Computers, Materials & Continua
DOI:10.32604/cmc.2022.024877
Article

A Secure Three-Party Authenticated Key Exchange Protocol for Social Networks

Vivek Kumar Sinha[1], **Divya Anand**[1,*], **Fahd S. Alharithi**[2] **and Ahmed H. Almulihi**[2]

[1]Department of Computer Science and Engineering, Lovely Professional University, Phagwara, Punjab, 144411, India
[2]Department of Computer Science, College of Computers and Information Technology, Taif University, Taif, 21944, Saudi Arabia
*Corresponding Author: Divya Anand. Email: divyaanand.y@gmail.com
Received: 03 November 2021; Accepted: 07 December 2021

Abstract: The 3PAKE (Three-Party Authenticated Key Exchange) protocol is a valuable cryptographic method that offers safe communication and permits two diverse parties to consent to a new safe meeting code using the trusted server. There have been explored numerous 3PAKE protocols earlier to create a protected meeting code between users employing the trusted server. However, existing modified 3PAKE protocols have numerous drawbacks and are incapable to provide desired secrecy against diverse attacks such as man-in-the-middle, brute-force attacks, and many others in social networks. In this article, the authors proposed an improved as well as safe 3PAKE protocol based on the hash function and the symmetric encryption for the social networks. The authors utilized a well-acknowledged AVISPA tool to provide security verification of the proposed 3PAKE technique, and findings show that our proposed protocol is safer in opposition to active as well as passive attacks namely the brute-force, man-in-the-middle, parallel attack, and many more. Furthermore, compared to other similar schemes, the proposed protocol is built with a reduced computing cost as our proposed protocol consumes less time in execution and offers high secrecy in the social networks with improved accuracy. As a result, this verified scheme is more efficient as well as feasible for implementation in the social networks in comparison to previous security protocols. Although multifarious authors carried out extensive research on 3PAKE protocols to offer safe communication, still there are vital opportunities to explore and implement novel improved protocols for higher safety in the social networks and mobile commerce environment in the future in opposition to diverse active as well as passive attacks.

Keywords: AVISPA tool; 3PAKE protocol; hash function; symmetric encryption; social networks

1 Introduction

Due to fast advancement in information as well as diverse networking technologies, pragmatic client authentication plays a vital role to safeguard services and multifarious resources from being cracked via unauthorized clients [1–5]. The 3PAKE (Three-Party Password-Based Authenticated Key Exchange) protocol permits two diverse clients over unsecured channels to have a talk for safe session codes and set up a safe channel through an authenticated server to secure their consequential communication [6–9]. Each of the legal clients stockpiles their scrutinizer calculated from their real key in the database of the isolated trustworthy servers and every client just needs to recall only words of identification i.e., an authentication key with a trustworthy server [10–12]. There have already been identified multifarious benefits of the 3PAKE protocols earlier by numerous researchers in past from security perspectives, however, one of the key benefits of this protocol recognized by some researchers is that it offers an easy method for a huge number of client-to-client communication settings, in addition, every client does not demand to recall numerous keys for diverse clients who converse with each other [13–15]. Furthermore, the 3PAKE protocol has a wide scope to implement in diverse electronics applications as well as in the social networks to safeguard the confidential information of the clients as demanded in the modern world [16–18]. There are multifarious benefits of the 3PAKE protocols usages in numerous applications, in addition to this, 3PAKE protocols provide mutual authentication as well as a safe information exchange e.g., authenticated trusted server helps in communications among buyers as well as sellers in e-commerce, etc.

In this article, an inexpensive 3PAKE protocol is developed for social networks utilizing hash function and symmetric encryption jointly to increase performance by reducing protocol executing rounds yet maintaining the equivalent protection capabilities as previous methods without relying just on a secret key of the server. Our proposed 3PAKE protocol is inexpensive as well as more robust against diverse attacks such as replay assaults, cryptanalysis assaults as well as man-in-the-middle assaults. To aid in the creation of our enhanced 3PAKE protocol for authenticity as well as privacy validation, the AVISPA verification software was used. Our enhanced 3PAKE protocol is subjected to a quantitative effectiveness study.

The origins of computing networks as well as the Internet may be found dated in the 1960s as well as early 1990s, correspondingly. Cellular phones began to link to the Internet through wireless channels in the 20^{th} century, and WiFi connections, numerous websites including several mobile apps are now available on a variety of gadgets, including smart mobiles, global positioning systems (GPS) gadgets, and many more. Access control has been recognized as the fundamental data protection problem in social network infrastructure that comprises authentication as well as authorization. Cyber-security threats are the most serious obstacles which computing systems, as well as social networks, face, in addition, access control has been identified as a key secrecy threat in the social networks. The authentication process is recognized as a vital element that provides safety to an apparatus, system, or application from illegal access directly or indirectly. Nowadays, security and privacy are becoming a key challenge due to diverse assaults over a network during information exchange particularly in social networks environment around the world.

However, earlier various researchers have been provided multifarious strategies to prevent various assaults such as man-in-the-middle assault, replay assault, and cryptanalysis assaults over the networks. But, existing protocols and strategies have certain limitations such as high computation complexity and more time-consuming that demands more attention towards novel cost-effective protocols that take minimal communication steps and search time. To commence with, just one element was utilized to validate participants in the network; although, such a method, especially in the scenario of credentials, may be readily hacked. Users often utilize similar credentials across many platforms, namely Gmail, Twitter, and Facebook. An unauthorized client may immediately hack any customer's profile, as well as a hacker may employ well-known techniques like gusting as well as social engineering to get entry to diverse system's resources and applications rather than the authorized client.

To safeguard the customer's profile against unwanted assaults, password authentication techniques based on the hash function and symmetric encryption must be utilized jointly to provide additional secrecy as demanded nowadays against diverse assaults.

2 Related Work

There has been done extensive research earlier on 3PAKE protocols to provide desired secrecy and confidentiality against diverse assaults. The following discussion would provide an overview of the limitation of existing protocols.

Chang et al. in [19], described an effective 3PAKE protocol rooted on LHL-3PAKE suggested by the author's Lee et al. This protocol does not need any public key as well as symmetric cryptosystems. This scheme has numerous limitations like in case of a missing session key, this would never disclose alternative session key as well as lack of mutual authentication among users and authenticated servers. Ruan et al. in [20], described another LR eCK secrecy prototypical for 3PAKE as well as suggested an improved LR 3PAKE scheme, after that presented formal secrecy evidence in the typical model. This approach is suitable and easy to implement in numerous applications and wireless networks, however, this protocol has certain restrictions namely high computation complexity, and offers secrecy only in conventional prototypical wherein no outflow assaults exist. Li et al in [21], analyzed Farash-Attari's scheme and depicts how their scheme does not provide resistance against secure code disclosure assault if the secure data is kept on the authenticated server side. The authors eliminated existing threats of Farash-Attari's scheme in this work, however, the suggested method provides secrecy only in the communication overhead scenario and in computation complexity environment.

Farash et al. in [22], disclosed the drawbacks of the Lee et al. secrecy scheme suggested earlier and analyzed the need for further improved 3PAKE protocols for enhancement in a more pragmatic manner. The authors proposed a modest countermeasure that preserves computation as well as communication efficacy of existing protocol suggested earlier, however, this proposed scheme does not provide enough secrecy against multifarious assaults namely man-in-the-middle and several others in social networks scenario. Zhang et al. in [23], investigated verified-rooted 3PAKE scheme analyzed its design, wherein authenticated server keeps secure code verifier in comparison to plain secure code. However, the suggested approach does not offer required secrecy against directory assaults and man-in-the-middle assaults in the model of the social network. Xie et al. in [24], suggested an enhanced 3PAKE scheme that is rooted in chaotic maps. This protocol offers certain advantages over existing secrecy schemes that are based on authenticated server public secrecy keys, however, the proposed protocol is less efficient and has more computation complexity in the social networks.

Lin et al. in [25], proposed another lightweight as well as lower computational complexity 3PAKE scheme rooted on exclusive OR (XOR) operation to provide secrecy against impersonation assaults and many others. This protocol is suffered from the shared key loss over authenticated servers due to the fast enhancement of numerous services namely cloud as well as ubiquitous computing, gadgets comprising lower computation power, and many more. Amin et al. in [26], suggested another effective 3PAKE scheme utilizing the smart card and rooted on cryptography hash function. The authors explored existing literature to identify the key challenges related to information loss during communication due to various assaults. Although, this investigated protocol is best fit only in the mutual authentication among clients and servers but has huge computation complexity in practical implementations in multifarious applications. Shu et al. in [27], proposed another enhanced 3PAKE that offers gigantic communication efficacy and provides enhances secrecy level in numerous scenarios and applications. However, this protocol comprises certain limitations related to the secrecy of the social network. Chen et al. in [28], suggested another improved 3PAKE scheme that is rooted on the chaotic-map for the enhanced secrecy level. But the suggested scheme is vulnerable in the environment of the social network due to multifarious assaults such as man-in-the-middle assaults and relay assaults. Lone et al. in [29], discussed the OTP (One Time Password) based user authentication approach in their research. The suggested scheme was implemented and validated using the android-rooted mobile phones to attain the desired secrecy. However, the suggested method has certain drawbacks such as user data leakage in case of OTP misuse and not much reliable in case of confidential data exchange over social networks.

3 Research Contributions

In this paper, a novel 3PAKE protocol has been developed for the social networks which utilize the hash function as well as symmetric-key encryption technique to enhance the performance parameters such as parseTime, searchTime, depth of plies, and visited nodes by minimizing the protocol executing rounds and offers higher secrecy against diverse attacks such as brute-force, man-in-the-middle, and parallel attack. The major contributions of our research are to design an improved and novel 3PAKE protocol that takes less time in execution, lowest computation complexity, as well as robust against diverse attacks, and is communication efficient in a pragmatic manner. However, multifarious researchers have done pragmatic work to design various secrecy protocols during the last decade to provide offer the desired secrecy to the users during the communication, but the existing protocol has certain disadvantages and does not offer the required secrecy in the modern world against various attacks such as man-in-the-middle, brute-force attacks, and several others. Therefore, considering this issue we designed a novel 3PAKE protocol that is based on the hash function and symmetric key encryption technique to offer the higher secrecy as well as consumes very little time that is required to manage the high-volume traffic over the social networks.

4 Research Methodology

When the medium of transmission is public networks, the major goals of networks privacy are verification of interacting users as well as the secrecy of sent information. As a result, numerous 3PAKE algorithms have already been created to accomplish such security standards at the same time. The 3PAKE algorithms permit two diverse users to validate one another by a secure server and further evaluate a confidential session code through a public network. In this work, the authors utilized the under-mentioned parameters to design the proposed 3PAKE protocol based on the hash function and symmetric encryption for higher secrecy and privacy of the social networks.

4.1 Notions Used

S_a represents a trusted server. C_A and C_B are two diverse users who want safe communication with one another with the assistance of the S_a. In this work, the authors utilized Diffie-Hellman Key Exchange (DHKE) scheme to design the suggested 3PAKE protocol based on the hash function and symmetric encryption. The DHKE is a way of safely interchanging cryptographic codes via a public channel. Our suggested protocol has been constructed utilizing the DHKE scheme, therefore, a definite cyclic cluster (C_G, e, f) must be chosen, that is originated via a component e of prime order f. N_u is a number that is arbitrarily chosen through user C_B for assurance of the newness. The N_u is frequently a pseudo-random or an arbitrary number allotted in a verification protocol to confirm that the previous message could not be utilized again under diverse assaults. Tab. 1 illustrates the notations used and their definitions.

Table 1: Illustrates the notations used and their definitions

S. No.	Notation	Definition
1	(C_G, e, f)	Definite cyclic cluster C_G created via a component e of prime order f
2	C_A and C_B	Two users that also denote their own uniqueness
3	PW_{ax}	Symmetric key exchanged between C_A and S
4	PW_{bx}	Symmetric key exchanged between C_B and S
5	N_u	An arbitrary number utilized once by C_B
6	S_a	Authenticated server
7	Ha(M)	Confidential unilateral hash function
8	$\{M\}_{ka}$	Ciphertext that symmetric encrypt M along with ka

4.2 Enhanced 3PAKE Protocol

Using our enhanced protocol two users C_A and C_B desire to exchange a fresh session code C_k with aid of server S_a for the next message. There is no direct authentication between user C_A and user C_B. They have to recourse to authenticated server S_a for the contract of sessions secure codes.

Fig. 1 illustrates the flow diagram of our enhanced 3PAKE protocol for the social networks using a hash function and symmetric encryption. The description of the steps of our suggested 3PAKE protocol are given in detail as follows:

Step 1: C_A selects an arbitrary number $a_n \in T_p$, evaluates d^{a_n} as well as one instance code H_a (C_A, d^{a_n}, PW_{ax}), obtains, $REQ_A = C_A, d^{a_n}, \{CA, d^{a_n}\}Ha(C_A, d^{a_n}, PW_{ax})$ then forwards REQ_A to C_B.

Step 2: By obtaining a piece of information from C_A, C_B initially verify the uniqueness of d^{a_n} and after that C_B selects an arbitrary number $b_n \in T_p$ and number utilized once N_u, evaluates d^{b_n} and one instance code H_a (C_B, d^{b_n}, PW_{bx}), obtains, $REQ_B = C_B, d^{b_n}, \{C_B, d^{b_n}\}H_a(C_B, d^{b_n}, PW_{bx})$ then forwards REQ_A and REQ_B to the authenticated server S_a.

Step 3: By obtaining REQ_B and REQ_A, authenticated server S_a initially verifies the uniqueness of the d^{a_n} and d^{b_n}, after that authenticated server S_a utilize obtained d^{a_n} and d^{b_n} to evaluate $H_a(C_A, d^{a_n}, PW_{ax})$ and H_a (C_B, d^{b_n}, PW_{bx}) order by and after that decrypts the REQ_A and REQ_B to verify and validate d^{a_n} and d^{b_n}. In case of, failed authentication, this session stopped, otherwise authenticated server S_a selects an arbitrary number $v_n \in T_p$, evaluates $d^{a_n v_n} = (d^{a_n})^{v_n}$, $d^{b_n v_n} = (d^{b_n})^{v_n}$ and obtains $C_AK_a = \{d^{a_n}, C_B, d^{b_n v_n}, N_u\}$ H_a (C_A, d^{a_n}, PW_{ax}), $C_AK_b = \{d^{b_n}, C_A, d^{a_n v_n}, N_u\}$ H_a (C_B, d^{b_n}, PW_{bx}), and lastly forwards C_AK_a and C_AK_b to the C_A.

Step 4: C_A decrypts C_AK_a, obtains $d^{a_n v_n}$ and N_u, evaluates $C_K = (d^{b_n v_n})^{a_n} = d^{a_n b_n v_n}$, then obtains $\{C_A, N_u, d^{a_n}\}C_K$, and forwards C_AK_b, $\{C_A, N_u, d^{a_n}\}C_K$ to C_B.

Step 5: By obtaining C_AK_b, $\{C_A, N_u, d^{a_n}\}_K$, initially C_B decrypts C_AK_b to obtain $d^{a_n v_n}$ and after that authenticate d^{b_n}, furthermore, C_B evaluates $C_K = (d^{a_n v_n})^{b_n} = d^{a_n b_n v_n}$ and after that decrypts $\{C_A, N_u, d^{a_n}\}C_K$ to authenticate N_u.

Step 6: Finally, the user C_A and user C_B identify the fresh session code C_K for further conversation and eliminate the chances of information losses in social networks during communication.

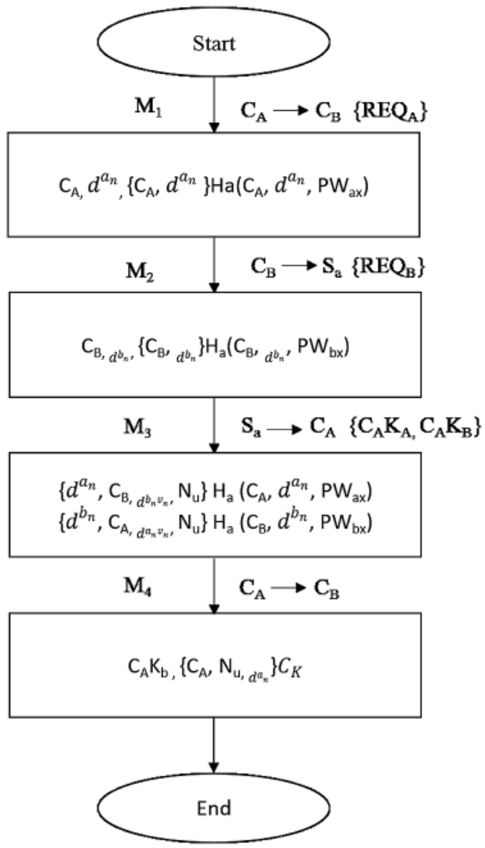

Figure 1: Illustrates the flow diagram of our enhanced 3PAKE protocol for the social networks using a hash function and symmetric encryption

The overall procedure of the proposed 3PAKE protocol is summarized as follows. The client C_A can authenticate the server S_a and the client C_B can authenticate the server S_a respectively by individual authentication invitations REQ_A and REQ_B and the response C_AK_a, C_AK_b. The client C_A and client C_B validate each other name with the help of d^{a_n} and N_u. In all the transferred messages, information despatcher individuality is involved for the client C_A and client C_B. The accurate client authentication is the first priority in the communication over social networks in order to provide the desired secrecy to the clients via authenticated server S_a. In order to provide the required secrecy to each and every client, a unique code word is assigned to all clients during the communication that is embedded in the distributed information which is transferred over the networks in the form of distributed messages via authenticated server. The suggested 3PAKE protocol is more robust against diverse attacks such as brute-force, man-in-the-middle, parallel attack, because our protocol mutually authenticates the client C_A and C_B as well as authenticated server S_a.

4.3 The AVISPA Tool

Our enhanced 3PAKE protocol for social networks is modeled and validated in the most popular AVISPA (Automated Validation of Internet Security Protocols and Applications) tool to authenticate diverse secrecy and privacy properties that our enhanced 3PAKE protocol was modeled to own. AVISPA toolkit is simply working using the push button to verify the internet secrecy and privacy-sensitive multifarious applications as well as protocols. HLPSL (High-Level Protocol Specification Language) is linguistic in which the diverse secrecy protocols are written in widely popular AVISPA software. Within HLPSL, numerous security protocols parameters are separated among roles. There are basic roles that are used to define the activities of a stand-alone agent during the execution of protocols or numerous sub-protocols. Several termed the composed roles, use such fundamental roles that describe a full protocol cycle, as well as protocols session among several agents, or the protocols models itself. Such a job is frequently referred to as an environmental role. In this article, authors specified their security goals using a collection of roles that describe protocol as well as an environmental role to define particular sessions which performance researchers want to evaluate.

5 Results and Discussion

By utilizing the AVISPA toolset to do privacy assessment as well as validation, authors prove that their suggested 3PAKE algorithm is trustworthy and therefore can operate appropriately for the social networks for higher secrecy and privacy as needed.

5.1 Enhanced 3PAKE Protocol Specifications

In the suggested 3PAKE protocol design that is defined in the HLPSL language, the basic roles are three namely the pekc_C_A, pekc_C_B, pekc_S_a, which represent the user C_A, C_B, and the authenticated server S_a, respectively. Herein we are presenting the one basic role that is S_a as illustrated in Fig. 2. The authenticated server S_a stands by to obtain the REQ_B, REQ_A from the user C_B and then forwards C_AK_A and C_AK_B to C_A. At the similar instance state S_t of the authenticated server, S_a will be altered via 0 to 1. There are certain symbols utilized in the basic role S_a are described in Tab. 2.

5.2 Security Analysis of Suggested 3PAKE Protocol

Initially, the authenticated server S_a obtains a message (C_B. Gy'.{C_B. Gy'.Nb'}_Hash (C_B. Gy'. PW_{bx}). C_A. Gx'.{C_A. Gx'}_Hash (C_A. Gx'. PW_{ax}) via Rcv ( ) function. After that, authenticated server S_a, selects an own arbitrary number N_z' as well as evaluates Gxz'. Lastly, authenticated server S_a forwards message {Gx'.C_B. Gyz'. Nb'}_Hash (C_A.Gx'.PW_{ax}).{Gy'.C_A. Gxz'}_Hash (C_B. Gy'. PW_{bx}) via Snd ( ) function. In this article, the authors utilized the DHKE scheme for the designing of the suggested 3PAKE protocol based on the hash function and symmetric encryption for the social network's privacy and secrecy. After defining basic roles instantly, there is a requirement to describe the composed roles that further define the new sessions for the suggested 3PAKE protocol. Fig. 2 illustrates the role of the authenticated server S_a for the suggested 3PAKE protocol for the social networks secrecy verification. Fig. 3 illustrates the session role for the suggested 3PAKE protocol for the social networks secrecy verification.

```
role pekc_Sa (CA, CB, Sa              : agent
            Snd, Rcv                  : channel (dy),
            PWax, PWbx                : symmetric_key,
            G                         : text,
            Hash                      : hash_func)
Played_by S def=
            local St                  : nat,
            Nz                        : text,
            Nb                        : text,
            Gx, Gy                    : message,
            Gyz, Gxz                  : message
    init St  : = 0
    transition
    St  = 0    /\ Rcv (CB. Gy'.{CB. Gy'.Nb'}
                    _Hash (CB. Gy'. PWbx). CA.Gx'.
                     {CA. Gx'}_Hash (CA. Gx'. PWax)) = |>
    St' : = 1 /\ Nz'   : = new()
            /\ Gxz' : = exp (Gx', Nz')
            /\ Gyz' : = exp (Gy', Nz')
            /\ Snd ({Gx'.CB. Gyz'. Nb'}
                    _Hash (CA.Gx'. PWax).
                     {Gy'. CA. Gxz'}_Hash(CB. Gy'. PWbx))
            /\ witness (Sa, CA, auth_a_s_gx, Gx')
            /\ witness (Sa, CB, auth_b_s_gy, Gy')
end role
```

Figure 2: Illustrates the role of the authenticated server S_a for the suggested 3PAKE protocol for the social networks secrecy verification

Table 2: Illustrates the symbols used in the S_a role

S. No.	Symbols	Meaning of the used symbol
1	Hash (.)	Represents hash function
2	Snd (M)	Forward message
3	C_A	Identity of the first user
4	C_B	Identity of the second user
5	S_a	Authenticated server
6	PW_{ax}, PW_{bx}	Represents symmetric keys used
7	Rcv (M)	Represents obtained message M
8	new ( )	Originate an arbitrary no. used once

```
role session (C_A, C_B, S_a          :  agent
              PW_ax, PW_bx,          :  symmetric_key,
              G                      :  text,
              Hash                   : hash_func)
def=
   local C_A_SND, C_A_RCV, C_B_SND, S_a_SND, S_a_RCV: channel (dy)
   composition
   pekc_C_A (C_A, C_B, S_a, C_A_SND, C_A_RCV, PW_ax, G, Hash)
  /\ pekc_C_B (C_A, C_B, S_a, C_B_SND, C_B_RCV, PW_bx, G, Hash)
  /\ pekc_S_a (C_A, C_B, S_a, S_a_SND, S_a_RCV, PW_ax, PW_bx, G, Hash)
end role
```

Figure 3: Illustrates the session role for the suggested 3PAKE protocol for the social networks secrecy verification

5.3 Informal Security Analysis

Within all session's fragments, every basic role namely the pekc_C_A, pekc_C_B, as well as pekc_S_a have been instanced with solid logic. In the end, a high-level role is an environment at all times described. The environment role comprises universal constants as well as an arrangement of one or further sessions. Fig. 4 illustrates the environmental role of our suggested 3PAKE protocol for the social networks secrecy verification. Herein, i is utilized to represent the intruder that takes part in the implementation of the suggested 3PAKE protocol utilizing a solid session. It is utilized for the detection of man-in-the-middle assaults. Herein, statement category channel (dy) symbolizes the intruder prototypical namely the Dolev-Yao model. By utilizing this model, the interloper has overall control of the network in such a manner that every message forwarded by the users would pass via the interloper. This interloper can analyze or enhance coming messages as soon as get to know demanded codes. As a result, users can transmit as well as receive data on any route they wish; the intended relationship among specific channels characteristics is preserved.

```
role environment ()
def=
    const
       a, b, s, i                    : agent
       PW_ax, PW_bx, PW_i            : symmetric_key,
       d                             : text,
       hash                          : hash_func,
       auth_a_b_nb                   : protocol_id,
       auth_b_a_dx                   : protocol_id,
       auth_a_s_gx                   : protocol_id,
       auth_b_s_gy                   : protocol_id,
       sec_a_b_gxyz                  : protocol_id,
    intruder_knowledge  =            {i, a, b, s, pwi, g, hash}
    composition
            session (a, b, s, PW_ax, PW_bx, g, hhash)
         /\ session (a, b, s, PW_ax, PW_bx, g, hhash)
         /\ session (i, b, s, PW_i, PW_bx, g, hhash)
         /\ session (a, i, s, PW_ax, PW_i, g, hhash)
end role
```

Figure 4: Illustrates the environmental role for the suggested 3PAKE protocol for the social networks secrecy verification

Fig. 5 illustrates the analysis goals for the suggested 3PAKE protocol for the social networks secrecy verification. We have analyzed the under-mentioned properties that are considered within the goal section. Herein symbol auth_C_A_S_A_gx means user C_A validates S_a over gx. Fig. 6 illustrates the simulation outcomes by OFMC back-end for the suggested 3PAKE protocol for the social networks secrecy verification.

```
goal
    authentication on auth_CA_SA_gx
    authentication on auth_CB_SA_gy
    authentication on auth_CA_SB_nb
    authentication on auth_CB_SA_gx
    secrecy_of sec_a_b_gxyz
end goal
```

Figure 5: Illustrates the analysis goals for the suggested 3PAKE protocol for the social networks secrecy verification

```
SUMMARY
    SAFE
DETAILS
    BOUNDED_NUMBER_OF_SESSIONS
PROTOCOL
    /home/avispa/web-interface-
computation/./tempdir/workfileEdDMf1/3PAKE.if
GOAL
    as_specified
BACKEND
    OFMC
COMMENTS
STATISTICS
  parseTime:  0.00s
  searchTime:  0.12s
  visitedNodes:  10 Nodes
  depth 4 plies
```

Figure 6: Illustrates the simulation outcomes by OFMC back-end for the suggested 3PAKE protocol for the social networks secrecy verification

Several 3PAKE protocols have been investigated in the past to generate a secure meeting code between users using a trustworthy server. However, existing modified 3PAKE protocols have various flaws and are unable to guarantee necessary anonymity in social networks against a variety of attacks such as man-in-the-middle, brute-force assaults, and others. In this article, the authors developed an enhanced and novel 3PAKE protocol that offers additional secrecy in social networks to offer higher secrecy as well as privacy as demanded in the modern world from various assaults between communications. All the experimental work was carried out on a personal computer installed with window 10 and comprising of a 64-bit operating system, 16 GB RAM (Random Access Memory), and an i7 processor. For the performance validations of the suggested 3PAKE protocol for social networks, we utilized a widely popular AVISPA toolset for the simulation.

5.4 Performance Evaluation

Fig. 6 illustrates the simulation outcomes by OFMC back-end for the suggested 3PAKE protocol for the social networks secrecy verification. Tab. 3 illustrates the outcomes and comparative analysis of the suggested 3PAKE protocol along with other existing protocols for the social networks. Islam et al. [30] protocol takes 0.00 s parseTime, communication steps 5, search time 0.66 s, depth plies 6, and the visited nodes 16. Pak et al. [31] protocol consume parse time 0.00 s, communication steps 5, search time 8.94 s, depth plies 6 and visited nodes number 1690. After simulation, the proposed 3PAKE protocol offers parseTime 0.00 s, searchTime 0.12 s, depth of 4 plies, visited nodes 10, and communication steps 2 that shows all parameters are reduced from the existing protocols, therefore our suggested 3PAKE protocol provides very little computation complexity along with reduced search time for the client's authentication over the server S_a. The parseTime gives the information regarding the initialization time of protocol execution for the authentication of clients and server. Initially, it is set to be 0.00 s to count the searchTime of clients and authenticated server in an efficient manner. Moreover, our proposed algorithm is more robust against diverse assaults namely the man-in-the-middle, replay, and cryptanalysis assaults, and many more. Our suggested 3PAKE protocol for social networks offers forward security. Any agreed code would not be compromised in case of even agreed codes derived via similar long-term coding substances throughout the succeeding run have been compromised. In our suggested 3PAKE protocol, components a_n, b_n, and v_n are arbitrarily chosen as well as self-governing to proposed 3PAKE protocol execution. Hence, compromised secret code PW_{ax}, PW_{bx}, as well as C_K could not disclose the earlier session codes.

Table 3: Illustrates the outcomes of the suggested 3PAKE protocol for the social networks

S. No.	Protocols	parseTime	Communication steps	searchTime	Depth (plies)	Visited Nodes
1	Islam et al. [30]	0.00 s	5	0.66 s	6	16
2	Pak et al. [31]	0.00	5	8.94 s	6	1690
3	Proposed 3PAKE protocol	0.00	2	0.12 s	4	10

6 Conclusion

In this article, the authors proposed a novel and low-cost 3PAKE protocol based on the hash function and symmetric encryption for social networks that offer additional secrecy for the confidential key as well as a session key, shared verification between users including the uniqueness of conveyed message and lastly faultless forward security for the session key. Our suggested 3PAKE protocol shows that it is highly efficient in comparison to the earlier modified protocols and provides less computation complexity along with reduced computations steps. This proposed 3PAKE protocol is simulated and a formal verification was done by using a widely popular AVISPA toolset. The proposed 3PAKE protocol takes parseTime 0.00 s, searchTime 0.12 s, depth of 4 plies, visited nodes 10, and communication steps 2, indicating that all parameters have been reduced from existing protocols. As a result, our proposed 3PAKE protocol is more robust and offers a very low computation complexity. Our recommended 3PAKE protocol is appropriate in a wide range of applications, particularly in resource-constrained situations as well as in real-time systems. However, several researchers have modified 3PAKE protocols for diverse applications in past but there are vital possibilities of more investigation on 3PAKE protocol in the future for further modification for mobile commerce environment for optimal outcomes.

Acknowledgement: This project was supported by the Taif University Researchers Supporting Project Number (TURSP-2020/347), Taif Unversity, Taif, Saudi Arabia.

Funding Statement: This project was funded by the Taif University Researchers Supporting Project Number (TURSP-2020/347), Taif Unversity, Taif, Saudi Arabia.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] M. S. Farash and M. A. Attari, "An efficient and provably secure three-party password-based authenticated key exchange protocol based on chebyshev chaotic maps," *Nonlinear Dynamics*, vol. 77, no. 2, pp. 399–411, 2014.
[2] J. H. Yang and T. J. Cao, "Provably secure three-party password authenticated key exchange protocol in the standard model," *Journal of Systems and Software*, vol. 85, no. 2, pp. 340–350, 2012.
[3] C. Liu, Z. Zheng, K. Jia and Q. You, "Provably secure three-party password-based authenticated key exchange from RLWE," in *Proc. Informaton Security Practice and Experience, 15th International Conference, ISPEC 2019*, Kuala Lumpur, Malaysia, November 26–28, pp. 56–72, 2019.
[4] X. F. Ding and C. G. Ma, "The three-party password-authenticated key exchange protocol with stronger security," *Jisuanji Xuebao/Chinese Journal of Computers*, vol. 10, no. 2, pp. 312–318, 2010.
[5] F. Zhao, P. Gong, S. Li, M. Li, and P. Li, "Cryptanalysis and improvement of a three-party key agreement protocol using enhanced chebyshev polynomials," *Nonlinear Dynamics*, vol. 74, no. 3, pp. 419–427, 2013.
[6] S. Deng, Y. Li and Y. Deng, "An efficient two-party key exchange protocol with strong security," *Wuhan University Journal of Natural Sciences*, vol. 10, no. 2, pp. 327–334, 2010.
[7] K. Suzuki and K. Yoneyama, "Exposure-resilient one-round tripartite key exchange without random oracles," in *Proc. Int. Conf. on Applied Cryptography and Network Security. ACNS. Lecture Notes in Computer Science*, Berlin, Heidelberg, Springer, vol. 7954, pp. 458–474, 2013. DOI 10.1007/978-3-642-38980-1_29.
[8] Y. Liu, F. Wei and C. Ma, "Multi-factor authenticated key exchange protocol in the three-party setting," in *Proc. Int. Conf. on Information Security and Cryptology. Inscrypt. Lecture Notes in Computer Science*, Berlin, Heidelberg, Springer, vol. 6584, pp. 255–267, 2010. DOI 10.1007/978-3-642-21518-6_18.
[9] W. Wang, L. Hu and Y. Li, "How to construct secure and efficient three-party password-based authenticated key exchange protocols," in *Proc. Int. Conf. on Information Security and Cryptology. Inscrypt. Lecture Notes in Computer Science*, Berlin, Heidelberg, Springer, vol. 6584, pp. 218–235, 2010. DOI 10.1007/978-3-642-21518-6_16
[10] N. W. Lo and K. H. Yeh, "Simple three-party password authenticated key exchange protocol," *Journal of Shanghai Jiaotong University (Science)*, vol. 16, no. 4, pp. 600–608, 2011.
[11] J. Zhao and D. Gu, "A security patch for a three-party key exchange protocol," *Wuhan University Journal of Natural Sciences*, vol. 4, no. 3, pp. 222–232, 2010.
[12] R. Padmavathy and C. Bhagvati, "Unknown key share attack on STPKE' protocol," in *Proc. Int. Conf. on Information Processing and Management. BAIP. Communications in Computer and Information Science*, Berlin, Heidelberg, Springer, vol. 70, pp. 605–608, 2010. DOI 10.1007/978-3-642-12214-9_111.
[13] E. J. Yoon, "On the security of Lv et al.'s three-party authenticated key exchange protocol using one-time key," in *IEEE International Conference on Advanced Infocomm Technology*, Berlin, Heidelberg, Springer, pp. 191–198, 2013.

[14] Z. Tan, "Privacy-preserving Two-factor Key agreement protocol based on chebyshev polynomials," *Security and Communication Networks*, vol. 8, no. 2, pp. 157–167, 2021.
[15] J. Fan, L. Qiao, Y. Cao, S. Liu, W. Zhang *et al.,* "A new password- and position-based authenticated key exchange," *Security and Communication Networks*, vol. 6, no. 6, pp. 514–524, 2021.
[16] H. Liang, J. Hu and S. Wu, "Re-attack on a three-party password-based authenticated key exchange protocol," *Mathematical and Computer Modelling*, vol. 57, no. 6, pp. 1175–1183, 2013.
[17] A. Terfa, A. James and K. Sever, "Multi-modal biometrics systems: Concepts, strengths, challenges and solutions," *International Journal of Advanced Trends in Computer Science and Engineering*, vol. 10, no. 3, pp. 1827–1831, 2021.
[18] D. Kwon, Y. Park and Y. Park, "Provably secure three-factor-based mutual authentication scheme with puf for wireless medical sensor networks," *Sensors*, vol. 4, no. 4, pp. 1410–1424, 2021.
[19] T. Y. Chang, M. S. Hwang and W. P. Yang, "A Communication-efficient three-party password authenticated key exchange protocol," *Information Sciences*, vol. 181, no. 1, pp. 217–226, 2011.
[20] O. Ruan, Q. Wang and Z. Wang, "Provably leakage-resilient three-party password-based authenticated key exchange," *Journal of Ambient Intelligence and Humanized Computing*, vol. 10, no. 3, pp. 163–173, 2019.
[21] C. T. Li, C. L. Chen, C. C. Lee, C. Y. Weng and C. M. Chen, "A novel three-party password-based authenticated key exchange protocol with user anonymity based on chaotic maps," *Soft Computing*, vol. 22, no. 5, pp. 2495–2506, 2018.
[22] M. S. Farash, M. A. Attari and S. Kumari, "Cryptanalysis and improvement of a three-party password-based authenticated key exchange protocol with user anonymity using extended chaotic maps," *International Journal of Communication Systems*, vol. 5, no. 6, pp. 317–328, 2014.
[23] Q. H. Zhang, X. X. Hu, W. F. Liu and J. H. Wei, "Improved verifier-based three-party password-authenticated Key exchange protocol," *Ruan Jian Xue Bao/Journal Software*, vol. 4, no. 6, pp. 175–185, 2020.
[24] Q. Xie, B. Hu and T. Wu, "Improvement of a chaotic maps-based three-party password-authenticated key exchange protocol without using server's public key and smart card," *Nonlinear Dynamics*, vol. 79, no. 4, pp. 2345–2355, 2015.
[25] C. Y. Lin and C. H. Fu, "A lightweight three-party authenticated key exchange protocol with XOR-based operation," *Chung Cheng Ling Hsueh Pao/Journal of Chung Cheng Institute of Technology*, vol. 8, no. 5, pp. 215–224, 2016.
[26] R. Amin and G. P. Biswas, "Cryptanalysis and design of a three-party authenticated key exchange protocol using smart card," *Arabian Journal for Science and Engineering*, vol. 40, no. 1, pp. 3135–3149, 2015.
[27] Q. Shu, S. B. Wang, B. Hu and L. D. Han, "Verifier-based three-party password-authenticated key exchange protocol from ideal lattices," *Journal of Cryptologic Research*, vol. 8, no. 2, pp. 294–306, 2021.
[28] C. M. Chen, W. Fang, S. Liu, T. Y. Wu, J. S. Pan *et al.,* "Improvement on a chaotic map-based mutual anonymous authentication protocol," *Journal of Information Science and Engineering*, vol. 34, no. 2, pp. 371–390, 2018.
[29] S. A. Lone and A. H. Mir, "A novel OTP based tripartite authentication scheme," *International Journal of Pervasive Computing and Communications*, vol. 8, no. 6, pp. 1345–1356, 2021.
[30] S. K. H. Islam, R. Amin, G. P. Biswas, M. S. Farash, X. Li *et al.,* "An improved three party authenticated key exchange protocol using hash function and elliptic curve cryptography for mobile-commerce environments," *Journal of King Saud University Computer and Information Sciences*, vol. 29, no. 3, pp. 311–324, 2017.
[31] K. Pak, S. Pak, C. Ho, M. Pak and C. Hwang, "Anonymity preserving and round effective three-party authentication key exchange protocol based on chaotic maps," *PLoS One*, vol. 10, no. 4, pp. 1371–1383, 2019.