A Secure Two-Factor Authentication Framework in Cloud Computing

Sandeep kaur, Gaganpreet kaur, 1 and Mohammad Shabaz 2

1Department of CSE, SGGSWU, Fatehgarh Sahib, India
2Arba Minch University, Arba Minch, Ethiopia

Correspondence should be addressed to Gaganpreet kaur; gagan1492003@yahoo.com and Mohammad Shabaz; mohammad.shabaz@amu.edu.et

Received 6 January 2022; Revised 8 February 2022; Accepted 11 February 2022; Published 12 March 2022

Academic Editor: Shah Nazir

Cloud computing technology has brought tremendous evaluation in the arena of IT (information technology). This technology paves the path of starting business with lowest investment by availing infrastructure as a service (IAAS), platform as a service (PAAS) and software as a service (SAAS) pay per uses model. Cloud computing services can be quickly and easily provisioned and discharged with minimum efforts and service provider (SP) relationship. Cloud computing characteristics such as on demand self-service, broad network access, resource pooling, and rapid elasticity lead the demand of computing. Despite these features, this platform is free to security issues and attacks specifically in terms of communication because of unsecure authentication and privacy. However, strong user authentication procedure impedes illegal access to the SP which is the principal requirement for securing cloud computing ecosystem. In this regard, we attempt to propose possible counter measures for the cloud ecosystem. Hence, this paper presented a novel one way hash and nonce-based two-factor secure authentication scheme with traditional user IDs, password, and OTP verification procedure that resist brute force attack, session and account hijacking attack, MITM attacks, and replay attacks.

1. Introduction

Cloud computing is a template for smoothening ubiquities, on demand, appropriate network access to shared pool of computing resources that can be quickly supplied and freed with minimum management efforts. There are four main characteristics that can change any platform to cloud computing platform: on-demand self-service; broad network access; resource pooling; and rapid elasticity; meanwhile, ensuring security, confidentiality, and authenticity, as cloud services may be incorporated either internally or by cloud hackers, is highly significant and major issue while using cloud services [1]. Authentication plays a foremost role in retaining security via unique access control procedures and a significant factor on confirming security for diverse applications [2]. In modern days, computing technologies are highly established to pull up the security of high level securities manufactured before a decade. In the current era, approximately 46% of the world’s population has Internet access, so this is very essential to authenticate the cloud users securely. Hence, impersonating the genuine user causes stealing data and frauds. “Password-based authentication, hardware-based authentication, and biometric authentication are the current authentication methods. Password-based authentication is by far the most prevalent authentication method; however, it is prone to difficulties owing to simple and cacheable passwords, as well as the use of the same password across several services, which might also result in a guessing/dictionary attack” [2]. Identifying the most secure authentication technique with high user acceptability is a huge challenge in the cloud environment since there are several threats that can create loop holes in the authentication process. To develop a foolproof authentication method for the cloud environment, an in-depth understanding of attacks on authenticity and the accompanying avoidance techniques is required.
In cloud computing environment, an encryption method is the most commonly used approach for security purpose. Due to privacy and security reasons, the private data of a client have to be transmitted in an encrypted mode. Symmetric and asymmetric cryptosystems are the latest categorized which are based on the key characteristics. In a symmetric cryptosystem, encryption and decryption keys are communicated between the source and destination. The popular symmetric cryptography methods comprise Data Encryption Standard (DES), RC5, Blowfish, 3DES, Two-Fish, RC6, and Advanced Encryption Standard (AES). On the other hand, in asymmetric approach, pair of a public and a private key is used. Here, private key is kept hidden and public key is revealed publicly. The famous asymmetric techniques are Rivest-Shamir-Adleman (RSA) and Elliptic Curve Cryptosystem (ECC) [20].

2. Literature Survey

General authentication techniques such as password-based authentication schemes, nonce-based mutual authentication schemes with smart cards, and time stamp-based authentication schemes are traditional algorithms for accessing services from remote servers that are more effective but cannot be applied to the cloud due to the smart card maintenance complexity. Two-factor authentication method has flaws of offline password guessing as well as smart card stolen attacks [5].

Only authorized users can access the data stored in the cloud, according to the authentication mechanism scheme for Internet banking systems in the cloud with multifactor authentication. Users are authenticated using a combination of factors such as their username, password, random number, and biometric fingerprint. The user's biometric fingerprint is used to encrypt the random number [6]. However, in this process, the encrypted arbitrary number is being sent to the registered phone number over open vulnerable surroundings leading to various attacks. Moreover, validating biometric fingerprint samples, additional computation power is required.

A conceptual basis for the 2FA (two-factor verification) technique mixes password (knowledge-based) and biometric (keystroke dynamic) verification elements [7].

A multifactor authentication (MFA) solution based on the reversed Lagrange polynomial, as an expansion of Shamir's secret sharing feature, addresses the situations of verifying identity even if some of the parts are misaligned or absent. It also assists in the qualifying of missing elements without revealing sensitive information to the validator; hence, when a user loses or keeps forgetting their 2F keys, an assign appropriate is ready to aid with authenticating by sending a private information to the user [17]. To complete the steps of MFA, the proposed solution is devised explicitly, so its management for 2FA and SFA is not acclaimed. Adding a haphazard timestamp factor is not able to provide useful level of biometric data guard, since spy could be able to instantaneously retrieve the factor secret.

Another factor out of band (OOB) authentication provides acceptable security against man-in-middle attack. The scheme [8] used three steps of verification: double encrypted username and password; e-mail and mobile number, one time password (OTP); and last entails the user's involvement on a graphical interface in terms of a predetermined amount of clicks on objects, buttons, and menu item choosing. This solution seems very time consuming and less feasible with cloud computing platform.

"Another Multimodal identification method is presented by combining fingerprint, iris, and palm print features. Each attribute has been subjected to image processing techniques such preprocessing, normalization, and feature extraction. By merging the attributes in two steps, a unique secret key is formed from the retrieved features. The secret key then encrypts the data to be safeguarded using three symmetric key encryption algorithms: DES, AES, and Blowfish. DES requires the least amount of time to execute, while AES outperforms the other two algorithms in terms of encryption procedure strength" [9]. Used authentication components are very expensive and beyond the approach of everyone and seams less feasible on the cloud environment.

Another paper [10] tries to demonstrate design flaws by studying a current hash features authentication strategy for cloud-based IoT devices with a misinterpreted privacy vs performance tradeoff due to an apparent design defect that is
also prevalent in several other similar measures. An access
management protocol method with privacy protection for IIoT
has been presented to allow secure communication for IIoT
[11]. The suggested scheme's security is demonstrated using a
random fountain concept, and further security talks indicate
that the suggested technique is resistant to different assaults.
This paper [12] presents and explicitly verifies the security of an
efficient privacy-preserving user authentication technique in-
cluding forward concealment for Industry 4.0. Among the
most common issues is balancing security and accessibility. To
address this issue, this paper [13] proposed a secure key three-
factor AKA protocol based on enlarged chaotic maps for
portable electronics, using "Fuzzy-Verifiers" and "Honey-
words" approaches. This research [14] proposes a user-centric
three-factor authentication strategy for portable tech that is
aided by a remote server.

Today, huge type of data is being transferred and stored
on a cloud ecosystem in an unencrypted mode. It comp-
ulsorily protects the confidential and stored data, since
unknown vulnerabilities lead to privacy and security con-
cerns. The purpose of this research is to develop an effective
encryption-based security method for sensitive data. Fur-
thermore, the framework provides 2F authentication of clients to the linked cloud system by employing encryption
keys, and the encrypted data can only be accessed once the
user successfully logsins to the system and to evade au-
thentication-related vulnerabilities.

While comparing the work done in this research with [15],
the primary goal of the previous research was to construct an
alternative interverification cryptography for the web based on
current cryptography principles and website technologies. It
consists of seed swap to an operating system token via an
account setup Transport Layer Security (TLS/SSL) tunnel,
encoded internal memory via an encryption key authentication
server (BC UBER) with a powerful decryption activity (PBE-
WithSHAAND Two-Fish-CBC), and asynchronous formation
about one authentications via the TOTP method (IETF RFC
6239), while this work introduces a two-way authentication
framework for cloud computing [16].

2.1. Proposed Secure Multifactor Cloud Authentication
Scheme. Our proposed system is modular in structure,
allowing us to analyze each hazard and its response sepa-
rately. This makes it easier to manage the cloud system and
allows administrators and users to integrate specialized
solutions to combat risks. Cloud system has two types of
entities: cloud server and cloud user. Proposed authenti-
cation procedure involves the following two phases: regis-
tration phase and login phase.

2.2. Registration Phase. This phase further has three steps.
Cloud users register themselves to cloud server to use the
services provided by the cloud server with the following
three main steps (Figure 1):

Step 1. In the first step, cloud user registers with user ID,
e-mail ID, and mobile number; the server validates and
verifies all provided information and sends e-mail and
mobile number OTP to validate the client.

(1) Client: the client sends username, e-mail ID, and
mobile number to the cloud server.

(2) Server: the server stores the received information
and sends e-mail OTP and SMS OTP to the client.

(3) Client: the client stores and receives e-mail OTP
and SMS OTP from the server.

Step 2. In the second step, the client enters the valid
OTPs and receives the key from the server for further
communicating securely to the server and other useful
information like password.

(1) Client: the client enters e-mail OTP and SMS OTP
to the cloud server.

(2) Server: the server verifies the submitted OTP and
generates EC-keypair.

(3) Server: the server sends the generated EC-public
key to the client for secure communication.

(4) Client: the client receives server EC-public key.

Step 3. In the third step, the client chooses password,
type of service, and duration of service and forwards all
information in a secure manner using shared server key
with the following advance security measures:

(1) Client generates and saves secure salted password
using PBDFK2, as shown in Figure 1.

\[
\text{Enc}_{cs, pk} \{H(\text{UserID}) || H(\text{SecureSaltedPassword}) || \text{nonceX} \}
\]

(2) Server: the server received secure password and
subscription details, service and duration.

After that, the server stores all information for user ID
for user identification credential in server database in
secure manner and generates cloud certificate that
consists user ID, subscription, and lifetime, which will
be send back to the user in encrypted format.
Server: the server encrypts subscription certificate using
its private key.
Server: the server again encrypts the encrypted sub-
scription certificate using received client nonce.
Server: then, the server sends successful message and
sends double encrypted subscription certificate to the
client.

\[
\text{Enc}_{\text{nonX}} \{\text{Enc}_{\text{cs, sk}} \{\text{CloudCertificate}}\}
\]

Client: the client decrypts again the certificate with
nonce and server public key.

\[
\text{CloudCertificate} = \text{Dec}_{\text{nonX}} \{\text{Dec}_{\text{cs, pk}} \{\text{EncCC}}\}
\]

Figure 2 shows the new cloud user registration form,
which is the first step of authentication.

2.3. Login and Authentication. The protocol further has the
following two layers or two-factor authentication for veri-
yfying the identity of requesting part.
2.3.1. First Factor Cloud Authentication. During the first phase, the user requests the first factor of authentication. The request is being received and processed by the cloud platform. The cloud platform consists of a database server and a web server. The credentials are authenticated by the database server against already registered records, and upon the authentication, a confirmation is sent back to the cloud server to communicate the authentication successfully back to the user. Here, cloud user provides user ID and password to the cloud server.

\[
\text{EncMsg1} = \text{Enc}_{\text{cs}_\text{pk}} \{ \text{H(UserID)} || \text{H(Password)} \}
\]

(i) Cloud server receives encrypted message (EncMsg1) and first decrypt and then verifies the user for given digital signature.

(ii) If the above step is verified, then cloud server sends OTP to both registered e-mail (OTP1) and mobile (OTP2) and waits for the second step of authentication, as shown in Figure 3.

2.3.2. Second Factor Cloud Authentication. After successful verification of the 1FA, the user is prompted to verify the second factor through an authenticator application. Upon receipt of the request, the cloud server verifies the first factor and sends the confirmation or rejection back to the cloud to process. After successful verification of the 1FA, the cloud sends the request to verify the second factor and sends an OTP request to the user to verify the device. Upon successful authentication, the user is granted access to the cloud. Cloud user goes through multifactor authentication procedure where in the first process, he securely submits traditional credentials like user ID and strong salted password to cloud server to be verified; if verified, then the server asked the user to submit other factor of authentication that is certificate already provided by the cloud server as his identity certificate and OTP on e-mail and mobile.

The following three things are submitted: (1) cloud certificate; (2) E-mail OTP; (3) mobile OTP. (Figure 4)

\[
\text{EncMsg2} = \text{Enc}_{\text{cs}_\text{pk}} \{ \text{H(CloudCertificate)} || \text{H(OTP1)} || \text{H(OTP2)} || \text{nonceY} \}
\]

(i) If all the above three factors are verified, then the user will be authenticated and can use cloud services, as shown in Figure 4, otherwise not.

Figures 5 and 6 show the proposed flow chart for 1FA and 2FA verification.

2.4. Simulations Environment. In this work, we have created our own simulation environment using Java net beans platform. We use the Lenovo laptop X270 as the host which installs Win 10 operation system with Core i5 CPU and 8GB RAM and gives 1 CPU and 1GB RAM to the virtual machine. Password-based encryption module in Java language, using Java Standard Edition compiler with version 1.8.0_121-b13, has been implemented here. So far, we have studied about secure hashes creation for passwords and making it more secure using salt. However, today’s concern is that hardware has become so fast that a bad actor may crack any password in less or more time than a brute force attack utilizing dictionary and rainbow tables. To address this issue, the overall concept is to slow down brute force strikes in order to reduce damage. I am using multilayer protection for secure communication. Hash password is generated by running the password through PBKDF2 to reduce the vulnerabilities of brute force attacks. PBKDF2 with HmacSHA1 makes the hash function slow enough to thwart assaults while yet being fast enough for the user to notice. I have used duly encryption technique Elliptic Curve Cryptography (ECC) and Advanced Encryption Standard (AES) with nonce for secure communication. In this work, processing times for the generating encryption/decryption service have been recorded.

2.5. Security Evaluation of the Proposed Framework. This study explores, identifies, and addresses these attacks while proposing and presenting a highly secure and robust multifactor authentication protocol and framework for cloud computing networks and systems to resist the following attacks.

2.5.1. Account Service and Traffic Hijacking. These threats involve man-in-the-middle attacks (MITM), denial-of-service attacks (DOS), and phishing attacks. Usually, stolen credentials cause the account hijacking attacks [17]. Moreover, the integrity, confidentiality, and availability of the offered services on cloud have been compromised by accessing the sensitive using the stolen credentials by attackers. To circumvent these types of attacks, credentials are being securely stored in encrypted form using salt and nonce in our work.Nonce is random number generated only once. This added uniqueness which makes it impossible for hackers to use prior communication to impersonate the legitimate parties for nefarious purpose.
2.5.2. Brute Force Attack. Today’s fast hardware is able to crack the SHA hashed secure passwords [6]. To make brute force attacks slower, one way hashing function PBKDF2WithHmacSHA1 is being used to slower the brute force attacks and minimize the damage influence in this work. “It gets slower for an attacker to brute force against your live system or a database dump if you iterate through the hashing operation several times. Furthermore, PBKDF2 employs salting; this defends against rainbow table assaults and clients who have made the mistake of reusing their password on several sites.”
2.5.3. Man-in-the-Middle Attack. MITM is cyber eavesdropping through which attackers breach communication between two parties. Our proposed model enables two-factor authentication or 2FA step verification for all external services to circumvent the MITM attack. Moreover, client credentials are tightly secured with double encryption to circumvent the attacks.

2.5.4. Cloud Account Hijacking. To operate this, attackers steal the account information and use it for the unauthorized or malicious activity. Moreover, an attacker uses compromised credentials of accounts such as passwords and e-mail to pretend to be the account owner causing account hijacking. In our proposed model, verification is done by using e-mail and mobile OTPs together while accessing cloud services to circumvent the attack.

2.5.5. Replay Attack. The objective of replay attack is impersonation. To accomplish this attack, an attacker play-acts to be a valid user or server and traps a victim to disclose the authenticating credentials in order to obtain unauthorized access to the cloud services. Moreover, an attacker seizes authentication data in transit and uses it later to achieve access. But a solid user authentication scheme can confine illegal access privileges which origin the replay attack [18]. In our work, the attack is being mitigated by using two-factor authentication in addition to passwords with nonce. Here, arbitrarily generated nonce values are being used and each value is private for all sessions. Moreover, the client responds encrypted concatenated credentials with nonce. As credentials are not in plain text, this approach counteracts the replay attacks.

2.6. RSA versus ECC. ECC is an encryption algorithm method based on the elliptic curves of elliptic curves over finite fields. For elliptic curves, the ECC approach solves the discrete logarithm problem (ECDLP). This encryption process is more difficult to break since there is no known solution to the mathematical problem provided by the equation creating the elliptical curve in a graph. Elliptic Curve Cryptography (ECC) offers equivalent encryption capacity same as Rivest-Shamir-Adleman (RSA) algorithm with a smaller key length. RSA is the most widely used asymmetric cryptographic algorithm in the present era. It is commonly used to encrypt the data on websites, emails,
Table 1: RSA.

| File size (KB) | Key gen time (ms) | Enc time (ms) | Dec time (ms) | Total time (ms) |
|----------------|-------------------|---------------|---------------|-----------------|
| 5  | 3115.2252         | 155.2538      | 1197.2716     | 4467.7526       |
| 10 | 3367.181          | 181.8243      | 2471.0014     | 6020.0067       |
| 15 | 4005.5048         | 203.6311      | 3527.697      | 7736.8329       |
| 20 | 4002.1642         | 235.3458      | 4913.911      | 7151.421        |
| 25 | 4007.6771         | 273.2908      |               | 10304.9454      |

RSA_AVG 7536.19172

Table 2: ECC.

| File size (KB) | Key gen time (ms) | Enc time (ms) | Dec time (ms) | Total time (ms) |
|----------------|-------------------|---------------|---------------|-----------------|
| 5  | 133.9693          | 32.5968       | 0.703899      | 167.269999      |
| 10 | 135.311501        | 32.5092       | 1.0082        | 168.828901      |
| 15 | 134.7082          | 33.2104       | 1.8264        | 169.745         |
| 20 | 137.0426          | 35.0611       | 2.3215        | 174.4252        |
| 25 | 136.3479          | 39.1073       | 4.6762        | 180.1314        |

ECC_AVG 172.0801

Figure 7: RSA total time.

Figure 8: ECC total time.
and applications, among other things. Cryptographers employed the prime factoring approach to accomplish one-way encryption of a communication consequently. The speed and security obtainable by an ECC are superior to RSA and allowing faster execution and a superior user experience. In this work, encryption/decryption time and key generation time of both RSA and ECC have been calculated and the experiment shows that calculated average time shows that ECC takes less time in comparison to RSA and provides better security that ECC is better than RSA, especially on memory-constrained devices and time. Tables 1 and 2 show the comparison of RSA and ECC for different file size. Figures 7 and 8 show their comparison graphically.

3. Result Analysis

A novel approach based on two-factor secure authentication scheme with traditional user IDs, password, and OTP verification procedure that resist brute force attack, session and account hijacking attack, MITM attacks, and replay attacks has been proposed. Two algorithm methods were discussed and compared as per their efficiency. Two methods were Elliptic Curve Cryptography (ECC) and Rivest-Shamir-Adleman (RSA) and their respective graphs were plotted for different file size which clearly illustrates the superiority of prior over latter. All the comparison has been done in tabular form and execution time has been recorded. The speed and security obtainable by an ECC are superior to RSA and allowing faster execution and a superior user experience. Experiment shows that calculated average time shows that ECC takes less time in comparison to RSA and provides better security that ECC is better than RSA, especially on memory-constrained devices and time.

4. Conclusion

Cloud computing has played a vital role in implementing interconnected networks and devices at a wider level while extended its capability to transform homes and organizations into an interconnected and smart environment. At the same time, this has made these environments vulnerable to numerous security and privacy attacks. Hence, the prime prerequisite for securing cloud environment is to use strong user authentication procedures for restricting illegitimate access. Moreover, a user authentication system designed for cloud should be resilient to protect cloud from numerous potential authentication attacks. This study is to manage the authentication system more efficiently and offers a specific solution to the user and administrator to counter the threat. Hence, it provides secure authentication services and prevents sensitive data from potential threats by defining the approach for retaining the security and privacy of the confidential transit and stored data. Ultimately, encrypted form of data on a cloud is becoming significant more and attaining importance. ECC takes less time in comparison to RSA and provides better security, especially on memory-constrained devices and time.

**Data Availability**

The data shall be made available on request.

**Conflicts of Interest**

The authors declare that they have no conflicts of interest.

**References**

[1] K. Latha and T. Sheela, "Block based data security and data distribution on multi cloud environment," *Journal of Ambient Intelligence and Humanized Computing*, 2019.

[2] T. Joseph, S. A. Kalaiselvan, S. U. Aswathy, R. Radhakrishnan, and A. R. Shamna, "A multimodal biometric authentication scheme based on feature fusion for improving security in cloud environment," *Journal of Ambient Intelligence and Humanized Computing*, vol. 12, no. 6, pp. 6141–6149, 2021.

[3] S. Jarecki, H. Krawczyk, and J. Xu, "OPAQUE: an asymmetric PAKE protocol secure against pre-computation attacks," in *Advances in Cryptology – EUROCRYPT 2018*, pp. 456–486, Springer International Publishing, Cham, 2018.

[4] D. Wang and P. Wang, "Two birds with one stone: two-factor authentication with security beyond conventional bound," *IEEE Transactions on Dependable and Secure Computing*, vol. 1, p. 1, 2016.

[5] O. León, J. Hernández-Serrano, and M. Soriano, "Securing cognitive radio networks," *International Journal of Communication Systems*, vol. 23, no. 5, pp. 633–652, 2010.

[6] S. Nagaraju and L. Parthiban, "Trusted framework for online banking in public cloud using multi-factor authentication and privacy protection gateway," *Journal of Cloud Computing*, vol. 4, no. 1, pp. 1–23, 2015.

[7] M. Olalere, M. Taufik Abdullah, R. Mahmud, and A. Abdullah, "Bring your own device: security challenges and A theoretical framework for two-factor Authentication," *International Journal of Computer Networks and Communications Security*, vol. 4, no. 1, pp. 21–32, 2016, http://www.ijcncs.org.

[8] C. Singh and T. D. Singh, "A 3-level multifactor Authentication scheme for cloud computing," *International Journal of Computer Engineering &Technology*, vol. 10, no. 1, pp. 184–195, 2019.

[9] D. Wang, X. Zhang, Z. Zhang, and P. Wang, "Understanding security failures of multi-factor authentication schemes for multi-server environments," *Computers & Security*, vol. 88, Article ID 101619, 2020.

[10] S. A. Chaudhry, A. Irshad, K. Yahya, N. Kumar, M. Alazab, and Y. B. Zikria, "Rotating behind privacy: an improved lightweight authentication scheme for cloud-based IoT environment," *ACM Transactions on Internet Technology*, vol. 21, no. 3, pp. 1–19, 2021.

[11] X. Li, J. Niu, M. Z. A. Bhuiyan, F. Wu, M. Karuppiyah, and S. Kumari, "A robust ECC-based provable secure authentication protocol with privacy preserving for industrial internet of things," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 8, pp. 3599–3609, 2018.

[12] C. Wang, D. Wang, G. Xu, and D. He, "Efficient privacy-preserving user authentication scheme with forward secrecy for industry 4.0," *Science China Information Sciences*, vol. 65, no. 1, 2022.

[13] S. Qiu, D. Wang, G. Xu, and S. Kumari, “Practical and provably secure three-factor authentication protocol based on extended chaotic-maps for mobile lightweight devices,” *IEEE
Transactions on Dependable and Secure Computing, vol. 1, p. 1, 2020.

[14] Q. Jiang, Y. Qian, J. Ma, X. Ma, Q. Cheng, and F. Wei, “User centric three-factor authentication protocol for cloud-assisted wearable devices,” International Journal of Communication Systems, vol. 32, no. 6, p. e3900, Article ID e3900, 2019.

[15] M. L. T. Uymatiao and W. E. S. Yu, “Time-based OTP authentication via secure tunnel (TOAST): a mobile TOTP scheme using TLS seed exchange and encrypted offline keystore,” in Proceedings of the 2014 4th IEEE International Conference on Information Science and Technology, Shenzhen, China, 26 April 2014.

[16] https://howtodoinjava.com/java/java-security/how-to-generate-secure-password-hash-md5-sha-pbkdf2-bcrypt-examples/.

[17] A. Ometov, S. Bezzateev, N. Mäkitalo, S. Andreev, T. Mikkonen, and Y. Koucheryavy, "Multi-factor authentication: a survey," Cryptography, vol. 2, no. 1, pp. 1–31, 2018.

[18] V. Singh and S. K. Pandey, "Revisiting cloud security threats: replay attack," 2018 4th International Conference on Computing Communication and Automation (ICCCA), in Proceedings of the 2018 4th International Conference on Computing Communication and Automation (ICCCA) Greater, pp. 1–6, Noida, India, 14 December 2018.

[19] S. Kaur and G. Kaur, "Threat and vulnerability analysis of cloud platform: a user perspective," in Proceedings of the 15th INDIACom; INDIACom-2021; IEEE Conference ID: 51348 2021 8th International Conference on Computing for Sustainable Global Development, pp. 508–514, New Delhi (INDIA), 17 March 2021.

[20] F. Ahmet, O. Mustacoglu Ferhat, and C. F. Catak Geoffrey, "Password-based encryption approach for securing sensitive data," Security and Privacy, pp. 1–12, 2020.