International Journal of Computer Information Systems and Industrial Management Applications
ISSN 2150-7988 Volume 18(11s) 2026 pp. 379-394
https://doi.org/10.70917/ijcisim-2026-3761
Article

Privacy Persevered Data Access in Cloud Computing Using Multi-Factor Authentication and Encryption Scheme

Rajakumar Ponnumani[1, *], T. Ganesh Kumar[2], N. Partheeban[3]

[1 2]School of Computer Science and Engineering, Galgotias University, Greater Noida, Uttar Pradesh, India.
[3]Department of Computer Science and Engineering, SRM Institute of Science and Technology, Delhi- NCR Campus, Uttar Pradesh, India
[*]Corresponding Email: prajakumarkk@gmail.com

Abstract: In the cloud authentication process authenticate user finds through cloud approaches to regulate whether user is reliable to entrance cloud presentations, properties and data services through confirming access privileges. The absence of appropriate and strong cloud authentication methodologies led to occurrence of certain cloud security attacks and threads. Mutual cloud risks are information revelation and moderating, account capture, Denial-of-Service (DoS) and advancement of rights. Classical authentication models, specifically contain username and passwords pattern, which pattern grow into helpless to cyber-criminals since rises in computing networks and power bandwidths. Furthermore, conventional encryption methodology is introduced to overcome computational overhead and difficulty. However, there is an essential for effective and privacy-preserving information access workflow that combines multi-factor authentication and encryption. Here, proposed model introduces a novel multi-factor authentication for improving security analysis in cloud surroundings. In MFA model contain several authentication process to verify user information, while authentication is successful, then user might access requested information services from cloud. Otherwise, authentication process is fails, user access denied. After getting access from cloud, data holder using Elliptic Curve Enclosed Partial Homomorphic Encryption (ECPHE) model to encrypt information with secret key. Here, data holder contain secret keys used for decrypting data retrieved from cloud environment. In experimental analysis proposed model obtains low encryption time of 25.1(Ms) for 5 (KB), 26.8(Ms) for 10(KB), 27.9(Ms) for 15(KB), 29.4(Ms) for 20(KB) and 30.6(Ms) for 25(KB), and additionally proposed model obtain some metrics that are combined with existing models to proven their effectiveness and robustness analysis.

Keywords: Cloud Environment, authentication, security attacks, Denial-of-Service, multi-factor authentication, Elliptic Curve cryptography, Homomorphic Encryption

1. Introduction

Cloud computing is a service transfer model which make resources available to the users through internet communication. This facilitates users to utilize pooled computational resources including storage, servers and applications without perturbing about maintaining those resources [1]. The key elements of cloud are physical environment for data storage, virtual environment and the services provided to users. Yet, all these elements are affected by security, confidentiality and authenticity issues [2]. In cloud environment, may security issues need to address such as confidentiality, integrity and effective authentication [3] [4] between service providers and users, when it comes to securing the data, authentication plays a crucial role [5]. Hence various authentication frameworks like knowledge-based [6], ownership-based, location-based and characteristic-based authentication [7] have developed to rectify the issues.

Although, password-based methods are widely used for authentication, it still possess some limitations like data overflow, usage of weak passwords and so on [8]. Common authentication techniques namely passwords, biometric possess significant risks in financial and banking sectors. These issues can be effectively mitigated by developing multi-factor authentication (MFA) approaches [9]. MFA system processes more than one authentication credentials

for providing robust authentication to user's data [10]. This authentication offers secure remote access, prevent data against theft and unauthorized access, further it enhances the trust and confidentiality of consumers. Compared with two-factor authentication frameworks and three-factor authentication, MFA possess better performances [11-12]. MFA system uses multiple encryption methods for securing the passwords to make it difficult for hackers. Further it enhance the security of cloud environments and reduce false alarms [13].

Most of the studies utilized conventional encryption algorithms like Data Encryption Standard (DES), Advanced Data Encryption Standard (AES) [14] and Elliptic Curve Cryptography (ECC) [15] algorithms for recommending authentication towards the security keys. However, these algorithms possess computational complexity and high processing power that led to security vulnerabilities. To overcome these kind of security issues various access control mechanisms have developed [16]. Access control mechanisms are commonly used in Machine Learning (ML) [17] and Deep learning (DL) techniques [18]. Further blockchain based techniques also utilize access control mechanisms [19]. MFA enhances the security of the cloud environment along with that, it can be used for securing the data against malicious attacks [20]. These advancements in MFA paves an effective way for developing a robust framework for secure data access. Addressing the limitations and advantages of the current techniques, a novel multi-factor authentication framework in cloud environment is developed in this research for secured data access.

1.1 Motivation and Objectives

Development of cloud computing, securing sensitive data has become a critical challenge. Traditional authentication mechanisms, such as password-based access control, are vulnerable to cyber threats, unauthorized access, and data breaches. Multi-factor authentication enhances security by requiring multiple layers of verification, reducing the risk of unauthorized access. Additionally, encryption techniques ensure that data remains protected even if access controls are compromised. Combining MFA with encryption provides a robust security framework that preserves privacy while enabling secure data access in cloud environments. Despite advancements in cloud security, existing access control mechanisms often fail to provide comprehensive protection against unauthorized access and data breaches. Many authentication schemes rely solely on passwords, which are prone to attacks like phishing, brute force, and credential theft. Moreover, conventional encryption methods may introduce computational overhead and complexity, affecting system performance. Therefore, there is a need for an efficient and privacy-preserving data access framework that integrates multi-factor authentication and encryption. This research aims to develop a secure cloud computing model that ensures authorized data access while maintaining privacy through a combination of Multi Factor Authentication and advanced encryption techniques. In this research main objectives is expressed as follows

- To implement multifactor authentication scheme for secured data access in the cloud environment.
- To introduce Elliptic curve enclosed Partial Homomorphic encryption (ECPHE) for data encryption to enhance the data security.
- To compare the performance of proposed approach with the recently developed approaches for cloud data security.

The remaining of this research articles is structured as follows. In Section 2 presents recent existing studies based on multi-factor authentication system. Section 3 explores proposed authentication process and encryption methodology. Section 4 offering performances evaluation of proposed model and their effective analysis. Section 5 concludes research article with future work.

2. Literature study

This section illustrates some of the recent existing studies based on multi-factor authentication system.

Midha et al. [21] developed a multi-factor authentication framework for securing the patients data in a cloud based software defined networks (SDN) environment. This study utilized a hash function for multi-factor authentication along with registration phase and login phase. The security analysis of the developed protocol is validated on AVISPA tool. This developed framework was validated on data confidentiality, mutual authentication, user anonymity, key freshness, data integrity, and computational cost and so on. Although this method provide confidentiality, it still needs improvements on various encryption and access policy systems for securing the data.

To mitigate the additional hardware requirement in authentication framework, Carrillo-Torres et al. [22] developed a MFA framework based on non-biometric mechanisms for image recognition. Further a functional prototype mechanism were developed for mobile applications. This method offers a relation between the two input

images for providing authenticity. The experiments were conducted on the basis of validating accuracy, authenticity, security and usability. Although it attained better accuracy of recognition, but failed to provide better authenticity.

To overcome the flaws of multiple smart card maintenance and password memorization, Shukla et al. [23] developed a secure multi-factor ECC authentication framework in cloud server. This study offer higher authentication protocol than two factor authorization and also mitigate the issues of user impersonation, denial of service and lack of security functionalities. This research possess system initialization, registration phase, login phase, password update phase and re-registration phase. To overcome the security loopholes, a novel ECC based authentication protocol were developed and a Scyther security verification tool were used to validate the correctness of the developed protocol. The performance of this approach is validated in terms of computational overhead and communication overhead, which appears to be high.

To develop a secure authentication framework, Sharphathy et al. [24] recommended a novel enhanced multi-factor authentication framework which improve the security in cloud environment. This research initiates with generating user credentials like username, password, email and mobile number. These details are encrypted with MAC and IP address. Then validate the user credentials to access the cloud system. The developed research is validated with existing algorithms computational time, accuracy and file size. This research enhanced the authentication features but failed to possess location based patterns for MFA.

To overcome the flaws of computation overhead and sensitivity issues, Chen et al. [25] demonstrated MFA scheme for cloud assisted internet of medical things. To enhance the security in cloud environment, this research developed a novel privacy preserving technique with post-quantum security. This study utilized hash functions and error reconciliation method for providing flexible authentication. The process begins with initialization, registration, and authentication and user generation for providing authenticated framework. The performance evaluation considers computational cost, communication cost and functionality features. Although, this method provide better performances, it still needs advanced encryption framework for secure data access in cloud. Table 1 illustrates the existing study analysis.

Table 1: Prior research analysis

Author & References	Approach used	Performance	Limitations
Midha et al. [21]	MFA for cloud based SDN	Provide better data confidentiality	Advanced encryption and access control algorithms may use
Carrillo-Torres et al. [22]	MFA based non-biometrics	Mitigate hardware requirements and provide better accuracy	Less authenticity of data
Shukla et al. [23]	MFA-ECC	Provides better authentication	High communication and computational overhead
Sharphathy et al. [24]	Enhanced MFA	Improves authentication	Better MFA based factors may use
Chen et al. [25]	MFA	Improved sensitivity and security	Advanced encryption techniques may use

2.1 Problem Statement

In this rapid development of communication methodology, authentication is process utilized to establish connection among two individuals. Here, connection depend on reliable and certainty that elaborate events is definitely authentic ones in forging association. In widespread process of authentication revolves around utilization of passwords that are utilized across range of services including websites, and multiple applications. But, passwords might be prone to cracking by simpler model might be directed without essential for widespread calculations. In this research analysis, analysis some previous methodology, advantages and disadvantages that discussed Advanced encryption and access control algorithms may use required [16], Less authenticity of data [17], High communication and computational overhead [18], Better MFA based factors may use [19] and Advanced encryption techniques is essential [20]. To overcome this limitations, proposed work introduces a novel MFA and encryption model to privacy-preserving cloud application that improve security analysis and provide effective performances.

3. Proposed methodology

In order to enhance the security of the user data in the cloud, number of access policies were introduced in the recent but each polices have a lack in security. In this paper, we introduce a multi-factor authentication scheme to

enhance privacy preservation. Initially, the client gives the request for the cloud server to access the data. Here, user verification will be carried out by using multiple authentication namely Password verification, one time token authentication, Conditional attributes analyses and also role based attribute access control verification. When any one of the verification is failed, the user can't access the data. During the password verification the system verifies the user's password. In one-time token authentication, a temporary code is sent via email with a time constraint. Figure 1 illuminates an overall proposed model architecture.

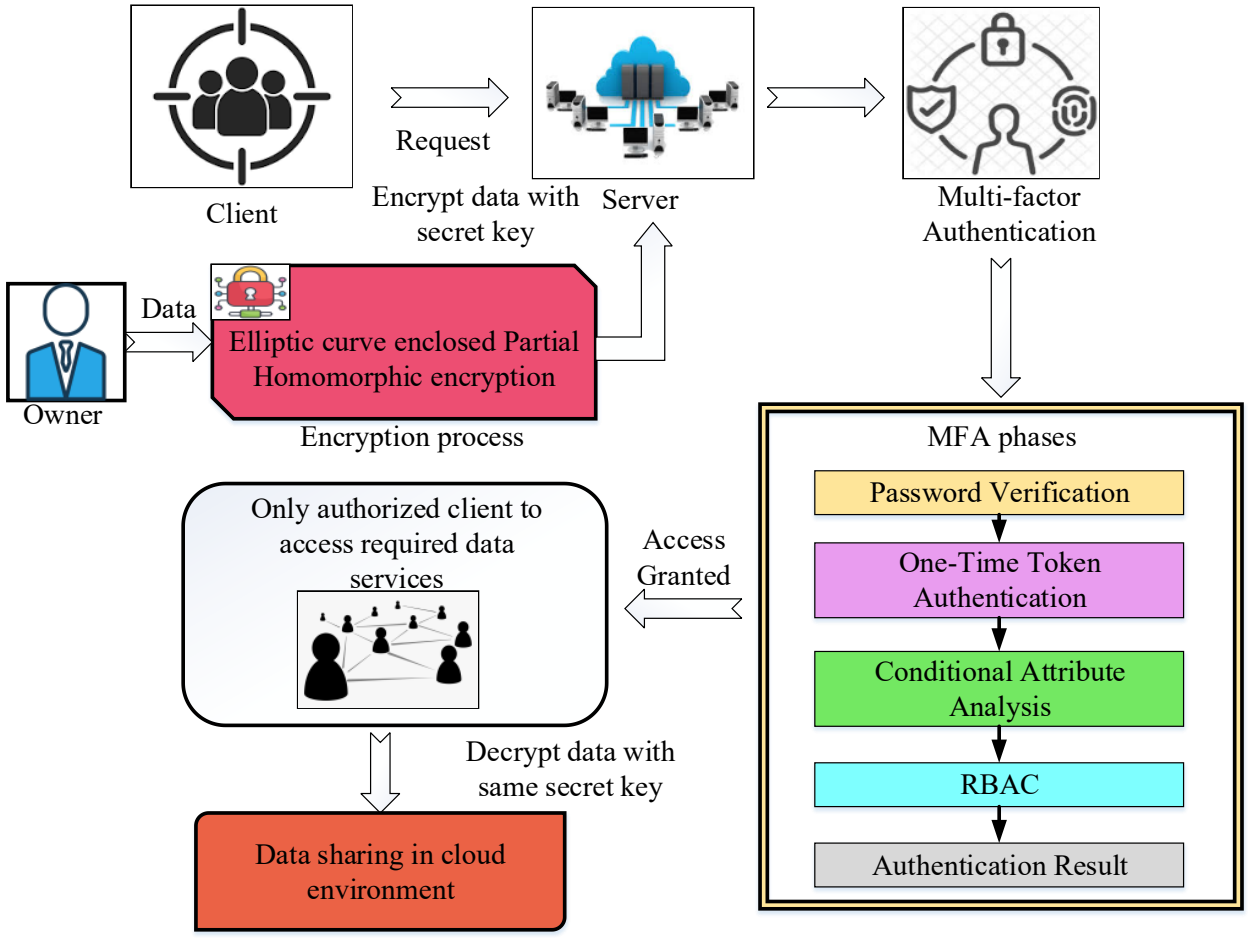

Figure 1: An overall proposed model architecture.

Then, the conditional Attribute Analysis will initiated which checks device, location and access level. The final stage of multifactor authentication is Role-Based Access Control (RBAC) check. Here, the user access is restricted based on predefined roles and permissions. Once the authentication is completed,

1. If authentication is successful, the user is granted access to the requested data services.

2. If authentication fails, access is denied.

At first, the data owner will encrypt the data by using the Elliptic curve enclosed Partial Homomorphic encryption (ECPHE). The user need to decrypt the data by using the keys generated by data owner. After decrypting the data, the user can retrieve and share those data files present in the cloud

3.1 Multiple Authentication Factor

Phase 1: User Authentication

In this multiple authentication factor includes Registration Center, server and user, which express in the following process:

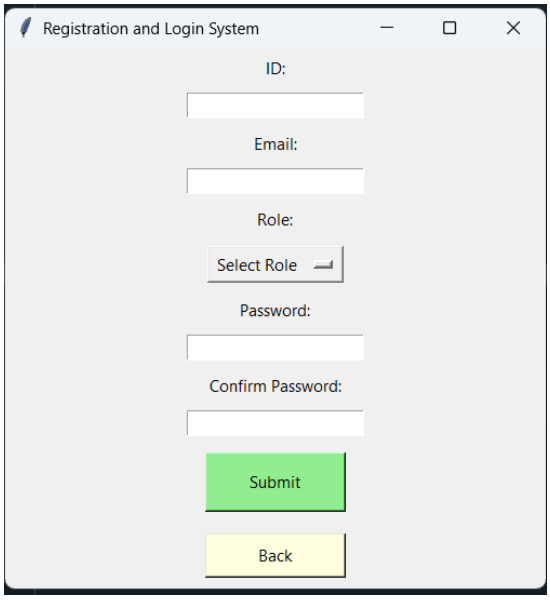

Figure 2: Registration process

Registration Center: Registration Center is only highly secure and trusted entity that is accountable for system initialization, user and service provider onboarding allocating related top-secret data upon process. Registration process is expressed as following figure 2.

Server: Cloud server is accountable for data storage, handling, calculation and managing of user services appeal in management system. Earlier offering services, cloud server essential register through; upon effective registering and this process might be utilize authentication data to verify user and attain session key for protected statement. Figure 3 illuminates cloud computing.

Figure 3: Cloud Server

Owner: Organization owner contains full authority for accessing cloud platform. Figure 4 shows owner login page.

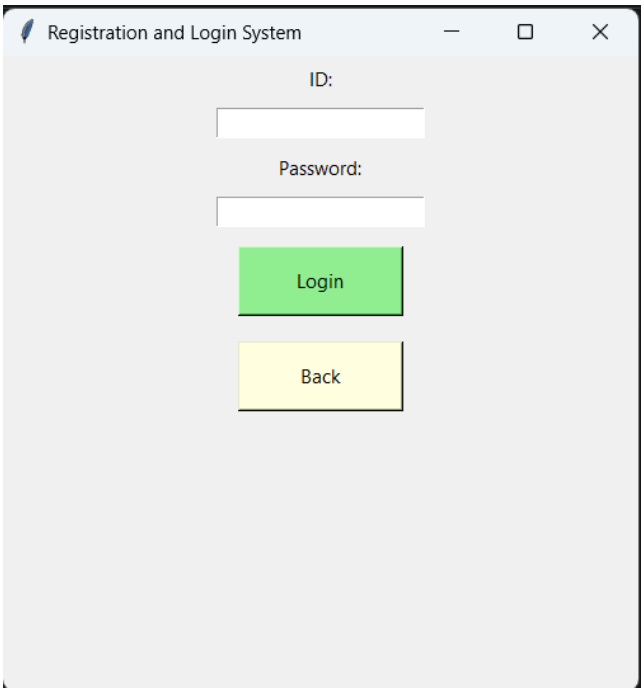

Figure 4: Owner login page.

User: Users is essential to safeguard their information, then primary users of management system consuming particular interaction rights based on their roles. might be register throughformerly originating communication through. Then produce top-secret information based on user-provided data for following authentication that safeguarding communication among and. Here, multi-factor authentication process [26] step is described as follows

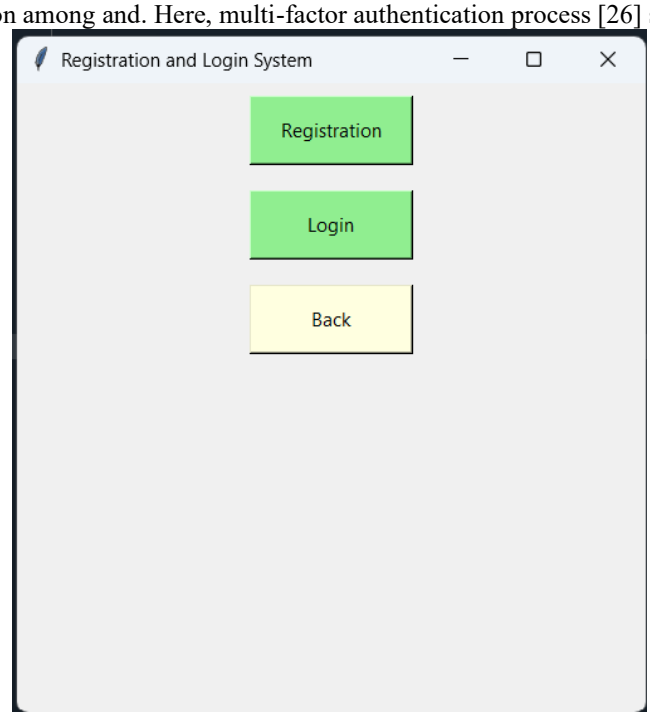

Figure 5: User login page.

Step 1: User Request:

send request to access organization information from. Hereprocess requires user identityand passwordto verify user authentication. Figure 5 represents user login page.

Step 2: Password Verification:

Here, input is andthat verifies if password verification =is matched, then system validates user submitted password compared to strongly recorded hashed values. If password verification fails, request have been terminated. Figure 6 illuminates Password verification process

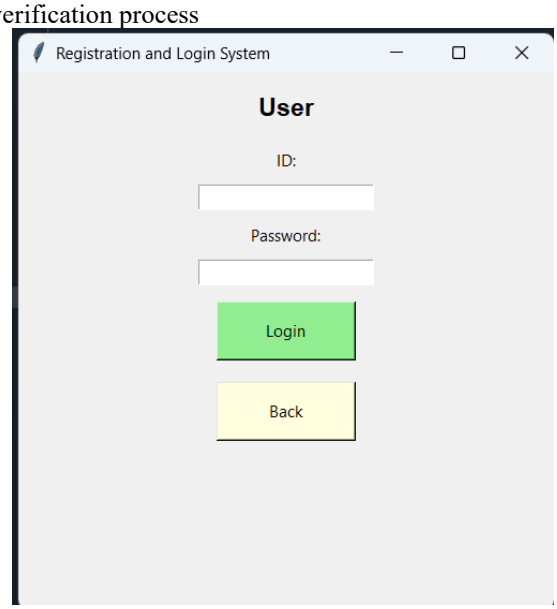

Figure 6: Password verification process

Step 3: One-time token authentication:

In this process one-time token authentication process create, which is unique and based on time-sensitive token that is generated and sent to user's registered email address. If essentially enter token within valid time period then only it is validated. If fails to enter within valid time, then access terminated. Figure 7 shows one-time token authentication process.

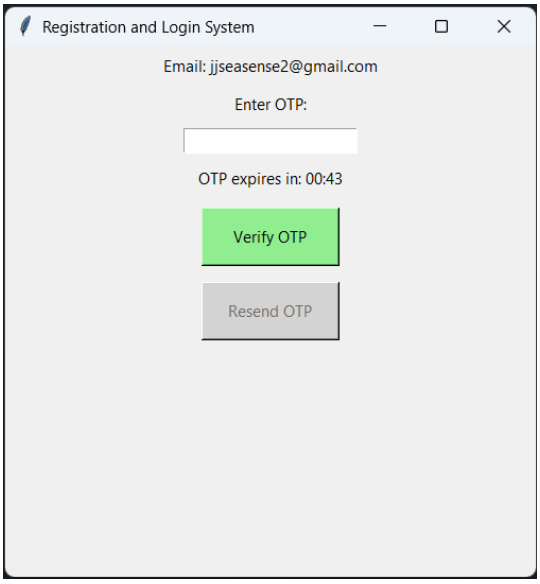

Figure 7: One-time token authentication process

Step 4: Conditional Attribute Analysis

After enter, process check users conditional attribute analysis like Device biometrics, user location and Access time (relate with permitted contact windows), this are match with information, then only access permitted to check another verification. If conditional attributes is unmatched to recorded information, then access is terminated. Conditional Attribute Analysis process is shows in figure 8.

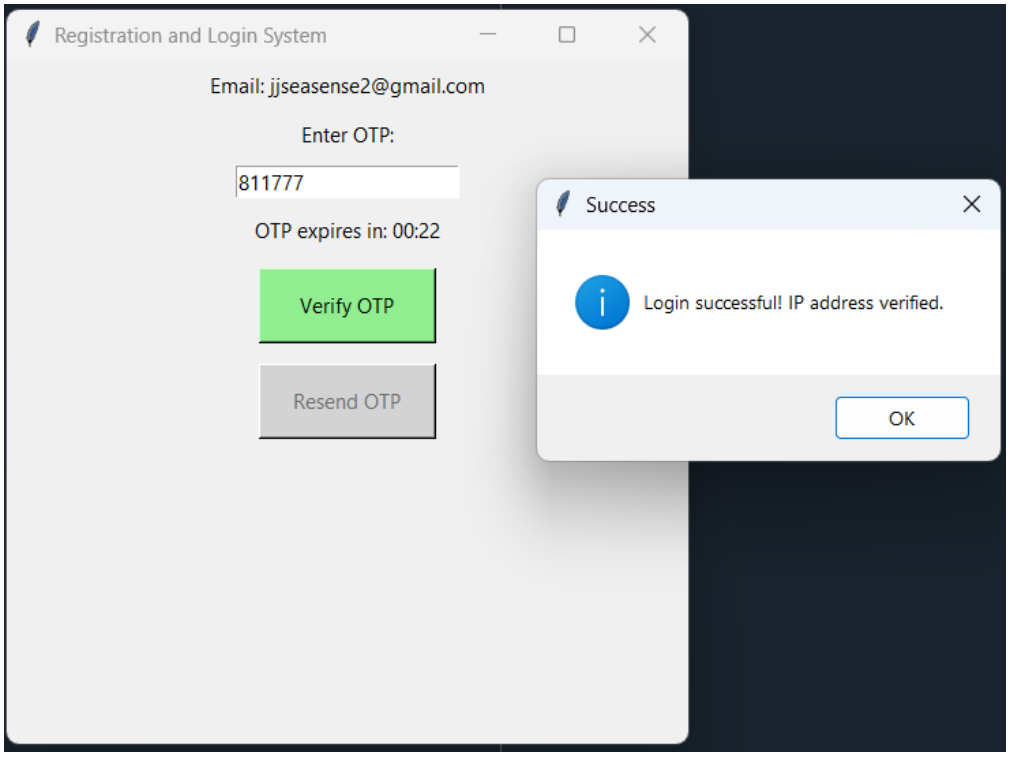

Figure 8: Conditional Attribute Analysis

Figure 8: Conditional Attribute Analysis

Step 5: RBAC

Here, process verifies user assigned position in organization that have permission to access only requested information service only. If position match with their organization assigned position, then access may permitted. If position unmatched with organization position, then access could be terminated.

Step 6: Authentication result

Finally, if all verification steps is successfully verified, then process allow to access information relevant to their organizational position. Otherwise, if step is unmatched with details then user is denied to access information.

3.2 Elliptic curve enclosed Partial Homomorphic encryption

Phase 2: Data Encryption and Access

In this process, a hybrid encryption model named as Elliptic curve enclosed Partial Homomorphic encryption that is utilized to encrypt information previously uploading to cloud.

Step 7: Data encryption by Owner

Here, ElGamal and Rivest, Shamir, Adleman (RSA) cryptosystem is protected symmetric-key cryptosystems, but their enormous keys compromise their privacy analysis. Elliptic curve [27] is collection of solutions from equation (1).

$$Z^2 = bij + b3j = i^3 + b2i^2 + 4bi + 6b \tag{1}$$

Here, co-efficient ofdenotes as elements of region and there might be values ofand to resolve equation throughandin field. This process is potential to create collection out of group of points on elliptic curve, but crucial curve point approaches through things specified in mentioned properties. Homomorphic encryption [28] is dominant cryptography methodology that ensuring particular computations to be achieved straight on ciphertext though enabling that approaches achieved on encrypted information produce identical outcomes to those attained on plaintext. Data encryption by Owner process is expressed in figure 9.

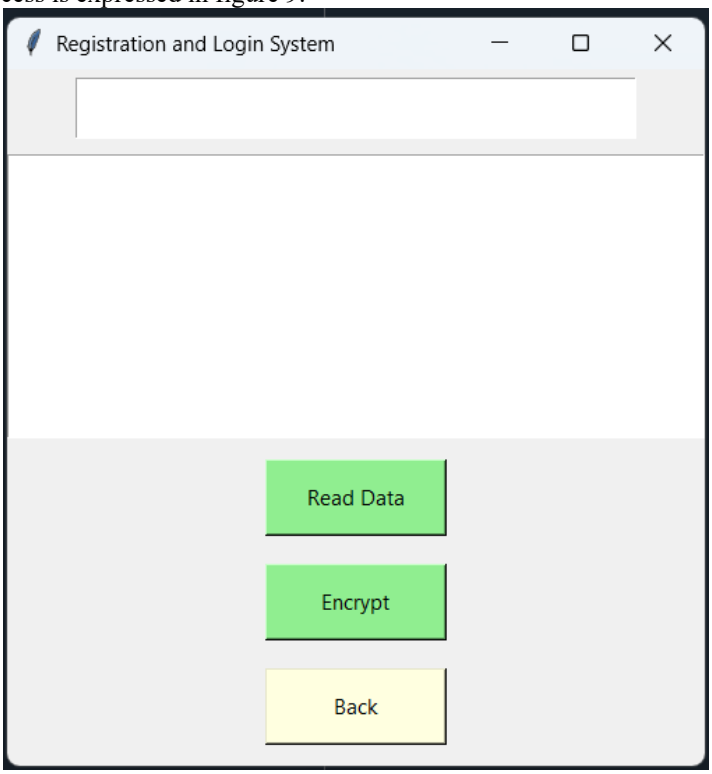

Figure 9: Data encryption by Owner

This process subsidises to data reliability security by permitting others to operate encrypted version of data while no one might be comprehend or access decrypted values. This methodology protect user privacy analysis and enables immediate access to encrypted information. So this process permits private queries to search engine that obtain encrypted information searches and improving efficiency of secure multiparty computation. Here, Homomorphic encryption process includes four main principles such as

1. KeyGen Function: This algorithm that obtain security parameter (SP) to produce both of secret keyand public key, KeyGen (SP).

2. Encryptionapproaches: This process is random algorithm which generate ciphertextwhich comes from plaintext,.

3. Decryptionapproaches: This process is random algorithm which generate plaintextthat comes from ciphertext and. This model effectively encrypt user data with secret key and this encrypt data is uploaded in cloud application.

4. Additive Homomorphic Encryption: Homomorphic encryption is additive if

(2)

whererepresent as encryption approaches and, denotes as plaintexts.

Step 8: Key Distribution

After successful, key management service and information owner securely sharewith authenticated.

Step 9: Data decryption and retrieval

Then, authenticatedonly have secret key which is utilized toinformation that are retrieved from cloud application. Here, retrieved information might withthat are viewed, stored or strongly shared depending on access privileges. Decryption process illuminated in figure 10.

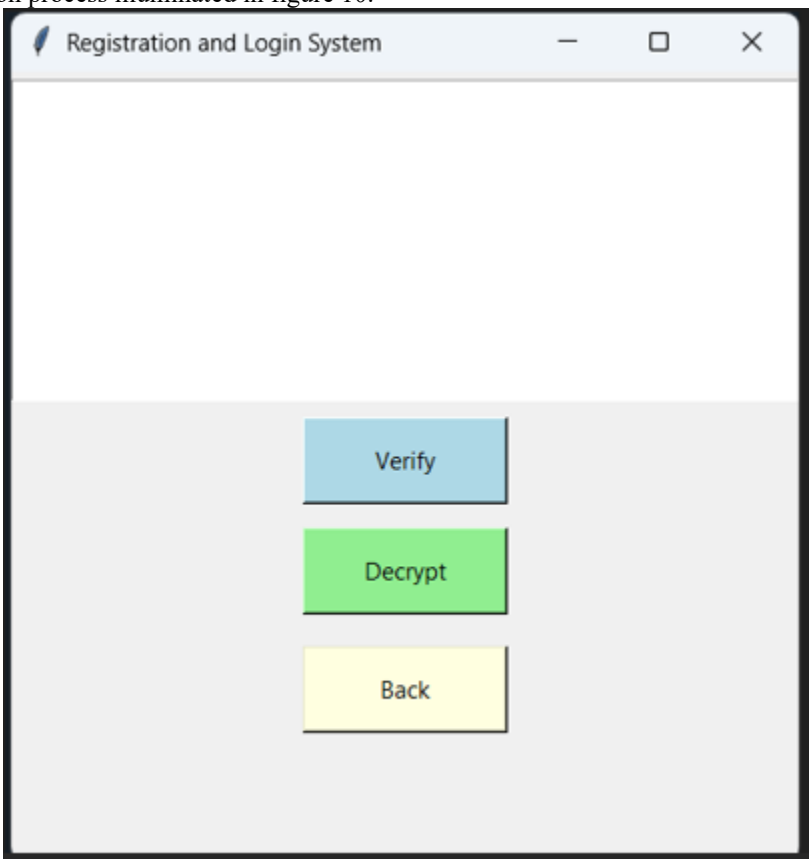

Figure 10: Decryption process

Step 10: Secure Logging and Monitoring

Final step in MFA access that send authentication message and this process conducted to enable only access role based information and additionally this process monitored for anomaly detection. To check factor length, while user provide authentication factor with length which includes 10 different characteristics in MFA process. Otherwise authentication factor is unmatched with relevant factor, then user access is denied. Confirm factor is valid or invalid, here user-authentication factor have valid time period, so user can't utilize pass on factor though logging in cloud. Associating factor value is entered through enter factor is correct and that its length is matched with earlier saved in server.

4. Simulation analysis

In this section, to calculate effectiveness of proposed methodology that contain entrance characters, multi-level authentication through collaboration, similarly authentication process and encryption process which provides security concerns to organization information, respectively. Experimental setup analysis is expressed in table 2.

Table 2: Experimental Setup

Experimental Setup	Configurations
Processor	Intel ® Core ™ i5-4670S

Experimental Setup	Configurations
RAM	16.0 GB
System type	64-bit operating system, x64-based processor
Pen and touch	No pen or touch input is available for this display
Implementation tool	Python

4.1 Expected outcomes

In this section, to evaluate performances of the proposed model by using some performance metrics such as Encryption time, decryption time, computational cost, key generation time and total execution time that are compared with different states of art models in order to prove the efficiency of the proposed methodology.

4.2 Performance Evaluation

In this section, proposed model is expresses in graphical representation that is compared with existing models namely AES [14], ECC [27], RSA [30], and Embedded Probabilistic Polynomial Time Algorithm (ePPTA) [29], respectively.

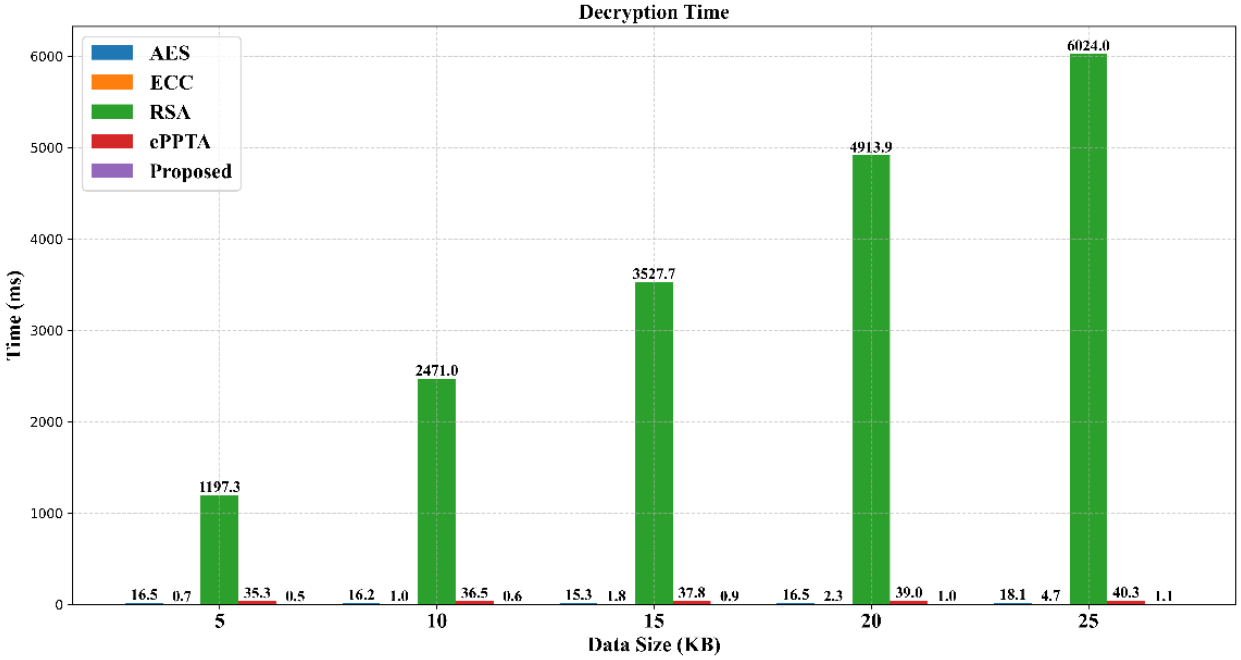

Figure 11: shows encryption time analysis. In this proposed ECPHE model including elliptic curves over finite areas. This process offering equivalent security analysis to DSA or RSA through minor key sizes. Here, varying data size to evaluate proposed model encryption time that obtains 25.1(Ms) for 5 (KB), 26.8(Ms) for 10(KB), 27.9(Ms) for 15(KB), 29.4(Ms) for 20(KB) and 30.6(Ms) for 25(KB), while value are lower than existing models and show effective performances analysis.

Figure 11 shows encryption time analysis. In this proposed ECPHE model including elliptic curves over finite areas. This process offering equivalent security analysis to DSA or RSA through minor key sizes. Here, varying data size to evaluate proposed model encryption time that obtains 25.1(Ms) for 5 (KB), 26.8(Ms) for 10(KB), 27.9(Ms) for 15(KB), 29.4(Ms) for 20(KB) and 30.6(Ms) for 25(KB), while value are lower than existing models and show effective performances analysis.

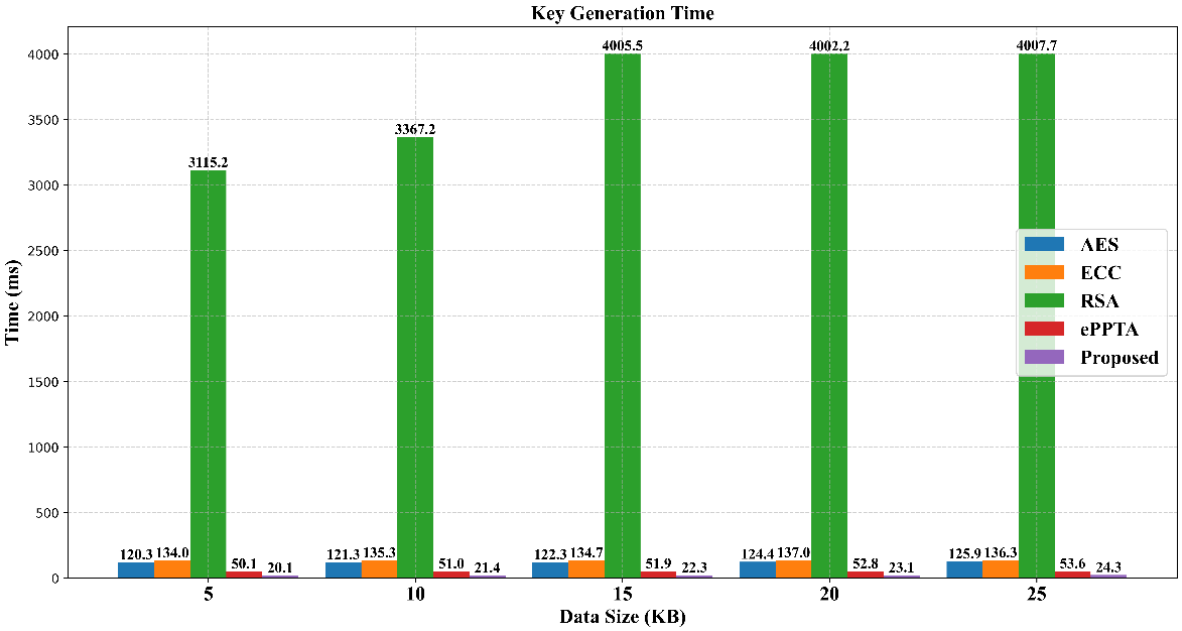

Figure 12: presents Decryption time analysis. Here, proposed model include Homomorphic encryption process using additive Homomorphic process to encrypt user data that enhance security analysis and effectiveness. Here, proposed model achieve low decryption time of 0.5(Ms) for 5 (KB), 0.6 (Ms) for 10 (KB), 0.9 (Ms) for 15 (KB), 1.0 (Ms) for 20 (KB) and 1.1 (Ms) for 25 (KB), this proposed model value is lower than existing models.

Figure 12 presents Decryption time analysis. Here, proposed model include Homomorphic encryption process using additive Homomorphic process to encrypt user data that enhance security analysis and effectiveness. Here, proposed model achieve low decryption time of 0.5(Ms) for 5 (KB), 0.6 (Ms) for 10 (KB), 0.9 (Ms) for 15 (KB), 1.0 (Ms) for 20 (KB) and 1.1 (Ms) for 25 (KB), this proposed model value is lower than existing models.

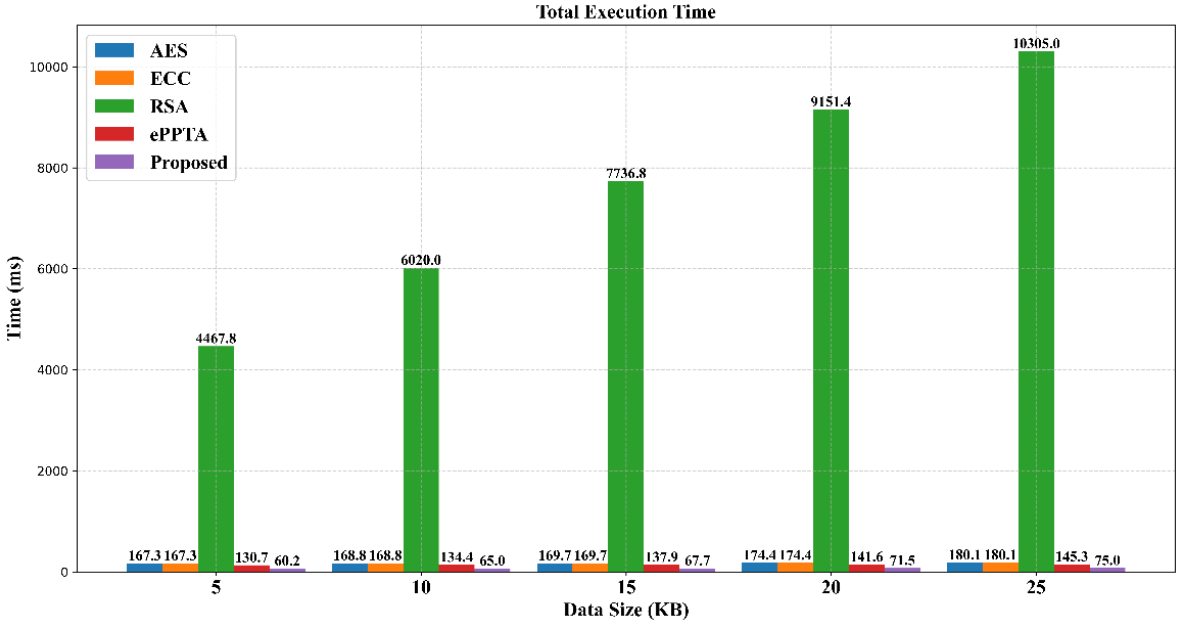

Figure 13: explores Key generation time analysis. Here, hybrid proposed ECPHE model using additive Homomorphic function to provide small secret key, which is utilized for encrypting user data before uploading cloud process. The proposed model obtain low key generation time of 20.1 (Ms) for 5 (KB), 21.4 (Ms) for 10 (KB), 22.3 (Ms) for 15 (KB), 23.1 (Ms) for 20 (KB) and 24.3 (Ms) for 25 (KB), while this proposed model performances obtain effective time analysis than other models.

Figure 13 explores Key generation time analysis. Here, hybrid proposed ECPHE model using additive Homomorphic function to provide small secret key, which is utilized for encrypting user data before uploading cloud process. The proposed model obtain low key generation time of 20.1 (Ms) for 5 (KB), 21.4 (Ms) for 10 (KB), 22.3 (Ms) for 15 (KB), 23.1 (Ms) for 20 (KB) and 24.3 (Ms) for 25 (KB), while this proposed model performances obtain effective time analysis than other models.

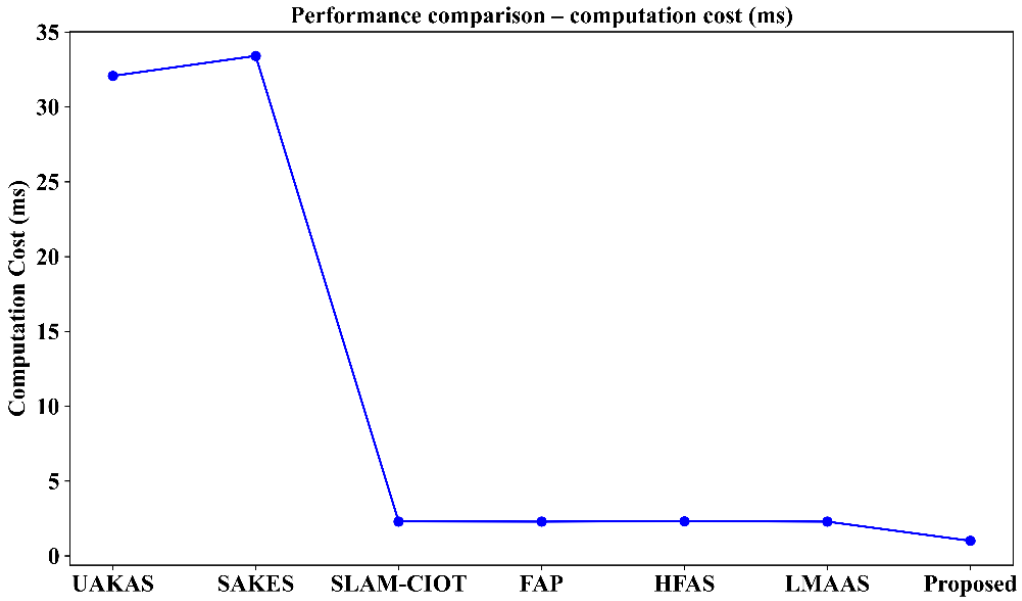

Figure 14: expresses execution time analysis. The proposed model using MFA model to process user authentication, in this process if any user access terminated then user cant access cloud services. Then proposed model achieve execution time of 60.2 (Ms) for 5 (KB), 65.0 (Ms) for 10 (KB), 67.7 (Ms) for 15 (KB), 71.5 (Ms) for 20 (KB) and 75.0 (Ms) for 25 (KB), respectively.

Figure 14 expresses execution time analysis. The proposed model using MFA model to process user authentication, in this process if any user access terminated then user cant access cloud services. Then proposed model achieve execution time of 60.2 (Ms) for 5 (KB), 65.0 (Ms) for 10 (KB), 67.7 (Ms) for 15 (KB), 71.5 (Ms) for 20 (KB) and 75.0 (Ms) for 25 (KB), respectively.

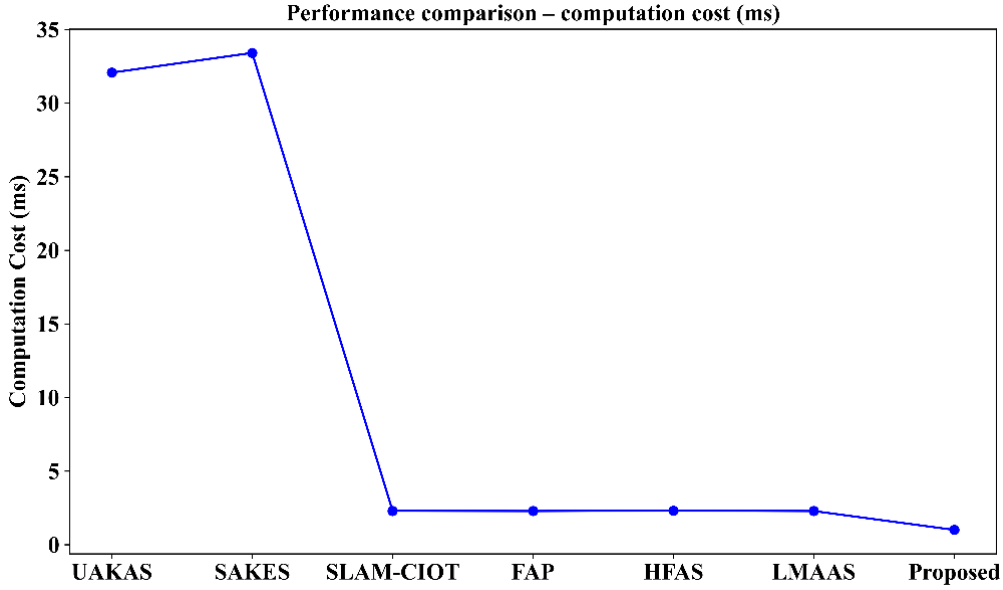

Figure 15: Computational cost analysis

Figure 15 demonstrates computational cost analysis. In this proposed model using MFA model to improve security analysis on cloud application and authenticate user only access cloud data while user have secret key to decrypt their retrieval information. In proposed model obtain low computational cost of 1.017 (Ms) which is compare with existing models [21] to show their effectiveness and robustness analysis.

5. Discussion

Cloud platform is one of the ideal platform which utilize internet source to deliver essential information services to users. Once employed in cloud, which is protective users information and preserving ones security is significance concerns that essential be addressed. In cloud authentication process play significance phase in process of authenticating identity of user information and protecting from unauthorized access to cloud sources. User verification and access mechanism is one of the important challenging limitation to address in cloud platform, however it also supreme crucial security apprehensions. In previous years, researchers suggested certain methodology named as MFA for cloud based SDN model [21] provide better data confidentiality, but this model facing limitations advanced encryption and access control might be required to improve reliability. In [22] MFA based non-biometrics offering mitigate hardware requirements and better accuracy, while this model have less authenticity of user data. In [23] MFA-ECC delivered better authentication, while it have high communication and computational overhead. In [24] enhanced MFA provides enhanced authentications, while this model provide low MFA factors. In [25] MFA model offering increased sensitivity and security analysis, while advanced encryption methodology might be required.

To overcome this limitations, the proposed model introduces MFA and encryption process for improving privacy preserving analysis. In this MFA model includes several authentication process namely user verification, password verification, one time token authentication, conditional attributes and last RBAC authentication. In this proposed model, RBAC model utilize for permitting based on predefined roles and permission, like owner can access all cloud information, finance department can access only finance sector information, IT department can access only IT sector information and HR department can only access HR relevant information, otherwise RBAC authentication denied any one of the verification, then user can't access any information from cloud platform. Here, authentication process is successful, user granted access to requested cloud services. Initially, data owner can upload their information by using ECPHE model, which used to encrypt information with secret keys. After getting access from cloud, user essentially required secret keys to decrypt information that is generated by data owner. Here, decrypted data might be retrieved that might share with organization or management. This proposed MFA process includes multiple authentication process with encryption model improve privacy-preserving and effective performances analysis.

6. Conclusion

In this research analysis, introduces a novel MFA with hybrid encryption model to improve privacy preserving in cloud platform. In this MFA module contain multiple authentication process like password verification, one-time token authentication, conditional attributes and final RBAC authentication, while process improving security analysis, scalability, and low computational cost and only authenticated user are access cloud platform. Primary, organization owner using ECPHE model to encrypt data with secret keys and then uploading encrypted data in the cloud approaches. After user getting access from server, user contain secret key to decrypt data from registered services. Now, user can access decrypting data which is retrieved from cloud services and share with management. In experimental analysis, proposed model achieve low encryption time 25.1(Ms) for 5 (KB), 26.8(Ms) for 10(KB), 27.9(Ms) for 15(KB), 29.4(Ms) for 20(KB) and 30.6(Ms) for 25(KB) and decryption time 0.5(Ms) for 5 (KB), 0.6 (Ms) for 10 (KB), 0.9 (Ms) for 15 (KB), 1.0 (Ms) for 20 (KB) and 1.1 (Ms) for 25 (KB) and computational cost 1.017 (Ms), respectively. This proposed model provides effective security analysis, scalability and flexibility analysis. In future, the proposed approach is further enhanced by quantum resistance based algorithm to mitigate the quantum attacks.

Reference

1. Alzoubi, Yehia Ibrahim, Alok Mishra, and Ahmet Ercan Topcu. "Research trends in deep learning and machine learning for cloud computing security." Artificial Intelligence Review 57, no. 5 (2024): 132.
2. Abdullayeva, Fargana. "Cyber resilience and cyber security issues of intelligent cloud computing systems." Results in Control and Optimization 12 (2023): 100268.
3. Jegadeesan, Subramani, Mohammad S. Obaidat, Pandi Vijayakumar, Maria Azees, and Marimuthu Karuppiah. "Efficient privacy-preserving anonymous authentication scheme for human predictive online education system." Cluster Computing 25, no. 4 (2022): 2557-2571.

4. Zhou, Yousheng, Yang Luo, Mohammad S. Obaidat, Pandi Vijayakumar, and Xiaojun Wang. "PAMI-anonymous password authentication protocol for medical internet of things." In 2021 IEEE Global Communications Conference (GLOBECOM), pp. 1-6. IEEE, 2021.
5. Vijayakumar, Pandi, Maria Azees, Sergei A. Kozlov, and Joel JPC Rodrigues. "An anonymous batch authentication and key exchange protocols for 6G enabled VANETs." IEEE Transactions on Intelligent Transportation Systems 23, no. 2 (2021): 1630-1638.
6. Mohammed, J. "Protecting Cloud Service Providers Based on an Efficient Password-based Authentication System." Int J Comput Digit Syst 16, no. 1 (2024): 1-15.
7. Jasmine, R. Megiba, J. Jasper, and M. R. Geetha. "An efficient secure cryptosystem using improved identity based encryption with multimodal biometric authentication and authorization in cloud environments." Wireless Networks (2024): 1-21.
8. Peñuelas-Angulo, Alejandro, Claudia Feregrino-Uribe, and René Cumplido. "An adaptive method for prevention of overflow in reversible data hiding schemes." Expert Systems with Applications 230 (2023): 120610.
9. Sasikumar, K., and Sivakumar Nagarajan. "Enhancing Cloud Security: A Multi-Factor Authentication and Adaptive Cryptography Approach Using Machine Learning Techniques." IEEE Open Journal of the Computer Society (2025).
10. Otta, Soumya Prakash, Subhrakanta Panda, Maanak Gupta, and Chittaranjan Hota. "A systematic survey of multi-factor authentication for cloud infrastructure." Future Internet 15, no. 4 (2023): 146.
11. Kaur, Sandeep, Gaganpreet Kaur, and Mohammad Shabaz. "A secure two-factor authentication framework in cloud computing." Security and Communication Networks 2022, no. 1 (2022): 7540891.
12. Saqib, Manasha, Bhat Jasra, and Ayaz Hassan Moon. "A lightweight three factor authentication framework for IoT based critical applications." Journal of King Saud University-Computer and Information Sciences 34, no. 9 (2022): 6925-6937.
13. Mostafa, Ayman Mohamed, Mohamed Ezz, Murtada K. Elbashir, Meshrif Alruily, Eslam Hamouda, Mohamed Alsarhani, and Wael Said. "Strengthening cloud security: an innovative multi-factor multi-layer authentication framework for cloud user authentication." Applied Sciences 13, no. 19 (2023): 10871.
14. Basco, Jhonna Zelle E., Annielyn F. Romualdo, Jefferson A. Saluta, Cereneo S. Santiago Jr, and Rowee M. Marfil. "Comparison of Data Encryption Standard (DES) and Advanced Encryption Standard (AES) in Security Issues of Cloud Computing: A Literature Review." In International Conference on Frontiers of Intelligent Computing: Theory and Applications, pp. 189-200. Singapore: Springer Nature Singapore, 2024.
15. Shakor, Mohammed Y., Mustafa Ibrahim Khaleel, Mejdl Safran, Sultan Alfarhood, and Michelle Zhu. "Dynamic AES encryption and blockchain key management: a novel solution for cloud data security." IEEE Access 12 (2024): 26334-26343.
16. UDEH, CHINEMELUM GOODNESS. "Privacy-Preserving Access Control for Smart Grids Using Homomorphic Encryption." (2025).
17. Prasad, SJ Suji, S. R. Ramprasad, P. Sivaraman, Karumuru Venkat Reddy, Bhanu Prakash Battula, and R. Manikandan. "Enhancing Blockchain-Based Access Control in Cloud Computing with Machine Learning Techniques." In 2024 International Conference on Emerging Research in Computational Science (ICERCS), pp. 1-5. IEEE, 2024.
18. Polamarasetti, Anand. "Role of Artificial Intelligence and Machine Learning to Enhance Cloud Security." In 2024 International Conference on Intelligent Computing and Emerging Communication Technologies (ICEC), pp. 1-6. IEEE, 2024.
19. Egala, Bhaskara S., Ashok K. Pradhan, Venkataramana Badarla, and Saraju P. Mohanty. "Fortified-chain: a blockchain-based framework for security and privacy-assured internet of medical things with effective access control." IEEE Internet of Things Journal 8, no. 14 (2021): 11717-11731.
20. Rawther, Shiju, and Sathyalakshmi Sivaji. "Protecting Cloud Computing Environments from Malicious Attacks Using multi-factor Authentication and Modified DNA Cryptography." Recent Patents on Engineering 19, no. 1 (2025): E050923220730.
21. Midha, Sugandhi, Sahil Verma, Mohit Mittal, N. Z. Jhanjhi, Mehedi Masud, and Mohammed A. AlZain. "A Secure Multi-factor Authentication Protocol for Healthcare Services Using Cloud-based SDN." Computers, Materials & Continua 74, no. 2 (2023).
22. Carrillo-Torres, Diego, Jesús Arturo Pérez-Díaz, Jose Antonio Cantoral-Ceballos, and Cesar Vargas-Rosales. "A novel multi-factor authentication algorithm based on image recognition and user established relations." Applied Sciences 13, no. 3 (2023): 1374.
23. Shukla, Shivangi, and Sankita J. Patel. "A design of provably secure multi-factor ECC-based authentication protocol in multi-server cloud architecture." Cluster Computing 27, no. 2 (2024): 1559-1580.
24. Sharphathy, M. Nandhini, and V. Sumalatha. "A Secure Multi Factor Authentication Framework in Cloud Computing." In 2024 5th International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV), pp. 761-767. IEEE, 2024.
25. Chen, Xiao, BaoCheng Wang, and Haibin Li. "A privacy-preserving multi-factor authentication scheme for cloud-assisted IoMT with post-quantum security." Journal of Information Security and Applications 81 (2024): 103708.

26. Zhu, Liufu, and Ding Wang. "Robust Multi-Factor Authentication for WSNs with Dynamic Password Recovery." IEEE Transactions on Information Forensics and Security (2024).
27. Lahraoui, Younes, Saiida Lazaar, Youssef Amal, and Abderrahmane Nitaj. "Securing Data Exchange with Elliptic Curve Cryptography: A Novel Hash-Based Method for Message Mapping and Integrity Assurance." Cryptography 8, no. 2 (2024): 23.
28. Alqahtani, Abdulrahman Saad, Youssef Trabelsi, P. Ezhilarasi, R. Krishnamoorthy, S. Lakshmisridevi, and S. Shargunam. "Homomorphic encryption algorithm providing security and privacy for IoT with optical fiber communication." Optical and Quantum Electronics 56, no. 3 (2024): 487.
29. Kebande, Victor R., Feras M. Awaysheh, Richard A. Ikuesan, Sadi A. Alawadi, and Mohammad Dahman Alshehri. "A blockchain-based multi-factor authentication model for a cloud-enabled internet of vehicles." Sensors 21, no. 18 (2021): 6018.
30. Liu, Kaijun, Guosheng Xu, Qiang Cao, Chenyu Wang, Jingjing Jia, Yuan Gao, and Guoai Xu. "A Rivest–Shamir–Adleman-Based Robust and Effective Three-Factor User Authentication Protocol for Healthcare Use in Wireless Body Area Networks." Sensors 23, no. 21 (2023): 8992.