International Journal of Engineering Inventions
e-ISSN: 2278-7461, p-ISSN: 2319-6491
Volume 11, Issue 3 [May.-June. 2022] PP: 336-343

Implementation of Privacy Authentication Key Protocol over Secure Cloud Storage

SK. YAKOOB[1], V. DIVYA[2], D. D SAI PRASANNA KUMARI[3], T. KISHORE[4], A. ARUN KUMAR[5], CH. SAI KISHORE REDDY[6]
[1]*Associate Professor,Dept. of CSE, Sai Spurthi Institute of Technology,Khammam,Telangana,India*
[2,3,4,5,6]*B.Tech Student, Dept. of CSE, Sai Spurthi Institute of Technology, Khammam,Telangana,India*

ABSTRACT:

With the development of distributed computing innovation as far as unwavering quality and effectiveness, an enormous number of administrations have relocated to the cloud stage. To helpful admittance to the administrations and secure the protection of correspondence in the public organization, three-factor Mutual Authentication and Key Agreement (MAKA) conventions for multi-server models gain wide consideration. Nonetheless, a large portion of the current three-factor MAKA conventions don't give a proper security evidence bringing about different assaults on the related conventions, or they have high calculation and correspondence costs. What's more the greater part of the three-factor MAKA conventions haven't a dynamic repudiation component, which prompts vindictive clients can not be immediately disavowed. To address these downsides, we propose a provable powerful revocable three-factor MAKA convention that accomplishes the client dynamic administration utilizing Schnorr marks and gives a conventional security evidence in the arbitrary prophet. Security investigation shows that our convention can satisfy different needs in the multi-server conditions. Execution examination shows that the proposed plot is appropriate for registering asset compelled savvy gadgets. The full form of the recreation execution demonstrates the practicality of the convention.

Index Terms—Protocols, Cloud computing, Smart cards, Authentication, Bioceramics.

Date of Submission: 02-06-2022 Date of Acceptance: 15-06-2022

---

1. INTRODUCTION

In the new decade, distributed computing innovation has been totally popularized. It can not just improve administration proficiency yet additionally decrease costs. An ever increasing number of organizations are putting their administrations on the cloud stage for improvement, the board and upkeep. This not just lessens the nearby upkeep trouble for these endeavors, yet in addition gives brought together security and activity the board for all administrations on the outsider cloud stage. Albeit outsider cloud stages have all the more remarkable advances and more standard specialized particulars to guarantee that the servers run in a somewhat solid climate, clients and servers convey in the public organization. In this way, validation and key understanding are basic for the correspondence security. The utilization of shared validation and key understanding (MAKA) conventions not just keep aggressors from mishandling server assets, yet additionally forestall vindictive aggressors acting like the server to get the client's data. In this way, the MAKA conventions have been widely contemplated since Lamport proposed a secret phrase based verification convention.

Prior MAKA conventions are intended for single-server engineering. As Internet clients develop dramatically, the quantity of cloud servers delivering unique administrations has likewise developed altogether. For the single-server engineering, it is hard for clients to keep an assortment of passwords for every server. To further develop client experience, numerous researchers propose more adaptable MAKA conventions for multi-server conditions. Joined with the brought together administration highlights of the cloud stage, such conventions can be helpfully applied. The conventions for multi-server structures model as displayed in clients and cloud servers just need to enroll in the enrollment focus (RC) to common verification and key agreement. However, the current three-factor MAKA conventions still have the accompanying imperfections.

1) Security weaknesses: Most of the current MAKA conventions dependent on the three elements haven't a formal verification, however some casual security examination. Also a few conventions were install uncertain elements

for example, key validation factors effortlessly extricated. We will dissect such shortcomings in the security examinations and cryptanalysis subsection.
2) Incomplete fundamental capacities: Some significant essential capacities, for example, dynamic client the executives, confirmation stage without RC, are not thought of in most MAKA conventions.
3) High expense: Some three-factor MAKA conventions didn't assess their genuine application climate, which results these conventions are not appropriate for the restricted asset of the gadgets. Consequently, it still a test to plan a powerful threefactor MAKA convention for accomplishing secure correspondence among client and server.

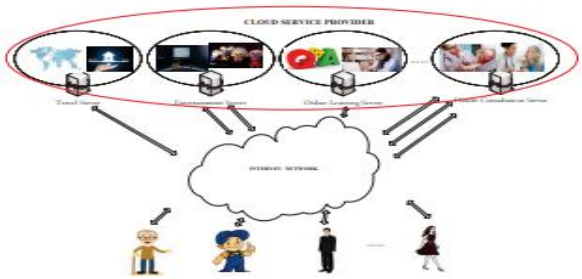

Fig. 1. Cloud service environment

2. Related Works

In 2001, Li et al. presented the idea of validation convention for multi-server conditions and proposed the first secret key based MAKA convention utilizing the neural organization. On account of the convoluted neural organization, Li et al's. convention isn't reasonable for shrewd gadgets with restricted processing power. To further develop productivity, Juang proposed a MAKA convention for multi-server structures by utilizing hash capacities and symmetric key cryptosystems. In the equivalent year, Chang et al. brought up that Juang's convention is defective as far as proficiency. They proposed a more productive MAKA conspire for multi-server conditions. In any case, in their convention RC imparts framework private key to all servers. This will without a doubt bring about numerous security weaknesses. To further develop security, some new MAKA conventions utilizing hash capacities and symmetric-key cryptosystems had likewise been proposed. In 2013, Liao et al. [10] proposed a multi-server distant client validation convention utilizing self-guaranteed public keys for versatile customers. Notwithstanding, their conspire doesn't build up a common meeting key and the correspondence cost is unsuitable.

To address this shortcoming, in light of unique mark, Lee et al. proposed a confirmation convention utilizing savvy card. In any case, Lin et al. and Chang et al. saw that as Lee et al's. convention experiences the disguise assault and the planning assault, separately. To improve security, Kim et al. proposed another biometrics-based confirmation convention utilizing brilliant card. Sadly, Scott pointed out that Kim et al's. convention can be totally undermined by a detached foe. Afterward, Khan et al. found that Lin et al's. plot likewise experiences the server mocking assault and proposed a further developed form. For multi-server models, Yoon et al. proposed a biometrics-based confirmation convention utilizing circular bend cryptosystem (ECC) and shrewd card. Sadly, Kim et al. and He brought up that Yoon et al.'scheme is shaky under the disconnected secret phrase speculating assault, the favored insider assault and the pantomime assault. Afterward, He et al. proposed a powerful biometrics-based validation plot for multi-server models. Nonetheless, Odelu et al. point out that He et al's. convention experiences the known meeting explicit impermanent data assault, the pantomime assault, etc. Be that as it may, every validation and key understanding in Odelu et al.'protocol requires the contribution of RC. In 2017, Reedy et al. additionally proposed a biometricsbased MAKA convention for multi-server conditions. Sadly, later our investigation in the security correlations also cryptanalysis subsection of this paper, their convention is weak the server pantomime assault and the man-inthe-center assault. Then again, the MAKA convention is additionally generally utilized in different conditions, like Passive Web of Things, Vehicles in Smart City, and Cell phones.

3. THE PROPOSED 3DRMAKA PROTOCOL

3.1 Initialization Phase

1) According the definition of bilinear pairing, RC selects two groups G_1, G_2 of the same prime order q and a bilinear paring e:$G_1 \times G_1 \rightarrow G_2$. Then, RC also chooses two random numbers $s_1, s_2 \in Z_q^*$ as the system private keys, a generator P of G_1 and a share key ASK.
2) RC calculates $P_{pub} = s_1 \cdot P$, $g = e(P,P)$, $g_{pub} = g^{s_2}$ and chooses nine secure hash functions: H_{00}:$\{0,1\}^* \rightarrow G_1$, H_{01}:$Z_q^* \rightarrow G_1$, H_1:$\{0,1\}^* \rightarrow Z_q^*$, H_2:$\{0,1\}^* \times Z_q^* \rightarrow Z_q^*$, H_3:$\{0,1\}^* \times Z_q^* \times Z_q^* \rightarrow Z_q^*$, H_4:$\{0,1\}^{2q} \rightarrow Z_q^*$, H_5:$G_2 \times Z_q^* \times \{0,1\}^* \rightarrow Z_q^*$, H_6:$G_2 \times \{0,1\}^* \times Z_q^* \rightarrow Z_q^*$, H_7:$G_2 \times G_2 \times G_2 \times G_2 \times Z_q^* \times \{0,1\}^* \rightarrow Z_q^*$.
3) RC publics the system parameters $\{q, G_1, G_2, P_{pub}, g, g_{pub}, e, P, H_{00}, H_{01}, H_1, H_2, H_3, H_4, H_5, H_6, H_7\}$.

3.2 Server Registration Phase

1) S_j transmits registration request with his/her identity ID_{sj} to RC securely.
2) RC computers $d_{sj} = s_1 \cdot H_{00}(ID_{sj})$, $H_1(ASK)$ and delivers them back to S_j under a secure channel.
3) Upon receiving $(d_{sj}, H_1(ASK))$, the S_j can validate the private key by checking whether the equation $e(d_{sj}, P)? = e(H_{00}(ID_{sj}), P_{pub})$ holds. If the equation holds, the private key is valid and vice versa.
4) RC maintains a table database T_{sj}, which stores the status of the corresponding registration servers.

3.3 Users Registration Phase

1) U_i inputs his/her identity ID_{ui}, password PW_{ui} and biometrics BIO_{ui}. Then U_i generates a

random number $r_{ui} \in Z_q^*$ and computers $Gen(BIO_{ui}) = (\theta_{ui}, \partial_{ui})$, $PID_{ui} = H_2(ID_{ui}, r_{ui})$, $PWD_{ui} = H_3(PW_{ui}, PID_{ui}, r_{ui})$, and $PBIO_{ui} = H_2(\partial_{ui}, r_{ui})$. Finally U_i transmits $(ID_{ui}, PID_{ui}, PWD_{ui}, PBIO_{ui})$ to RC through an out of band (secure) channel.

2) RC calculates $d_{ui} = s_1 \cdot H_{01}(PID_{ui})$, $G_{ui} = d_{ui} \oplus PWD_{ui}$, $V_{ui} = H_4(PWD_{ui}, G_{ui})$ for corresponding user. To reduce the user's computational burden, RC computes $e(d_{ui}, H_{00}(ID_{sj}))$ for the user based on valid server entries in the T_{sj} table database. And then generates a T_{ui} table whose data is $R_{sj} = e(d_{ui}, H_{00}(ID_{sj})) \oplus PWD_{ui} \oplus PBIO_{ui}$. RC inserts $(T_{ui}, G_{ui}, V_{ui}, H_1(ASK))$ into smartcard(SC) for corresponding user and sends SC to the user under a secure channel. Finally, RC creates a form database T_{sui} with hash of user identity information in which also stores the status of the corresponding registration users to dynamically manage users.

3) Upon receiving SC, U_i computes $W_{ui} = r_{ui} \oplus H_1(\partial_{ui})$, $h_1 = H_1(ASK) \oplus r_{ui} \oplus PBIO_{ui}$ and then replaces $H_1(ASK)$ with θ_{ui}, W_{ui}, $H_i(i = 00, 01, 1, \ldots, 7)$, h_1, g_{pub}.

3.4 Time Key Update Phase

1) Before updating the time key for a user, RC checks the status of the corresponding anonymous user PID_{ui} in T_{sui}. Then, RC chooses a random number $b_{ui} \in Z_q^*$, valid time period t and computes $B_{ui} = g^{b_{ui}}$, $d_{tui} = b_{ui} + H_5(B_{ui}, PID_{ui}, t) \cdot s_2 mod q$ for the legitimate user. RC transmits (B_{ui}, d_{tui}, t) to the corresponding user through a public channel.

2) Upon receiving (B_{ui}, d_{tui}, t), the user first enters ID_{ui}, BIO_{ui} and then computes $\partial_{ui} = Rep(BIO_{ui}, \theta_{ui})$, $r_{ui} = W_{ui} \oplus H_1(\partial_{ui})$, $PID_{ui} = H_2(ID_{ui}, r_{ui})$. U_i checks $g^{d_{tui}} ? = B_{ui} \cdot g_{pub}^{H_5(B_{ui}, PID_{ui}, t)}$ to verify the validity of the time key. If the equation holds, the user inserts $(B_{ui}, d_{tui}, t)$to SC. The elements contained in the SC are $\{T_{ui}, G_{ui}, V_{ui}, h_1, \theta_{ui}, W_{ui}, H_i(i = 00, 01, 1, \ldots, 7), g_{pub}, B_{ui}, d_{tui}, t\}$.

3.5 Login and Mutual Authentication Phase

1) U_i inputs his/her ID_{ui}, PW_{ui} and BIO_{ui} into SC. SC uses its stored information to calculate $\partial_{ui} = Rep(BIO_{ui}, \theta_{ui})$, $r_{ui} = Wui \oplus H_1(\partial_{ui})$, $PID_{ui} = H_2(ID_{ui}, r_{ui})$, $PWD_{ui} = H_3(PW_{ui}, PID_{ui}, r_{ui})$, $PBIO_{ui} = H_2(\partial_{ui}, r_{ui})$. SC validates whether the equation $V_{ui} ? = H_4(PWD_{ui}, G_{ui})$ holds. If the equation holds, the user logins successfully, otherwise, rejects the request.

2) Using the information in table T_{ui}, the user chooses a target server ID_{sj}. SC generates a random number $N_1 \in Z_q^*$ and calculates $H_1(ASK) = h_1 \oplus r_{ui} \oplus PBIO_{ui}$, $k_{ui} = g^{N_1}$, $F_{ui} = PID_{ui} \oplus H_6(k_{ui}, ID_{sj}, H_1(ASK))$. Then, SC sends $(F_{ui}, k_{ui}, B_{ui}, d_{tui}, t)$ to the corresponding server S_j.

3) Upon receiving the messages, S_j first verifies the time key correctness by checking $g^{d_{tui}} ? = B_{ui} \cdot g_{pub}^{H_5(B_{ui}, PID_{ui}, t)}$, where $PID_{ui} = F_{ui} \oplus H_6(k_{ui},$

$ID_{sj}, H_1(ASK)$). If the equation holds, S_j continues next steps; otherwise, rejects the request.

4) S_j chooses a random number $N_2 \in Z_q^*$ and computes $k_{1t} = e(d_{sj}, H_{01}(PID_{ui}))$, $k_{sj} = g^{N_2}$ and $D_{sj} = H_7(k_{1t}, k_{sj}, k_{ui}, g_{pub}, PID_{ui}, ID_{sj})$. Then, S_j transmits (D_{sj}, k_{sj}) to the corresponding U_i.
5) Upon receiving (D_{sj}, k_{sj}), U_i computes $k_1 = R_{sj} \oplus PWD_{ui} \oplus PBIO_{ui}$ and then checks whether the $D_{sj}? = H_7(k_1, k_{sj}, k_{ui}, g_{pub}, PID_{ui}, ID_{sj})$ holds. If the equation holds, U_i computes $k_u = k_{sj}^{N_1}$, $D_{ui} = H_7(g_{pub}, k_{ui}, k_{sj}, k_1, PID_{ui}, ID_{sj})$, the session key $sk = H_7(k_u, g_{pub}, k_{sj}, k_{ui}, PID_{ui}, ID_{sj})$. Then, U_i sends D_{ui} to S_j.
6) When S_j receives the message D_{ui}, he/she checks whether the $D_{ui}? = H_7(g_{pub}, k_{ui}, k_{sj}, k_{1t}, PID_{ui}, ID_{sj})$ holds. If the equation holds, S_j computes $k_s = k_{ui}^{N_2}$ and the session key $sk = H_7(k_s, g_{pub}, k_{sj}, k_{ui}, PID_{ui}, ID_{sj})$.

3.6 Password and Biometrics Change Phase

1) U_i enters his/her ID_{ui}, PW_{ui}, BIO_{ui} and new PW_{nui}, BIO_{nui} into SC. The SC computes $\partial_{ui} = Rep(BIO_{ui}, \theta_{ui})$, $r_{ui} = W_{ui} \oplus H_1(\partial_{ui})$, $PID_{ui} = H_2(ID_{ui}, r_{ui})$, $PWD_{ui} = H_3(PW_{ui}, PID_{ui}, r_{ui})$, $PBIO_{ui} = H_2(\partial_{ui}, r_{ui})$. The SC validates whether the equation $V_{ui}? = H_4(PWD_{ui}, G_{ui})$ holds. If not, SC terminates the follow-up operations.
2) SC computes $PWD_{nui} = H_3(PW_{nui}, PID_{ui}, r_{ui})$, $Gen(BIO_{nui}) = (\theta_{nui}, \partial_{nui})$, $PBIO_{nui} = H_2(\partial_{nui}, r_{ui})$ and then uses them to update other relevant informations in SC, namely $R_{nsj} = R_{sj} \oplus PWD_{ui} \oplus PBIO_{ui} \oplus PBIO_{nui} \oplus PWD_{nui} \rightarrow T_{nui}$, $G_{nui} = G_{ui} \oplus PWD_{ui} \oplus PWD_{nui}$, $V_{nui} = H_4(PWD_{nui}, G_{nui})$, $h_{n1} = h_1 \oplus PBIO_{ui} \oplus PBIO_{nui}$, $W_{nui} = W_{ui} \oplus H_1(\partial_{ui}) \oplus H_1(\partial_{nui})$. Finally, SC replaces $(T_{ui}, G_{ui}, V_{ui}, h_1, W_{ui}, \theta_{ui})$ with $(T_{nui}, G_{nui}, V_{nui}, h_{n1}, W_{nui}, \theta_{nui})$.

3.7 New Server Update Phase

1) When a new server S_{nj} has finished registration, the RC updates the T_{sj} and broadcasts ID_{nsj} all valid users in the T_{sui}.
2) Upon receiving ID_{nsj}, users input ID_{ui}, PW_{ui}, BIO_{ui} and ID_{nsj} into SC. The SC computes $\partial_{ui} = Rep(BIO_{ui}, \theta_{ui})$, $r_{ui} = W_{ui} \oplus H_1(\partial_{ui})$, $PID_{ui} = H_2(ID_{ui}, r_{ui})$, $PWD_{ui} = H_3(PW_{ui}, PID_{ui}, r_{ui})$, $PBIO_{ui} = H_2(\partial_{ui}, r_{ui})$, $d_{ui} = G_{ui} \oplus PWD_{ui}$, $R_{nsj} = e(d_{ui}, H_{00}(ID_{nsj})) \oplus PWD_{ui} \oplus PBIO_{ui}$. Then, the SC inserts R_{nsj} into T_{ui}.

4. PERFORMANCE ANALYSIS

In this part, we will break down the presentation of the proposed 3DRMAKA convention and the connected examination plans as far as calculation time, correspondence costs and the necessary number of round trip times (RTT). Contingent upon the organization delay the RTT time can turn into the predominant expense for a convention. A more broad examination can be gotten from paper. To accomplish a solid security level of 1024-

bits RSA calculation, we pick a Tate matching and super-solitary bend $y_2 = x_3 - 3_x$ modp over Fp which Fp is 512 pieces limited field. And afterward we pick a subgroup of G1 with request $q = 2^{159} + 2^{17} + 1$ that is created from focuses on elliptic bend over a limited field Fp. In the first place, we characterize the accompanying documentations.

- T_{map}: Time to execute a bilinear-pairing operation.
- T_{mtp}: Time to execute a map-to-point hash operation.
- T_{exp}: Time to execute a modular exponentiation operation.
- T_{pa}: Time to execute a point addition operation.
- T_h: Time to execute a general hash operation.
- T_{mul}: Time to execute a multiplication operation in G_2.
- T_{pmul}: Time to execute a scalar multiplication operation in G_1.
- T_{sed}: Time to execute a symmetric key encryption/decryption algorithm.

4.1 Computation Cost

For examination, we sum up as far as the quantity of tasks and the hour of execution to finish a common validation and key arrangement in our plan and He et al., Liao et al., Reddy et al. and Odelu et al. plans, separately. Expect to be that RC and server have a similar figuring power

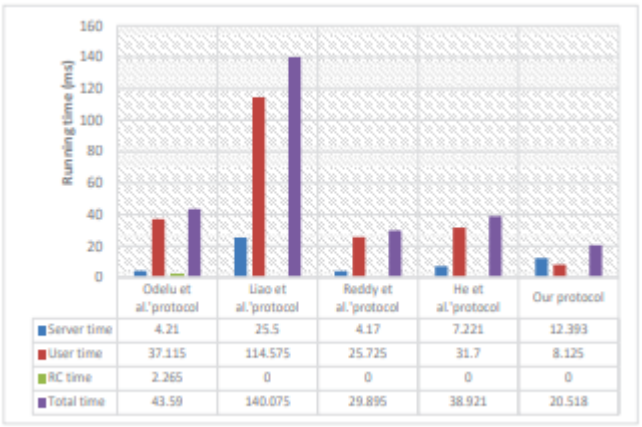

Fig. 2. Computation cost comparisons

4.2 Communication and RTT Cost

In light of the past conversation of safety level, we have accepted that the length of p and q are 512 pieces and 160 bits individually. In this way, the size of a component in G_1 or G_2 also the length of hash capacities Hi (I = 1, . . . , 7) yield are 1024 pieces and 160 pieces individually. Accept the length of both client's personality and legitimate time t are 32 pieces.

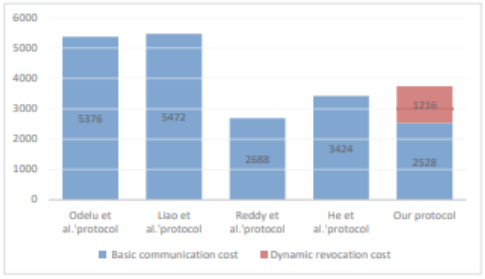

Fig. 03. Communication cost comparisons

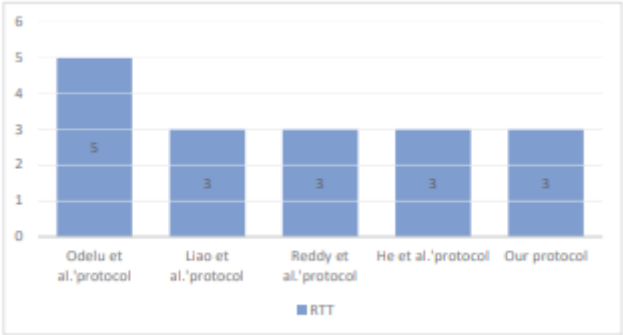

Fig. 04. The required number of round trip times

To demonstrate that our convention is actually strong, our programming recreation executes a full-highlighted demo programming. Joined with our hypothetical evidence, we can better clarify the specialized possibility of our plan. As, our demo not just verify each other yet additionally arrange the meeting key

Fig. 05. Server result of authentication and agreement key

Fig. 06. Client result of authentication and agreement key

Note that our investigation is an unadulterated programming show, so it is streamlined as far as the need to remove biometrics from equipment. We straightforwardly utilize the data entered by the client as biometrics token. This work is predominantly in view of the MIRACL open source project. To carry out our convention, we have made minor changes to a portion of the source code in this open source project. To control the length of the article, we have transferred the definite exhibit process, arrangement climate, code, and so forth as advantageous materials.

5. CONCLUSION

To oppose the weariness of secret key assault on the two-factor MAKA conventions, an enormous number of three-factor MAKA conventions have been proposed. Notwithstanding, practically all threefactor MAKA conventions don't give formal verifications and dynamic client the executives component. To accomplish more adaptable client the executives and higher security, this paper proposes another three-factor MAKA convention that upholds dynamic disavowal and gives formal evidence. The security shows that our convention accomplishes the security properties of prerequisites from multi-server conditions. Then again, through the far reaching examination of execution, our convention doesn't forfeit proficiency while working on the capacity. Despite what is generally expected, the proposed convention enjoys incredible benefits as far as the complete calculation time.

6. REFERENCES

[1]. D. He, S. Zeadally, N. Kumar, and J. Lee, "Anonymous authentication for wireless body area networks with provable security," IEEE Systems Journal, pp. 1–12, 2016

[2]. J.-L. Tsai, "Efficient multi-server authentication scheme based on one-way hash function without verification table," Computers & Security, vol. 27, no. 3C4, pp. 115–121, 2008.

[3]. D. Wang and P. Wang, Offline Dictionary Attack on Password Authentication Schemes Using Smart Cards. Springer International Publishing, 2015.

[4]. H. Kim, S. Lee, and K. Yoo, "Id-based password authentication scheme using smart cards and fingerprints," Operating Systems Review, vol. 37, no. 4, pp. 32–41, 2003.
[5]. H. Kim, W. Jeon, K. Lee, Y. Lee, and D. Won, "Cryptanalysis and improvement of a biometrics-based multi-server authentication with key agreement scheme," in International Conference on Computational Science and ITS Applications, 2012, pp. 391–406.
[6]. M. L. Das, A. Saxena, and V. P. Gulati, "A dynamic id-based remote user authentication scheme," IEEE Transactions on Consumer Electronics, vol. 50, no. 2, pp. 629–631, 2004
[7]. D. He, S. Zeadally, N. Kumar, and W. Wu, "Efficient and anonymous mobile user authentication protocol using self-certified public key cryptography for multi-server architectures," IEEE Transactions on Information Forensics and Security, vol. 11, no. 9, pp. 2052– 2064, 2016.
[8]. P. Xie, J. Feng, Z. Cao, and J. Wang, "Genewave: Fast authentication and key agreement on commodity mobile devices," IEEE/ACM Transactions on Networking, vol. PP, no. 99, pp. 1–13, 2018.
[9]. D. Pointcheval and J. Stern, "Security proofs for signature schemes," in International Conference on Theory and Application of Cryptographic Techniques, 1996, pp. 387–398.
[10]. J. C. Cha and J. H. Cheon, "An identity-based signature from gap diffie-hellman groups," public key cryptography, pp. 18–30, 2003.
[11]. H. H. Kilinc and T. Yanik, "A survey of sip authentication and key agreement schemes," IEEE Communications Surveys and Tutorials, vol. 16, no. 2, pp. 1005–1023, 2014.
[12]. X. Huang, Y. Xiang, A. Chonka, J. Zhou, and R. H. Deng, "A generic framework for three-factor authentication: Preserving security and privacy in distributed systems," IEEE Transactions on Parallel and Distributed Systems, vol. 22, no. 8, pp. 1390–1397, 2011.
[13]. W. Juang, "Efficient multi-server password authenticated key agreement using smart cards," IEEE Transactions on Consumer Electronics, vol. 50, no. 1, pp. 251–255, 2004.