IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received July 8, 2021, accepted July 19, 2021, date of publication July 28, 2021, date of current version August 10, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3101111

An Efficient Provably Secure Verifier-Based Three-Factor Authentication Technique Using PDL for Data Exchange in TMIS

VISHESH P. GAIKWAD[1], JITENDRA V. TEMBHURNE[1], CHANDRASHEKHAR MESHRAM[2], CHENG-CHI LEE[3,4], (Member, IEEE), AND CHUN-TA LI[5], (Member, IEEE)

[1]Department of Computer Science and Engineering, Indian Institute of Information Technology at Nagpur, Nagpur 440006, India
[2]Department of Post Graduate Studies and Research in Mathematics, Jayawanti Haksar Government Post-Graduation College, College of Chhindwara University, Betul, Madhya Pradesh 460001, India
[3]Department of Library and Information Science, Research and Development Center for Physical Education, Health, and Information Technology, Fu Jen Catholic University, New Taipei City 24205, Taiwan
[4]Department of Computer Science and Information Engineering, Asia University, Wufeng Shiang, Taichung 41354, Taiwan
[5]Department of Information Management, Tainan University of Technology, Tainan 710302, Taiwan

Corresponding authors: Cheng-Chi Lee (cclee@mail.fju.edu.tw), Chandrashekhar Meshram (cs_meshram@rediffmail.com), and Chun-Ta Li (th0040@mail.tut.edu.tw)

This work was supported in part by Visvesvaraya Ph.D. Scheme through the Ministry of Electronics and Information Technology (MeitY) by the Government of India under Grant MEITY-PHD-3039, and in part by the Ministry of Science and Technology, Taiwan, under Contract MOST 109-2410-H-165-001 and Contract MOST 110-2410-H-165-001-MY2.

ABSTRACT In healthcare services, telecare medicine information systems (TMIS) is the viable solution offered currently. Moreover, to provide best security to the TMIS, it attracted the various researchers to investigate the security challenges in TMIS. Subsequently, the security of TMIS is improving but the application becoming widespread hence needs robust security technique. An efficient verifier-based 3-party authentication technique in telecare medicine information systems for data exchange, which permits only two users/patients to store their verifier in the database of an authentication server, computed using own password. The authentication system will then validate the user's verifier and help them safely and easily share electronic medical records. In this work, we present an efficient provably secure verifier-based 3-party authentication technique using partial discrete logarithm (PDL) for exchanging data in TMIS. The presented technique not utilizing any public keys of the server, and does not require additional messages and number for key confirmation rounds. The proposed technique has higher security compared to the related verifier-based methods, has lower computational costs and fewer communications, and is therefore ideal for TMIS.

INDEX TERMS TMIS, partial discrete logarithm, data exchange, authentication, entropy smoothing hash function.

I. INTRODUCTION

With the rapid advancement of the internet and information technology, facilitates the development of telecare medicine information systems (TMIS). TMISs are generally utilized to provide healthcare delivery of Medical services. TMIS offers the storage and maintenance of medical information which is highly sensitive and belongs to the registered users; specifically it stores electronic medical records (EMR) conveniently and efficiently. These sensitive information are accessed and shared through public communication channel by the medical institutes, hospitals, academia, and doctors to enhance decision capability. It supports telecare medicine services directly delivered to the patients at home via public networks. Further, gradual development of e-healthcare systems also provides medical services directly at a doorstep of patient which is an economical alternative for patients and healthcare service suppliers with decrease travel expenses. TMIS require a powerful secured and efficient authentication mechanism for protecting patient's private information such as EMR, healthcare information, etc.

Subsequently, many authentication schemes or methods were developed in the recent times for TMIS. Mostly, it used for data exchange in TMIS that enables two users can share a

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

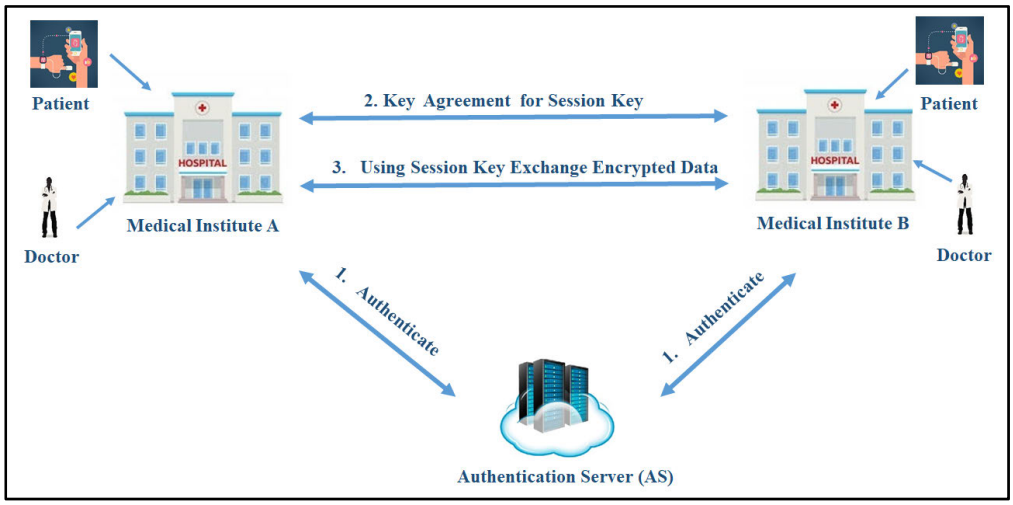

FIGURE 1. 3-party authentication technique for data transfer in TMIS.

common session key securely to acquire a secure connection between them via centralized authentication server. So that the two users can securely, efficiently and conveniently exchange their electronic medical records over public channel. Furthermore, set of identified research on TMIS and ERP systems utilizing hash based authentication, user security and authentication using AVISPA, RFID based authentication, chaotic maps and dynamic identity based secure authentication for e-healthcare [1], and cloud-assisted [2] secure medical system for mobile emergency for secure data exchange in e-healthcare environment has been proposed to offer security and authorization.

A 3-party authentication technique for data transfer in TMIS that enables two users in medical institutes and hospitals negotiate a common session key securely and secure channel is established by authentication server (AS). Afterwards, exchange of electronic medical records and other healthcare information is performed by two users securely and conveniently. The systematic working of 3-party authentication technique is presented in Fig. 1.

Nevertheless, a verifier-based security approach calculated a verifier from user's password and keeps this verifier in AS. Authentication server does not require any user password hence does not store it. Actual password's ownership is verified by AS using a technique to resist stolen verifiers attack. But, the copy of verifier table can be stolen from AS database by the attacker [3]–[5]. Varieties of verifier–based 3-party authentication methods [3]–[6] were proposed. In 2005 Lee *et al.* [4] proposed an efficient verifier-based 3-party authentication approach without server's public keys. Kwon *et al.* [6] illustrated a round-efficient and secure verifier-based 3-party authentication scheme without public keys at server side. Here, the key confirmation is achieved using the session key. If the EMRs are ciphertext and utilized [6] without key confirmation then the received encrypted EMR records are corrected or not, will be immediately identified by the receiver.

In *e*-healthcare, the user's privacy and security of healthcare information is a terribly vital issue. The user may be a *patient*, a *doctor*, a *nurse* or any *medical employee*, moreover, healthcare information may vary from person to person. In addition, TMIS server stores the complete medical history of the patients registered in a hospital for the treatment of disease. So to provide security, numerous two factor authentication schemes for TMIS were proposed, in which a user is required to provide both passwords and smart cards to prove his/her identity. However, secret parameters can be duplicated and smart card can be compromised becomes the major concerns. The issues pointed in two-factor can be solved by using three-factor authentication schemes which is presented in this paper.

An improved emergency system for *m*-healthcare is designed in [7] using chaotic maps. This proposed system protects against mutual authentication and user anonymity, and also perform computation in reduced cost. Herein, the drawbacks in Lee *et al.* [8] scheme are identified and more secure system for *m*-healthcare is presented. In [9], key agreement, password authentication, and chaotic maps based scheme for TMIS to maintain user anonymity is proposed. After investigating the schemes in [10], the different modification suggested by the authors is to overcome the shortcomings.

The contributions in this article are listed as follows:

1) We proposed an efficient verifier-based authentication technique for TMIS using PDL. The PDL is computationally difficult problem, and offers more security for the authentication technique.
2) The proposed technique utilized entropy smoothing hash which is secure and collision-resistant, and bitwise XOR operation.
3) We proposed two variant of authentication technique such as message-competent and round-competent
4) The presented scheme provides security proofs in random oracle model.

TABLE 1. Notations.

Symbols	Meanings
q, p, q_1', p_1'	Prime numbers
$p_1, q_1, \mathcal{N}$	Two large primes p_1 and $q_1$such that$\mathcal{N} = q_1 p_1$, $\mathcal{N}$ is an integer.
g, g_1, g_2	Generators g, g_1, g_2 in group $\mathcal{Z}^*_{\mathcal{N}^2}$, group in which hardness of Diffie-Hellman problem (DHP) [11] is considered.
AS	Authentication server
$pw_{\mathcal{U}_\mathcal{A}}$	$pw_{\mathcal{U}_\mathcal{A}}$ is a password and shared between User $\mathcal{U}_\mathcal{A}$ and AS.
$V_{\mathcal{U}_\mathcal{A}}, V_{\mathcal{U}_\mathcal{A},1}, V_{\mathcal{U}_\mathcal{A},2}$	$V_{\mathcal{U}_\mathcal{A}}, V_{\mathcal{U}_\mathcal{A},1}$, and $V_{\mathcal{U}_\mathcal{A},2}$ are verifiers computed from $pw_{\mathcal{U}_\mathcal{A}}$.
$pw_{\mathcal{U}_\mathcal{B}}$	$pw_{\mathcal{U}_\mathcal{B}}$ is a password and shared between User $\mathcal{U}_\mathcal{B}$ and AS.
$V_{\mathcal{U}_\mathcal{B}}, V_{\mathcal{U}_\mathcal{B},1}, V_{\mathcal{U}_\mathcal{B},2}$	$V_{\mathcal{U}_\mathcal{B}}, V_{\mathcal{U}_\mathcal{B},1}$ and $V_{\mathcal{U}_\mathcal{B},2}$ are verifiers computed from $pw_{\mathcal{U}_\mathcal{B}}$.
$MAC_\kappa(\mathcal{M})$	On $\mathcal{M}$, message authentication code is applied consist of strong shared key κ [6].
$H(.)$	A collision-free one-way hash function.
$\mathcal{F}$	A family of secured pseudorandom functions.
$\mathcal{U}_\mathcal{A} \rightarrow \mathcal{U}_\mathcal{B} : \mathcal{M}$	Message $\mathcal{M}$ sending from $\mathcal{U}_\mathcal{A}$ to $\mathcal{U}_\mathcal{B}$ via common channel
$\mathcal{M}_0, \mathcal{M}_1$	Message $\mathcal{M}_0$concatenates to message $\mathcal{M}_1$

5) Our new procedure is client-friendly in that it provides the client with the power to directly modify/update their password and personal biometric key without having to contact the base station.
6) Thorough security examinations, including a formal analysis have demonstrated that the proposed technique is protected against different recognized attacks.

The organizations of this research work are as follows. The concepts related to verifier-based authentication schemes are reviewed in Section 2. The mathematical assumptions are described in Section 3. Section 4 highlights the investigation of new efficient verifier-based technique without using server's public keys for TMIS. The proposed technique's security analysis is presented in Section 5. Simulation of proposed technique is discussed in Section 6 and performance evaluation is demonstrated in Section 7. Finally, all the conclusions are listed in Section 8.

II. BACKGROUND AND MATERIAL

In this section, we review the various definitions [3, 31] related to this work before to present review related to verifier-based authentication schemes to identify the research gap. Firstly, we list all the notations used in this work and same has been shown in Table 1. A and B are representing the communication parties and AS represent a trustworthy authentication server.

A. PARTIAL DISCRETE LOGARITHM (PDL)

Let $\mathcal{N}$ be an integer with prime modulus such that $\mathcal{N} = q_1 p_1$, which means q and p are primes of the structure $p_1 = 2p_1' + 1$ and $q_1 = 2q_1' + 1$, where q_1' and p_1' are also primes. $S(l)$ represents an arrangement of safe prime numbers of length l. Let $\mathcal{G} = \mathcal{QR}_{\mathcal{N}^2}$ the cyclic group of quadratic residues modulo $\mathcal{N}^2$. We have $ord\ (\mathcal{G}) = \frac{\lambda(\mathcal{N}^2)}{2} = pp'qq' = \frac{\mathcal{N}\lambda(\mathcal{N})}{2}$, with $\lambda\ (\mathcal{N}) = 2q'p'$. The maximal order of a component in this group is $\frac{\mathcal{N}\lambda(\mathcal{N})}{2}$, and each component of order $\mathcal{N}$ is of the form $\alpha = (1 + k\mathcal{N})$.

Definition 1 (PDL): Let g be a component of maximal order in $\mathcal{G}$. We also assume that $g^{\lambda(\mathcal{N})}(mod\mathcal{N}^2) = (\mathcal{N} + 1)\ (mod\mathcal{N}^2)$, that is $k = 1$. For given g and $z = g^a mod\mathcal{N}^2$ (for some $a \in [1, ord\ (\mathcal{G})]$), Paillier [30] defined the PDL as the computational problem of computing $a(mod\mathcal{N})$. We expect this issue is difficult, as expressed in the accompanying suspicion.

Assumption 1 (PDL over $\mathcal{Z}^*_{\mathcal{N}^2}$) : For every probabilistic polynomial time (PPT) algorithm A, there exists a negligible function *negl*() such that for sufficiently large l.

$$Pr\left[A\ (\mathcal{N}, g, z) = a(mod\mathcal{N}) | q_1, p_1 \leftarrow SP\left(\frac{l}{2}\right); \mathcal{N} = q_1 p_1; g \leftarrow \mathcal{G}; a \leftarrow [1, ord\ (\mathcal{G})]; z \leftarrow g^a(mod\mathcal{N}^2)\right] = negl(l)$$

III. RELATED WORKS

Three-factor authentication approach for TMIS is proposed by Tan [12] wherein a user passes biometrics, smart card, and password for authentication. In addition, server and remote user authenticates each other mutually and sharing of session key between them is accomplished. Progressively, Yan [13] found flaws in Tan's scheme which is vulnerable to denial-of-service (DoS) attack, and improved scheme is proposed to overcome Tan's scheme flaws. Further, Wu *et al.* [14] presented three-factor authentication techniques for TMIS, progressively Tan [12] pointed and overcomes the drawbacks of Awasthi *et al.* which is not providing user anonymity, three-factor security, and vulnerable to reflection attack. In addition, scheme proposed by Tan *et al.* is protective against all the known attacks.

In 2011, Das [15] proposed an improved biometrics-based remote user authentication scheme using smart cards. The scheme was composed of three phases: 1) registration phase, 2) login phase, and 3) authentication phase. Furthermore in 2012, An [16] found that the Das [15] scheme has some major security flaws such as user impersonation attack, server masquerading attack, password guessing attack, insider attack, and mutual authentication between the user and the server. Authors also proposed a biometrics-based remote user authentication scheme using smart card that can resist against user impersonation attack, server masquerading attack, password guessing attack, and insider attack.

However, in 2013 Khan and Kumari [17] found that the An scheme [16] has failed to resist server masquerading attack, user impersonation attack, and password guessing attack. A lightweight biometric based remote user authentication scheme to overcome all these drawbacks is proposed in [16]. In 2014 Wen *et al*. [18] developed an enhanced biometrics-based remote user authentication scheme to overcome the drawbacks found in [17], here scheme in [17] fails to provide user anonymity. In 2015 Mir and Nikooghadam [19] designed biometrics-based authentication key agreement scheme. Authors claimed that their scheme is secured, ensures minimal computational time, and best suited for TMIS. But in 2018, Chaudhry *et al.* [20] examined the protocol of Mir and Nikooghadam [19] and proved that the stolen smart card and patient anonymity violation attacks are possible. To overcome these attacks, Chaudhry *et al.* [20] proposed an improved 3-factor authentication scheme based on a lightweight symmetric key primitive. But, in this case the communication and computation cost is higher.

In the same year, Lu *et al*. [21] targeted for providing a strong user anonymity and hence proposed a biometrics and smart cards based authentication scheme for multi-server environments. However, Chaudhry *et al*. [22] found that the scheme [21] is vulnerable to user impersonation attack, thus designed an improved scheme. In [23], a biometrics-based AKA scheme for multi-server environment with strong user anonymity is developed. However, Odelu *et al.* [24] showed that scheme in [23] fails to resist known session temporary information attack, and their scheme cannot resist the replay attack and impersonation attack, moreover further improvement is proposed by the authors.

In 2018, Amin *et al*. [25] presented a lightweight authentication scheme based on IoT enabled device. Here, the data is generated from various smart devices in the IoT environment which is one of the biggest concerns. Thus, cloud computing is utilized to process a large amount of data. However, the scheme suffers from an insider attack and lost smart card attack. In [26], a lightweight authentication scheme using a hash function and XOR function for the cloud environment is suggested.

In 2019, Barman *et al*. [27] proposed a scheme specifically for multi-server environments and usable in TMIS. However, Ali *et al*. [28] showed that scheme presented in [27] has a weakness against user impersonation, lack of anonymity, and secret key reveal. In addition, a new improved 3-factor symmetric-key based secure AKA scheme for multi-server environments is designed to overcome aforementioned attacks. Furthermore, an Elliptic Curve Cryptography (ECC) based secure 3-factor authentication protocol with forward secrecy is proposed in [29]. This protocol is based on fuzzy commitment scheme to handle the biometric information. Meanwhile, fuzzy verifier and honey list techniques are used to solve the contradiction of local password verification and mobile device lost attack. For the verification of an authentication scheme ProVerify tool was utilized.

In [39], another authentication scheme is designed for mobile readers by utilizing hash function with XOR operation. This implementation is more trustworthy as compared to other public key schemes. The drawbacks of Zheng *et al*. [40] are addressed, reply attacks and impersonation attacks are successfully handled. An application of Graphical Authentication (GA) scheme for the smart devices is proposed in [41]. An integration of two techniques were adopted i.e. PassPoints and press touch code to secure the smart device against the three attacks such as brute force, smudge, and shoulder surfing. Moreover, the performance of the scheme is evaluated on the various parameters such as usability, functionality, and security.

Recently, we witness the increase of mobile users and to offer efficient security scheme is in high demand. In [42], efficient authentication scheme is developed for mobile users under cloud computing environment wherein verification of data integrity of mobile user, authentication of user at audit process, and reduced computation and communication cost were addressed. In addition, authors claimed that the scheme is more suitable for real-life applications. In [43], the investigation of security in vehicular ad hoc networks (VANETs) is presented to mitigate the authentications issues in vehicle. Here, the safety of communication is the critical issue in increasing number of vehicles. Hence, anonymity preserving authentication scheme on fog-computing for VANETs is proposed to offer reduce communication, efficient vehicle authentication (by self-authentication). Subsequently, analysis of security challenges in Internet of Things (IoT) is presented in [44] to provide the authentication in resource constrained devices. A lightweight and flexible Group authentication schemes (GAS) is proposed which is energy efficient, and secure against man-in-the-middle and relay attacks. Moreover, massive machine type communication (MMTC) is adopted for key distribution and key agreement. Authors claims that the applicability of scheme is suitable for 6G networks where fast authentication is requested. Table 2 shows the comparison between the existing schemes based on their strengths and weaknesses.

Through the aforementioned literature, we found that to exchange data securely under TMIS, an efficient verifier-based 3-factor authentication technique is required. So, we propose an authentication technique using Partial

TABLE 2. Comparison of existing schemes.

Ref.	Strengths	Weaknesses
[4]	A verifier-based 3-party authentication approach without server's public keys.	Wang and Mo [46] identified in [4] that if an attacker has stolen verifier, then it is not resistant to an impersonation attack.
[46]	Solved the impersonation attack problems which are occurred in Lee et al. scheme and designs efficient verifier-based key agreement protocol for 3-parties without server's public key.	This scheme does not realize key confirmation. If the transmitted EMRs are encrypted by using an unconfirmed key, their integrity and confidentiality are unsure.
[6]	Secure against known-key attacks and provides perfect forward secrecy.	Authors of [39] identified in [6] that it do not realize key confirmation. If the transmitted EMRs or medical health data are encrypted by using an unconfirmed key, then uncertain about integrity and confidentiality.
[39]	Password table problem does not exist.	It does not provide anonymity, vulnerable to tracking attack, and computation cost is higher.
[21]	A robust biometrics and public-key based authentication scheme is designed, targeted to overcome the server masquerading, insecure against forgery, and lacks perfect forward secrecy attacks.	Vulnerable to the offline password guessing attack.
[38]	An efficient chaos-based 3PAKE protocol without using smart cards is proposed, which neither requires symmetric cryptosystems nor server's public key.	Insecure in online and offline password guessing attacks, password table problem exist, and vulnerable to impersonation attack.
[51]	Resolved the issues like password-guessing, user impersonation, insider, smartcard theft attacks, and facilitate user anonymity.	Privileged insider attack, denial of service attack, fails to provide forward secrecy, and three-factor secrecy.
[50]	Secured against a well-known attack like privileged insider attack, denial of service attack, but fails to provide forward secrecy and three-factor secrecy.	It [46] is insecure against user and server impersonation attacks and a known session specific temporary information attack.

Discrete Logarithm (PDL) that comprises the key confirmation process without using extra number of rounds and messages. Moreover, PDL provide more security, as it is difficult to compute and thus, improves the overall security. Thus, comparing with similar state-of-the-art authentication schemes, our technique provides higher security, fewer transmission, and lower computational cost.

IV. PROPOSED EFFICIENT VERIFIER-BASED AUTHENTICATION TECHNIQUE FOR TMIS

This section introduces an effective provably secure 3-party authentication technique for TMIS based on verifier, which does not allow the use of public keys from the server and is built on DHP [11]. In addition, the proposed technique is applied by simultaneous rearranging and sending messages, and key confirmation is performed without additional number of rounds and messages. The proposed technique involves three sub-techniques of 2-party authenticated key exchange (2PAKE), including a sub-technique involving $\mathcal{U}_{\mathcal{A}}$ and AS, a sub-technique involving $\mathcal{U}_{\mathcal{B}}$ and A, and a sub-technique involving $\mathcal{U}_{\mathcal{A}}$ and $\mathcal{U}_{\mathcal{B}}$. Eventually, use of the hash feature offers confirmation of identity. Fig. 2 shows the technique being proposed for the authentication.

A. MESSAGE-COMPETENT VERIFIER-BASED AUTHENTICATION TECHNIQUE FOR TMIS

In this subsection, we demonstrate an efficient message-competent verifier-based authentication technique.

Originally, $\mathcal{U}_{\mathcal{A}}$ shares verifiers $\mathrm{V}_{\mathcal{U}_{\mathcal{A}}} = \boldsymbol{g}^{\mathrm{t}_{\mathcal{U}_{\mathcal{A}}}} (mod \mathcal{N}^2)$ for password $\mathcal{PW}_{\mathcal{U}_{\mathcal{A}}}$ with AS, and $\mathcal{U}_{\mathcal{B}}$ shares verifiers $\mathrm{V}_{\mathcal{U}_{\mathcal{B}}} = \boldsymbol{g}^{\mathrm{t}_{\mathcal{U}_{\mathcal{B}}}} (mod \mathcal{N}^2)$ for password $\mathcal{PW}_{\mathcal{U}_{\mathcal{B}}}$ with AS, respectively, where $\mathrm{t}_{\mathcal{U}_{\mathcal{A}}} = \mathrm{H}(\mathcal{U}_{\mathcal{A}}, \mathrm{AS}, \mathcal{PW}_{\mathcal{U}_{\mathcal{A}}})$ and $\mathrm{t}_{\mathcal{U}_{\mathcal{B}}} = \mathrm{H}\left(\mathcal{U}_{\mathcal{B}}, AS, \mathcal{PW}_{\mathcal{U}_{\mathcal{B}}}\right)$.

1. $\mathcal{U}_{\mathcal{A}} \rightarrow AS : \mathcal{U}_{\mathcal{A}}, \mathcal{U}_{\mathcal{B}}, X_{U_A}$

$\mathcal{U}_{\mathcal{A}}$ chooses $a \epsilon_R Z^*_{q_1}$, calculates $X_{\mathcal{U}_{\mathcal{A}}} = \boldsymbol{g}^a \left(mod \mathcal{N}^2\right)$ and sends it to AS.

2. $AS \rightarrow \mathcal{U}_{\mathcal{B}} : X_{\mathcal{U}_{\mathcal{A}}}, X_{S\mathcal{U}_{\mathcal{A}}}, X_{S\mathcal{U}_{\mathcal{B}}}$

AS chooses $c, d \epsilon_R Z^*_{q_1}$, and usages $V_{\mathcal{U}_{\mathcal{A}}}$ and $V_{\mathcal{U}_{\mathcal{B}}}$ to calculate $X_{S\mathcal{U}_{\mathcal{A}}} = \left(V_{\mathcal{U}_{\mathcal{A}}}\right)^{\mathrm{c}} \oplus V_{\mathcal{U}_{\mathcal{A}}} (mod \mathcal{N}^2)$ and

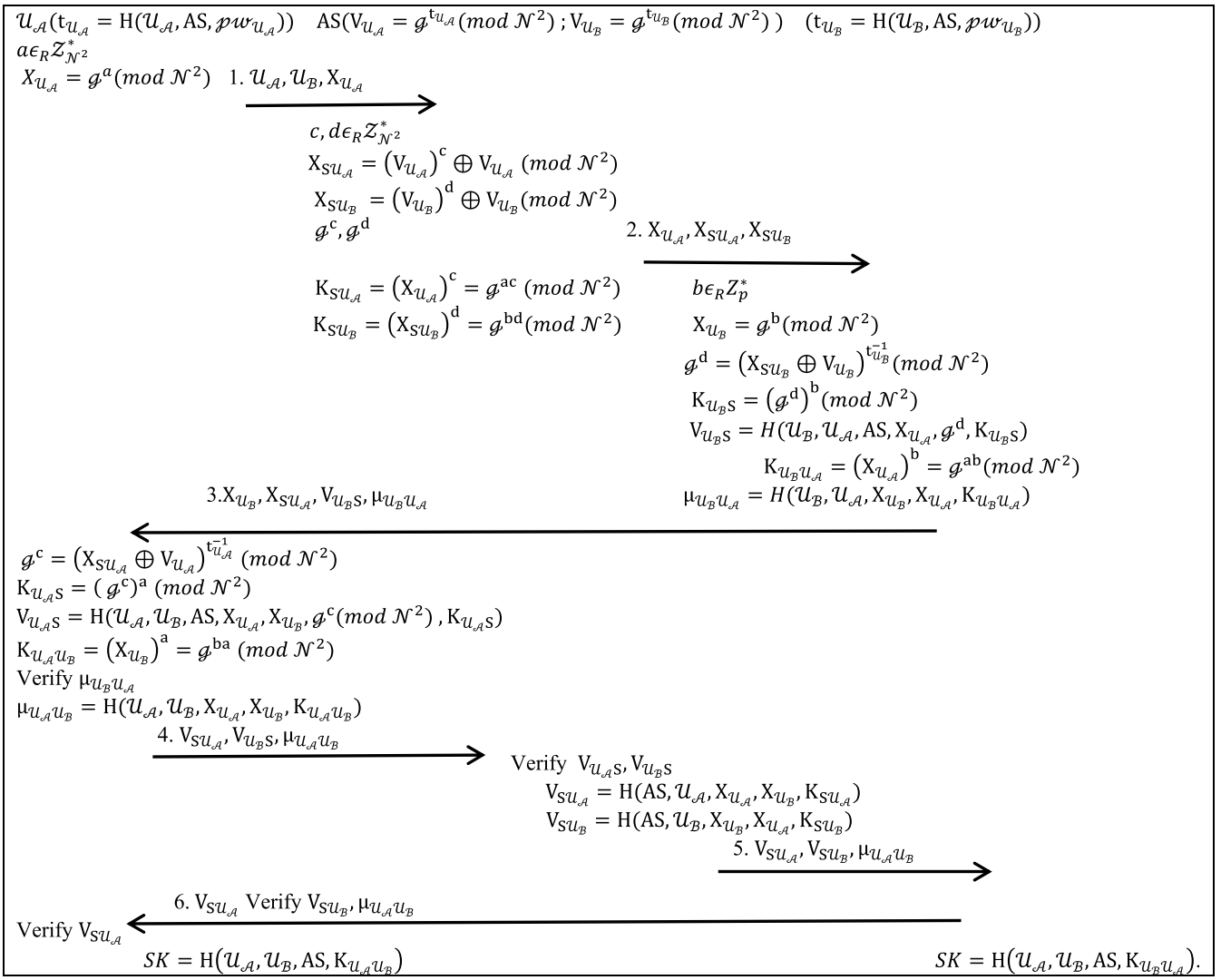

FIGURE 2. Projected message for efficient verifier-based technique for TMIS.

$X_{S\mathcal{U}_\mathcal{B}} = (V_{\mathcal{U}_\mathcal{B}})^d \oplus V_{\mathcal{U}_\mathcal{B}}(mod\mathcal{N}^2)$. Then, AS sends $(X_{\mathcal{U}_\mathcal{A}}, X_{S\mathcal{U}_\mathcal{A}}, X_{S\mathcal{U}_\mathcal{B}})$ to $\mathcal{U}_\mathcal{B}$, and calculates g^c, g^d, $K_{S\mathcal{U}_\mathcal{A}} = (X_{\mathcal{U}_\mathcal{A}})^c = g^{ac}(mod\mathcal{N}^2)$ and $K_{S\mathcal{U}_\mathcal{B}} = (X_{S\mathcal{U}_\mathcal{B}})^d = g^{bd}(mod\mathcal{N}^2)$.

3. $\mathcal{U}_\mathcal{B} \rightarrow \mathcal{U}_\mathcal{A} : X_{\mathcal{U}_\mathcal{B}}, X_{S\mathcal{U}_\mathcal{A}}, X_{\mathcal{U}_\mathcal{B}S}, \mu_{\mathcal{U}_\mathcal{B}\mathcal{U}_\mathcal{A}}$

$g^d = (X_{S\mathcal{U}_\mathcal{B}} \oplus V_{\mathcal{U}_\mathcal{B}})^{t^{-1}_{\mathcal{U}_\mathcal{B}}}(mod\mathcal{N}^2)$, $K_{\mathcal{U}_\mathcal{B}S} = (g^d)^b = g^{bd}(mod\mathcal{N}^2)$, $V_{\mathcal{U}_\mathcal{B}S} = H(\mathcal{U}_\mathcal{B}, \mathcal{U}_\mathcal{A}, AS, X_{\mathcal{U}_\mathcal{A}}, g^d, K_{\mathcal{U}_\mathcal{B}S})$ and $\mu_{\mathcal{U}_\mathcal{B}\mathcal{U}_\mathcal{A}} = H(\mathcal{U}_\mathcal{B}, \mathcal{U}_\mathcal{A}, X_{\mathcal{U}_\mathcal{B}}, X_{\mathcal{U}_\mathcal{A}}, K_{\mathcal{U}_\mathcal{B}\mathcal{U}_\mathcal{A}})$ where $t_{\mathcal{U}_\mathcal{B}} = H(\mathcal{U}_\mathcal{B}, AS, \mathcal{pw}_{\mathcal{U}_\mathcal{B}})$, and sends $(X_{\mathcal{U}_\mathcal{B}}, X_{S\mathcal{U}_\mathcal{A}}, X_{\mathcal{U}_\mathcal{B}S}, \mu_{\mathcal{U}_\mathcal{B}\mathcal{U}_\mathcal{A}})$ to $\mathcal{U}_\mathcal{A}$.

4. $\mathcal{U}_\mathcal{A} \rightarrow AS : V_{S\mathcal{U}_\mathcal{A}}, V_{\mathcal{U}_\mathcal{B}S}, \mu_{\mathcal{U}_\mathcal{A}\mathcal{U}_\mathcal{B}}$

$\mathcal{U}_\mathcal{A}$ calculates $g^c = (X_{S\mathcal{U}_\mathcal{A}} \oplus V_{\mathcal{U}_\mathcal{A}})^{t^{-1}_{\mathcal{U}_\mathcal{A}}}(mod\mathcal{N}^2)$, $K_{\mathcal{U}_\mathcal{A}S} = (g^c)^a = g^{ac}(mod\mathcal{N}^2)$, $V_{\mathcal{U}_\mathcal{A}S} = H(\mathcal{U}_\mathcal{A}, \mathcal{U}_\mathcal{B}, AS, X_{\mathcal{U}_\mathcal{A}}, X_{\mathcal{U}_\mathcal{B}}, g^c, K_{\mathcal{U}_\mathcal{A}S})$ and $K_{\mathcal{U}_\mathcal{A}\mathcal{U}_\mathcal{B}} = (X_{\mathcal{U}_\mathcal{B}})^a = g^{ba}(mod\mathcal{N}^2)$, where $a \epsilon_R Z^*_{q_1}$ and $t_{\mathcal{U}_\mathcal{A}} = H(\mathcal{U}_\mathcal{A}, AS, \mathcal{pw}_{\mathcal{U}_\mathcal{A}})$. If $\mathcal{U}_\mathcal{A}$ effectively verifies $\mu_{\mathcal{U}_\mathcal{B}\mathcal{U}_\mathcal{A}}$, then $\mathcal{U}_\mathcal{B}$ Chooses $b \epsilon_R Z^*_{q1}$ and calculates $X_{\mathcal{U}_\mathcal{B}} = g^b(mod\mathcal{N})$, $K_{\mathcal{U}_\mathcal{B}\mathcal{U}_\mathcal{A}} = (X_{\mathcal{U}_\mathcal{A}})^b = g^{ab}(mod\mathcal{N}^2)$ $\mathcal{U}_\mathcal{A}$ calculates $\mu_{\mathcal{U}_\mathcal{B}\mathcal{U}_\mathcal{A}} = H(\mathcal{U}_\mathcal{B}, \mathcal{U}_\mathcal{A}, X_{\mathcal{U}_\mathcal{B}}, X_{\mathcal{U}_\mathcal{A}}, K_{\mathcal{U}_\mathcal{B}\mathcal{U}_\mathcal{A}})$ and sends $(V_{S\mathcal{U}_\mathcal{A}}, V_{\mathcal{U}_\mathcal{B}S}, \mu_{\mathcal{U}_\mathcal{A}\mathcal{U}_\mathcal{B}})$ *to AS.*

5. $AS \rightarrow \mathcal{U}_\mathcal{B} : V_{S\mathcal{U}_\mathcal{A}}, V_{S\mathcal{U}_\mathcal{B}}, \mu_{\mathcal{U}_\mathcal{A}\mathcal{U}_\mathcal{B}}$

If AS effectively verifies $V_{S\mathcal{U}_\mathcal{A}}$ and $V_{\mathcal{U}_\mathcal{B}S}$, then calculates $V_{S\mathcal{U}_\mathcal{A}} = H(AS, \mathcal{U}_\mathcal{A}, X_{\mathcal{U}_\mathcal{A}}, X_{\mathcal{U}_\mathcal{B}}, K_{S\mathcal{U}_\mathcal{A}})$ and $V_{S\mathcal{U}_\mathcal{B}} = H(AS, \mathcal{U}_\mathcal{B}, X_{\mathcal{U}_\mathcal{B}}, X_{\mathcal{U}_\mathcal{A}}, K_{S\mathcal{U}_\mathcal{B}}))$ and sends $(V_{S\mathcal{U}_\mathcal{A}}, V_{SU_\mathcal{B}}, \mu_{\mathcal{U}_\mathcal{A}\mathcal{U}_\mathcal{B}})$ to $\mathcal{U}_\mathcal{A}$.

6. $\mathcal{U}_\mathcal{B} \rightarrow \mathcal{U}_\mathcal{A} : V_{S\mathcal{U}_\mathcal{A}}$

If $\mathcal{U}_\mathcal{B}$ effectively verifies $\mu_{\mathcal{U}_\mathcal{A}\mathcal{U}_\mathcal{B}}$ and $V_{S\mathcal{U}_\mathcal{B}}$, then sends $V_{S\mathcal{U}_\mathcal{A}}$ to $\mathcal{U}_\mathcal{A}$. $\mathcal{U}_\mathcal{A}$ in the end verifies $V_{S\mathcal{U}_\mathcal{A}}$. Therefore, $\mathcal{U}_\mathcal{A}$ and $\mathcal{U}_\mathcal{B}$ have $SK = H(\mathcal{U}_\mathcal{A}, \mathcal{U}_\mathcal{B}, AS, K_{\mathcal{U}_\mathcal{A}\mathcal{U}_\mathcal{B}}) = H(\mathcal{U}_\mathcal{A}, \mathcal{U}_\mathcal{B}, AS, K_{\mathcal{U}_\mathcal{B}\mathcal{U}_\mathcal{A}})$ as a common session key shared between them.

B. ROUND-COMPETENT VERIFIER-BASED AUTHENTICATION TECHNIQUE FOR TMIS

We've demonstrated an efficient round-competent verifier-based authentication technique in this subsection. The projected authentication technique can be implemented

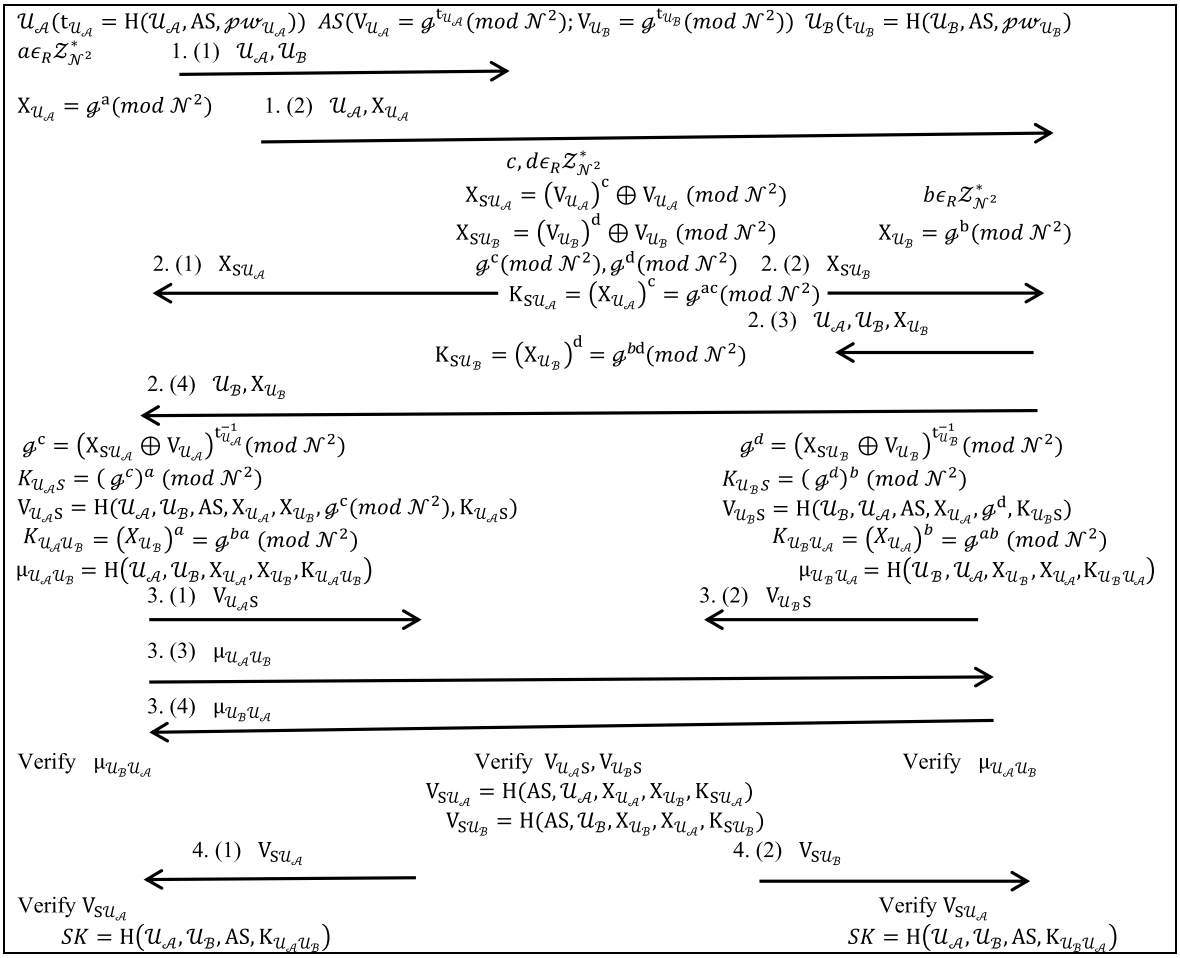

FIGURE 3. Round-competent verifier-based authentication technique for TMIS.

by concurrent rearrangement and messages sending, and obtaining a round-efficient method, which is indicated in Fig. 3. The variants of round-efficient can be executed as follows in following four rounds.

1. (1) $\mathcal{U}_\mathcal{A} \rightarrow$ AS: $\mathcal{U}_\mathcal{A}, \mathcal{U}_\mathcal{B}$
   (2) $\mathcal{U}_\mathcal{A} \rightarrow \mathcal{U}_\mathcal{B} : \mathcal{U}_\mathcal{A}, X_{\mathcal{U}_\mathcal{A}}$
2. (1) AS $\rightarrow \mathcal{U}_\mathcal{A} : X_{S\mathcal{U}_\mathcal{A}}$
   (2) AS $\rightarrow \mathcal{U}_\mathcal{B} : X_{S\mathcal{U}_\mathcal{B}}$
   (3) $\mathcal{U}_\mathcal{B} \rightarrow$ AS : $\mathcal{U}_\mathcal{A}, \mathcal{U}_\mathcal{B}, X_{\mathcal{U}_\mathcal{B}}$
   (4) $\mathcal{U}_\mathcal{B} \rightarrow \mathcal{U}_\mathcal{A} : \mathcal{U}_\mathcal{B}, X_{\mathcal{U}_\mathcal{B}}$
3. (1) $\mathcal{U}_\mathcal{A} \rightarrow$ AS : $V_{\mathcal{U}_\mathcal{A}S}$,
   (2) $\mathcal{U}_\mathcal{B} \rightarrow$ AS:$V_{\mathcal{U}_\mathcal{B}S}$
   (3) $\mathcal{U}_\mathcal{A} \rightarrow \mathcal{U}_\mathcal{B} : \mu_{\mathcal{U}_\mathcal{A}\mathcal{U}_\mathcal{B}}$
   (4) $\mathcal{U}_\mathcal{B} \rightarrow \mathcal{U}_\mathcal{A} : \mu_{\mathcal{U}_\mathcal{B}\mathcal{U}_\mathcal{A}}$
4. (1) AS $\rightarrow \mathcal{U}_\mathcal{A} : V_{S\mathcal{U}_\mathcal{A}}$
   (2) AS $\rightarrow \mathcal{U}_\mathcal{B} : V_{S\mathcal{U}_\mathcal{B}}$

V. SECURITY ANALYSIS AND DISCUSSIONS

Here, we have demonstrated the security analysis of proposed authentication technique.

A. SESSION KEY SECURITY (AKE SECURITY)

The security concept describes that a *foe* can't effectively differentiate from a challenger between two encrypted messages by the same random string or session key by an impartial coin C. The *foe* opts for a reply and sends message to the challenger. An impartial coin C$\epsilon\{0, 1\}$ is flipped by the challenger and chooses to return the message encrypted by the real session key, if C $=$ 1 or encrypted by a random string, if C $=$ 0. The opponent attempts to correctly conjecture the value of the secret bit. The authenticated key exchange (AKE)-advantage of a *foe*'s case is that it breaches a procedure's in-distinguishability is $Adv^{ake}_{\mathbb{P}}(\mathcal{U}_\mathcal{A})$. The procedure $\mathbb{P}$ is AKE-secure, if $Adv^{ake}_{\mathbb{P}}(\mathcal{U}_\mathcal{A})$ is negligible [29]–[32].

B. ENTROPY SMOOTHING HASH

A family of keyed hash function $\mathbb{H} : \{\mathbb{H}_\mathcal{K}\}_{\mathcal{K}\in\mathcal{K}}$ and each $\mathbb{H}_\mathcal{K}$ is a function that maps G group to $\{0, 1\}^l$. Let, D be an algorithm with an element of $\mathcal{K}$, an element of $\{0, 1\}^l$, and a bit of output as input. D's ES-advantage is defined as $|\Pr[\mathcal{K} \in \mathcal{K}, r \in Z_R : D(r, \mathbb{H}_\mathcal{K}(r)) = 1] - \Pr[h \in Z_R, r_A \in Z_R : D(r, h) = 1]|$ and is represented as ε_{es}. The $\mathbb{H}$ is then entropy smoothing, if the ES benefit ε_{es} of any effective algorithm is negligible [33], [34].

The lemma presented in [34] is utilized in our game series, and is defined as:

Lemma 1 (difference lemma): Let $\mathcal{U}_{\mathcal{A}}$, $\mathcal{U}_{\mathcal{B}}$ and $\mathcal{F}$ be events defined in some probability distribution, and suppose that $\mathcal{U}_{\mathcal{A}} \wedge \neg\mathcal{F} \leftrightarrow \mathcal{U}_{\mathcal{B}} \wedge \neg\mathcal{F}$. Then,

$$|\Pr[\mathcal{U}_{\mathcal{A}}] - \Pr[\mathcal{U}_{\mathcal{B}}] \leq \Pr[\mathcal{F}].$$

C. SESSION KEY SECURITY (AKE SECURITY) FOR THE PROPOSED TECHNIQUE

The presented technique is divided into three sub-technique for 2PAKE. Theorem 1 initially shows that the 2PAKE sub-techniques containing $\mathcal{U}_{\mathcal{A}}$ and *AS*, and involving $\mathcal{U}_{\mathcal{B}}$ and *AS* have AKE security, if the hash function used is secure and the hypotheses of the Decisional DH (DDH) are in *G*.

Theorem 1: The probability of a *foe* breaching the AKE security of 2PAKE procedure involving $\mathcal{U}_{\mathcal{A}}$ and *AS*:

$$Adv^{ake}_{2pake} \leq 2(Adv^{ddh}_{G}\left(\mathcal{U}_{\mathcal{A}_{ddh}}\right) + \varepsilon_{es} + \frac{1}{\mathcal{N}^2}),$$

where Adv^{ddh}_{G} is the advantage of a DDH attacker solving the DDH problem; ε_{es} is the ES-advantage of some efficient algorithm and is negligible, if *h* is entropy smoothing; the password is a dictionary of size $\mathcal{N}^2$.

Proof: Game G_i determines ε_i event probability that the *foe* wins this game. The G_0 start game is the real attack on the 2PAKE procedure. The final game G_4 concludes a negligible advantage for breaking the 2PAKE procedure's AKE security.

Game G_0 : This game is a test for the real attack. We have, by the definition

$$Adv^{ake}_{2pake}\left(\mathcal{U}_{\mathcal{A}}\right) = |2\Pr[E_0] - 1| \tag{1}$$

Game G_1 : This game contemplates password guessing attacks. Since, the $\mathcal{PW}_{\mathcal{U}_{\mathcal{A}}}$ password is encrypted using a one-way cryptographic function, each calculation of $\left(V_{\mathcal{U}_{\mathcal{A}}}\right)^{\mathrm{c}} \oplus V_{\mathcal{U}_{\mathcal{A}}}$, where $V_{\mathcal{U}_A} = \boldsymbol{g}^{H(\mathcal{U}_{\mathcal{A}}, AS, \mathcal{PW}_{\mathcal{U}_{\mathcal{A}}})}$ and C is a specific arbitrary number, is dissimilar. The *foe* therefore has no details to test his/her claims about password. Then, we have

$$|\Pr[E_0] - \Pr[E_1]| \leq \frac{1}{\mathcal{N}^2}. \tag{2}$$

Game G_2 : The game turns, game G_1 into game G_2, computing H, simply by randomly selecting it rather than as a hash. Then, we got

$$|\Pr[E_1] - \Pr[E_2]| \leq \varepsilon_{es}. \tag{3}$$

Game G_3 : This game turns, G_2 game into G_3 game by utilizing a triple (X, Y, Z) sample from a random distribution $(\boldsymbol{g}^x, \boldsymbol{g}^y, \boldsymbol{g}^z)$ instead of a triple DDH distribution.

Let, $\mathcal{U}_{\mathcal{A}_{ddh}}$ be a challenger that attempts to break the distinguishability of DDH problem in the group $\boldsymbol{G}$, and let $\mathcal{U}_{\mathcal{A}_{ake}}$ be an adversary i.e. designed to break the protection by session key. By flipping an impartial $\mathrm{C} \in \{0, 1\}$ coin, $\mathcal{U}_{\mathcal{A}_{ddh}}$ chooses to return the real $K_{\mathcal{U}_{\mathcal{A}}S}$ session key (if $\mathrm{C} = 1$) or an arbitrary string (if $\mathrm{C} = 0$) to $\mathcal{U}_{\mathcal{A}_{ake}}$.

Then, $\mathcal{U}_{\mathcal{A}_{ake}}$ produces, and it predict bit C', if $\mathrm{C}' = \mathrm{C}$ then wins. The yield is returned exactly it was in the previous experiment executed except for (X, Y, Z) it received as input. If $\mathcal{U}_{\mathcal{A}_{ake}}$ yields C, then $\mathcal{U}_{\mathcal{A}_{ddh}}$ yields 1; else 0.

If (X, Y, Z) is a true triple Diffie-Hellman, $\mathcal{U}_{\mathcal{A}_{ddh}}$ runs like $\mathcal{U}_{\mathcal{A}_{ake}}$ in G_3 and thus like $\Pr\left[\mathcal{U}_{\mathcal{A}_{ddh}} \text{ yields } 1\right] = \Pr[E_3]$. If (X, Y, Z) is a triple random, $\mathcal{U}_{\mathcal{A}_{ddh}}$ must run $\mathcal{U}_{\mathcal{A}_{ake}}$ in G_4 and thus $\Pr\left[\mathcal{U}_{\mathcal{A}_{ddh}} \text{yields } 1\right] = \Pr[E_4]$. Hence, we have

$$|\Pr[E_3] - \Pr[E_4]| \leq Adv^{ddh}_{G}\left(\mathcal{U}_{\mathcal{A}_{ddh}}\right) \tag{4}$$

Subsequently, all the session keys are arbitrary and independent, and we do not find any information leaked about them, we have

$$\Pr[E_4] = \frac{1}{2} \tag{5}$$

By summing Eq. (1)–(5) and we use Lemma 1,

$$Adv^{ake}_{2pake}\left(\mathcal{U}_{\mathcal{A}_{ake}}\right) \leq 2(Adv^{ddh}_{G}\left(\mathcal{U}_{\mathcal{A}_{ddh}}\right) + \varepsilon_{es} + \frac{1}{\mathcal{N}^2})$$

Therefore, the proof is done.

Theorem 2 shows that if the used hash function is secure and DDH assumptions hold in the group $\boldsymbol{G}$, the proposed 2PAKE sub-technique that involves $\mathcal{U}_{\mathcal{B}}$ and *AS* has AKE security. Because, we can conclude Theorem 2 by using Theorem 1, this does not pose the proof of Theorem 2 here.

Theorem 2: The probability of an adversary breaching the 2PAKE procedure's AKE defense with *B* and *AS* involved:

$$Adv^{ake}_{2pake} \leq 2(Adv^{ddh}_{G} + \varepsilon_{es} + \frac{1}{\mathcal{N}^2}),$$

where the parameters Adv^{ddh}_{G}, $\mathcal{N}$ and ε_{es} are same as in Theorem 1.

The reliability of hash function and DDH assumption hold in $\boldsymbol{G}$ is shown by Theorem 3, hence the proposed 3-party verifier-based technique would have AKE reliability.

Theorem 3: The probability of an adversary compromising the AKE security of the proposed verifier-based system:

$$Adv^{ake}_{3pake} \leq 2(3(Adv^{ddh}_{G} + \varepsilon_{es}) + \frac{2}{\mathcal{N}^2}),$$

where Adv^{ake}_{2pake} denotes the advantage that the opponent breaks the AKE security of the 2PAKE technique and are characterized in Theorem 1 and Theorem 2; and Adv^{ddh}_{G}, $\mathcal{N}$ and ε_{es} as a parameters are used shown in theorems 1 and 2.

Proof: The starting game G_0, assumed to be a real attack on the proposed verifier-based technique and G_4, the terminal game concludes a negligible advantage in breaking the proposed verifier-based technique's AKE protection.

Game G_0 : Real attack is tested in this game. By definition we've

$$Adv^{ake}_{3pake}\left(\mathcal{U}_{\mathcal{A}}\right) = |2\Pr[E_0] - 1| \tag{6}$$

Game G_1 : After deleting session key, $K_{\mathcal{U}_{\mathcal{A}}S}$ is replaced in 2PAKE with $\mathcal{U}_{\mathcal{A}}$ and *S* as a random $K'_{\mathcal{U}_{\mathcal{A}}S}$, then game is modifies. By [32], [35], the adversary's $\mathcal{U}_{\mathcal{A}_{2pake-1}}$ successful probability between G_0 and G_1 is at least twice the probability

that the underlying 2PAKE involving $\mathcal{U}_{\mathcal{A}}$ and S will breach the defence. Then, we got

$$|\Pr[E_1] - Pr[E_0] \leq Adv^{ake}_{2pake}\left(\mathcal{U}_{\mathcal{A}_{2pake-1}}\right) \quad (7)$$

Game G_2 : The preceding game is revised here by substituting $K_{\mathcal{U}_{\mathcal{B}}S}$, session key in 2PAKE with a $K'_{\mathcal{U}_{\mathcal{B}}S}$. We have similar claims used in the previous game

$$|\Pr[E_2] - Pr[E_1] \leq Adv^{ake}_{2pake}\left(\mathcal{U}_{\mathcal{A}_{2pake-2}}\right) \quad (8)$$

Game G_3 : This game transforms, game G_1 into game G_2, calculating $\mathbb{H}$ by simply randomly selecting it instead of as a hash. Then, we got

$$|\Pr[E_2] - \Pr[E_3]| \leq \varepsilon_{es} \quad (9)$$

Game G_4 : The identical arguments are adopted from Theorem 1, hence game G_3 turns into game G_4 by utilizing a triple sample (X, Y, Z) from algorithm $(\boldsymbol{g}^x, \boldsymbol{g}^y, \boldsymbol{g}^z)$ which performs random distribution, instead of a triple DDH. Then, we got

$$|\Pr[E_3] - Pr[E_4] \leq Adv^{ddh}_{G}\left(\mathcal{U}_{\mathcal{A}_{ddh}}\right) \quad (10)$$

and

$$\Pr[E_3] = \frac{1}{2} \quad (11)$$

By summing Eq. (8)–(11), and we use Lemma 1,

$$\begin{aligned} &Adv^{ake}_{3pake}\left(\mathcal{U}_{\mathcal{A}_{ake}}\right) \\ &\leq 2Adv^{ake}_{2pake}\left(\mathcal{U}_{\mathcal{A}_{ake_{2pake-1}}}\right) + 2\varepsilon_{es} \\ &\quad + Adv^{ake}_{2pake}\left(\mathcal{U}_{\mathcal{A}_{2pake-2}}\right) + 2Adv^{ddh}_{G}\left(\mathcal{U}_{\mathcal{A}_{ddh}}\right) \\ &\leq 2(3(Adv^{ddh}_{G} + \varepsilon_{es}) + \frac{2}{N^2}) \end{aligned}$$

Therefore, the proof is done.

Theorem 4: The new 3-party authentication technique based on a verifier can withstand stolen verifier attacks.

Proof: In the presented technique, a challenger $\mathcal{U}_{\mathcal{A}}$ takes a fake of the verifier $V_{\mathcal{U}_A}$ for $\mathcal{U}_{\mathcal{A}}$, where $\mathrm{V}_{\mathcal{U}_{\mathcal{A}}} = \boldsymbol{g}^{\mathcal{U}_{\mathcal{A}}}(mod\mathcal{N}^2)$, $\mathcal{P}_{\mathcal{W}\mathcal{U}_{\mathcal{A}}}$ is password of $\mathcal{U}_{\mathcal{A}}$ and $\mathrm{t}_{\mathcal{U}_{\mathcal{A}}} = \mathrm{H}(\mathcal{U}_{\mathcal{A}}, \mathcal{AS}, \mathcal{P}_{\mathcal{W}\mathcal{U}_{\mathcal{A}}})$, in the database of AS. Due to the PDL problem, *foe* cannot derive the correct $\mathrm{t}_{\mathcal{U}_{\mathcal{A}}}$ from $V_{\mathcal{U}_{\mathcal{A}}}$. He/she cannot calculate $\boldsymbol{g}^{\mathrm{c}} = \left(\mathrm{X}_{\mathrm{S}\mathcal{U}_{\mathcal{A}}} \oplus \mathrm{V}_{\mathcal{U}_{\mathcal{A}}}\right)^{\mathrm{t}^{-1}_{\mathcal{U}_{\mathcal{A}}}}(mod\mathcal{N}^2)$, and refer out the validate messages $\left(\mathrm{V}_{\mathcal{U}_{\mathcal{A}}\mathrm{S}}, \mathcal{V}_{\mathcal{U}_{\mathcal{B}}\mathrm{S}}, \mu_{\mathcal{U}_{\mathcal{A}}\mathcal{U}_{\mathcal{B}}}\right)$ to AS, where $K_{\mathcal{U}_{\mathcal{A}}S} = (\boldsymbol{g}^c)^a = \boldsymbol{g}^{ac}(mod\mathcal{N}^2)$, $\mathrm{V}_{\mathcal{U}_{\mathcal{A}}\mathrm{S}} = \mathrm{H}\left(\mathcal{U}_{\mathcal{A}}, \mathcal{U}_{\mathcal{B}}, AS, \mathrm{X}_{\mathcal{U}_{\mathcal{A}}}, \mathrm{X}_{\mathcal{U}_{\mathcal{B}}}, \boldsymbol{g}^{\mathrm{c}}, \mathrm{K}_{\mathcal{U}_{\mathcal{A}}\mathrm{S}}\right)$ and $\mu_{\mathcal{U}_{\mathcal{A}}\mathcal{U}_{\mathcal{B}}} = \mathrm{H}(\mathcal{U}_{\mathcal{A}}, \mathcal{U}_{\mathcal{B}}, \mathrm{X}_{\mathcal{U}_{\mathcal{A}}}, \mathrm{X}_{\mathcal{U}_{\mathcal{B}}}, \mathrm{K}_{\mathcal{U}_{\mathcal{A}}\mathcal{U}_{\mathcal{B}}})$. The challenger $\mathcal{U}_{\mathcal{A}}$ cannot masquerade as a legitimate user. Likewise, if the $\mathcal{U}_{\mathcal{A}}$ challenger takes a fake of the $\mathrm{V}_{\mathcal{U}_{\mathcal{B}}}$ verifier for the $\mathcal{U}_{\mathcal{B}}$ recipient, he/she cannot still extract the correct $t_{\mathcal{U}_{\mathcal{B}}}$, calculate $V_{\mathcal{U}_{\mathcal{B}}S}$ and $\mu_{\mathcal{U}_{\mathcal{B}}\mathcal{U}_{\mathcal{A}}}$, and gives $\left(\mathrm{X}_{\mathcal{U}_{\mathcal{A}}}, \mathrm{X}_{\mathrm{S}\mathcal{U}_{\mathcal{A}}}, \mathrm{X}_{\mathcal{U}_{\mathcal{B}}\mathrm{S}}, \mu_{\mathcal{U}_{\mathcal{B}}\mathcal{U}_{\mathcal{A}}}\right)$ to $\mathcal{U}_{\mathcal{A}}$. Therefore the proposed technique will withstand the stolen verifier attacks.

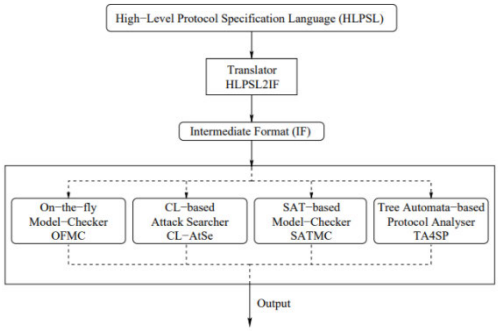

FIGURE 4. Architecture of the AVISPA [49].

```
role uscra(UA, AS, UB : agent, SKas,SKab : symmetric_key, H: hash_func, SND, RCV :
channel(dy))
played_by UA
def=
local State: nat,
    UAB,KSA,SK,IDa,IDb,IDas,PWa: text,
Ta,Lg,Na,G,Xb,VBS,UBA,XSA,KAB,KUB  : text,
 %  : text,
 VAS,Va,Xa,Tai,KAS,Gc,Nc,Gd,Nb : text
const sp1, sp2, sp3, sp4, ua ub ni, ub ua mcu, as ub nj, ub as mcg: protocol id
init State := 0
transition
%%%%%%%%%%%%Registration phase
1. State = 0 /\ RCV(start) =|>
State' := 1 /\ PWa' := new()
/\ Ta':=H(IDa.IDas.PWa')
/\ SND({Ta'}_SKas)
%%%%%%%%%%%%Login & Authentication phase
/\ secret({PWa'}, sp1, {UA})

2. State = 1  /\ RCV(Lg') =|>
State' := 2 /\ PWa' := new()
/\ Na' := new()
/\ Xa':=exp(G.Na')
/\ SND({Xa'.IDa.IDb}_SKas)
/\ witness(UA,UB,ua_ub_ni,Na')

3. State = 2
/\ RCV({exp(G.Nb').XSA'.H(IDb.IDa.IDas.exp(G.Na').Gd'.exp(Gd'.Nb')).UBA'}_SKab) =|>
State' := 3
/\ PWa' := new()
/\ Gc':=exp(xor(XSA'.exp(G.H(IDa.IDas.PWa'))).Tai)
/\ KAS':=exp(Gc'.Na')
/\ VAS':=H(IDa.IDb.IDas.exp(G.Na').exp(G.Nb').Gc'.KAS')
/\ KAB':=exp(exp(G.Nb').Na')
/\ UAB':=H(IDa.IDb.exp(G.Na').exp(G.Nb').KAB')
/\ SND({VAS'.H(IDb.IDa.IDas.exp(G.Na').Gd'.exp(Gd'.Nb')).UAB'} SKas)

3. State = 3
/\ RCV(H(IDas.IDa.exp(G.Na').exp(G.Nb').KSA')) =|>
State' := 4
% genrate secret key
/\ KUB' := new()
/\ IDas' := new()
/\ SK' := H(IDa.IDb.IDas'.KUB')
/\ SND({SK'}_SKab)
/\ Nc' := new()
/\ request(UA,UB,ub_ua_mub,Nc')
end role
```

FIGURE 5. Role specification in HLPSL for User A (Patient/Doctor).

VI. FORMAL VERIFICATION ON AVISPA

In this section, we simulate the proposed authentication protocol technique for the formal verification using Automated Validation of Internet Security Protocols and Applications (AVISPA) [47], [48] for checking security and authenticity properties. Moreover, verification of proposed protocol using AVISPA v.1.1 is modelled in High-Level Protocol Specification Language (HLPSL). AVISPA is well known verification tool to verify the proposed protocol is secure against replay attack and man-in-the-middle attack. All experimentations are performed on Intel Core i5-8365U CPU @1.90 GHz with 8GB RAM and 1 TB HDD using 64-bit Linux operating system.

AVISPA tool can be implemented by the following four back-ends;

1. On-the-Fly Model-Checker (OFMC)
2. Constraint-Logic-based Attack Searcher (CL-AtSe)
3. Tree Automate-Based Protocol Analyzer (TA4SP)
4. SAT-Based Model-Checker (SATMC)

```
role authenticationserver(UA, AS, UB : agent, SKas, SKab,SKbs : symmetric_key,H: hash_func, SND, RCV : channel(dy))
played_by AS
def=
local State: nat,
Nc,Va,G,Vb : text,
 Ta,Tb,Lg,IDa,IDb,Xa,Sc,Sd,XSA,XSB,Nj,Nb: text,
 Gc,Gd,KSA,KSB,Na,Xb,VAS,VBS,UAB,VSA,IDas : text,
 VSB : text,|
 SKi, SKj, SKc: text
const sp1, sp2, sp3, sp4 : protocol_id,
ua_ub_ni, ub_ua_mub, as_ub_nj, ub_as_mcg: protocol_id
init State := 0
transition
%%%%%%%%%%%%Registration phase
1. State = 0 /\ RCV({Ta'}_SKas) =|>
State' := 1  /\ Va' := exp(G.Ta')
/\ Tb' := new()
 /\ Vb' := exp(G.Tb')
/\Lg' := new()
/\ SND({Lg'}_SKbs)
 /\ secret({Va',Vb'},sp2,{AS})
 %%%%%%%%%%%%Login & Authentication phase

2. State = 2
/\ RCV({IDa.IDb.exp(G.Na')}_SKas) =|>
State' := 3 /\ Sc':= new() /\ Sd' := new()
/\ Ta' := new()
/\ Tb' := new()
/\ Xb' := new()
/\ XSA':=xor(exp(G.Ta').exp(exp(G.Ta').Sc'))
/\ XSB':=xor(exp(G.Tb').exp(exp(G.Tb').Sd'))
/\ Gc':=exp(G.Sc')
/\ Gd':=exp(G.Sd')
/\ KSA':=exp(exp(G.Na'),Sc')
/\ KSB':=exp(Xb',Sd')
/\ SND{exp(G.Na').XSA'.XSB'}_SKbs)
/\ Nj':= new()
/\ witness(AS,UB,as_ub_nj,Nj')
3. State = 3
/\ RCV({H(IDa.IDb.IDas.exp(G.Na').Xb'.Gc'.exp(Gc'.Na')).H(IDb.IDa.IDas.exp(G.Na').Gd'. exp(Gd'.Nb')).UAB'}_SKas) =|>
State' := 4
%% verify VAS & VBS
/\ Sc':= new() /\ Sd' := new()
/\ VSA':= H(IDas.IDa.(exp(G.Na')).Xb'.exp(exp(G.Na'),Sc'))
/\ VSB':=H(IDas.IDb.Xb'.exp(G.Na').exp(Xb',Sd'))
/\ SND{VSA'.VSB'.UAB'}_SKbs)
/\ Nc':= new()
/\ request(AS,UB,ub_as_mcg,Nc')
end role
```

FIGURE 6. Role specification in HLPSL for the authentication server.

```
played_by UB
def=
local State: nat,
 PWb,Tb,IDb,IDas,Xa,XSA,Nb,Xb,G,Sc: text,
 Gd,KBA,VBS,IDa,UBA,XSB,Nc,KSA,KAB,IDab,KUB,SK,Na: text,
 Vb,Tbi,KBS,VSA,VSB,UAB,Nj,Ni : text,
 SKi, SKj, SKc: text
const sp1, sp2, sp3, sp4, ua_ub_ni, ub_ua_mub, as_ub_nj, ub_as_mcg : protocol_id
init State := 0
transition
%%%%%%%%%%%%% Registeration  phase %%
1. State = 0 /\ RCV(start) =|>
State' := 1 /\ PWb' := new()
/\ Tb':=H(IDb.IDas.PWb')
 /\ SND({Tb'}_SKbs)
 /\ secret({PWb'}, sp2, {UB})
%%%%%%%%%%%%%Login & Authentication phase %%%

2. State = 1 /\ RCV({exp(G.Na').XSA'.XSB'}_SKbs) =|>
State' := 2
/\ Nb':= new()
/\ Tbi' := new()
/\ Xb':= exp(G.Nb')
/\ Gd':= exp(xor(XSB'.exp(G.Tbi')).Tbi')
/\ KBS':= exp(Gd'.Nb')
/\ KBA':= exp(exp(G.Na').Nb')
/\ VBS':= H(IDb.IDa.IDas.exp(G.Na').Gd'.KBS')
/\ UBA':= H(IDb.IDa.Xb'.exp(G.Na').KBA)
/\ SND({Xb'.XSA'.VBS'.UBA'}_SKab)

3. State = 2
/\ RCV({VSA'.VSB'.UAB'}_SKbs) =|>
State' := 3
/\ Nb':= new()
/\ Na' := new()
/\ Nc' := new()
/\ Sc' := new()
/\ VSA':=H(IDas.IDa.exp(G.Na').exp(G.Nb').exp(exp(G.Na'),Sc'))
/\ UAB':=H(IDa.IDb.exp(G.Na').exp(G.Nb').exp(exp(G.Nb').Na'))
 /\ SND(VSA')
4. State = 3
/\ RCV({H(IDa.IDb.IDab'.KUB')}_SKab) =|>
State' := 4
/\ Ni':= new()
/\ Nj':= new()
/\ Nc':= new()
/\ SK' := H(IDa.IDb.IDab'.KUB')
 /\ witness(UB,UA,ub_ua_mub,Nc')
 /\ witness(UB,AS,ub_as_mcg,Nc')
  /\ request(UA,UB, ua_ub_ni,Ni')
 /\ request(AS,UB, as_ub_nj,Nj')
end role
```

FIGURE 7. Role specification in HLPSL for User B (Patient/Doctor).

AVISPA is based on HLPSL for describing the protocols security properties. HLPSL is a role based language where each participants in a module known by some basic role.

```
role session(UA, AS, UB : agent, SKas, SKab,SKbs:
symmetric_key, H: hash_func)
def=
local SN1, SN2, SN3, RV1, RV2, RV3: channel(dy)
composition
usera(UA,AS, UB, SKas,SKab,H, SN1, RV1)
/\ authenticationserver(UA,AS,UB, SKas,SKab,SKbs, H, SN2, RV2)
/\ userb(UA, AS, UB,SKab, SKas, H, SN3,
RV3)
end role
```

FIGURE 8. Role specification in HLPSL for the session.

```
role environment()
def=
const ua, as, ub : agent,
skas, skbs,skab : symmetric_key,
h: hash_func,
gidj,hidi,idi: text,
ua_ub_ni, ub_ua_mub, as_ub_nj, ub_as_mcg:
protocol_id,
sp1,sp2,sp3,sp4: protocol_id
intruder_knowledge = {ua,as,ub,gidj,hidi,idi,h}
composition
session(ua,as,ub,skas,skbs,skab,h)
/\session(i,as,ub,skas,skbs,skab, h)
/\session(ua,i,ub, skas,skbs,skab,h)
/\session(ua,as,i, skas,skbs,skab,h)
end role
```

FIGURE 9. Role specification in HLPSL for the environment.

```
goal
secrecy_of sp1, sp2, sp3, sp4
authentication_on ua_ub_ni
authentication_on ub_ua_mub
authentication_on as_ub_nj
authentication_on ub_as_mcg
end goal
environment()
```

FIGURE 10. Role specification in HLPSL for the goal.

Roles like a participant role for representing participants in a protocol, composition role for scenario in a basic role. As shown in Fig. 4, HLPSL specifications are translated into intermediate format (IF) by the translator (*hlpsl2if*) then IF is converted into one of the four back-ends output format.

A. SPECIFYING AVISPA IN PROPOSED PROTOCOL TECHNIQUE

For HLPSL implementation, in proposed protocol the basic roles for each participants defined are User *A* (Patients/Doctor), User *B* (Patient/Doctor), and Authentication server (*AS*). Fig. 5 shows the role for User *A*, Fig. 6 represents the role for *AS*, and Fig. 7 indicates the role for User *B*. The role of session, environment, and goal is presented in Fig. 8, Fig. 9, and Fig. 10 respectively.

The basic terminologies used for HLPSL are indicated as follows;

- *secret* (UA, IDa, *AS*): IDa denotes an information *A* that is only known to *AS*.
- *witness* (UA, UB, *ua_ub_ni*, N*a*): *ua_ub_ni* is a protocol id which denotes a weakness authentication factor, N*a* that is used by UA to authenticate UB.
- *request* (UA,UB, *ua_ub_mub*, N*c*): *ua_ub_mub* is a protocol id, denotes a strong authentication factor, N*c*.

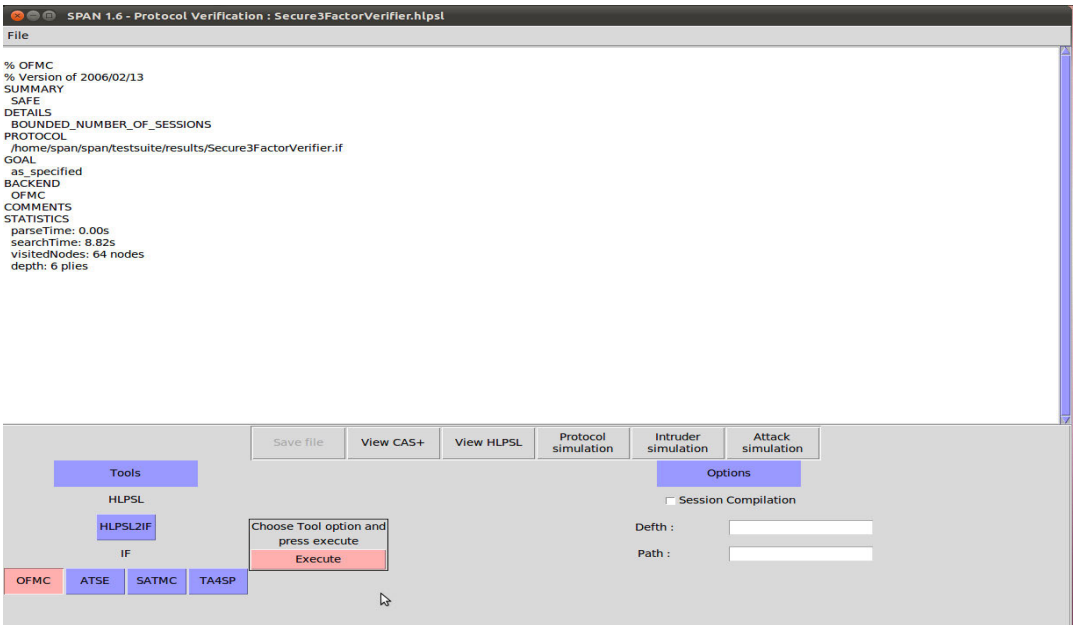

FIGURE 11. Final result of the formal security analysis using AVISPA generated by OFMC back-end.

TABLE 3. Attacks and Vulnerabilities (R1: withstand online password guessing attacks, R2: withstand stolen verifier attacks, R3: Secure issue key confirmation, R4: withstand user impersonation attacks, R5: User's Anonymity, R6: Resistance to tracking attacks, and R7: offline password guessing attack).

Ref.	R1	R2	R3	R4	R5	R6	R7
Lee *et al.*'s technique [8]	Y	N	N	N	Not Provided	N	N
Wang *et al.*'s technique [38]	Y	Y	N	N	N	N	N
Kwon *et al.*'s technique [6]	Y	Y	N	N	N	N	N
Lin-Lee's technique [10]	Y	Y	Y	Y	N	N	N
Lu *et al.*'s technique [21]	Y	Y	Y	Y	Y	Y	N
Deebak *et. al.*'s technique [36]	Y	Y	Y	Y	Y	N	Y
Chen *et al.*'s technique [37]	Y	Y	Y	N	Y	Y	Y
Proposed technique	Y	Y	Y	Y	Y	Y	Y

UB requests to UA for Nc to authenticate. UA represent the User A, UB represent the User B.

B. AVISPA SIMULATION RESULTS FOR PROPOSED PROTOCOL TECHNIQUE

To simulate the proposed technique, we used OFMC back-end of AVISPA as shown in Fig. 11. The results ensure that the proposed technique is secured against passive and active attacks such as replay attack, man-in-the-middle attack, and user anonymity attack which are the primary major secure requirements in TMIS.

VII. PERFORMANCE ANALYSIS

To analyses the performance of proposed technique we target to investigate on the storage cost, communication and computational overheads. To do so, the comparison of proposed technique is performed with other related authentications schemes. Table 3 presents the various attacks and vulnerabilities targeted in the performance evaluation.

A. COMPUTATION COST

The performance metrics related to existing similar authentication schemes and our technique is presented in Table 4. Here, we compared the proposed technique with Deebak *et al.*'s [36] technique, Chen *et al.*'s [37] technique, Wang *et al.*'s [38] technique, Chen *et al.*'s technique [45], Sahoo *et al.*'s technique [54], Wu *et. al.*'s technique [55] and Moghadam *et al.*'s technique [56]. To perform comparison amongst our authentication technique, the various operations are chosen such as modular exponential operations, Hash/MAC operations, and other properties of authentication technique.

For the analysis of performance, we utilized the symbols T_H, T_{EXP}, T_{XOR}, T_{ED}, T_{EL} and T_{MD} to indicate hash/MAC operations, exponentiation operations, XOR ($\oplus$) operations,

TABLE 4. Comparison of computation cost with other 3PAKA schemes.

Authentication technique / Properties	[36]	[37]	[38]	[45]	[56]	[54]	[55]	Proposed technique
A	$2T_{EXP} + 2T_{XOR} + 6T_H = 1206T_H$	$3T_{EXP} + 2T_H = 1802\ T_H$	$4T_{EXP} + 1T_{XOR} + 3T_H + 2T_{ED} = 2405\ T_H$	$3T_{EXP} + 6T_H = 1806\ T_H$	$2T_{ED} + 5T_H + 3T_{EL} = 1810\ T_H$	$2T_{ED} + 8T_H + 3T_{EL} = 1813\ T_H$	$1T_{ED} + 9T_H + 3T_{EL} = 1813\ T_H$	$2T_{EXP} + 1T_{XOR} + 4T_H = 1204\ T_H$
Transmissions messages / rounds for A	3m/1r	5m/2r	3m/2r	4m/2r	4m/4r	4m/2r	4m/3r	6 m/4r
B	$2T_{EXP} + 2T_{XOR} + 6T_H = 1206\ T_H$	$3T_{EXP} + 2T_H = 1802T_H$	$4T_{EXP} + 1T_{XOR} + 3T_H + 2T_{ED} = 2405T_H$	$3T_{EXP} + 6T_H = 1806T_H$	$2T_{ED} + 5T_H + 3T_{EL} = 1810\ T_H$	$2T_{ED} + 3T_H + 2T_{EL} = 1207\ T_H$	$1T_{ED} + 9T_H + 2T_{EL} = 1212\ T_H$	$2T_{EXP} + 1T_{XOR} + 4T_H = 1204\ T_H$
Transmissions messages / rounds for B	6m/1r	11m/2r	8m/1r	4m/2r	4m/4r	4m/3r	4m/3r	6 m/4r
S	$3T_{EXP} + 2T_{XOR} + 4T_H = 1804T_H$	$2T_{EXP} + 2T_H = 1202\ T_H$	$6T_{EXP} + 2T_{XOR} + 4T_H + 3T_{ED} = 3607\ T_H$	$4T_{EXP} + 6T_H = 2406\ T_H$	$3T_H + 2T_{EL} = 1205\ T_H$	$2T_{ED} + 4T_H + 2T_{EL} = 1208\ T_H$	$1T_{ED} + 3T_H + 2T_{EL} = 1206\ T_H$	$3T_{EXP} + 2T_{XOR} + 4T_H = 1804\ T_H$
Transmissions messages / rounds for S	10m/2r	2m/1r	1m/4r	2m/1r	4m/4r	4m/2r	4m/3r	6 m/4r
Total	$7T_{EXP} + 6T_{XOR} + 16T_H = 4216\ T_H$	$8T_{EXP} + 6T_H = 4806\ T_H$	$14T_{EXP} + 4T_{XOR} + 10T_H + 7T_{ED} = 8417T_H$	$10T_{EXP} + 16T_H = 6018\ T_H$	$4T_{ED} + 13T_H + 8T_L = 4825T_H$	$6T_{ED} + 15T_H + 7T_L = 4228T_H$	$3T_{ED} + 21T_H + 7T_{EL} = 4231\ T_H$	$7T_{EXP} + 12T_H + 4T_{XOR} = 4212\ T_H$
Total time (ms)	$4216T_H \approx 2120.64$	$4806T_H \approx 2417.41$	$8417T_H \approx 4233.76$	$6018\ T_H \approx 3027.054$	$4825\ T_H \approx 2426.975$	$4228\ T_H \approx 2126.684$	$4231\ T_H \approx 2128.193$	$4212\ T_H \approx 2118.63$

Encryption/Decryption, elliptic curve scalar multiplication point and multiple/division operations respectively. Table 4 presents the comparison among the various techniques and shows the computation cost for verifier-based 3PAKA schemes without server public key (SPK). We also, represented graphically in Fig. 12 the computation costs comparison among various verifier-based 3PAKA schemes without SPK wherein proposed technique takes less cost.

Adopting the experiment results from [35], and [52]–[54] it is observed that the computation time of exponentiation operations is less than elliptic curve scalar multiplication point. Here, we mapped different computation times with hashing time as shown: $T_{MD} = 2.5T_H$, $T_{ED} = T_H$, $T_{EXP} = 600T_H$ and $T_{EL} = 601T_H$. Hence, the rank in term of complexity is expressed as $T_H \approx T_{ED} < T_{MD} < T_{EXP} < T_{EL}$. According to [53], T_H is 0.503 ms, and T_H time unit can be translated to ms. Obviously, our proposed system outperforms other schemes, and indicating the highest level of efficiency. Moreover, our protocol only uses bitwise XOR operation and one-way hash function, $H(\cdot)$, where T_{XOR}, represent execution time for bitwise XOR operation and T_H, represent execution time for one-way hash function. We observed that the value of T_{XOR} is negligible in the experimentation. In Table 4, we compared our technique with other authentication techniques [36]–[38], [45], [54], and [55]. The computation cost of our technique is cost effective compared to the mentioned schemes.

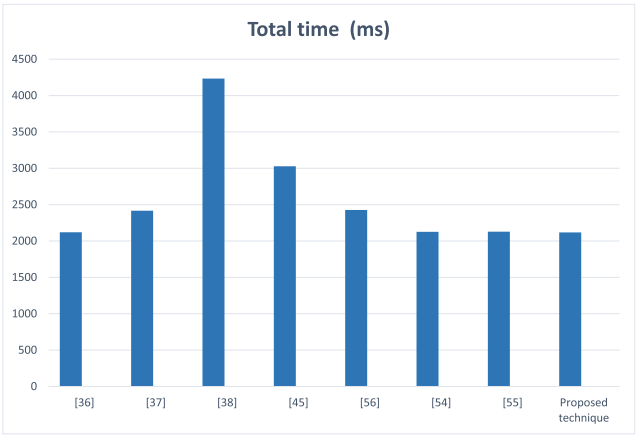

FIGURE 12. Computation cost comparison among various verifier-based 3PAKA schemes without SPK.

B. COMMUNICATION AND STORAGE COST

In this section, we present the results based on the communication cost and storage cost required by the various schemes

TABLE 5. Comparison of communication cost with other 3PAKA schemes.

Authentication technique → / Properties ↓	[36]	[37]	[38]	[45]	Proposed Technique
Total Communication cost (in bits)	$7L_{EXP} + 16L_H = 11264$ bits	$8L_{EXP} + 6L_H = 9728$ bits	$14L_{EXP} + 10L_H + 7L_{ED} = 18688$ bits	$10\ L_{EXP} + 16L_H = 14336\ bits$	$7L_{EXP} + 12L_H = 10240$ bits
Total Communication cost (in KB)	1.2815 KB	1.2147 KB	2.336 KB	1.792 KB	1.28 KB

in comparison with the proposed technique. Table 5 shows the comparative analysis of communication cost required for the proposed scheme and other methods.

According to Chen *et al.* [45], to compare the communication cost in bits, we assumed that the output of a random integer is 128-bit, a hash function (SHA-256) is $L_H = 256bit$, and modular exponential operation of $L_{exp} = 1024bit$. Generally, T_{MD} is much larger than T_H ($\approx 2.5 \times T_H$) assumed $L_{MD} = 640bit$. From Table 5, we see that the proposed protocol technique costs less in bits compared to the existing techniques [36]–[38], and [45].

Based on [45], we evaluated the storage cost (in bits) for User *A* (Patient/Doctor), *AS* (Authentication Server) and User *B* (Patient / Doctor) of the three participants.

User $\mathcal{U}_\mathcal{A}$ (Patient / Doctor) stores $\mathcal{U}_\mathcal{A}$ and $t_{\mathcal{U}_\mathcal{A}}$. As an example of hash function, we utilized SHA256 and output of SHA256 is 256 bits. Using SHA256, we get $t_{\mathcal{U}_\mathcal{A}} = 256$ bits. While considering ID for user i.e. $\mathcal{U}_\mathcal{A} = 128$ bits. Thus, the total storage required by user $\mathcal{U}_\mathcal{A}$ (Patient / Doctor) is $256 + 128 = 384$ bits. Moreover, authentication server stores $\mathcal{U}_\mathcal{A}$, $\mathcal{U}_\mathcal{B}$, $V_{\mathcal{U}_\mathcal{A}}$ and $V_{\mathcal{U}_\mathcal{B}}$. As we are using SHA256, we obtained $V_{\mathcal{U}_\mathcal{A}} = V_{\mathcal{U}_\mathcal{B}} = 256$ bits. The user's ID is $\mathcal{U}_\mathcal{A} = \mathcal{U}_\mathcal{B} = 128$ bits. Therefore, the total storage required by *AS* is $(2 \times 256) + (2 \times 128) = 768$ bits. Nevertheless, user *B* (Patient / Doctor) stores $\mathcal{U}_\mathcal{B}$ and $t_{\mathcal{U}_\mathcal{B}}$. Therefore, the total storage required by user *B* is $128 + 256 = 384$ bits. Hence, the total storage cost required for the proposed technique is 1,536 bits.

VIII. CONCLUSION

In this paper, we explored the principles of verifier-based authentication technique without using public keys of the server, and established reliable and efficient verifier-based authentication technique using PDL wherein exchange of data in TMIS is performed in the absence of server's public key. In addition, the key confirmation is performed without additional rounds numbers and messages, and requires only four rounds and six messages. The proposed technique provides higher security and requires low computational costs as compared to other verifier-based authentication techniques. Moreover, our technique needs fewer transmissions and is proven to be secure under random oracle model. Hence, it is practically more suitable to use for TMISs. In future work, we will develop an efficient bio-hashing based three-factor authentication using the concept of proposed technique for telecare medical information systems.

ACKNOWLEDGMENT

The authors would like to thank anonymous reviewers of IEEE Access Journal for their careful and helpful comments.

COMPLIANCE WITH ETHICAL STANDARDS

CONFLICT OF INTEREST

We declare that we have no conflict of interest.

HUMAN AND ANIMAL RIGHTS

The paper does not contain any studies with human participants or animals performed by any of the authors.

INFORMED CONSENT

Informed consent was obtained from all individual participants included in the study

REFERENCES

[1] C.-T. Li, C.-C. Lee, C.-Y. Weng, and S.-J. Chen, "A secure dynamic identity and chaotic maps based user authentication and key agreement scheme for e-healthcare systems," *J. Med. Syst.*, vol. 40, no. 11, pp. 1–10, Nov. 2016.

[2] C.-T. Li, C.-C. Lee, and C.-Y. Weng, "A secure cloud-assisted wireless body area network in mobile emergency medical care system," *J. Med. Syst.*, vol. 40, no. 5, p. 117, Mar. 2016.

[3] H. T. Yeh, H. M. Sun, and T. Hwang, "Efficient three-party authentication and key agreement protocols resistant to password guessing attacks," *J. Inf. Sci. Eng.*, vol. 19, no. 6, pp. 1059–1070, 2003.

[4] S. W. Lee, H. S. Kim, and K. Y. Yoo, "Efficient verifier-based key agreement protocol for three parties without server's public key," *Appl. Math. Comput.*, vol. 167, no. 2, pp. 996–1003, 2005.

[5] T.-F. Lee, J.-L. Liu, M.-J. Sung, S.-B. Yang, and C.-M. Chen, "Communication-efficient three-party protocols for authentication and key agreement," *Comput. Math. With Appl.*, vol. 58, no. 4, pp. 641–648, Aug. 2009.

[6] J. O. Kwon, I. R. Jeong, K. Sakurai, and D. H. Lee, "Efficient verifier-based password-authenticated key exchange in the three-party setting," *Comput. Standards Interfaces*, vol. 29, no. 5, pp. 513–520, Jul. 2007.

[7] C.-C. Lee, C.-W. Hsu, Y.-M. Lai, and A. Vasilakos, "An enhanced mobile-healthcare emergency system based on extended chaotic maps," *J. Med. Syst.*, vol. 37, no. 5, pp. 1–12, Oct. 2013.

[8] C.-C. Lee, C.-L. Chen, C.-Y. Wu, and S.-Y. Huang, "An extended chaotic maps-based key agreement protocol with user anonymity," *Nonlinear Dyn.*, vol. 69, nos. 1–2, pp. 79–87, Jul. 2012.

[9] C.-T. Li, C.-C. Lee, and C.-Y. Weng, "A secure chaotic maps and smart cards based password authentication and key agreement scheme with user anonymity for telecare medicine information systems," *J. Med. Syst.*, vol. 38, no. 9, pp. 1–11, Sep. 2014.

[10] C. C. Lee, C. T. Li, and C. W. Hsu, "A three-party password-based authenticated key exchange protocol with user anonymity using extended chaotic maps," *Nonlinear Dyn.*, vol. 73, no. 1, pp. 125–132, Jul. 2013.

[11] W. Diffie and M. E. Hellman, "New directions in cryptography," *IEEE Trans. Inf. Theory*, vol. IT-22, no. 6, pp. 644–654, Nov. 1976.

[12] Z. Tan, "A user anonymity preserving three-factor authentication scheme for telecare medicine information systems," *J. Med. Syst.*, vol. 38, no. 3, pp. 1–9, Mar. 2014.

[13] Z. Tan, "An efficient biometrics-based authentication scheme for telecare medicine information systems," *Network*, vol. 2, no. 3, pp. 200–204, 2013.

[14] Z.-Y. Wu, Y.-C. Lee, F. Lai, H.-C. Lee, and Y. Chung, "A secure authentication scheme for telecare medicine information systems," *J. Med. Syst.*, vol. 36, no. 3, pp. 1529–1535, 2012.

[15] A. K. Das, "Analysis and improvement on an efficient biometric-based remote user authentication scheme using smart cards," *IET Inf. Secur.*, vol. 5, no. 3, pp. 145–151, Sep. 2011.

[16] Y. An, "Security analysis and enhancements of an effective biometric-based remote user authentication scheme using smart cards," *J. Biomed. Biotechnol.*, vol. 2012, pp. 1–6, Jul. 2012.

[17] M. K. Khan and S. Kumari, "An improved biometrics-based remote user authentication scheme with user anonymity," *BioMed Res. Int.*, vol. 2013, pp. 1–9, Nov. 2013.

[18] F. Wen, W. Susilo, and G. Yang, "Analysis and improvement on a biometric-based remote user authentication scheme using smart cards," *Wireless Pers. Commun.*, vol. 80, no. 4, pp. 1747–1760, Feb. 2015.

[19] O. Mir and M. Nikooghadam, "A secure biometrics based authentication with key agreement scheme in telemedicine networks for e-health services," *Wireless Pers. Commun.*, vol. 83, no. 4, pp. 2439–2461, 2015.

[20] S. A. Chaudhry, H. Naqvi, and M. K. Khan, "An enhanced lightweight anonymous biometric based authentication scheme for TMIS," *Multimedia Tools Appl.*, vol. 77, no. 5, pp. 5503–5524, 2018.

[21] Y. Lu, L. Li, H. Peng, and Y. Yang, "A biometrics and smart cards-based authentication scheme for multi-server environments," *Secur. Commun. Netw.*, vol. 8, no. 17, pp. 3219–3228, Nov. 2015.

[22] S. A. Chaudhry, H. Naqvi, M. S. Farash, T. Shon, and M. Sher, "An improved and robust biometrics-based three factor authentication scheme for multiserver environments," *J. Supercomput.*, vol. 74, no. 8, pp. 3504–3520, Aug. 2018.

[23] D. He and D. Wang, "Robust biometrics-based authentication scheme for multiserver environment," *IEEE Syst. J.*, vol. 9, no. 3, pp. 816–823, Sep. 2015.

[24] V. Odelu, A. K. Das, and A. Goswami, "A secure biometrics-based multi-server authentication protocol using smart cards," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 9, pp. 1953–1966, Sep. 2015.

[25] R. Amin, N. Kumar, G. Biswas, R. Iqbal, and V. Chang, "A light weight authentication protocol for IoT-enabled devices in distributed cloud computing environment," *Future Gener. Comput. Syst.*, vol. 78, pp. 1005–1019, Jan. 2018.

[26] L. Zhou, X. Li, K.-H. Yeh, C. Su, and W. Chiu, "Lightweight IoT-based authentication scheme in cloud computing circumstance," *Future Gener. Comput. Syst.*, vol. 91, pp. 244–251, Feb. 2019.

[27] S. Barman, H. P. H. Shum, S. Chattopadhyay, and D. Samanta, "A secure authentication protocol for multi-server-based e-healthcare using a fuzzy commitment scheme," *IEEE Access*, vol. 7, pp. 12557–12574, 2019.

[28] Z. Ali, S. Hussain, R. H. U. Rehman, A. Munshi, M. Liaqat, N. Kumar, and S. A. Chaudhry, "ITSSAKA-MS: An improved three-factor symmetric-key based secure AKA scheme for multi-server environments," *IEEE Access*, vol. 8, pp. 107993–108003, 2020.

[29] M. Abdalla, P. A. Fouque, and D. Pointcheval, "Password-based authenticated key exchange in the three-party setting," in *Proc. Int. Workshop Public Key Cryptogr.* Berlin, Germany: Springer, 2005, pp. 65–84.

[30] M. Bellare, D. Pointcheval, and P. Rogaway, "Authenticated key exchange secure against dictionary attacks," in *Proc. Int. Conf. Theory Appl. Cryptograph. Techn.* Berlin, Germany: Springer, 2000, pp. 139–155.

[31] H. A. Wen, T. F. Lee, and T. Hwang, "Provably secure three-party password-based authenticated key exchange protocol using Weil pairing," *IEE Proc.-Commun.*, vol. 152, no. 2, pp. 138–143, Apr. 2005.

[32] R. Gennaro and V. Shoup, "A note on an encryption scheme of Kurosawa and Desmedt," IACR Cryptol. ePrint Arch., Tech. Rep. 2004/194, 2004. [Online]. Available: http://eprint.iacr.org/2004/194

[33] V. Shoup, "Sequences of games: A tool for taming complexity in security proofs," IACR Cryptol. ePrint Arch., Tech. Rep. 2004/332, 2014. [Online]. Available: http://www.shoup.net

[34] T.-F. Lee and T. Hwang, "Simple password-based three-party authenticated key exchange without server public keys," *Inf. Sci.*, vol. 180, no. 9, pp. 1702–1714, May 2010.

[35] 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.

[36] B. D. Deebak, R. Muthaiah, K. Thenmozhi, and P. I. Swaminathan, "Analyzing three-party authentication and key agreement protocol for real time IP multimedia server–client systems," *Multimedia Tools Appl.*, vol. 75, no. 10, pp. 5795–5817, May 2016.

[37] C. M. Chen, L. Xu, W. Fang, and T. Y. Wu, "A three-party password authenticated key exchange protocol resistant to stolen smart card attacks," in *Advances in Intelligent Information Hiding and Multimedia Signal Processing*. Cham, Switzerland: Springer, 2017, pp. 331–336.

[38] Q. Wang, O. Ruan, and Z. Wang, "Security analysis and improvements of three-party password-based authenticated key exchange protocol," in *Proc. Int. Conf. Emerg. Internetworking, Data Web Technol.* Cham, Switzerland: Springer, 2017, pp. 497–508.

[39] M. Safkhani and A. Vasilakos, "A new secure authentication protocol for telecare medicine information system and smart campus," *IEEE Access*, vol. 7, pp. 23514–23526, 2019.

[40] L. Zheng, C. Song, N. Cao, Z. Li, W. Zhou, J. Chen, and L. Meng, "A new mutual authentication protocol in mobile RFID for smart campus," *IEEE Access*, vol. 6, pp. 60996–61005, 2018.

[41] S. Azad, N. E. A. C. Nordin, N. N. A. Rasul, M. Mahmud, and K. Z. Zamli, "A secure hybrid authentication scheme using passpoints and press touch code," *IEEE Access*, vol. 7, pp. 166043–166053, 2019.

[42] S. M. Ganesh and S. P. Manikandan, "An efficient integrity verification and authentication scheme over the remote data in the public clouds for mobile users," *Secur. Commun. Netw.*, vol. 2020, pp. 1–13, May 2020.

[43] M. Han, S. Liu, S. Ma, and A. Wan, "Anonymous-authentication scheme based on fog computing for VANET," *PLoS ONE*, vol. 15, no. 2, Feb. 2020, Art. no. e0228319.

[44] Y. Aydin, G. K. Kurt, E. Ozdemir, and H. Yanikomeroglu, "A flexible and lightweight group authentication scheme," *IEEE Internet Things J.*, vol. 7, no. 10, pp. 10277–10287, Oct. 2020.

[45] C.-M. Chen, K.-H. Wang, K.-H. Yeh, B. Xiang, and T.-Y. Wu, "Attacks and solutions on a three-party password-based authenticated key exchange protocol for wireless communications," *J. Ambient Intell. Hum. Comput.*, vol. 10, no. 8, pp. 3133–3142, Aug. 2019.

[46] R.-C. Wang and K.-R. Mo, "Security enhancement on efficient verifier-based key agreement protocol for three parties without server's public key," *Int. Math. Forum*, vol. 1, no. 20, pp. 965–972, 2006.

[47] (2003). *The AVISPA Project, Funded By the European Union in the Future and Emerging Technologies (FET Open) Programme, Project Number: IST-2001-39252*. Accessed: Jul. 11, 2020. [Online]. Available: http://www.avispa-project.org/

[48] *SPAN: A Security Protocol Animator for AVISPA*. Accessed: Jul. 11, 2020. [Online]. Available: http://www.avispa-project.org/

[49] L. Viganò, "Automated security protocol analysis with the AVISPA tool," *Electron. Notes Theor. Comput. Sci.*, vol. 155, pp. 61–86, May 2006.

[50] F. Wang, G. Xu, C. Wang, and J. Peng, "A provably secure biometrics-based authentication scheme for multiserver environment," *Secur. Commun. Netw.*, vol. 2019, pp. 1–15, Jun. 2019.

[51] R. Ali and A. K. Pal, "An efficient three factor-based authentication scheme in multiserver environment using ECC," *Int. J. Commun. Syst.*, vol. 31, no. 4, p. e3484, Mar. 2018.

[52] D. He, S. Zeadally, N. Kumar, and W. Wu, "Efficient and anonymous mobile user authentication protocol using self-certified public key cryptography for multi-server architectures," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 9, pp. 2052–2064, Sep. 2016.

[53] K. Kaur, S. Garg, G. Kaddoum, M. Guizani, and D. N. K. Jayakody, "A lightweight and privacy-preserving authentication protocol for mobile edge computing," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2019, pp. 1–6.

[54] S. S. Sahoo, S. Mohanty, and B. Majhi, "A secure three factor based authentication scheme for health care systems using IoT enabled devices," *J. Ambient Intell. Humanized Comput.*, vol. 12, no. 1, pp. 1419–1434, Jan. 2021.

[55] T.-Y. Wu, L. Yang, Z. Lee, C.-M. Chen, J.-S. Pan, and S. H. Islam, "Improved ECC-based three-factor multiserver authentication scheme," *Secur. Commun. Netw.*, vol. 2021, pp. 1–14, Jan. 2021.
[56] M. F. Moghadam, M. Nikooghadam, M. A. B. A. Jabban, M. Alishahi, L. Mortazavi, and A. Mohajerzadeh, "An efficient authentication and key agreement scheme based on ECDH for wireless sensor network," *IEEE Access*, vol. 8, pp. 73182–73192, 2020.

VISHESH P. GAIKWAD received the B.E. degree in computer engineering from U.C.O.E., Umrer, and Nagpur University, Nagpur, Maharashtra, India, in 2009, and the M.E. degree in mobile technology from G.H. Raisoni COE, Nagpur, in 2013. He is currently pursuing the Ph.D. degree in computer science and engineering with the Indian Institute of Information Technology, Nagpur. He is working as an Assistant Professor with the Department of Computer Science and Engineering, Priyadarshini Bhagwati C.O.E, Nagpur University. He is the author of more than ten articles published in international conferences and journals. His research interests include cryptography and network security, deep learning, and cloud computing. He is a member of ISTE and IAENG Society.

JITENDRA V. TEMBHURNE received the B.E. degree in computer technology from Kavikulguru Institute of Technology and Science (KITS), Ramtek, and Nagpur University, Maharashtra, India, in 2003, the M.E. degree in computer science and engineering from MGM's College of Engineering, SRTMU Nanded, Maharashtra, in 2011, and the Ph.D. degree in computer science and engineering from Visvesvaraya National Institute of Technology, Nagpur, Maharashtra, 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. 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 a member of IAENG Society.

CHANDRASHEKHAR MESHRAM received the Ph.D. degree from R.T.M. Nagpur University, Nagpur, Maharashtra, India. He was a Postdoctoral Fellow under Dr. D. S. Kothari Postdoctoral Fellowship in New Delhi, India. He is currently working as an Assistant Professor with the Department of Post Graduate Studies and Research in Mathematics, Jaywanti Haksar Government Post Graduation College, College of Chhindwara University, Betul, Madhya Pradesh, India. He had published over 100 scientific articles on the above research fields in international journals and conferences. 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 is a member of IAENG, Hong Kong, IACSIT, Singapore, EATCS, Greece, EAI, ILAS, Haifa, Israel, Science and Engineering Institute (SCIEI), Machine Intelligence Research Labs (MIR Labs), USA, Society: Intelligent Systems, KES International Association, U.K., and The Society of Digital Information and Wireless Communications (SDIWC). He is a Life Time Member of Indian Mathematical Society and Cryptology Research Society of India. He is a regular reviewer of sixty international journals and international conferences.

CHENG-CHI LEE (Member, IEEE) received the Ph.D. degree in computer science from the National Chung Hsing University (NCHU), Taiwan, in 2007. He is currently a Distinguished Professor with the Department of Library and Information Science, Fu Jen Catholic University. He had published over 200 scientific articles on the above research fields in international journals and conferences. His current research interests include data security, cryptography, network security, mobile communications and computing, and wireless communications. He is a member of the Chinese Cryptology and Information Security Association (CCISA), the Library Association of The Republic of China, and the ROC Phi Tau Phi Scholastic Honor Society. He is an Editorial Board Member of *International Journal of Network Security*, *Journal of Computer Science*, *Cryptography*, *International Journal of Internet Technology and Secured Transactions*, and *The Open Automation and Control Systems Journal*. He served as a reviewer for many SCI-index journals, other journals, and other conferences.

CHUN-TA LI (Member, IEEE) received the Ph.D. degree in computer science and engineering from the National Chung Hsing University, Taiwan, in 2008. He is currently a full-time Professor with the Department of Information Management, Tainan University of Technology. His research interests include information security, wireless sensor networks, mobile computing, security protocols for IoTs, and *ad-hoc* networks. He had published more than 120 international journal and international conference papers on the above research fields. He is a member of Chinese Information Security Association (CCISA), IFIP WG 11.3, and Machine Intelligence Research Labs (MIR Labs). He is an Editorial Board Member of *International Journal of Network Security* (IJNS). He received the 2011 IJICIC Most Cited Paper Award from *International Journal of Innovative Computing, Information and Control*. He served as a reviewer for many SCI-index journals.