ZERO-KNOWLEDGE AND OTP CLOUD-BASED TWO-FACTOR AUTHENTICATION FOR DATA TRANSFER

JAINA SAICHAND [1] Y. YESU BABU [2] TADIKAMALA VINEELA [3] G.SIDDHANTH [4]
[1234] ASST. PROFESSOR, DEPARTMENT OF ARTIFICIAL INTELLIGENCE,
[1,2,3,4] SRI MITTAPALLI COLLEGE OF ENGINEERING

Abstract:

These days, cloud computing is an important consideration for companies of all kinds, from mom-and-pop shops to global corporations. A major issue that hinders the technology's widespread deployment is the lack of security. The first level of protection in cloud computing is password authentication, which makes sure that only authorised users may access the data kept on the cloud server. Things seem to be going swimmingly for biometric and token-based multi-factor authentication systems. High costs, trouble transporting, and no revocation capabilities are just a few of the problems that come with using multi-factor. Popular attacks like offline password guessing and man-in-the-middle seed monitoring also fail to protect it. This article proposes two-factor authentication (2FA) as a solution to the aforementioned issues and a cost-effective one. We use Zero-Knowledge and One-Time Password (OTP) cloud-based two-factor authentication as our design paradigm. For instance, our proposed system includes features such as freely chosen passwords, session keys that protect user anonymity, and reciprocal authentication. Additionally, the authentication procedure is quite fast.

1. Introduction

Users have the freedom to access their data from anywhere at any time thanks to cloud computing, which allows them to store it on a remote server. The capacity to access user data whenever needed, from any device, and without worrying about software or hardware infrastructures is only one of many advantages of storing user data in the cloud. Users may save money by adjusting the exploitation scale to their needs without paying more [1, 2, 3]. These authentication techniques are based on the user's password. The majority of individuals leave themselves open to malicious attacks because they use passwords that are simple to remember, such their names or phone numbers. In contrast, more secure but harder to remember passwords are complex ones that are created randomly. On top of that, hackers may trigger system disruptions by using a dictionary attack on users who use easily-guessable passwords. Opponents have two choices when using dictionaries [4, 5]. An off-line guessing attack is the first kind of assault in which the perpetrator tries to get the communication details of valid users' login requests, checks them against a dictionary, and then launches assaults. As an adversary selects a new password at random from his dictionary, we compute communication values and compare them to the data we have on file. In such instance, you should try again using the password you used. Second, online guessing is used in the dictionary attack. To impersonate a valid user and submit a service request, an adversary utilises a string of passwords taken from his dictionary. If an attacker's first password attempt fails, he will try a different one. One typical defence against this kind of assault is to set a timer that will expire after a certain amount of failed attempts. In order to properly implement cloud authentication ideas, two-factor authentication (2FA) is recommended [6]. The first step in accessing any cloud service is for the user to log in using their credentials. It asks for the user's second factor after checking that their username and password are stored in the database of the cloud server. A user is authorised to access the resources of a cloud server when their second factor is valid on that server. As for the second part, it may be any number of tokens or smart cards. Only one genuine user has pre-registered their second factor with the server. However, the service provider's security might be at risk in the event of its loss or theft since the token is expensive, vulnerable to MITM Seed-tracing, and cannot survive loss or theft. Token organisation across different cloud servers is a big issue for both consumers and providers. When a large number of users try to verify at once, the system's procedure becomes unbearably slow because of the constraints of personal physiological authentication. Furthermore, further software and hardware is needed for the biometric component.

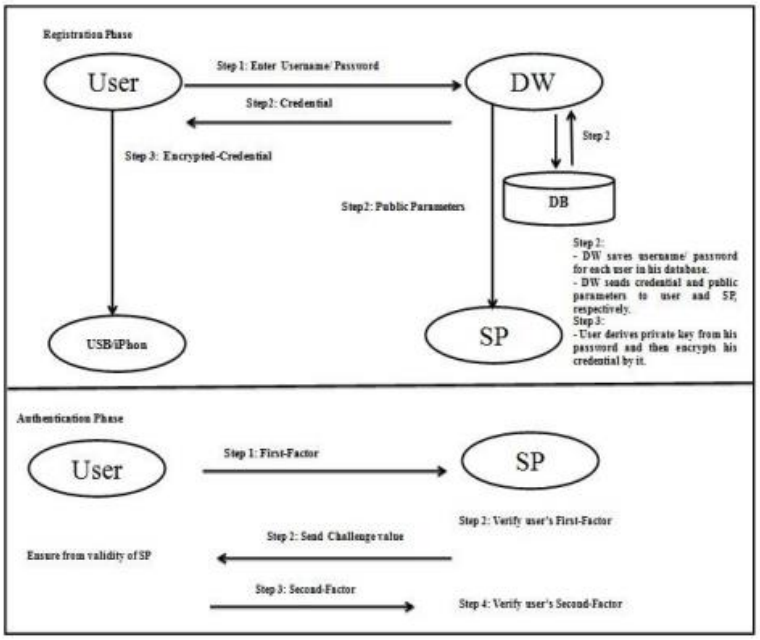

Registration Phase
User
Step 1: Enter Username/ Password
DW
Step2: Credential
Step 2
Step 3: Encrypted-Credential
DB
Step2: Public Parameters
Step 2:
- DW saves username/ password for each user in his database.
- DW sends credential and public parameters to user and SP, respectively.
Step 3:
- User derives private key from his password and then encrypts his credential by it.
USB/iPhon
SP
Authentication Phase
User
Step 1: First-Factor
SP
Step 2: Verify user's First-Factor
Step 2: Send Challenge value
Ensure from validity of SP
Step 3: Second-Factor
Step 4: Verify user's Second-Factor

Figure.1. Basic architecture of our proposed authentication.

A few of research have investigated potential solutions to deal with this kind of data. There have been worries about migration as of late. Take Dana in 2011 as an example. In Petcu's[6] view, cloud incompatibility is the biggest problem with cloud computing, and a new protocol is being considered as a solution to make clouds more portable. To provide the groundwork for the deployment of composite motion applications into or movement across clouds, Binz et al. [7] created a cloud-based computing model. [8] Cloud data portability databases were made possible by a technology that Shirazi et al. described in 2012. We began by acknowledging the enormous practical significance of researching data movement across cloud platforms. Many issues with transferring data to the cloud have not yet found solutions. There are obvious obstacles that reduce the efficacy of current cloud data transfer projects.To rephrase, there is an immediate need for more research on cloud data migration, especially to help with the transfer of user data between cloud servers when they change phones. Second, there are further security limits since it is difficult to demonstrate trustworthiness across several clouds in practice, particularly for applications that need the transfer of sensitive data. Security of communication keys, mutual authentication, and prevention of data breaches are among the many concerns. Possible solutions to these problems include authentication and key agreement procedures. This study proposes a novel anonymous-identity-based authentication and key agreement mechanism with the aim of simplifying and enhancing data transmission across multi-clouds. We are unaware of any prior usage of authentication and key agreements by peer cloud servers. Notable contributions from the paper include the following. To solve the problem of trust between cloud servers, we provide a PCAKA approach that relies on anonymous identities to facilitate peer-to-peer cloud authentication and key agreement. Using elliptic curve certificate-free encryption, our method is able to generate secure session keys for use across cloud service providers, guaranteeing the confidentiality of session data. We streamline operations without sacrificing security by doing away with the need for a trusted authority (TA). Data owners who are in need of data migration services may function as a trusted third party in our scheme by using cloud servers. This allows them to independently check each other and create trustworthy session keys for all users.

2. Related Work

Zigzag authentication is used in peer-to-peer networks [8]. They provided two different approaches to ZKPI (Zero-Knowledge Public Infrastructure), one of which required a key exchange mechanism for inter-network key exchange and the other of which did not. A new method that allows the prover to prove their identify with minimum computer needs has been approved, which increases their job capacity [9]. They are able to achieve their goals with the use of smart cards and bilinear pairing on the verifier side. Security is further enhanced by using zero-knowledge. Isomorphic graphs (ZKPA) are proposed by [10] as a means to implement and assess Zero-Knowledge Proof Authentication.We recommend a cloud model that focusses on pay as you go rather than the verifier side's time-consuming bilinear pairing strategy. By implementing Zero-Knowledge and requiring just one password per user, we are able to achieve anonymous authentication. Achieving great performance, cheap cost, and excellent security is the aim of the proposed approach. For the first time, Viet and colleagues (11, 12) introduced anonymous password authentication by combining the PIR system with a password scheme. There is no denying that this strategy is flawed. One need for PIR to function in P2P networks is ZN authentication [8]. But they did suggest a modified version of Zero-Knowledge Public Infrastructure (ZKPI) that called for a way for network peers to trade keys with one another. A new method was devised to improve the prover's performance, allowing him to confirm his identity with very minimum computer resources [9]. They are able to achieve their goals with the use of smart cards and bilinear pairing on the verifier side. Security is further enhanced by using zero-knowledge. Isomorphic graphs (ZKPA) are proposed by [10] as a means to implement and assess Zero-Knowledge Proof Authentication. We recommend a cloud model that focusses on pay as you go rather than the verifier side's time-consuming bilinear pairing strategy. By implementing Zero-Knowledge and requiring just one password per user, we are able to achieve anonymous authentication. Achieving great performance, cheap cost, and excellent security is the aim of the proposed approach. For the first time, Viet and colleagues (11, 12) introduced anonymous password authentication by combining the PIR system with a password scheme. There is no denying that this strategy is flawed. To begin, PIR need

3. System Analysis

The agent may undo the principal's delegation choices using the re-encryption key and the RIB-BPRE mechanism. They also noted that cloud users have issues due to the fact that identity-based broadcast agent re-encryption (RIB-BPRE) techniques do not use cloud computing. Liu et al. proposed a method for secure multi-owner data sharing in cloud-based dynamic groups. Through the use of group signature and dynamic broadcast encryption technologies, each user of the cloud is able to communicate data anonymously with others. A cloud user data integrity check approach was introduced by Yuan et al. [15] that makes use of agent tag update technology and polynomial authentication tags. This method allows for multi-user modification and has other desirable properties, such as resistance to collusive attacks. Ali et al. [16] proposed the SeDaSC method, which uses a single encryption key, for secure data exchange in the cloud. There are a plethora of capabilities available to you with this system, including N distinct kinds of data control, data interchange, and compatibility with both older and newer versions of the system. A new attribute-based data sharing approach was created by Li et al. [17] using cloud computing to assist mobile users with limited resources. The authentication and key agreement method has been the subject of much study; it enables the two parties to secretly calculate the session key over an open channel. No matter how strong the adversary's computer is, Maurer [18] claimed in 1993 that the only way to achieve total cryptographic security is with a mismatch in the received signals. But they neglected to consider the advantage of honest communicators. does the trick to provide total cryptographic protection, regardless of the strength of the enemy's computers. Using patient symptom matching as a basis, Lu and Lin (19) devised a medical key negotiation approach. He et al. [32] noted that Lu's technique is lacking in two key areas: identification monitoring and resistance modification. The team continued by developing an Android app for experimental analysis and proposing a cross-domain handshake approach for usage in medical mobile social networks. He et almethod.'s was shown to be susceptible to a replay attack later on by Liu and Ma [20].

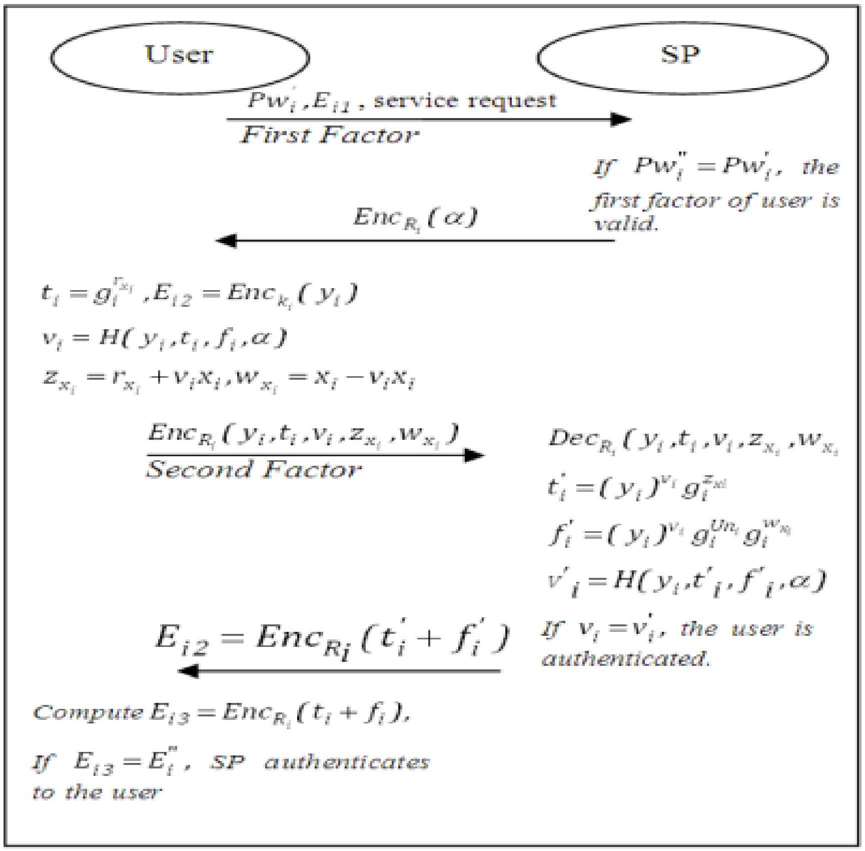
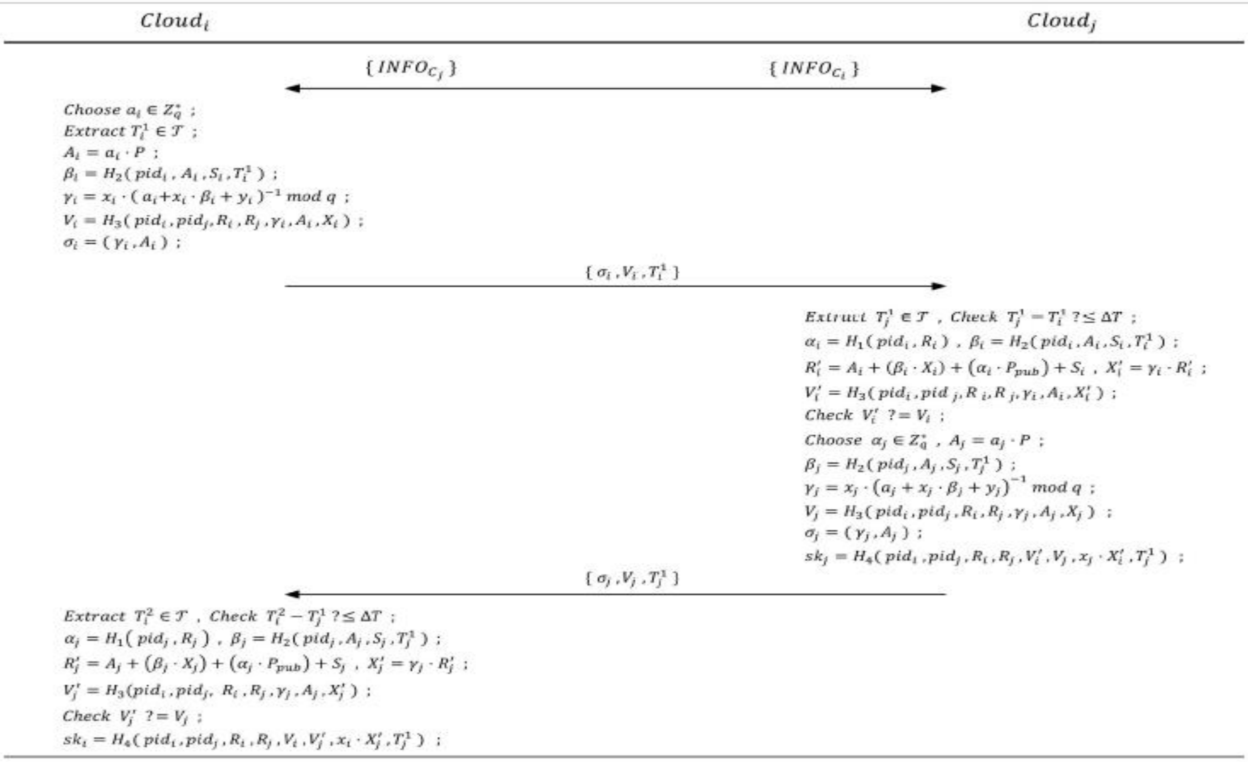

User
SP
Pw_i', E_{i1}, service request
First Factor
If $Pw_i'' = Pw_i'$, the first factor of user is valid.
$Enc_{R_i}(\alpha)$
$t_i = g_i^{r_{x_i}}, E_{i2} = Enc_{k_i}(y_i)$
$v_i = H(y_i, t_i, f_i, \alpha)$
$z_{x_i} = r_{x_i} + v_i x_i, w_{x_i} = x_i - v_i x_i$
$Enc_{R_i}(y_i, t_i, v_i, z_{x_i}, w_{x_i})$
Second Factor
$Dec_{R_i}(y_i, t_i, v_i, z_{x_i}, w_{x_i}$
$t_i' = (y_i)^{v_i} g_i^{z_{xi}}$
$f_i' = (y_i)^{v_i} g_i^{Un_i} g_i^{w_{xi}}$
$v'_i = H(y_i, t'_i, f'_i, \alpha)$
$E_{i2} = Enc_{R_i}(t_i' + f_i')$
If $v_i = v_i'$, the user is authenticated.
Compute $E_{i3} = Enc_{R_i}(t_i + f_i)$,
If $E_{i3} = E_i''$, SP authenticates to the user

Figure 1. Mutual Authentication of our proposed scheme

We take care of the authentication process problem in the cloud service provider configuration. We came up with an innovative technique that uses cryptographic technologies instead of saving a password file on the server. This way, we could avoid the extra devices and expenses that come with traditional identity-of-second-factor methods, such as tokenisation and biometrics.The following best describes our role in this paper:Some major advantages of the proposed approach are as follows: The user and the service provider both have access to the authenticated session keys. Passwords are user-manageable. When a user's authentication keys are lost, the revocation step begins. Some of its features are a low price tag, ease of deployment and management, and straightforward interaction with existing infrastructure. Our research presents a new two-factor authentication setup that combines the power of two cryptographic applications. The first factor is generated by the zero-knowledge factor, and the second factor is examined using the new One-Time Password (OTP) approach. We relieve some of the load on the cloud server by not storing password files there. Additionally, synchronised clocks are unnecessary in our proposed system since we use random numbers instead of timestamps. Our proposed solution is impenetrable against insider attacks, replay attacks, forging attacks, man-in-the-middle seed-tracing attacks, and offline guessing attacks.

4. Implementation


$Cloud_i$
$Cloud_j$
$\{INFO_{C_j}\}$
$\{INFO_{C_i}\}$
$Choose\ a_i \in Z_q^*$;
$Extract\ T_i^1 \in \mathcal{T}$;
$A_i = a_i \cdot P$;
$\beta_i = H_2(pid_i, A_i, S_i, T_i^1)$;
$\gamma_i = x_i \cdot (a_i + x_i \cdot \beta_i + y_i)^{-1} \bmod q$;
$V_i = H_3(pid_i, pid_j, R_i, R_j, \gamma_i, A_i, X_i)$;
$\sigma_i = (\gamma_i, A_i)$;
$\{\sigma_i, V_i, T_i^1\}$
$Extruct\ T_j^1 \in \mathcal{T}$, $Check\ T_j^1 - T_i^1\ ?\leq \Delta T$;
$\alpha_i = H_1(pid_i, R_i)$, $\beta_i = H_2(pid_i, A_i, S_i, T_i^1)$;
$R_i' = A_i + (\beta_i \cdot X_i) + (\alpha_i \cdot P_{pub}) + S_i$, $X_i' = \gamma_i \cdot R_i'$;
$V_i' = H_3(pid_i, pid_j, R_i, R_j, \gamma_i, A_i, X_i')$;
$Check\ V_i'\ ?= V_i$;
$Choose\ \alpha_j \in Z_q^*$, $A_j = a_j \cdot P$;
$\beta_j = H_2(pid_j, A_j, S_j, T_j^1)$;
$\gamma_j = x_j \cdot (a_j + x_j \cdot \beta_j + y_j)^{-1} \bmod q$;
$V_j = H_3(pid_i, pid_j, R_i, R_j, \gamma_j, A_j, X_j)$;
$\sigma_j = (\gamma_j, A_j)$;
$sk_j = H_4(pid_i, pid_j, R_i, R_j, V_i', V_j, x_j \cdot X_i', T_j^1)$;
$\{\sigma_j, V_j, T_j^1\}$
$Extract\ T_i^2 \in \mathcal{T}$, $Check\ T_i^2 - T_j^1\ ?\leq \Delta T$;
$\alpha_j = H_1(pid_j, R_j)$, $\beta_j = H_2(pid_j, A_j, S_j, T_j^1)$;
$R_j' = A_j + (\beta_j \cdot X_j) + (\alpha_j \cdot P_{pub}) + S_j$, $X_j' = \gamma_j \cdot R_j'$;
$V_j' = H_3(pid_i, pid_j, R_i, R_j, \gamma_j, A_j, X_j')$;
$Check\ V_j'\ ?= V_j$;
$sk_i = H_4(pid_i, pid_j, R_i, R_j, V_i, V_j', x_i \cdot X_j', T_j^1)$;

Ensuring that only authorised individuals may access sensitive information is a crucial function of SP. Setup, Registration, and Authentication are the three main parts of the process. User interface (UI) delivers login credentials to data warehouse (DW), which stores them as keys (critical information) for further stages during setup and registration. As part of the registration process, DW provides SP and users with crucial authentication information (public parameters, credentials). Included in the user's credential file is their two-factor authentication information. To encrypt their credential file, the legitimate user uses a key that is derived from their password. In addition, the user may choose to store his encrypted credential file on any other device they like. At the beginning of each session, the user would transmit SP his first factor. Then, when the SP is ready to log in, he uses his key to decrypt his credentials, checks the user's first factor, and then sends the user a challenge value to make sure the SP is legitimate. After the user has finished, SP verifies the second factor by sending it back to the user.

5. Performance Evaluation

Security risk assessments

An attacker may execute a replay attack by capturing the login message of a valid user and transmitting it back to the server. The next time the user logs into the system, an attacker might use this message to impersonate them. For the SP's verification to be safe against replay attacks, it is recommended that all new login requests match the SP's keys exactly. Our work will remain unaffected by the attack unless the clocks are synchronised. Consequently, our method does not use a timestamp but rather a random number generator. That makes it impossible for an adversary to launch a comparable attack.Our technology is robust enough to resist a forgery assault.

Anyone trying to impersonate Ui will be caught red-handed. Using two-factor authentication, your account should remain secure even if an attacker successfully impersonates Ui. An adversary cannot possibly know how to compute the first factor or how to get the second factor. This means that a hacker who attempts to use a forged login message will be met with complete and utter failure.

Full forward secrecy is achievable with our technology. It's a safety measure that stops the setup procedure from exposing agreed-upon secret keys, like Ri's secret key. Our work is completely secure from prying eyes as the secret key needs to be generated just once for the authenticated session Ri. The adversary will never be able to use the secret key Ri to log in, even if he gets his hands on it. Which means this key will be invalid once the user logs out. A single party, Ri, cannot divulge the data pertaining to long-term secret keys (such as secret key I k and user's password Pwi). Consequently, full forward secrecy may be assured using the proposed technique.

To find out how effective and efficient our work is, we conduct a number of tests in this field. Response time grows linearly with the number of users, as seen in Figure 2. Further evidence of the speed of our solution is the fact that each user's average login and authentication time is 0.0385 seconds. You may see a summary of our plan's time commitment in the table.

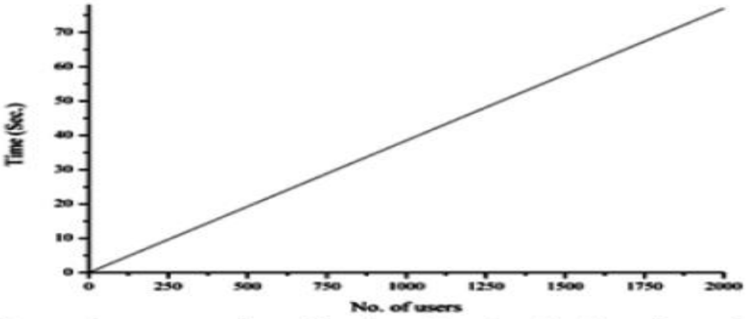
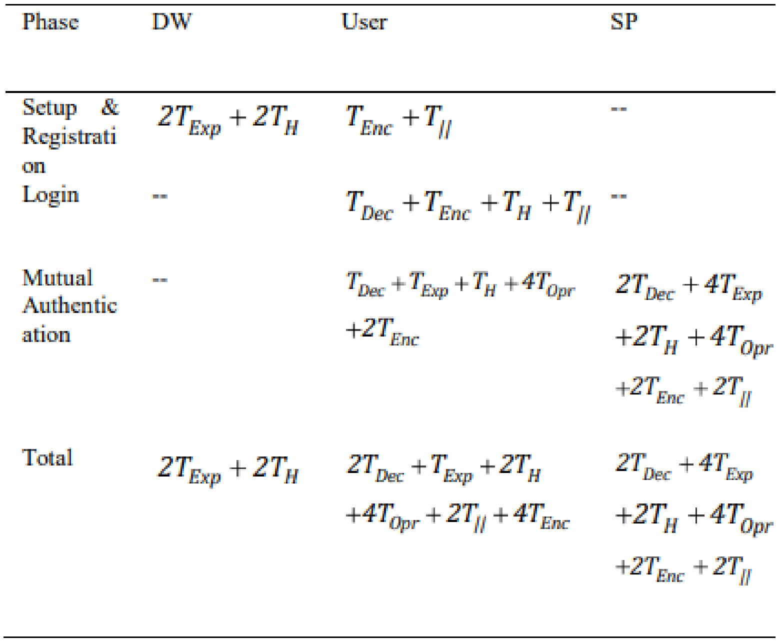


Figure. 3. Average time of login and authenticating phases for our proposed scheme



Phase	DW	User	SP
Setup & Registration	$2T_{Exp}+2T_H$	$T_{Enc}+T_{\|\|}$	--
Login	--	$T_{Dec}+T_{Enc}+T_H+T_{\|\|}$	--
Mutual Authentication	--	$T_{Dec}+T_{Exp}+T_H+4T_{Opr}$ $+2T_{Enc}$	$2T_{Dec}+4T_{Exp}$ $+2T_H+4T_{Opr}$ $+2T_{Enc}+2T_{\|\|}$
Total	$2T_{Exp}+2T_H$	$2T_{Dec}+T_{Exp}+2T_H$ $+4T_{Opr}+2T_{\|\|}+4T_{Enc}$	$2T_{Dec}+4T_{Exp}$ $+2T_H+4T_{Opr}$ $+2T_{Enc}+2T_{\|\|}$

By tracking SP's response time, we were able to gauge how well our effort was working. During our testing, 2,000 users signed in, and we found that each user spent less than two seconds really using the system.

6. Conclusion

We have introduced a cloud-based two-factor authentication system that is both efficient and secure, using a zero-knowledge technique, one-time passwords, and unlinkability. Rather of relying on the service provider to store their passwords, our suggested approach takes use of the fact that customers already save them in the cloud. The service provider has a great opportunity to boost processing speed with this functionality. Additionally, our suggested method is secure against man-in-the-middle (MITM), forgery, replay, offline, and parallel session threats. Freely selected passwords, user privacy, mutual authentication, session key agreement, and the absence of a synchronised clock are just a few of the numerous benefits of our work. Our method outperforms the state-of-the-art in terms of performance, achieving high security at a reduced communion cost.

References:

[1] C. I. network information center, “The 44th china statistical report on internet development,” http://www.cnnic.net.cn/hlwfzyj/hlwxzbg/hlwtjbg/ 201908/P020190830356787490958.pdf, 2019.

[2] B. Li, J. Li, and L. Liu, “Cloudmon: a resource-efficient iaas cloud monitoring system based on networked intrusion detection system virtual appliances,” Concurrency and Computation: Practice and Experience, vol. 27, no. 8, pp. 1861–1885, 2015.

[3] J. Cui, H. Zhou, H. Zhong, and Y. Xu, “Akser: attribute-based keyword search with efficient revocation in cloud computing,” Information Sciences, vol. 423, pp. 343–352, 2018.

[4] J. Cui, H. Zhong, W. Luo, and J. Zhang, “Area-based mobile multicast group key management scheme for secure mobile cooperative sensing,” Science China Information Sciences, vol. 60, no. 9, p. 098104, 2017.

[5] J. Cui, H. Zhou, Y. Xu, and H. Zhong, “Ooabks: Online/offline attributebased encryption for keyword search in mobile cloud,” Information Sciences, vol. 489, pp. 63–77, 2019.

[6] D. Petcu, “Portability and interoperability between clouds: challenges and case study,” in European Conference on a Service-Based Internet. Springer, 2011, pp. 62–74.

[7] T. Binz, F. Leymann, and D. Schumm, “Cmotion: A framework for migration of applications into and between clouds,” in 2011 IEEE International Conference on Service-Oriented Computing and Applications (SOCA). IEEE, 2011, pp. 1–4.

[8] M. N. Shirazi, H. C. Kuan, and H. Dolatabadi, “Design patterns to enable data portability between clouds’ databases,” in 2012 12th International Conference on Computational Science and Its Applications. IEEE, 2012, pp. 117–120.

[9] X. Liang, Z. Cao, H. Lin, and J. Shao, “Attribute based proxy reencryption with delegating capabilities,” in Proceedings of the 4th International Symposium on Information, Computer, and Communications Security, 2009, pp. 276–286.

[10] K. Liang, M. H. Au, J. K. Liu, W. Susilo, D. S. Wong, G. Yang, Y. Yu, and A. Yang, “A secure and efficient ciphertext-policy attributebased proxy re-encryption for cloud data sharing,” Future Generation Computer Systems, vol. 52, pp. 95–108, 2015.

[11] P. Xu, T. Jiao, Q. Wu, W. Wang, and H. Jin, “Conditional identity-based broadcast proxy re-encryption and its application to cloud email,” IEEE Transactions on Computers, vol. 65, no. 1, pp. 66–79, 2015.

[12] M. Sun, C. Ge, L. Fang, and J. Wang, “A proxy broadcast re-encryption for cloud data sharing,” Multimedia Tools and Applications, vol. 77, no. 9, pp. 10 455–10 469, 2018.

[13] G. Chunpeng, Z. Liu, J. Xia, and F. Liming, “Revocable identitybased broadcast proxy re-encryption for data sharing in clouds,” IEEE Transactions on Dependable and Secure Computing, 2019.

[14] X. Liu, Y. Zhang, B. Wang, and J. Yan, “Mona: Secure multi-owner data sharing for dynamic groups in the cloud,” IEEE transactions on parallel and distributed systems, vol. 24, no. 6, pp. 1182–1191, 2012.

[15] J. Yuan and S. Yu, “Efficient public integrity checking for cloud data sharing with multi-user modification,” in IEEE INFOCOM 2014-IEEE Conference on Computer Communications. IEEE, 2014, pp. 2121– 2129.

[16] M. Ali, R. Dhamotharan, E. Khan, S. U. Khan, A. V. Vasilakos, K. Li, and A. Y. Zomaya, “Sedasc: secure data sharing in clouds,” IEEE Systems Journal, vol. 11, no. 2, pp. 395–404, 2015.

[17] J. Li, Y. Zhang, X. Chen, and Y. Xiang, “Secure attribute-based data sharing for resource-limited users in cloud computing,” Computers & Security, vol. 72, pp. 1–12, 2018.

[18] Srinu, Nidamanuri, Sampathi Sivahari, and Mastan Rao Kale. "Leveraging Radial Basis Function Neural Networks for Rainfall Prediction in Andhra Pradesh." *2022 International Conference on Computer, Power and Communications (ICCPC)*. IEEE, 2022.

[19] Muppavarapu, Rajasekhar, and Mastan Rao Kale. "An Effective Live Video Streaming System."