symmetry

MDPI

Article

Security Verification of Social Network Model Using Improved Three-Party Authenticated Key Exchange Protocol

Vivek Kumar Sinha [1], Divya Anand [1,2,*], Sandeep Kaur [3], Pankaj Singh [4,*] and Irene Delgado Noya [2,5]

[1] Department of Computer Science and Engineering, Lovely Professional University, Phagwara 144411, India; sinha.vivekkumar7@gmail.com
[2] Higher Polytechnic School, Universidad Europea del Atlantico, C/Isabel Torres 21, 39011 Santander, Spain; irene.delgado@uneatlantico.es
[3] Department of Computer Science, Guru Nanak College for Women, Banga 144505, India; sandeep_nagra@yahoo.com
[4] Department of Electronic Engineering, Yeungnam University, Gyeongsan 38541, Korea
[5] Department of Project Management, Universidad Internacional Iberoamericana, Campeche 24560, Mexico
* Correspondence: divyaanand.y@gmail.com (D.A.); pankaj_singh86@ynu.ac.kr (P.S.)

Abstract: The proper verification of users plays a vital role during communication over a social network to protect the personal data of users. Multifarious protocols have been implemented to secure the confidential data of the users, but these protocols have various limitations and are incapable of providing secrecy of data against various attacks, such as replay and cryptanalysis attacks. In this article, the authors proposed a novel method for security verification of the social network model using an improved three-party authenticated key exchange (3PAKE) protocol based on symmetric encryption and (ECC) elliptic curve cryptography. The outcome of the paper demonstrates that our proposed algorithm provides the desired secrecy to the confidential data exchange over social networks in real-time and consumes less time in comparison to existing protocols. Our protocol consumes a search time of 0.09 s, overall communication steps took 2 during the verification, and depth plies was 3 along with 20 visited nodes. The 3PAKE protocol has been considered a suitable approach for social network secrecy during information exchange between user and server, thereby providing greater secrecy to the user in data exchange over social networks and more robustness against multifarious known attacks, such as cryptanalysis and replay attacks in real-time.

Keywords: 3PAKE; elliptic curve cryptography; symmetric encryption; social network; security verification

Citation: Sinha, V.K.; Anand, D.; Kaur, S.; Singh, P.; Noya, I.D. Security Verification of Social Network Model Using Improved Three-Party Authenticated Key Exchange Protocol. *Symmetry* **2022**, *14*, 1567. https://doi.org/10.3390/sym14081567

Academic Editor: Debiao He

Received: 21 June 2022
Accepted: 27 July 2022
Published: 29 July 2022

1. Introduction

Due to the continuous technological advancements in the area of computer networks as well as information technology, the accurate authentication of users over communication networks is becoming very necessary to secure the essential data of the users during communication. Credential security methods provide easy as well as pragmatic alternatives to person recognition since they enable users to create as well as maintain their personal credentials unescorted by the need for external equipment [1]. Individuals, on the other hand, consider it harder to remember lengthy randomized sequences. Instead, individuals choose normal linguistic words that individuals may immediately identify. Natural linguistic terms, namely credentials, on the other hand, are taken from quite a small range of alternatives but instead are thus vulnerable to credential cracking attempts [2–4].To maintain the secrecy of the confidential dataset, there is a requirement of novel protocols which could offer the desired secrecy to the secure information in real-time communication as means of the authenticated server [5]. Although, multifarious investigators have developed varied approaches earlier for providing the desired secrecy to the confidential information while two parties want to communicate with each other over the authenticated

server [6]. However, these kinds of explored approaches have multifarious limitations these days because of the rapid communication infrastructure developments as the number of customers has increased dramatically during the last few years over the limited channels.

To provide the required privacy to the users while communicating with each other, there is a requirement to develop a more pragmatic and secure protocol that is robust against multifarious attacks, such as the man-in-the-middle as well as the cryptanalysis attacks [7,8].One of the easy and pragmatic solutions for providing the desired secrecy to the confidential dataset in the communication process is the implementation of the password authentication approaches. Multifarious kinds of password-based authentication approaches have been investigated during the previous years but the 3PAKE (third-party password authenticated keys exchanges) procedure is a pragmatic solution to maintain the secrecy of the confidential datasets as per the need of the users [9–11]. The 3PAKE secrecy technique provides a means to safe communication while multiple users want to establish a communication link with each other for information interchange through the authenticated server in the desired manner. Some of the researchers developed as well as implemented multifarious kinds of the 3PAKE protocols to offer the required secrecy to the clients [12,13].

Previously, considerable investigation on 3PAKE methods to ensure needed anonymity, as well as privacy across a variety of cyber-attacks was conducted. The accompanying discourse will offer an outline of known method limitations. O. Ruan et al. in [14], demonstrated a successful 3PAKE technique based in their research which is based on the symmetric encryption and hash function. This method, like symmetric cryptographic protocols, does not require a shared password. The above technique comprises many flaws, including the inability to reveal an alternate access password in the event of a lost identity password, including the absence of verification between consumers as well as authorized providers. R. Muthumeenakshi et al. in [15], disclose another improved 3PAKE protocol to provide the desired secrecy to the confidential information within the VANETs (vehicular ad hoc network) environment. The VANET is simply a cellular network that comprises higher-speed automobiles which may establish a communication link to each other as means of a built-in wireless line. The proposed protocol is capable of providing the required secrecy only within the traditional communication media along with the data verification failure conditions. The major drawback of this method is that it is incapable of handling cryptanalysis attacks in real-time communication.

Q. Shu et al. in [16] disclose another 3PAKE technique as means of the ideal lattice. Because of the rapid development of social networking, multiple clients require to create secure meeting passwords as means of the authenticated remote server for safe information exchange during real-time communication over social networks. In previously explored protocols, the client's communication passcode was required, which is to be saved inside the server database, but keeping the saved password on the server is not considered safe due to the possibility of a disclosure attack. Therefore, the existing method does not provide the required secrecy in the modern social network environment. J. Zhao et al. in [17], disclose the new 3PAKE approach for providing secure data exchange in real-time, however, the suggested protocol is incapable to provide the required secrecy due to the conventional hash-function approach. Client identity secrecy is one of the key challenges in the social network model. While client anonymity has not been offered, any striker will be capable of recognizing the clients during real-time communication. The hash-based 3PAKE protocols are not capable enough in social network models because of the cryptanalysis attacks. C. T. Li et al. in [18] disclose another 3PAKE protocol based on the chaotic map methods. The suggested protocol provides a means to the clients in real-time communication for exchanging the secret meeting code by means of the authenticated server, but this protocol has limitations in the case of social network verification due to many clients and the incapacity to handle the diverse attacks, namely the man-in-the-middle attack, which is a serious concern nowadays.

M. Kim et al. in an article [19] explored another 3PAKE technique to offer secrecy in wireless communication. This protocol was developed to secure the healthcare dataset in real-time communication, but it has many flaws which are related to data privacy as the suggested techniques are incapable of handling the client anonymity in real-time, which is one of the major concerns. H. Xiong et al. in an article [20], disclose another improved 3PAKE protocol for confidential data exchange as means of the server. However, the existing technology has varied vulnerabilities related to secure data secrecy and is incapable of handling multiple attacks, such as (KCI) key compromise impersonation, in real-time. Q. Xie et al. in [21] explored and discussed another improved 3PAKE technique that is based on the chaotic map and does not utilize the authenticated server public code words. This method offers the required secrecy in the symmetrical cryptosystems but has flaws in providing secrecy in the social network model due to diverse kinds of attacks during the communications such as the key guessing attack in real-time communication.

However, these kinds of existing protocols provided confidentiality to the exchanged dataset only in conventional models wherein there were possibilities of minimal attacks during the communication via the authenticated server. The earlier developed 3PAKE methods have numerous vulnerabilities due to cryptanalysis attacks as well as the man-in-the-middle attacks in case of information translation as means of social networks. People exchange multifarious kinds of confidential datasets by means of social networks in day-to-day life and due to excess traffic over the authenticated server, there are high possibilities of information leakage by various attackers in real-time communication [22–24]. To resolve such kinds of problems, there is a requirement for the development of a novel 3PAKE protocol that is capable of eliminating the chances of side channel assaults in the real-time information interchange by means of the authenticated server.

In addition, there is a necessity for a 3PAKE approach which is more robust as well as secure given there are high possibilities of information leakages and thereby offers higher secrecy to the user while communicating with each other through communication server [25–27]. Individuals are constantly moving toward sophisticated living as Smart Information Systems emerge. Major architectures of smart information systems include the World Wide Web and wireless communications, including wearable devices. Numerous sophisticated endpoints, namely cell phones, are present within some of those contexts. Whenever client A wishes to connect safely alongside client B, both should initially utilize the server's assistance to produce mutual encryption keys that are much strong for connection. Such an approach of secure datasets interchange between the two diver parties is recognized as the 3PAKE strategy. There have been found significant advantages of using the 3PAKE methods in various applications across the globe. Additionally, 3PAKE methods offer collaborative verification along with secure data interchange, for example, a validated trustable server aids in messaging between producers and consumers throughout e-commerce, and many others. Multifarious kinds of secrecy methods have already been explored for providing the required secrecy to the confidential datasets in real-time communication. However, most of the methods have diverse limitations due to the rapid changes in the communication infrastructure across the globe. Therefore, the existing protocols are incapable of handling real-time attacks, such as man-in-the-middle as well as cryptanalysis attacks, and many others of similar kinds in the communication procedure, drawing significant attention towards this issue. To solve such existing identified issues, the authors developed a new and more robust 3PAKE protocol that is capable of handling these aforementioned assaults during real-time communication in a shorter period while providing additional safety to the user for information exchange over social networks.

The security of social networks is becoming a very challenging and important concern these days globally. In this work, the authors proposed a novel 3PAKE protocol for the security verification of social networks, which is based on symmetric encryption and ECC jointly to provide higher secrecy in the modern social network environment against diverse assaults. This protocol was developed for considering the scenario of the easy to implement within the hardware of the modern social network in less time and with minimal effort.

Further, our protocol is more efficient and presents fewer computational complexities in its real-time hardware implementation scenario in comparison with the existing protocols. Table 1 illustrates the existing state-of-the-art techniques used for security verification and their drawbacks.

Table 1. Illustrates the existing state-of-the-art techniques used for security verification and their drawbacks.

S. No	Name of Author	Publication Year	Technique Used	Drawbacks
1	O. Ruan et al. [14]	2019	Symmetric encryption and Hash function	Inability to reveal an alternate access password in the event of a lost identity password.
2	R. Muthumeenakshi et al. [15]	2017	Server-client authentication process and batch message dispatch	Higher transmission overload and delay in service response.
3	Q. Shu et al. in [16]	2021	Ideal lattices	Lower computing as well as communication efficiency in real-time.
4	J. Zhao et al. [17]	2012	Trapdoor test technique	This proposed protocol has higher computational complexity as well as a large execution time.
5	C. T. Li et al. [18]	2018	Quadratic residues as well as Chebyshev chaotic maps	Unable to defend against a password disclosure assault.
6	M. Kim et al. [19]	2020	Biometric-based key exchange	Insecure against insider assaults as well as impersonation assaults
7	H. Xiong et al. [20]	2013	The hash function and no server public keys	Incapable of handling multiple attacks namely (KCI) Key Compromise Impersonation and many others
8	Q. Xie et al. in [21]	2015	Chaotic map	Incapable of handling key guessing attacks and others in real-time.

2. Materials and Methods

Accurate authentication of the users is becoming one of the major challenges and concerns nowadays to maintain the secrecy of the transmitting information, such as audio/video or text messages in real-time during the communication between two diverse parties over the server. Network security is an essential parameter and a key challenge to protecting secure information as demanded in the modern world because it plays a key role in the communication procedure. There have been explored and developed multifarious kinds of the secrecy protocol in previous years for providing the required secrecy to the users while they communicate with each other over the server. However, the existing secrecy protocols have numerous drawbacks in the real world due to the continuous development of communication technologies and infrastructure because the users are constantly increasing over the communication spectrum. To resolve these existing issues, there is a need to develop new kinds of secrecy protocols that provide higher secrecy against various kinds of assaults, namely cryptanalysis as well as replay attacks, including man-in-the-middle assaults in real-time during the communication over the server.

To eliminate the drawbacks of existing protocols, the authors proposed a safe and robust protocol for security verification of social networks utilizing an enhanced three-party authenticated key exchange (3PAKE) protocol. In this work, we utilized two approaches jointly i.e., ECC (elliptical curve cryptography) along with the (SE) symmetric encryption to

protect the shared information between the diverse users over the network in comparison to other existing costly protocols that consume more time, etc. We developed the proposed secrecy protocol for the security verification of social networks in two diverse stages, i.e., the first is the initialization of the system and the second is authentic keys interchange. For the secrecy validation of our enhanced 3PAKE protocol, we selected client $CL_A$and client CL_B along with one authentic server SR_A. Table 2 illustrates the major notions utilized in our enhanced 3PAKE protocol for the secrecy verification of social networks.

Table 2. Illustrates the major notions utilized in our enhanced 3PAKE protocol for the secrecy verification of social networks.

S. No	Notions Utilized	Definition
1	CL_A	Client
2	CL_B	Client
3	SR_A	Authentic Server
4	dP_A/V_A	Private Secret Code Words
5	dP_B/V_B	Private Secret Code Words
6	rp_A	Integer
7	rp_B	Integer
8	$InDP_A$	Request
9	$InDP_B$	Response

2.1. Initialization of the System

This section may be divided into subheadings. It should provide a concise and precise description of the experimental results, their interpretation, as well as the experimental conclusions that can be drawn. In this stage of secrecy verification, first, the authentic server SR_A initializes as well as chooses certain parameters such as the number of clients in communication over the authentic server. Both clients, i.e., CL_A and CL_B, register to the authentic server SR_A. System specifications comprise the finite field, i.e., F_s on big prime s as well as ECC cluster through the p point QS on curve ES_s (p, q): $r^2 = t^2 + pt + q \pmod s$, wherein p, q $\in F_s$ and $5p^3 + 28\ q^2 \neq 0 \pmod s$. For the registration stage client, CL_A along with CL_B registers over authentic server SR_A to create the public as well as private secret code words pairs i.e., dP_A/V_A and dP_B/V_B, wherein the $V_A = dP_AQ$, $V_B = dP_BQ$, and dP_A, $dP_B \in ZP_n^*$. Authentic server SR_A selects private code words $dP_s \in ZP_n^*$, as well as evaluates the public code words $UP_s = dP_sQS$. The authentic code word interchange stages can be illustrated as shown herein.

Round 1 $CL_A \rightarrow CL_B$ {$InDP_A$, Request}
A: $rp_A \in ZP_n^*$, $wp_A \in ZP_q^*$
$RP_A = rp_AV_A$, $\widehat{RP_A} = rp_AV_S$
$KP_A = dP_A\ \widehat{RP_A} = kP_{At}, kP_{Ar}$
$WP_{AX} = wP_AQS$, $CP_A = EP_{At}$ (RP_A, WP_{AX})
$CL_A \rightarrow SR_A$ {$InDP_A$, $InDP_B$, CP_A, RP_A}
Round 2 $CL_B \rightarrow CL_A$ {$InDP_B$, Response}
B: $rp_B \in ZP_n^*$, $wp_B \in ZP_q^*$
$RP_B = rp_BV_B$, $\widehat{RP_B} = rp_BV_S$
$KP_B = dP_B\ \widehat{RP_B} = kP_{Bt}, kP_{Br}$
$WP_{BX} = wP_BQS$, $CP_B = EP_{Bt}$ (RP_B, WP_{BX})
$CL_B \rightarrow SR_A$ {$InDP_B$, $InDP_A$, CP_B, RP_B}
Round 3 SR_A: $KP_A = dP_SRP_A = (kP_{At}, kP_{Ar})$
$KP_B = dP_SRP_B = (kP_{gt}, kP_{Br})$
(RP_A, WP_A) = DP_{AK} (CP_A)
(RP_B, WP_B) = DP_{BK} (CP_B)
Checked: Obtained RP_A = ? Decrypted RP_A
Checked: Obtained RP_B = ? Decrypted RP_B

2.2. Secured Code Interchange Phase of Proposed Protocol

In our proposed 3PAKE protocol for security verification of the social network model, we selected three main entities which are described as authenticated client CL_A, authenticated client CL_B, along with the server SR_A. To validate the proposed security verification protocol, the authenticated client CL_A and the authenticated client CL_B want to create a safe session code word for each other. The secure session codeword is to be exchanged by means of the trusted server over the public network in real-time communication. The validation process was done in diverse three phases that are described as given herein.

Phase 1. This phase is the initial phase of the suggested 3PAKE protocol. In this phase, the authenticated client CL_A executes the given rounds.

Step 1: To select the integer for initialization i.e., $rp_A \in ZP_n^*$ arbitrarily and after that evaluate the $CH_A = CH (CR_A || CD_A)$ and $CR_A = CH_A . CQ$.

Step 2: To evaluate the $CK_A = CD_A . CU_S = CD_A . CD_S . CQ$ and $KC_{AS} = CH (CID_A || CID_B || CR_A || CK_A)$.

Step 3: To translate the (CID_A, request) along with the (CID_A, CID_B, CR_A, KC_{AS}) to the authenticated client CL_B as well as authenticated server SR_A, respectively.

Phase 2. While the authenticated client CL_A successfully translates the initialization message data packet (CID_A, request). Then, the authenticated client CL_B execute these following steps described as herein.

Step 1. To select the integer for initialization i.e., $rp_B \in ZP_n^*$ arbitrarily and after that evaluate the $CH_B = CH (CR_B || CD_B)$ and $CR_B = CH_B . CQ$.

Step 2: To evaluate the $CK_B = CD_B . CU_S = CD_B . CD_S . CQ$ and $KC_{BS} = CH (CID_B || CID_A || CR_B || CK_B)$.

Step 3: To translate the (CID_B, request) along with the (CID_B, CID_A, CR_B, KC_{BS}) to the authenticated client CL_A as well as authenticated server SR_A, respectively.

Phase 3. While obtaining the (CID_A, CID_B, CR_A, KC_{AS}) and (CID_B, CID_A, CR_B, KC_{BS}) via authenticated client CL_A and authenticated client CL_B, the authenticated server SR_A executes the given operations.

Step 1: To determine symmetric code words for authentication $CK_A = Cd_S . CU_A = Cd_A . Cd_S . CQ$ and $CK_B = Cd_S . CU_B = Cd_B . Cd_S . CQ$, respectively.

Step 2: To evaluate the $\overline{KC}_{AS} = CH (CID_A || CID_B || CR_A || CK_A)$ utilizing the acquired CR_A as well as evaluated CK_A. CS determine condition $\overline{KC}_{AS} = ? KC_{AS}$. While this is not met, the authenticated server SR_A translates the verification unsuccessful dispatch to the authenticated client CL_B or authenticated server SR_A evaluates the $KC_{AS} = CH (CID_A || CID_B || CR_A || CK_A)$ and translates the dispatch (CR_B, KC_{SA}) to authenticated client CL_A.

Step 3: To evaluate the $\overline{KC}_{BS} = CH (CID_B || CID_A || CR_B || CK_B)$ utilizing the acquired CR_B as well as evaluated CK_B. CS determine condition $\overline{KC}_{BS} = ? KC_{BS}$. While this is not met, then the authenticated server SR_B translates the verification unsuccessful dispatch to the authenticated client CL_A or authenticated server SR_B evaluates the $KC_{BS} = CH (CID_B || CID_A || CR_B || CR_B || CK_A)$ and translates the dispatch (CR_A, KC_{SB}) to authenticated client CL_B.

Step 4: By obtaining the (CR_B, KC_{SA}), the authenticated client CL_A evaluates the $\overline{KC}_{AS} = CH (CID_A || CID_B || CR_A || CK_A)$ utilizing the own CR_A as well as CK_A originated in phase 1 along with the acquired CR_B. After that, the authenticated client CL_A verifies the condition $\overline{KC}_{AS} = ? KC_{AS}$. While the outcome comes positive, then the authenticated client CL_A evaluates session code words $CSK = CH (CID_A || CID_B || CR_A || CK_B || CK)$, wherein the $CK = CH_A . CR_B = CH_A . CH_B . CQ$. Otherwise, in other conditions, the authenticated client CL_A discards the proposed protocol. After that, the authenticated client CL_B executes the following operation in real-time after acquiring the dispatch (CR_B, KC_{SB}) from the authenticated server SR_A.

Step 5: By obtaining the (CR_A, KC_{SB}), the authenticated client CL_B evaluates the $\overline{KC}_{BS} = CH (CID_B || CID_A || CR_B || CK_B)$ utilizing the own CR_B as well as CK_B originated in phase 2 along with the acquired CR_A. After that, the authenticated client

CL_B verifies the condition $\overline{KC}_{BS}$ = ? KC_{BS}. While the outcome becomes positive, the authenticated client CL_B evaluates session code words CSK = CH (CID_A || CID_B || CR_A || CK_B || CK), wherein the CK = CH_B . CR_A = CH_A . CH_B . CQ. Otherwise, in other conditions the authenticated client CL_B discards the proposed protocol in the real-time execution over the public network.

2.3. The AVISPA Tool

This experiment was carried out by utilizing the globally recognized and accepted software product named the AVISPA (Automated Validation of Internet Security Protocols and Applications) tool to validate the proposed 3PAKE protocol for the social network model. This product provides a means to the researcher to verify the network security protocols in a desired and secured manner in the real-time and aids to the research as means of less time consumption as well as desired secrecy of the input datasets during the execution of the secrecy protocols. The AVISPA software product can determine whether the specified secrecy protocol is safe in real-time and provides required secrecy to the clients during the communication over the public networks or whether the specified protocol is unsafe and does not provide the desired level of secrecy in real-time. The AVISAP tool provides an easy user interface to the researchers for the formal security verification of the secrecy protocols in real-time in an efficient manner [28,29].

3. Performance Evaluation and Discussion

This experiment has been done by utilizing the most popular simulation tool named AVISPA [30]. In this article, the authors proposed a novel secrecy protocol to provide the required secrecy to the customers during real-time communication over the public networks in a more secure manner as desired in the modern communication infrastructure.

3.1. Specifications of Suggested 3PAKE Protocol

Communication infrastructure is continuously altering due to the constant technological advancements in the arena of communication these days because of the continuous increment of the customers over the limited networks. Therefore, there is a need to develop a new secrecy protocol that provides a means for secure communication and eliminates the chances of information losses during communication over public networks. To resolve the aforementioned drawback, the authors proposed a novel 3PAKE secrecy protocol that is based on symmetric encryption and elliptical curve cryptography (ECC) techniques.

3.2. Secrecy Analysis and Verification of Proposed 3PAKE Protocol

The secrecy validation of our suggested 3PAKE protocol has been carried out by means of the globally recognized AVISPA tool installed using a personal computer (PC) system and having the following system configuration: RAM 16 GB, Intel(R) Core(TM) i3-1005G1 CPU @ 1.20 GHz and 64-bit operating system. It is indeed worth noting as AVISPA has been developed by means of a role-based language, which implies that each member has a specific job to perform throughout the protocol's implementation. Every function is self-contained, receiving basic starting data through variables as well as interacting with everyone via routes. It is indeed worth noting whether the connection is protected or insecure in real-time during the communication. Table 3 shows the symbols utilized in various roles, such as session, environment, and goal for the implementation of our proposed 3PAKE protocol, for secrecy verification of the social networks in real-time communication through an authenticated server.

Table 3. Depicts the symbols utilized in various roles such as session, environment, and goal.

S. No	Symbol	Meaning/Definition of the Specified Symbols
1	CL_A	Authenticated Client
2	CL_B	Authenticated Client
3	SR_A	Authenticated Server
4	subs1	Protocol ID
5	subs2	Protocol ID
6	subs3	Protocol ID
7	new ()	Generate a random no. utilized one time

The main symbols utilized for the implementation of our proposed protocol are described herein. CL_A and CL_B represent the authenticated clients who want to communicate with each other as means of the authenticated server which is represented by the chosen symbol SR_A. The specified role for the authenticated client CLA in the HLPSL simulator is described as follows:

role alex (CL_A, SR_A, CL_B: agent),
% CH is hash function
CH, Mul: hash_func, Snd, Rcv: channel (dy))
Played_by CL_A
Def =
local State : nat,
DCL_A, UCL_A, $IDCL_A$, $IDCL_B$, $CRCL_A$, CQ, CUS: text,
HCL_A, RCL_A, RCL_B, KCL_A, CCL_ASR_A, CSR_AKCL_A : message,
Inc : hash_func
const alex_server, server_max, alex_max, alex_server,
Subs1, subs2, subs3 : protocol_id
Init State :=0
transition
1.State = 0 /\ Rcv (start) = |>
State' : = 1 /\ DCL_A' := new ()
/\ UCL_A' := Mul (DCL_A'. CQ)
/\ $RACL_A$' := new ()
/\ HCL_A' := CH (RCL_A'. DCL_A')
/\ RCL_A' := Mul (HCL_A'. CQ)
/\ KCL_A' := Mul (DCL_A. USR_A)
/\ CCL_ASR_A' := CH ($CIDCL_A$. $CIDCL_B$. CR_A'. KCL_A')
/\ Snd ($CIDCL_A$. $CIDCL_B$. $CRCL_A$'. KCL_A')
/\ Secret ({$CDCL_A$'}, subs1, {CL_A, SR_A})
2. State = 1 /\ Rcv (RCL_B. CSR_A') = |>
State' := 2 /\ CK' := Mul ($CHCL_A$. RCL_B)
/\ SR_AKCL_A' := CH ($CIDCL_A$. $CIDCL_B$. RCL_A. RCL_B.K')
End role

The specified role for the authenticated client CL_B in the HLPSL simulator is described as follows:

role max (CL_B, SR_A, CL_A : agent),
% CH is hash function
CH, Mul: hash_func, Snd, Rcv: channel (dy))
Played_by CL_B
Def =
local State : nat,
DCL_B, UCL_B, $IDCL_B$, $IDCL_B$, $CRCL_B$, CQ, CUS: text,
HCL_B, RCL_B, RCL_A, KCL_B, CCL_BSR_B, CSR_BKCL_B : message,
Inc : hash_func

const alex_server, server_max, alex_max, alex_server,
Subs1, subs2, subs3 : protocol_id
Init State :=0
transition
1.State = 0 /\ Rcv (start) = |>
State' : = 1 /\ DCL_B' := new ()
/\ UCL_B' := Mul (DCL_B'. CQ)
/\ $RACL_B$' := new ()
/\ HCL_B' := CH (RCL_B'. DCL_B')
/\ RCL_B' := Mul (HCL_B'. CQ)
/\ KCL_B' := Mul (DCL_B. USR_B)
/\ CCL_BSR_B' := CH ($CIDCL_B$. $CIDCL_A$. CR_B'. KCL_B')
/\ Snd ($CIDCL_B$. $CIDCL_A$. $CRCL_B$'. KCL_B')
/\ Secret ({$CDCL_B$'}, subs1, {CL_B, SR_B})
2. State = 1 /\ Rcv (RCL_A. CSR_B') = |>
State' := 2 /\ CK' := Mul ($CHCL_B$. RCL_A)
/\ SR_AKCL_B' := CH ($CIDCL_A$. $CIDCL_B$. RCL_A. RCL_B.K')
End role

For the accurate verification of our proposed 3PAKE protocol, we chose multifarious protocol IDs, namely the subs1, subs2, as well as subs3, to verify the suggested 3PAKE protocol against multifarious attacks such as man-in-the-middle as well as cryptanalysis attacks in real-time for providing additional safety to the client's confidential information over the social networks. The function new () is utilized to generate a random number, which is to be utilized one time during the implementation of the suggested 3PAKE protocol. The specified role for the authenticated server SR_A in the HLPSL simulator is described as follows.

role server SR_A (SR_A, CL_A, CL_B: agent,
% CH is hash function
CH, Mul: hash_func,
Snd, Rcv: channel (dy))
played_by SR_A
Def =
local State : nat,
DSR_A, UCL_B, UCL_A, $IDCL_A$, $IDCL_B$, $CRCL_B$, CQ, $CUSR_A$: text,
HCL_B, RCL_B, RCL_A, SR_AKCL_B, CCL_BSR_A, CSR_AKCL_B : message,
Inc : hash_func
const alex_server, server_max, alex_max, alex_server,
Subs1, subs2, subs3 : protocol_id
Init State :=0
transition
1.State = 0 /\ Rcv ($CIDCL_A$. $CIDCL_B$. $CRCL_A$'. $CKCL_A$') Rcv ($CIDCL_A$. $CIDCL_B$. $CRCL_B$'. CK .CL_B')
State' : = 1 /\ $CUSR_A$' := Mul (DSR_A'. CQ)
/\ $CKCL_ACL_A$' := Mul (DAR_A'. UCL_A)
/\ $CKCL_BCL_B$' := Mul (DAR_A'. UCL_B)
/\ CSR_ACL_A' := CH ($CIDCL_A$. $CIDCL_B$. CR_A . CR_B'. $CKCL_ACL_A$')
/\ CSR_ACL_B' := CH ($CIDCL_B$. $CIDCL_A$. CR_B . CR_A'. $CKCL_BCL_B$')
/\ Snd ($CRCL_B$. $CRSR_ACL_A$')
/\ Snd ($CRCL_A$. $CRSR_ACL_B$')
/\ Secret ({$CDSR_A$'}, subs3, {SR_A})
End role

3.3. Informal Secrecy Evaluation

Key interchange methods provide significant cryptographic techniques, enabling a couple of customers to create a shared meeting passcode that may be utilized to safeguard conversation across an unstable broadcast network. Because of rapid progress in communication as well as internet systems, effective customer verification is becoming increasingly important for protecting data as well as assets via unauthorized customers. The 3PAKE protocol enables multiple customers to communicate securely across untrusted networks by exchanging protected session credentials as well as establishing an encrypted connection as means of authorized server. The specified role for the session in the HLPSL simulator is defined as follows:

role session ($CL_{B,}$ SR_A, CL_A : agent),
CH, Mul: hash_func),
def =
local CSI, CSJ, CRI, CRJ, CTI, CTJ: channel (dy)
composition
Alex (CLA, SRA, CLB, CH, Mul, CSI, CRI)
Server (CLA, SRA, CLB, CH, Mul, CSJ, CRJ)
max (CLA, SRA, CLB, CH, Mul, CTI, CTJ)
End role

All valid customers store their scrutinizer, which is to be computed through their genuine password, inside the directory of separated trusted servers. Therefore, any customer just has to remember credentials of recognition, i.e., verification passwords along with the authenticated trusted server in real-time communication. The validation of the suggested 3PAKE protocol intruder has been demonstrated utilizing the DolevYao strategy. The role system provides a means for describing the varied sessions, including multifarious principles, along with the other kinds of the roles, such as the environment role in the real-time implantation of the protocol.

The specified role for the environment in the HLPSL simulator is described as follows:

role environment
def =
const CLA, SRA, CLB: agent,
Ch, mul: hash_func,
cida, cidb, cua, cub, cda, cdb, cra, crb, sds, us, cas, cbs, csa, csb,
kka, kkb, ha, hb, ka, kb, raa, rbb: text,
alex_server, server_max, alex_max, alex_server,
subs1, subs2, subs3 : protocol_id
intruder_knowledge = {a, s, b, h, mul, csa, csb, cas, cbs, ra, rb}
composition
session (a, s, b, h, mul)
/\ session (s, a, b, h, mul)
/\ session (b, s, a, h, mul)
End role

The specified role for the goal in the HLPSL simulator is described as follows:

role goal
secrecy_of subs1
secrecy_of subs2
secrecy_of subs3
authentication_on alex_server_raa
authentication_on max_server_raa
End goal

From a safety viewpoint, innumerable investigators have recognized countless advantages of something like 3PAKE methods throughout the previous era. However, another main advantage of this methodology recognized by several scientists would be that the proposed 3PAKE strategy provides an easy technique for a large amount of user-to-user communication scenarios. In addition, every customer does not have to remember cryptographic codes for various customers that want to communicate along with each other. Additionally, this 3PAKE method may be used in a variety of digital systems along with social media to protect customer's sensitive data, as is required in today's environment. This section demonstrates the main outcomes of the suggested 3PAKE technique over back-end OFMC by means of utilizing the globally recognized AVSIPA software. The simulation results obtained via the OFMC back-end of the proposed 3PAKE secrecy protocol for public network authentication are demonstrated as follows:

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: 0.09s
visitedNodes: 20 Nodes
depth 6 plies

Table 4 demonstrates the performance comparison and results of the suggested 3PAKE method for secrecy verification of the social network model. K. Pak et al. [31] protocol parseTime was 0.00 s, depth in plies was 7, and overall visited nodes was 18, including the overall only six communication steps during the real-time communication. Y. Tang et al. [32] protocol have consumed the parseTime 0.00 s, overall search time of authenticated clients in communication 0.88 s, depth in the plies 5, along with the overall communication step 6 and all visited nodes 17 in the real-time communication. Our improved 3PAKE protocol is capable of handling the numerous existing attacks against social network verification, namely the man-in-the-middle attack, as well as similar attacks, such as cryptanalysis attacks. Our suggested protocol is more secure and entails less computation complexity in comparison to the K. Pak et al. [31] and Y. Tang et al. [32] protocols as our suggested protocol takes only searchTime 0.09 s along with parseTime 0.00 s. The overall communication steps was considered 2 during the verification and depth plies was 3. Last but not the least, overall visited nodes was 20. This experiment was carried out with a high degree of precision and secrecy to eliminate the possibilities of real-time errors.

Table 4. Demonstrates the performance comparison and results of the suggested 3PAKE method for secrecy verification of the social network model.

S. No	Protocols Name	No. of Total Visited Nodes	SearchTime	ParseTime	No. of Communication Steps	Depth (In Plies)
1	K. Pak et al. [31]	18	7.74 s	0.00 s	6	7
2	Y. Tang et al. [32]	17	0.88 s	0.00 s	6	5
3	Suggested 3PAKE method	20	0.09 s	0.00 s	2	6

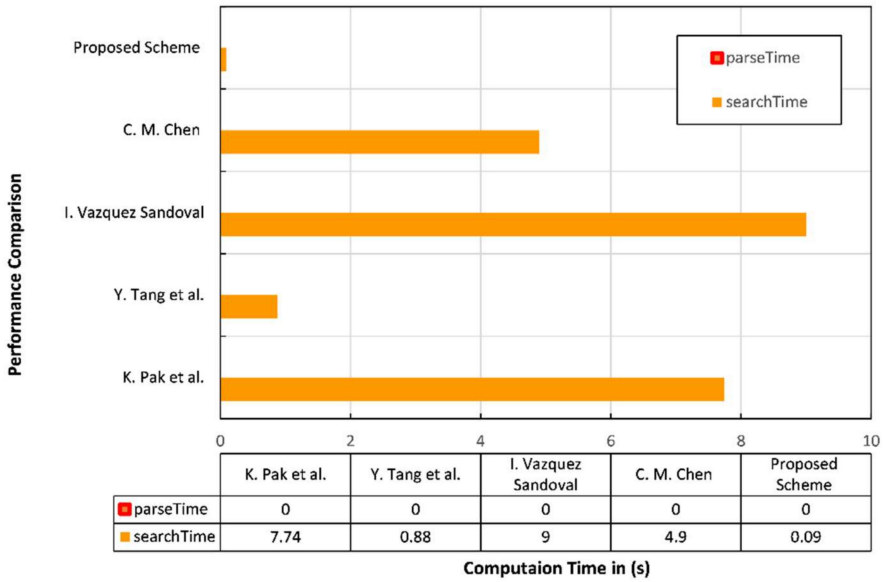
In previous years, multifarious research has been carried out in this arena to protect the confidential information of the users in social networks. However, there are vital opportunities for more research in this field to resolve the existing issues related to the confidentiality of the secure information exchange over social networks. Meanwhile, multiple investigators have changed the 3PAKE methods for numerous purposes in previous years, although there are significant opportunities for additional study into 3PAKE technique customization for the social networking scenario for best results. In the future, there are vital possibilities for further research in this arena to discover more pragmatic, improved secrecy protocols to offer desired secrecy against various secrecy assaults.

4. Simulation Results

Security verification of social networks is becoming a serious issue nowadays due to multifarious known assaults, such as cryptanalysis as well as the man-in-the-middle attacks, and many more. The secrecy of the confidential datasets is one of the major challenges. However, in previous years, researchers have proposed numerous techniques for resolving the existing threats. However, due to massive technological advancements in the present communication infrastructure, the possibility of data leakage is becoming a significant issue. To resolve these aforementioned threats, the authors constructed an improved 3PAKE protocol for secrecy verification of the social network model. While comparing the suggested scheme along with the previously constructed protocols, it is to be found that our scheme minimizes the space complexity as well as enhances the computational efficacy along with overall communication steps. This protocol requires two rounds of communication steps for accurate negotiation of the session codes. Moreover, this protocol is capable of, in opposition to the server passcode disclosure assaults, entire server-internal assaults, including the man-in-the-middle as well as replay assaults in real-time communication. This suggested scheme offers higher secrecy as well as minimal overhead, which could encounter all communication necessities of wide-reaching lower bandwidth networks.

Figure 1 demonstrates the suggested scheme time of execution along with multifarious discovered 3PAKE protocols in recent years. It is to be clear from Figure 1 that our scheme's performance constraint, namely the entire searchTime, is optimal and reduced in comparison to the existing protocols. Our scheme consumes the searchTime 0.09 s while the existing K. Pak et al. [31], Y. Tang et al. [32], I. Vazquez Sandoval et al. [33] and C. M. Chen et al. [34] protocols consume 7.74 s, 0.88 s, 9 s, and 4.9 s, respectively which is higher in comparison to our scheme. Due to the large execution time, all existing protocols have huge computational complexity in real-time execution. Thus, our suggested scheme is a pragmatic choice and a suitable alternative to all the existing protocols presently. Both the values of parseTime as well as searchTime are measured optimal and pragmatic in comparison to the existing protocols.

Figure 2 depicts the proposed scheme visited nodes as well as communication steps along with the diverse 3PAKE protocols explored during the last decade by various researchers. From Figure 2, it is clear that the suggested protocol is capable to visit over the 20 nodes, while the existing K. Pak et al. [31], Y. Tang et al. [32], I. Vazquez Sandoval et al. [33] and C. M. Chen et al. [34] protocols visit just over 18, 17, 13, and 15 nodes, respectively. Further, our protocol takes two communication steps in the testing procedure, which is optimal and minimum, while the existing protocols, i.e., K. Pak et al. [31], Y. Tang et al. [32], I. Vazquez Sandoval et al. [33], and C. M. Chen et al. [34], take 6, 6, 4, and 5 communication steps, respectively. The authors offered the concept as well as information regarding the AVISPA simulation software and then represented the entire HLPSL coding explanation with the simulation outcomes of the proposed protocol.



	K. Pak et al.	Y. Tang et al.	I. Vazquez Sandoval	C. M. Chen	Proposed Scheme
parseTime	0	0	0	0	0
searchTime	7.74	0.88	9	4.9	0.09

Figure 1. Demonstrates the proposed scheme time of execution along with the diverse 3PAKE protocols [31–34].

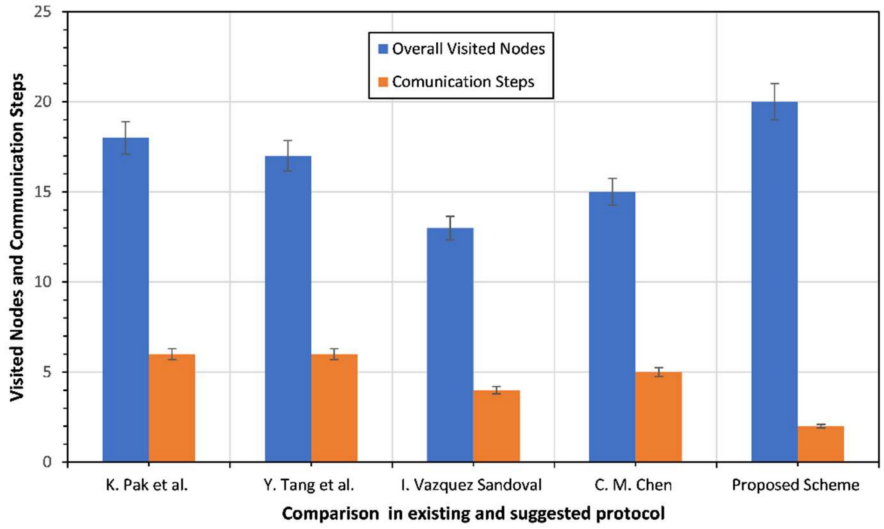


Figure 2. Demonstrates the proposed scheme visited nodes as well as communication steps along with the diverse 3PAKE protocols [31–34].

5. Conclusions and Future Work

The secrecy of confidential information is constantly becoming a major challenge all around the globe because of the rapid increment in the number of clients over the limited networks. Secure data are easily stolen in real-time while diverse parties want to communicate with each other by means of multifarious methods, such as brute-force attacks as well as cryptanalysis, and numerous other certain kinds of real-time assaults, drawing more attention towards the development and implementation of the novel protocols that are capable of providing desired secrecy to the user while communicating with each other. In this research paper, the investigators developed a simple and new 3PAKE protocol which is based on the method of elliptical curve cryptography (ECC) along with the symmetric encryption (SE) jointly. While comparing the suggested 3PAKE along with the previously explored secrecy protocol, it is to be found that the suggested 3PAKE protocol is more robust and secure in the social network security verification as required in the current social network models. The proposed 3PAKE protocol is more robust and secure against various known attacks, such as cryptanalysis and other similar kinds of attacks, such as man-in-the-

middle attacks. Our proposed 3PAKE protocol entails much less computational complexity in comparison to the protocols developed earlier by the researchers as our suggested protocol takes only searchTime 0.09 s along with parseTime 0.00 s. The overall number of communication steps was considered 2 during the verification and depth plies was 3. Last but not least, the overall visited nodes was 20, which is to be considered a pragmatic value in the case of data secrecy in the social network environment. Meanwhile, multiple investigators have changed the 3PAKE methods for numerous purposes in previous years, although there are significant opportunities for additional studies considering 3PAKE technique customization for the social networking scenario for best results. In the future, there are vital possibilities for further research in this arena to discover more pragmatic, improved secrecy protocols to offer desired secrecy against various secrecy assaults.

Author Contributions: Conceptualization, V.K.S. and D.A.; Methodology, V.K.S., D.A. and S.K.; Validation, P.S. and I.D.N.; Formal analysis, P.S. and I.D.N.; Investigation, D.A., P.S. and I.D.N.; Resources, D.A., S.K.; Data curation, V.K.S. and D.A.; Writing—original draft preparation, V.K.S., D.A. and S.A.; Writing – Review & Editing, P.S.; Funding acquisition, P.S. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported by the National Research Foundation of Korea (NRF) grant funded by the Korean government (NRF-2022R1G1A1004799).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Zheng, Y.; Hu, S.; Wei, L.; Chen, Y.; Wang, H.; Yang, Y.; Li, Y.; Xu, B.; Huang, W.; Chena, L. Design and analysis of a security-enhanced three-party authenticated key agreement protocol based on chaotic maps. *IEEE Access* **2020**, *8*, 66150–66162. [CrossRef]
2. Islam, S.H.; Amin, R.; Biswas, G.; Farash, M.S.; Li, X.; Kumari, S. An improved three party authenticated key exchange protocol using hash function and elliptic curve cryptography for mobile-commerce environments. *J. King Saud Univ.-Comput. Inf. Sci.* **2017**, *29*, 311–324. [CrossRef]
3. Yoon, E.-J.; Yoo, K.-Y. Cryptanalysis of an efficient three-party password-based key exchange scheme. *Procedia Eng.* **2012**, *29*, 3972–3979. [CrossRef]
4. Sahi, A.; Lai, D.; Li, Y. Three-party password-based authenticated key exchange protocol based on the computational Diffie-Hellman assumption. *Int. J. Commun. Netw. Distrib. Syst.* **2018**, *21*, 560. [CrossRef]
5. Farash, M.S.; Attari, M.A. An efficient and provably secure three-party password-based authenticated key exchange protocol based on Chebyshev chaotic maps. *Nonlinear Dyn.* **2014**, *77*, 399–411. [CrossRef]
6. Farash, M.S.; Attari, M.A.; Kumari, S. Cryptanalysis and improvement of a three-party password-based authenticated key exchange protocol with user anonymity using extended chaotic maps. *Int. J. Commun. Syst.* **2017**, *30*, e2912. [CrossRef]
7. Lin, C.Y.; Fu, C.H. A lightweight three-party authenticated key exchange protocol with XOR-based operation. *Chung Cheng Ling Hsueh Pao/J. Chung Cheng Inst. Technol.* **2016**, *8*, 215–224.
8. Chang, T.-Y.; Hwang, M.-S.; Yang, W.-P. A communication-efficient three-party password authenticated key exchange protocol. *Inf. Sci.* **2011**, *181*, 217–226. [CrossRef]
9. He, D.; Chen, Y.; Chen, J. An Id-Based Three-Party Authenticated Key Exchange Protocol Using Elliptic Curve Cryptography for Mobile-Commerce Environments. *Arab. J. Sci. Eng.* **2013**, *38*, 2055–2061. [CrossRef]
10. Yeh, K.-H.; Lo, N.W.; Hsiang, T.-R.; Wei, Y.-C.; Hsieh, H.-Y. Chaos between password-based authentication protocol and dictionary attacks. *Adv. Sci. Lett.* **2013**, *19*, 1048–1051. [CrossRef]
11. Xie, Q.; Hu, B.; Dong, N.; Wong, D.S. Anonymous three-party password-authenticated key exchange scheme for telecare medical information systems. *PLoS ONE* **2014**, *9*, e102747. [CrossRef]
12. Yang, J.-H.; Chang, C.-C. An efficient three-party authenticated key exchange protocol using elliptic curve cryptography for mobile-commerce environments. *J. Syst. Softw.* **2009**, *82*, 1497–1502. [CrossRef]
13. Amin, R.; Biswas, G.P. Cryptanalysis and Design of a Three-Party Authenticated Key Exchange Protocol Using Smart Card. *Arab. J. Sci. Eng.* **2015**, *40*, 3135–3149. [CrossRef]
14. Ruan, O.; Wang, Q.; Wang, Z. Provably leakage-resilient three-party password-based authenticated key exchange. *J. Ambient Intell. Humaniz. Comput.* **2019**, *10*, 163–173. [CrossRef]
15. Muthumeenakshi, R.; Reshmi, T.; Murugan, K. Extended 3PAKE authentication scheme for value-added services in VANETs. *Comput. Electr. Eng.* **2017**, *59*, 27–38. [CrossRef]

16. Shu, Q.; Wang, S.B.; Hu, B.; Han, L.D. Improved verifier-based three-party password-authenticated key exchange protocol from ideal lattices. *J. Cryptologic Res.* **2021**, *2021*, 6952869. [CrossRef]
17. Zhao, J.; Gu, D. Provably secure three-party password-based authenticated key exchange protocol. *Inf. Sci.* **2012**, *184*, 310–323. [CrossRef]
18. Li, C.-T.; Chen, C.-L.; Lee, C.-C.; Weng, C.-Y.; Chen, C.-M. A novel three-party password-based authenticated key exchange protocol with user anonymity based on chaotic maps. *Soft Comput.* **2018**, *22*, 2495–2506. [CrossRef]
19. Kim, M.; Moon, J.; Won, D.; Park, N. Revisit of password-authenticated key exchange protocol for healthcare support wireless communication. *Electronics* **2020**, *9*, 733. [CrossRef]
20. Xiong, H.; Chen, Y.; Guan, Z.; Chen, Z. Finding and fixing vulnerabilities in several three-party password authenticated key exchange protocols without server public keys. *Inf. Sci.* **2013**, *235*, 329–340. [CrossRef]
21. Xie, Q.; Hu, B.; Wu, T. Improvement of a chaotic maps-based three-party password-authenticated key exchange protocol without using server's public key and smart card. *Nonlinear Dyn.* **2015**, *79*, 2345–2358. [CrossRef]
22. Lv, C.; Ma, M.; Li, H.; Ma, J.; Zhang, Y. An novel three-party authenticated key exchange protocol using one-time key. *J. Netw. Comput. Appl.* **2013**, *36*, 498–503. [CrossRef]
23. Lee, C.C.; Chiu, S.T.; Li, C.T. Improving security of a communication-efficient three-party password authentication key exchange protocol. *Int. J. Netw. Secur.* **2015**, *17*, 1–6.
24. Sinha, V.K.; Anand, D.; Alharithi, F.S.; Almulihi, A.H. A Secure Three-Party Authenticated Key Exchange Protocol for Social Networks. *Comput. Mater. Contin.* **2022**, *71*, 6293–6305. [CrossRef]
25. Tan, Z. An enhanced three-party authentication key exchange protocol for mobile commerce environments. *J. Commun.* **2010**, *5*, 436–443. [CrossRef]
26. Yin, A.; Guo, Y.; Song, Y.; Qu, T.; Fang, C. Two-round password-based authenticated key exchange from lattices. *Wirel. Commun. Mob. Comput.* **2020**, *2020*, 8893628. [CrossRef]
27. Lo, N.W.; Yeh, K.H. A practical three-party authenticated key exchange protocol. *Int. J. Innov. Comput. Inf. Control* **2010**, *6*, 2469–2483.
28. Zargar, S.; Shahidinejad, A.; Ghobaei-Arani, M. A lightweight authentication protocol for IoT-based cloud environment. *Int. J. Commun. Syst.* **2021**, *34*, e4849. [CrossRef]
29. Huang, H.; Lu, S.; Wu, Z.; Wei, Q. An efficient authentication and key agreement protocol for IoT-enabled devices in distributed cloud computing architecture. *Eurasip J. Wirel. Commun. Netw.* **2021**, *2021*, 150. [CrossRef]
30. Viganò, L. Automated Security Protocol Analysis with the AVISPA Tool. *Electron. Notes Theor. Comput. Sci.* **2006**, *155*, 61–86. [CrossRef]
31. Pak, K.; Pak, S.; Ho, C.; Pak, M.; Hwang, C. Anonymity preserving and round effective three-party authentication key exchange protocol based on chaotic maps. *PLoS ONE* **2019**, *14*, e0213976. [CrossRef] [PubMed]
32. Tang, Y.; Li, Y.; Zhao, Z.; Zhang, J.; Ren, L.; Li, Y. Improved Verifier-Based Three-Party Password-Authenticated Key Exchange Protocol from Ideal Lattices. *Secur. Commun. Netw.* **2021**, *2021*, 6952869. [CrossRef]
33. Sandoval, I.V.; Atashpendar, A.; Lenzini, G.; Ryan, P.Y.A. *PakeMail: Authentication and Key Management in Decentralized Secure Email and Messaging via PAKE*; Springer: Berlin/Heidelberg, Germany, 2021. [CrossRef]
34. Chen, C.-M.; Wang, K.-H.; Yeh, K.-H.; Xiang, B.; Wu, T.-Y. Attacks and solutions on a three-party password-based authenticated key exchange protocol for wireless communications. *J. Ambient Intell. Humaniz. Comput.* **2019**, *10*, 3133–3142. [CrossRef]