* (t', ϵ')*-PDL holds in* $\mathcal{G}_{g,\eta}$*, where*

$$t' \leq t + \tau\,(12\mathbb{i}_s + 8\mathbb{i}_{\varepsilon})$$

$$\epsilon' \geq \epsilon\left[\frac{\epsilon^4}{(\mathbb{i}_{\hbar 1} + \mathbb{i}_{\hbar 2})^6} - \frac{3}{\eta^2}\right]$$

and amount of extract $(\mathbb{i}_{\varepsilon})$ *and amount of signature* $(\mathbb{i}_s)$ *inquiries. Similarly,* $\mathbb{i}_{\hbar 1}$ *and* $\mathbb{i}_{\hbar 2}$ *are the quantities of inquiries related to* $\hbar 1$*- and* $\hbar 2$ *-oracle inquiries, that* $\mathbb{A}$ *can make individually. Whereas* τ *is the time for an exponentiation in* $\mathcal{G}_{g,\eta}$.

Proof: We utilize RO to investigate the proposed SSS scheme's security. We defined that an EUF-ST-CMA foe Υ that $(t, \mathbb{i}_{\hbar_1}, \mathbb{i}_{\hbar_2}, \mathbb{i}_{\varepsilon}, \mathbb{i}_s, \epsilon)$-breaks the SSS scheme, where Υ is a PPT program, equipped with a large public sequence consisting arbitrary bits, and requesting polynomial quantity of ROs, ε, s, $\hbar 1$ and $\hbar 2$. So, we need a "*simulator*" method which utilizes "*partition approach*". The partition approach which was first used in FDH's security dispute [43]. The main logic is to divide the i (identity-space) into i_E and i_s as a disjoint sets, depending on a one-sided coin's effect. The simulator is set up to respond to both signing and extracting inquiries about i_E identities. In any circumstance, it fails, if the challenger carries out a focus inquiry on i_s; it can respond only to i_s signing identity inquiry. To conclude, the simulator is sure about the challenger can transmit a fake identity from i_s. So, the correct proportions of the sets are decided upon review. Randomizer $\mathcal{Y}$, depending on the after effect of a one-sided coin, is set in the concern case. As a novel $\mathcal{Y}$ holds up for individual identity, $\mathcal{Y}$'s organization chooses that an identity matches with i_E or i_s. We are concerned with the situation that no signature inquiry by Υ on $\widehat{id}$ or $\widehat{\mathcal{Y}}$ should not respond by the simulator when signature inquiry on $\widehat{id}$ and the event that Υ marks $\hbar 1(\widehat{\mathcal{Y}}, \widehat{id})$ i.e. oracle inquiry corresponds to $\hbar 2(\widehat{id}, \widehat{\mathcal{X}}, \widehat{m})$.

Security Reduction $(\mathcal{R})$**:** Let PDL illustration be specified by $\pi := (\mathcal{G}_{g,\eta}, \eta, g, g^{\alpha})$. The reduction comprises conjuring the algorithm $M_{Y,n}$ i.e. multiple-forking on $\mathcal{C}$ as a cover which is shown in the Algorithm 2. Subsequently, it secures a game plan of two congruence's in two questions and responds in due order regarding α. It may be affirmed that $\mathcal{R}$ in fact return the correct response for the partial discrete logarithm occurrence. The blueprint of $\mathcal{C}$ proceeds after.

Algorithm 2 Multiple-forking lemma on C.

```
Set $mpk = \left(\mathbb{G}_{g,\eta}, \eta, g, g^{\alpha}\right) = \pi$
$(v, \{\varsigma_0, \varsigma_1, \varsigma_2, \varsigma_3\}) \leftarrow M_{\mathcal{C},1}(mpk = \pi)$
if $(v = 0)$ then return
Refer to $\varsigma_i$ as $(\widehat{v}_i, w_i, u_i)$
return
$(\widehat{v}_0 - \widehat{v}_1)(u_3 - u_2) - (\widehat{v}_2 - \widehat{v}_3)(u_1 - u_0)/(w_1 - w_0)$
$(u_1 - u_0)(u_3 - u_2)$
```

The Cover ($\mathcal{C}$)**:** Expect that $\mathbb{i} := \mathbb{i}_{\hbar_1} + \mathbb{i}_{\hbar_2}$ and $S := \mathcal{Z}^*_{\eta^2}$. The $\mathcal{C}$ continues as input the *mpk* and $\{s_1, \ldots, s_\delta\}$. It return a triple (i, j, ς) where j relating to i is the goal $\mathfrak{h}_1$-record with respect to $\mathfrak{h}_2$-record and side-yield, ς. Remembering the exact purpose of tracking the record of this RO inquiry, $\mathcal{C}$ maintains ℓ a counter, initially set to ℓ. It also maintains a table $L_{\mathfrak{h}}$ with respect to $L_{\mathfrak{h}_2}$, dealing with the RO, $\mathfrak{h}_1$ with respect to other $\mathfrak{h}_2$. The game started by $\mathcal{C}$ of the EUF-ST-CMA by passing *mpk* i.e. challenge *mpk* to Υ (challenger). Due to the following determinations, the inquiries made by Υ easily handle under EUF-ST-CMA.

RO inquiry, $\mathfrak{h}_1$ $(\mathcal{Y}, id)$: $L_{\mathfrak{h}1}$ covers tuples of the game plan

$$\langle \mathcal{Y}, id, w, \ell, \delta\rangle \in \mathbb{G}_{g,\eta} \times \{0,1\}^* \times \mathcal{Z}^*_{\eta^2} \times \mathcal{Z}^+ \times \mathcal{Z}^*_{\eta^2} \cup \{\perp\}$$

Here, the inquiry, $(\mathcal{Y}, id)$ into the $\mathfrak{h}_1$-oracle, the resulting yield is w. The survey record is maintained in the ℓ-domain. In order to complete, either (a part of) secret key for id, or a '$\perp$', the domain is unacceptable in the event. $\mathfrak{h}_1(\mathcal{Y}, id)$ is new if no $\langle \mathcal{Y}, id_i, w_i, \ell_i, \delta_i\rangle$ in $L_{\mathfrak{h}1}$ such that $(\mathcal{Y}_i = \mathcal{Y}) \wedge (id_i = id)$. In the event, when tuple occurs, the oracle is formerly expected to return the yield to some degree w_i. A crisp, write, inquiry $\mathfrak{h}_1$-oracle is managed as plans: *i*) return $w \leftarrow s_\ell \left(mod\, \eta^2\right)$ as the yield, and *ii*) growth $\langle \mathcal{Y}, id, w, \ell, \perp\rangle$ to $L_{\mathfrak{h}1}$ and boost by 1.

RO inquiry, $\mathfrak{h}_2(id, \mathcal{X}, m)$: L_{h_2} covers structure tuples

$$\langle id, B, m, u, \ell\rangle \in \{0,1\}^* \times \mathbb{G}_{g,\eta} \times \{0,1\}^* \times \mathcal{Z}^*_{\eta^2} \times \mathcal{Z}^+$$

Usually, $(id, \mathcal{X}, m)$ is the $\mathfrak{h}_2$-oracle inquiry with the resulting yield being u. In the ℓ-domain the inquiry record is put away. In this way, a RO investigation $\mathfrak{h}_2(id, \mathcal{X}, m)$ is new if no $\langle id_i, \mathcal{X}_i, m_i, u_i\rangle$ in $L_{\mathfrak{h}2}$ so that $(id_i = id) \wedge (\mathcal{X}_i = \mathcal{X}) \wedge (m_i = m)$ is not available. In the event, when tuple occurs, then u_i is given back by the oracle. A fresh, unequivocal, inquiry $\mathfrak{h}_2$-oracle is managed as: *i*) the yield return as $\leftarrow s_\ell \left(mod\, \eta^2\right)$, and *ii*) growth $\langle id, \mathcal{X}, m, u, \ell\rangle$ to $L_{\mathfrak{h}2}$ and ℓ is increase by 1.

Extract inquiry $\mathbb{i}_E(id)$**:** Consequently the *msk* α is unclear to $\mathcal{C}$, in order to generate the client secret key *usk* it requires to sensibly record $\mathfrak{h}_1$-oracle in the direction.

1. In the incident that there occurs a tuple $\langle \mathcal{Y}_i, id_i, w_i, \ell_i, \delta_i\rangle$ in $L_{\mathfrak{h}1}$ such that $(id_i = id) \wedge (\delta_i \neq \perp)$, $\mathcal{C}$ proceeds $usk = (\delta_i, \mathcal{Y}_i)$ as the secrete key.
2. Otherwise, $\mathcal{C}$ preferences $\delta \in_R \mathcal{Z}^*_{\eta^2}$, sets $w \leftarrow s_\ell \left(mod\, \eta^2\right)$ and $\mathcal{Y} = (g^{\alpha})^{-w} g^{\delta} \left(mod\, \eta^2\right)$. It then adds $\langle \mathcal{Y}, id, w, \ell, \delta\rangle$ to $L_{\mathfrak{h}1}$ as well as increments by one (a verifiable import $\mathfrak{h}_1$-oracle inquiry). Finally, as the secrete key it returns $usk = (\delta, \mathcal{Y})$.

Signature inquiry $\mathbb{i}_s(id, m)$: Inquiries for signature are answered by generating *usk* first (by inquiring with $\mathbb{i}_E$ on id), which is trailed by trickery S.

1. If there occurs a tuple $\langle \mathcal{Y}_i, id_i, w_i, \ell_i, \delta_i\rangle$ in $L_{\mathfrak{h}1}$ such that $(id_i{=}\ id) \wedge (\delta_i \neq \perp)$, $\mathcal{C}$ proceeds $usk = (\delta_i, \mathcal{Y}_i)$, secrete key. At this point, $\mathcal{C}$ utilized the facts of *usk* to run S and return the signature.
2. Otherwise, $\mathcal{C}$ produces *usk* similar to step (2) of Extract investigation and runs S to return the signature.

At the end of simulation, a profitable opponent yields a valid fiddling $\widehat{\varsigma} = (\widehat{\mathcal{X}}, \widehat{v}, \widehat{\mathcal{Y}})$ on a $(\widehat{id}, \widehat{m})$. Let $\langle \mathcal{Y}_i, id_i, w_i, \ell_i, \delta_i\rangle$ be the tuple in $L_{\mathfrak{h}1}$ that relays to the $\mathfrak{h}_1$-inquiry objective. In essence, let $\langle m_i, \mathcal{X}_i, w_i, u_i, \ell_i, \rangle$ be in $L_{\mathfrak{h}2}$ which relays to $\mathfrak{h}_2$-inquiry objective. $\mathcal{C}$ proceeds, $(\ell_i \ell_j, (\widehat{v}, w_j, u_i))$ as particular yield of its own. The ς contains $(\widehat{v}, w_j, u_i)$, side-yield we notice.

Arrangement of the Forgery: Assessment, signature inquiries are answered by performing an identity extract inquiry taken after learning S. So, the resultant private keys are from the construction $usk = (\delta, \mathcal{Y})$, where $\mathcal{Y} = (g^{\alpha})^{-w} g^{\gamma} \left(mod\, \eta^2\right)$ and we are taking $\mathscr{k} \leftarrow (\ell - uw) \left(mod\, \eta^2\right)$. If a fake is provided using the same $\mathcal{Y}$ as defined as signature enquiry function ($\mathcal{R}$) on id, then v will represents as $v \leftarrow (\mathscr{k} - u(-\alpha w + \delta + \alpha w)) \left(mod\, \eta^2\right) = (\mathscr{k} - \delta u) \left(mod\, \eta^2\right)$. No answer comprise to PDL challenge α in this manner, and these fakes are not important to $\mathcal{R}$. In any circumstance, the occurrence that Υ not able to establish an enquiry for signature on $\widehat{id}$ or $\widehat{\mathcal{Y}}$ was not fixed once by a simulator i.e. yield function on an enquiry for signature on $\widehat{id}$. The event confirms that Υ not able to forge using $\mathcal{Y}$, which is the component of id signature enquiry, and thus, fake generated towards valid v, construction $v = (\mathscr{k} - u(\ell - uw)) \left(mod\, \eta^2\right)$ would be essential.

A. CORRECTNESS OF THE PARTIAL DISCRETE LOGARITHM

Now, $\mathcal{R}$ usages Algorithm 1 ($M_{Y,n}$) to resolve partial DL challenge. Algorithm 1 runs on *mpk* that includes oracles $\mathfrak{h}_1$ and $\mathfrak{h}_2$ as a part of reply attacks. When failure to Algorithm 1 occurs, $\mathcal{R}$ must abort somewhere ($\text{abort}_{3,1}$). In an event of forking, $\mathcal{R}$ achieves 4-(related) side-yield sets $\{\varsigma_0, \varsigma_1, \varsigma_2, \varsigma_3\}$, where ς_i (for $i = 0\ to\ 3$) is takes the form $(\widehat{v}_i, w_i, u_i)$. Let $\widehat{r}_0$ indicate $log_g \widehat{\mathcal{X}}_1 = log_g \widehat{\mathcal{X}}_0$, similarly $\widehat{r}_2$ indicate $log_g \widehat{\mathcal{X}}_2 = log_g \widehat{\mathcal{X}}_3$; let $\widehat{k}$ indicate $log_g \widehat{\mathcal{Y}}_0 = log_g \widehat{\mathcal{Y}}_1 = log_g \widehat{\mathcal{Y}}_2 = log_g \widehat{\mathcal{Y}}_3$. As the multiple-forking has been successful, we have:

$$\Big\{\widehat{v}_0 = (\widehat{\mathscr{k}}_0 - u_0(\widehat{\ell} - \alpha w_0)) \left(mod\, \eta^2\right), \widehat{v}_1$$
$$= (\widehat{\mathscr{k}}_0 - u_1(\widehat{\ell} - \alpha w_0)) \left(mod\, \eta^2\right), \widehat{v}_2$$

$$= (\widehat{\hbar}_1 - u_2 (\widehat{\ell} - \alpha w_1)) \left(mod\, \eta^2\right), \widehat{v}_3$$
$$= (\widehat{\hbar}_1 - u_3 (\widehat{\ell} - \alpha w_1)) \left(mod\, \eta^2\right)\Big\}$$

It is a four-congruence structure in the four (successful) unknowns $\{\widehat{\ell}, \widehat{\hbar}_0, \widehat{\hbar}_2, \alpha\}$. Using the expression given below, α can be answered.

$$\alpha := \frac{(\widehat{v}_0 - \widehat{v}_1)(u_3 - u_2) - (u_1 - u_0)(\widehat{v}_2 - \widehat{v}_3)}{(w_1 - w_0)(u_1 - u_0)(u_3 - u_2)} \left(mod\, \eta^2\right) \tag{2}$$

By (2) we observe that $\mathfrak{R}$ yields correctly as per the Algorithm 2.

B. PROBABILITY ANALYSIS

We observe and accomplish that if Algorithm 1 is successful (probability of n'), the incident abort$_{3,1}$ does not occur. In this way we comprehensive with the statement that if the multiple forking calculation is successful, the event abort$_{3,1}$ not occur (allowed this probability to be part of ξ'). Similarly,

$$\Pr[\neg abort_{3,1}] = \xi' \tag{3}$$

The abort$_{3,1}$ is the solitary abort involved in $\mathfrak{R}$, occurring if failure to $M_{Y,3}$. Thus effectiveness of $\mathfrak{R}$ is if we have $M_{Y,3}$ and (3)

$$\varepsilon' = \Pr[\neg \text{abort}_{3,1}] = \xi'$$

We specify probability that $M_{Y,3}$ will be successful in run 3^{rd} as ξ''. Since no abort is included in the mid-stage of the question, $M_{Y,3}$ is successful in the mid-stage of 3^{rd} run if there $\varUpsilon$ is a true fake, i.e. $\xi'' = \varepsilon$. Put (1) from Lemma 1 with $\eta = 3$, $\delta = \mathbb{i}_{h_1} + \mathbb{i}_{\hbar_2}$ and $|S| = \eta^2$, we've got it.

$$\xi' \geq \xi''(\frac{\xi''^{\eta}}{\delta^{2\eta}} - \frac{\eta}{|S|}) \quad \text{or } \xi' \geq \xi''(\frac{\xi''^{3}}{\delta^{2\eta}} - \frac{3}{|S|})$$

then

$$\varepsilon' \geq \varepsilon \left[\frac{\varepsilon^4}{(\mathbb{i}_{\hbar_1} + \mathbb{i}_{\hbar_2})^6} - \frac{3}{\eta^2}\right]$$

Time Examination: Time performance (τ) for an exponentiation in $G_{g,\eta}$ at that stage the time performance by:

$$t' \leq t + \tau\,(12\mathbb{i}_s + 8\mathbb{i}_\varepsilon)$$

It continues for the notation of the extract inquiry and signature inquiry respectively at most four and six exponentiation. This contributes in the running time to the part $\tau\,(12\mathbb{i}_s + 8\mathbb{i}_\varepsilon)$. The double aspect originates from the algorithm of several generalized forkings, later it includes the double running the challenger. Which concludes Theorem 5.1 argument.

Formal security can validate using AVISPA software. The experimentation is performed on Intel Core i5-8365U CPU @1.90 GHz with 8GB RAM and 1 TB HDD using 64-bit Windows 10 operating system. Automated Validation of Internet Security Protocols and Applications (AVISPA) [51] [52] is utilized for checking the authenticity and security properties. Moreover, verification of proposed protocol using AVISPA v.1.1 is modelled in High-Level Protocol Specification Language (HLPSL).

VI. COMPARISON ANAYSIS

We evaluated the performance of our SSS scheme over the existing schemes presented in Shen *et al.*[44] scheme, He *et al.* [45] scheme, Ramadan *et al.* [46] scheme, and Zhang *et al.* [47] scheme. The comparison has been done based on the computational cost of these methods. The comparative study has used the notations mentioned in the Table 1.

TABLE 1. Symbolic notations used for computing computational cost.

Notation	Meaning (execution time)
$\mathbb{t}_{exp}$	modular exponentiation in group
$\mathbb{t}_{mul}$	modular multiplication
$\mathbb{t}_{hash}$	one way hash function
$\mathbb{t}_{pair}$	one bilinear pairing operation
$\mathbb{t}_{inv}$	one modular inverse operation

For simplicity, the relationships among these notations in terms of $\mathbb{t}_{hash}$ have been used. The relationship among these notations with respect to $\mathbb{t}_{hash}$ is shown in Table 2 [48]–[51].

TABLE 2. Relationship among notations.

Sr. No.	Relationships among notations
1	$\mathbb{t}_{mul} \approx 2.5\ \mathbb{t}_{hash}$
2	$\mathbb{t}_{inv} \approx 7.5\ \mathbb{t}_{hash}$
3	$\mathbb{t}_{exp} \approx 600\ \mathbb{t}_{hash}$
4	$\mathbb{t}_{pair} \approx 1550\ \mathbb{t}_{hash}$

The computational complexity order among the metrics is shown in below.

$$\mathbb{t}_{hash} < \mathbb{t}_{mul} < \mathbb{t}_{inv} < \mathbb{t}_{exp} < \mathbb{t}_{pair}$$

It has seen that the cost for signing stage and the cost for the verification stage dominates the cost for the other stages,

TABLE 3. Comparison among existing scheme with the proposed scheme.

Sr. No.	Scheme	Signing Stage	Verification Stage	Total Cost (ms)
1	Shen *et al.* [44]	$1\mathbb{t}_{hash} + 3\mathbb{t}_{mul} = 4.2755$	$2\mathbb{t}_{hash} + 3\mathbb{t}_{pair} = 2339.956$	2344.2315
2	He *et al.* [45]	$2\mathbb{t}_{hash} + 7\mathbb{t}_{mul} + 4\ \mathbb{t}_{exp} = 1217.0085$	$2\mathbb{t}_{hash} + 1\mathbb{t}_{mul} + 1\mathbb{t}_{pair} = 781.9135$	1998.922
3	Ramadan *et al.*[46]	$1\mathbb{t}_{hash} + 5\mathbb{t}_{mul} = 9.3055$	$2\mathbb{t}_{mul} + 3\mathbb{t}_{pair} + 3\ \mathbb{t}_{exp} + 1\ \mathbb{t}_{inv} = 3250.6375$	3259.943
4	Zhang *et al.* [47]	$1\mathbb{t}_{hash} + 1\mathbb{t}_{mul} + 4\ \mathbb{t}_{exp} = 1208.9605$	$1\mathbb{t}_{hash} + 3\ \mathbb{t}_{exp} = 905.903$	2114.8635
5	**Proposed scheme**	$\mathbf{1\mathbb{t}_{hash} + 1\mathbb{t}_{mul} + 2\ \mathbb{t}_{exp} = 605.3605}$	$\mathbf{1\mathbb{t}_{mul} + 3\ \mathbb{t}_{exp} + 1\ \mathbb{t}_{inv} = 910.43}$	**1515.7905**

the computational cost for the signing as well as verification stage have been used for the comparative analysis. The computational cost for $\mathfrak{t}_{hash}$ is considered as 0.503 ms [52]. In this paper, the proposed scheme has been compared to [44]–[47]. Table 3 show the comparison based on the computational cost for signing stage and the verification stage. It has seen from Table 3 that the proposed scheme is efficient in signing stage in comparison with He *et al.* [45], and Zhang *et al.* [47]. It has also seen from Table 3 that the schemes Shen *et al.* [44], and Ramadan *et al.* [46] performing better than the proposed scheme in signing stage.

Fig. 4 shows the graphical representation of computational cost for signing stage. Fig. 5 show the computational cost requirement by the existing schemes and the proposed scheme for verification stage. It is seen from Table 3 and from Fig. 5 that, the proposed scheme for verification stage is efficient than the schemes Shen *et al.* [44], and Ramadan *et al.* [46]. It is also seen from Table 3 that the schemes He *et al.* [45], and Zhang *et al.* [47] are more efficient than the proposed SSS in this paper for verification stage. Fig. 6 show the comparison based on the total cost including signing stage and verification stage. Fig. 6 show that the proposed SSS in this paper is efficient than [44]–[47]. The total computational cost required for the proposed SSS is **1515.7905 ms.** The comparative analysis based on the computational cost show the effectiveness of the proposed SSS over the existing schemes in the literature.

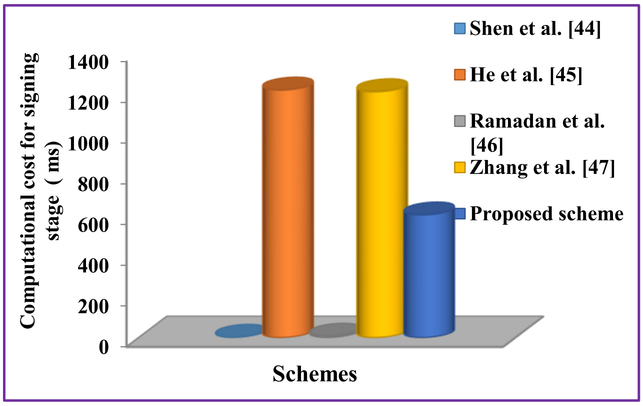


FIGURE 4. Computational cost for signing stage.

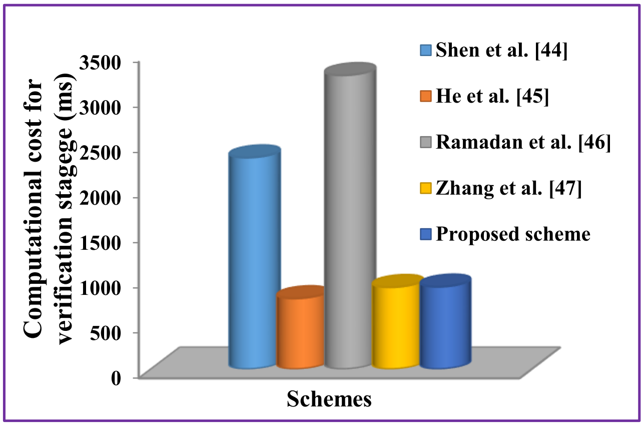


FIGURE 5. Computational cost for verification stage.

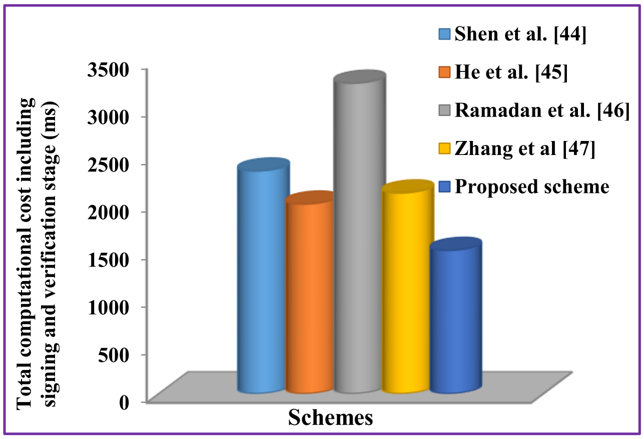


FIGURE 6. Total computational cost for signing stage and verification stage.

VII. CONCLUSION

HC-IoT is very much connected to the life of peoples, particularly in business, smart cards, online banking transactions, online messaging, healthcare and sensitive data exchange, etc. Safety of sensitive data is crucial in HC-IoT to provide secure solution to forgery attacks. In asymmetric public key cryptography, authenticity and ownership is managed by digital signatures as a reliable option. We implemented new construction in this article to obtain provably secure partial discrete logarithm-based SSS scheme in RO model. Such a system is decidedly without a doubt comprehended and utilized for quite a while under different settings. The framework is protected against the existential unforgeability of EUF-ST-CMA that exhaust a Forking Lemma variation. The security is demonstrated in the RO model based on partial discrete logarithm supposition. The presented framework does not use pairings, resulting in achieving proficiency and execution simplicity, does not rely on the hardness of pairing-based cryptosystem. This found suitable to use in resource-binding circumstances where main focus is to save communication, computation and code of implementation.

ACKNOWLEDGMENT

The authors are grateful to the Deanship of Scientific Research, King Saud University for funding through Vice Deanship of Scientific Research Chairs.

REFERENCES

[1] A. Shamir, "Identity-based cryptosystems and signature schemes," in *Proc. CRYPTO* (Lecture Notes in Computer Science), vol. 196. Berlin, Germany: Springer-Verlag, 1984, pp. 47–53.

[2] D. Boneh and M. Franklin, "Identity-based encryption from the Weil pairing," in *Proc. CRYPTO* (Lecture Notes in Computer Science). Berlin, Germany: Springer-Verlag, 2001, pp. 213–229.

[3] C. Cocks, "An identity based encryption scheme based on quadratic residues," in *Proc. IMA Int. Conf. Cryptogr. Coding* (Lecture Notes in Computer Science), vol. 2260. Berlin, Germany: Springer-Verlag, 2001, pp. 360–363.

[4] L. Harn and S. Yang, "ID-based cryptographic schemes for user identification, digital signature, and key distribution," *IEEE J. Sel. Areas Commun.*, vol. 11, no. 5, pp. 757–760, Jun. 1993.

[5] M. C. Gorantla, R. Gangishetti, and A. Saxena, "A survey on ID-based cryptographic primitives," *IACR Cryptol. ePrint Arch.*, p. 94, 2005.

[6] Y. Zheng, H.-Y. Wang, and R.-C. Wang, "Grid authentication from identity-based cryptography without random oracles," *J. China Universities Posts Telecommun.*, vol. 15, no. 4, pp. 55–59, Dec. 2008.

[7] C. Meshram, S. A. Meshram, and M. Zhang, "An ID-based cryptographic mechanisms based on GDLP and IFP," *Inf. Process. Lett.*, vol. 112, no. 19, pp. 753–758, Oct. 2012.

[8] D. Shin, "A socio-technical framework for Internet-of-Things design: A human-centered design for the Internet of Things," *Telematics Informat.*, vol. 31, no. 4, pp. 519–531, Nov. 2014.

[9] A. Pintus, D. Carboni, A. Serra, and A. Manchinu, "Humanizing the Internet of Things–toward a human-centered Internet-and-Web of things," in *Proc. 11th Int. Conf. Web Inf. Syst. Technol. (WEBIST)*, 2015, pp. 498–503.

[10] A. Wafa, C. A. Zayani, I. Amous, and F. Sèdes, "User-centric IoT: Challenges and perspectives," in *Proc. 12th Int. Conf. Mobile Ubiquitous Comput., Syst., Services Technol. (UBICOMM)*, 2018, pp. 27–34.

[11] M. B. Mohamad Noor and W. H. Hassan, "Current research on Internet of Things (IoT) security: A survey," *Comput. Netw.*, vol. 148, pp. 283–294, Jan. 2019.

[12] A. Tewari and B. B. Gupta, "Security, privacy and trust of different layers in Internet-of-Things (IoTs) framework," *Future Gener. Comput. Syst.*, vol. 108, pp. 909–920, Jul. 2020.

[13] C. P. Schnorr, "Efficient signature generation by smart cards," *J. Cryptol.*, vol. 4, no. 3, pp. 161–174, Jan. 1991.

[14] D. Pointcheval and J. Stern, "Security arguments for digital signatures and blind signatures," *J. Cryptol.*, vol. 13, no. 3, pp. 361–396, Jun. 2000.

[15] A. Boldyreva, A. Palacio, and B. Warinschi, "Secure proxy signature schemes for delegation of signing rights," *J. Cryptol.*, vol. 25, no. 1, pp. 57–115, Jan. 2012.

[16] P. V. Reddy and P. Gopal, "Identity-based key-insulated aggregate signature scheme," *J. King Saud Univ. Comput. Inf. Sci.*, vol. 29, no. 3, pp. 303–310, Jul. 2017.

[17] C. Meshram, "An efficient ID-based cryptographic encryption based on discrete logarithm problem and integer factorization problem," *Inf. Process. Lett.*, vol. 115, no. 2, pp. 351–358, Feb. 2015.

[18] J. Zhang and Q. Dong, "Efficient ID-based public auditing for the outsourced data in cloud storage," *Inf. Sci.*, vols. 343–344, pp. 1–14, May 2016.

[19] H. Wang, J. Domingo-Ferrer, B. Qin, and Q. Wu, "Identity-based remote data possession checking in public clouds," *IET Inf. Secur.*, vol. 8, no. 2, pp. 114–121, Mar. 2014.

[20] X. A. Wang, J. Ma, F. Xhafa, M. Zhang, and X. Luo, "Cost-effective secure E-health cloud system using identity based cryptographic techniques," *Future Gener. Comput. Syst.*, vol. 67, pp. 242–254, Feb. 2017.

[21] D. He, S. Zeadally, L. Wu, and H. Wang, "Analysis of handover authentication protocols for mobile wireless networks using identity-based public key cryptography," *Comput. Netw.*, vol. 128, pp. 154–163, Dec. 2017.

[22] C. H. Tan, T. F. Prabowo, and D.-P. Le, "Breaking an ID-based encryption based on discrete logarithm and factorization problems," *Inf. Process. Lett.*, vol. 116, no. 2, pp. 116–119, Feb. 2016.

[23] T.-Y. Wu, J. C.-W. Lin, C.-M. Chen, Y.-M. Tseng, J. Frnda, L. Sevcik, and M. Voznak, "A brief review of revocable ID-based public key cryptosystem," *Perspect. Sci.*, vol. 7, pp. 81–86, Mar. 2016.

[24] T.-Y. Wu, T.-T. Tsai, and Y.-M. Tseng, "Revocable ID-based signature scheme with batch verifications," in *Proc. 8th Int. Conf. Intell. Inf. Hiding Multimedia Signal Process.*, Jul. 2012, pp. 49–54.

[25] Y.-M. Tseng and T.-T. Tsai, "Efficient revocable ID-based encryption with a public channel," *Comput. J.*, vol. 55, no. 4, pp. 475–486, Apr. 2012.

[26] T.-T. Tsai, Y.-M. Tseng, and T.-Y. Wu, "A fully secure revocable ID-based encryption in the standard model," *Informatica*, vol. 23, no. 3, pp. 487–505, Jan. 2012.

[27] T.-T. Tsai, Y.-M. Tseng, and T.-Y. Wu, "Provably secure revocable ID-based signature in the standard model," *Secur. Commun. Netw.*, vol. 6, no. 10, pp. 1250–1260, Oct. 2013.

[28] T.-T. Tsai, Y.-M. Tseng, and T.-Y. Wu, "RHIBE: Constructing revocable hierarchical ID-based encryption from HIBE," *Informatica*, vol. 25, no. 2, pp. 299–326, Jan. 2014.

[29] C. Meshram, P. L. Powar, M. S. Obaidat, C.-C. Lee, and S. G. Meshram, "Efficient online/offline IBSS protocol using partial discrete logarithm for WSNs," *IET Netw.*, vol. 7, no. 6, pp. 363–367, Nov. 2018.

[30] C. Meshram, Y.-M. Tseng, C.-C. Lee, and S. G. Meshram, "An IND-ID-CPA secure ID-based cryptographic protocol using GDLP and IFP," *Informatica*, vol. 28, no. 3, pp. 471–484, Jan. 2017.

[31] Y. Wang, M. Wang, J. Zou, J. Xu, and J. Wang, "Provably secure identity-based encryption and signature over cyclotomic fields," *Wireless Commun. Mobile Comput.*, vol. 2019, Oct. 2019, Art. no. 1742386, doi: 10.1155/2019/1742386.

[32] I. Ali, T. Lawrence, and F. Li, "An efficient identity-based signature scheme without bilinear pairing for vehicle-to-vehicle communication in VANETs," *J. Syst. Archit.*, vol. 103, Feb. 2020, Art. no. 101692.

[33] S. Katsumata, T. Matsuda, and A. Takayasu, "Lattice-based revocable (hierarchical) IBE with decryption key exposure resistance," *Theor. Comput. Sci.*, vol. 809, pp. 103–136, Feb. 2020.

[34] C. Xie, J. Weng, J. Weng, and L. Hou, "Scalable revocable identity-based signature over lattices in the standard model," *Inf. Sci.*, vol. 518, pp. 29–38, May 2020, doi: 10.1016/j.ins.2020.01.008.

[35] Y.-H. Hung, Y.-M. Tseng, and S.-S. Huang, "Revocable ID-based signature with short size over lattices," *Secur. Commun. Netw.*, vol. 2017, pp. 1–9, Jan. 2017.

[36] W. Liu, J. Liu, Q. Wu, B. Qin, D. Naccache, and H. Ferradi, "Efficient subtree-based encryption for fuzzy-entity data sharing," *Soft Comput.*, vol. 22, no. 23, pp. 7961–7976, Dec. 2018.

[37] C. Meshram, C.-C. Lee, S. G. Meshram, and M. K. Khan, "An identity-based encryption technique using subtree for fuzzy user data sharing under cloud computing environment," *Soft Comput.*, vol. 23, no. 24, pp. 13127–13138, Dec. 2019.

[38] C. Meshram, C.-C. Lee, A. S. Ranadive, C.-T. Li, S. G. Meshram, and J. V. Tembhurne, "A subtree-based transformation model for cryptosystem using chaotic maps under cloud computing environment for fuzzy user data sharing," *Int. J. Commun. Syst.*, vol. 33, no. 7, p. e4307, May 2020.

[39] C. Meshram, C.-C. Lee, S. G. Meshram, and A. Meshram, "OOS-SSS: An efficient online/offline subtree-based short signature scheme using Chebyshev chaotic maps for wireless sensor network," *IEEE Access*, vol. 8, pp. 80063–80073, 2020.

[40] P. Paillier, "Public key cryptosystem based on discrete logarithm residues," in *Proc. Eurocrypt* (Lecture Notes in Computer Science), vol. 1592. Berlin, Germany: Springer, 1999, pp. 223–238.

[41] M. Bellare and G. Neven, "Multi-signatures in the plain public-key model and a general forking lemma," in *Proc. 13th ACM Conf. Comput. Commun. Secur. (CCS)*, New York, NY, USA, 2006, pp. 390–399.

[42] M. Bellare, C. Namprempre, and G. Neven, "Security proofs for identity-based identification and signature schemes," in *Proc. Adv. Cryptol. (EUROCRYPT)* (Lecture Notes in Computer Science), vol. 3027. Berlin, Germany: Springer-Verlag, 2004, pp. 268–286.

[43] J. Coron, "On the exact security of full domain hash," in *Proc. Adv. Cryptol. (CRYPTO)* (Lecture Notes in Computer Science), vol. 1880. Berlin, Germany: Springer-Verlag, 2003, pp. 229–235.

[44] L. Shen, J. Ma, X. Liu, F. Wei, and M. Miao, "A secure and efficient ID-based aggregate signature scheme for wireless sensor networks," *IEEE Internet Things J.*, vol. 4, no. 2, pp. 546–554, Apr. 2017.

[45] D. He, Y. Zhang, D. Wang, and K.-K.-R. Choo, "Secure and efficient two-party signing protocol for the identity-based signature scheme in the IEEE P1363 standard for public key cryptography," *IEEE Trans. Dependable Secure Comput.*, vol. 17, no. 5, pp. 1124–1132, Sep. 2020.

[46] M. Ramadan, Y. Liao, F. Li, and S. Zhou, "Identity-based signature with server-aided verification scheme for 5G mobile systems," *IEEE Access*, vol. 8, pp. 51810–51820, 2020.

[47] G. Zhang, Y. Liao, Y. Fan, and Y. Liang, "Security analysis of an identity-based signature from factorization problem," *IEEE Access*, vol. 8, pp. 23277–23283, 2020.

[48] M. Benasser Algehawi and A. Samsudin, "A new identity based encryption (IBE) scheme using extended Chebyshev polynomial over finite fields," *Phys. Lett. A*, vol. 374, no. 46, pp. 4670–4674, Oct. 2010.

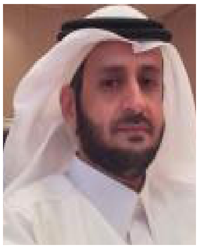
[49] M. H. Ibrahim, S. Kumari, A. K. Das, M. Wazid, and V. Odelu, "Secure anonymous mutual authentication for star two-tier wireless body area networks," *Comput. Methods Programs Biomed.*, vol. 135, pp. 37–50, Oct. 2016.

[50] C. Meshram, M. S. Obaidat, and K.-F. Hsiao, "An efficient EUF-ID-CMA secure identity-based short signature scheme using discrete logarithm," in *Proc. Int. Conf. Comput., Inf. Telecommun. Syst. (CITS)*, Aug. 2019, pp. 1–5.

[51] AVISPA. *Automated Validation of Internet Security Protocols and Applications*. Accessed: Oct. 2014. [Online]. Available: http://www.avispa-project.org/

[52] AVISPA. *AVISPA Web Tool*. Accessed: Oct. 2014. [Online]. Available: http://www.avispa-project.org/web-interface/expert.php/

CHANDRASHEKHAR MESHRAM received the Ph.D. degree from R.T.M. Nagpur University, Nagpur, India. He is currently an Assistant Professor with the Department of Post Graduate Studies and Research in Mathematics, Jayawanti Haksar Government Post Grraduation College, Chhindwara University, Betul, India. His research interests include cryptography and its application, neural networks, the IoT, WSN, medical information systems, ad hoc networks, number theory, fuzzy theory, time series analysis and climate change, mathematical modeling, and chaos theory. He had published over 95 scientific articles on the above research fields in international journals and conferences. He is regular reviewer of 60 international journals and international conferences. He is also a member of IAENG, Hong Kong, WASET, New Zealand, CSTA, USA, ACM, USA, IACSIT, Singapore, EATCS, Greece, IAROR, The Netherland, EAI, ILAS, Haifa, Israel, the Science and Engineering Institute (SCIEI), Machine Intelligence Research Labs (MIR Labs), USA, Society: Intelligent Systems, KES International Association, U.K., Universal Association of Computer and Electronics Engineers (UACEE), and The Society of Digital Information and Wireless Communications (SDIWC), and a Life–time member of the Indian Mathematical Society and Cryptology Research Society of India. He received the Postdoctoral Fellow under Dr. D. S. Kothari postdoctoral fellowship from New Delhi, India.



AHMED ALSANAD received the Ph.D. degree in computer science from De Montfort University, U.K., in 2013. He is currently an Associate Professor with the Information System Department and the Chair Member of Pervasive and Mobile Computing, CCIS, King Saud University, Riyadh, Saudi Arabia. He has authored and coauthored more than 12 publications, including refereed IEEE/ACM/ Springer journals, conference papers, and book chapters. His research interests include cloud computing, health informatics, ERP, and CRM.

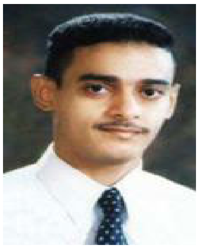
JITENDRA V. TEMBHURNE received the B.E. degree in computer technology from the Kavikulguru Institute of Technology and Science (KITS), Ramtek, Nagpur University, India, in 2003, the M.E. degree in computer science and engineering from the MGM's College of Engineering, SRTMU Nanded, India, in 2011, and the Ph.D. degree in computer science and engineering from the Visvesvaraya National Institute of Technology, Nagpur, India, in 2017. From 2005 to 2011, he was an Assistant Professor with the Computer Technology Department, KITS Ramtek, Nagpur University. From 2016 to 2018, he was an Assistant Professor with the Computer Engineering Department, SVPCET, Nagpur. Since 2018, he has been an Assistant Professor with the Computer Science and Engineering Department, Indian Institute of Information Technology (IIIT), Nagpur, India. He is the author of more than 15 articles published in international conferences and journals. His research interests include parallel computing on multi-core and many-core hardware, data science, deep learning, medical imaging, and cryptography and security. He is also a member of IAENG Society.

SHAILENDRA W. SHENDE received the M.Tech. degree in computer science and engineering form the Visvesvaraya National Institute of Technology, Nagpur, India, in 2010. He is currently an Associate Professor with the Department of Information Technology, Yeshwantrao Chavan College of Engineering, Nagpur. His current research interests include high performance parallel computing, GPU computing and its applications, machine learning, network security, and the IoT. He had published over 12 scientific articles on the above research fields in international journals and conferences. He is also a member of ACM and CSI.

KAILASH WAMANRAO KALARE received the B.E. degree in information technology from Rashtrasant Tukdoji Maharaj Nagpur University, Nagpur, India, and the master's degree in computer science and engineering from the Visvesvaraya National Institute of Technology, Nagpur. He is currently pursuing the Ph.D. degree in computer science and engineering with the Indian Institute of Information Technology, Design, and Manufacturing, Jabalpur, India. His research interests include cryptography and security, image reconstruction, and deep learning.

SARITA GAJBHIYE MESHRAM received the M.Tech. degree in soil and water engineering from the College of Agricultural Engineering, Jawaharlal Nehru Krishi Vishwa Vidhyalaya, Jabalpur, India, in 2009, and the Ph.D. degree in water resource development and management from IIT Roorkee (U.K.), India, in 2015. She was the Dr. D. S. Kothari Postdoctoral Fellow with the Department of Mathematics and Computer Sciences, Rani Durgawati University, Jabalpur. She is currently associated as a Research Faculty with the Department for Management of Science and Technology Development, Ton Duc Thang University, Ho Chi Minh City, Vietnam, and the Faculty of Environment and Labour Safety, Ton Duc Thang University. Her current research interests include geographical information systems, rainfall-runoff sediment yield modeling, and SCS-CN. She is carrying out her research work in the field of rainfall-runoff, sediment yield, water quality, and application of RS and GIS water network and cryptographic protocols. She had published over 80 research articles in refereed journals, conference and workshop proceedings, and books. She is also a member of some international societies and reviewer of reputed journals. She received the Gold Medal for her M.Tech. degree.

MUHAMMAD AZEEM AKBAR received the M.Sc. and M.S. degrees in computer science from the University of Agriculture Faisalabad (UAF), Faisalabad, Pakistan, and the Ph.D. degree in software engineering from Chongqing University, China. He is currently working as a Postdoctoral Researcher with the Nanjing University of Aeronautics and Astronautics, Nanjing, China. He has published more than 25 research articles in well-reputed journals and conferences. He has an Outstanding Academic carrier. His research interests include global software development, requirements engineering, empirical studies, global software requirements change management, software defect prediction, the Internet of Things, code recommender systems, and software risk management.



ABDU GUMAEI received the Ph.D. degree in computer science from King Saud University, Riyadh, Saudi Arabia, in 2019. He is currently an Assistant Professor with the College of Computer and Information Sciences, King Saud University. He worked as a Lecturer and taught many courses such as programming languages at the Computer Science Department, Taiz University, Yemen. He has authored and coauthored more than 30 journal and conference papers in well-reputed international journals. He received a patent from the United States Patent and Trademark Office (USPTO) in 2013. His research interests include software engineering, image processing, computer vision, machine learning, networks, and the Internet of Things (IoT).