International Journal of Computer Trends and Technology
ISSN: 2231–2803 / https://doi.org/10.14445/22312803/IJCTT-V72I6P122

Volume 72 Issue 6, 168-178, June 2024

Original Article

Empowering Cloud Security: Pioneering an Interactive Multi-Factor Authentication Framework for Cloud User Verification

Rajender Reddy Pell Reddy

Cybersecurity Specialist VA, USA.

Corresponding Author : rpellreddy@gmail.com

Received: 19 April 2024 Revised: 26 May 2024 Accepted: 17 June 2024 Published: 30 June 2024

Abstract *- Multiple-factor authentication in the cloud is an essential security feature that fortifies cloud security against illegal breaches in data and access. Multi-factor authentication enables cloud computing to be more secure for enterprises and less unpleasant for customers by confirming that individual authorized users can access apps, data, services, and resources. A security structure's architecture and the necessary level of protection determine exactly how many authentication factors are essential. Thus, the process of integrating a safe MFA system into a cloud platform is difficult. The adaptive MFA multi-layer interaction-based authentication system discussed in this paper incorporates intrusion detection and access control features together with an automated authentication method selection process. The main objective is to improve a secure cloud platform that hinders hackers' access to the cloud system by having fewer false positive alerts. Multiple authentication factors are integrated with a user's geofence location and IP address confirmation technique to strengthen the individuality verification of cloud users, improve the authentication mechanism, and decrease false alarms. These elements include the duration, legitimacy, and importance of the user aspect. The data are safeguarded against disclosure by an additional CP-ABHE technique. The CP-ABHE encryption method is employed to hide the login credentials on the cloud directory provider. The suggested system performed an excellent occupation of spotting potentially dangerous users and trespassers, thereby stopping any deliberate attacks on the data and cloud services.*

Keywords *- Ciphertext Policy-Attribute-based Homomorphic encryption, Cloud authentication, False positive alarm, Multi-factor authentication (MFA).*

1. Introduction

Cloud computing is a relatively recent technological development on the internet that provides various services, including servers, processing power, storage systems, networks, apps, and more. Cloud computing presents more advanced alternatives in terms of power management, cost-effectiveness, time efficiency, and space usage than traditional approaches [1-3]. These services are provided by three main service models that this technology employs: Platform as a Service (PaaS), Infrastructure as a Service (IaaS), and Software as a Service (SaaS). They each offer different service layers that range from operating systems and computing systems to databases and programming frameworks [4-5].

Cloud authentication is essential for confirming user's identities on various cloud platforms and determining if they can be trusted with access to cloud-based resources, data, apps, and services. It guarantees compliance with access rights and privileges, which is essential for preserving the integrity of cloud security. Cloud settings are susceptible to several security risks and assaults when weak or inadequate cloud authentication approaches are used [6-8].

The primary layer of defence against unauthorized access is an effective set of authentication methods, which safeguards resources, data, applications, and services. These methods include digital device authentication, biometric authentication, certificate-based authentication, Token authentication, password-based authentication, digital sign-on (SSO), graphical password authentication, third-party authentication, two-factor authentication, and multifactor authentication MFA.

To strengthen security, lower password vulnerabilities, assure regulatory compliance, and promote enterprise mobility, businesses have recently embraced multi-factor authentication in cloud-based applications. Along with a username and password, MFA security requires a second or third form of proof of identity when a user seeks to access applications and services in the cloud [9-11].

Cloud computing multi-factor authentication involves the use of digital or electronic authentication techniques, allowing access to the user only after the successful submission of two or more authentication factors. These factors can be classified as belonging to one of the following categories: knowledge (PINs, passwords), possession (identity cards, smartphones with OTP apps), inheritance (biometric data, such as iris and fingerprint scans), location (MAC addresses), time (scheduled time intervals), and behaviour (keystroke rhythm, gait). Because MFA lessens the possibility of unwanted access if one factor is compromised, identity assurance is improved [12-15].

Securing cloud infrastructure has widespread challenges amid high stakes. Cloud complexity, tool sprawl, and organizational divisions that operate independently and avoid sharing information cause security gaps. Organizations building their cloud need to see and understand actual risk – but shortages in processes prevent better control. Hence this paper proposes an authentication strategy sorter (ASS) and interactive intrusion detection stages to present a collaborating, adaptable, and safe MFA multi-layer authentication structure. ASS is predicated on a pool of diverse authentication methods and prior user authentication data knowledge. The administrator can install a suitable authentication mechanism based on the demands of the organization. An authentication method will be chosen from the pool by the administrator and activated by these guidelines. The proposed structure utilizes the user's browser and last location to evaluate user behaviour and provides interactive intrusion detection methods. This structure provides an adaptable and affordable authentication mechanism based on intrusion detection systems, ASS methodology, and Ciphertext Policy-Attribute-based Homomorphic Encryption. Our research's contribution is demonstrated in the following manner:

- Providing the ASS methodology to enhance the authentication procedure by choosing the best authentication method according to user behavior.
- Delivering interactive reactions to user behavior based on position and avoidance web browser evidence to strengthen and enforce intrusion detection security measures.
- The suggested CP-ABHE encryption for data security and hiding login credentials on the cloud directory provider is an improvement in the right direction for improving data privacy and confidentiality in cloud environments.
- Conducting experiments to validate and demonstrate the effectiveness of the suggested structure.

The rest of this paper can be browsed as follows:

In Section 2, a review of the literature on various MFA factors and approaches in cloud-based contexts is covered.

Section 3 presents the suggested cloud MFA multi-layer authentication structure.

Section 4 presents the authentication algorithm's implementation, and outcomes are given.

Section 5 provides an overview of the conclusions.

2. Related works

Cloud security benefits greatly from MFA, which uses multiple factors to authenticate user identities and reduces the danger of unwanted access. This survey examines several MFA components, deployment techniques, and security posture impacts, examining tactics to improve access restrictions without compromising user ease.

Said et al. [16] introduced this survey to examine various MFA components, deployment strategies, and the effects on security posture. Additionally, it examines methods to enhance access limitations without rendering them more difficult to navigate. The framework included creating user authentication factors, granting user privileges, registering users, and performing multi-layer authentication. To identify malevolent users and verify user identity, intrusion detection systems were incorporated. The cloud databases were designed to protect data during transmission and storage by implementing the Advanced Encryption Standard (AES) algorithm.

Mihailescu et al. [17] developed a searchable encryption system for cloud environments that includes biometric authorization and authentication. The system's components were covered, including the searchable encryption technique, biometric authentication, and traditional user authentication. Steps include entering credentials, calculating hash values, and creating user hashes were each component of the authentication procedure. The cloud server employed encryption and decryption techniques to guarantee that all activities were correct and delivered correct documents. Modern methodology, the elaborated plan, security analysis, and performance analysis were also included in this research.

Chen et al. [18] introduced a key agreement protocol-based, secure three-factor authentication system for e-health clouds to improve security. Symmetric encryption /decryption, concatenation, bitwise XOR, one-way hash function, and elliptic curve cryptography were among the methods employed in the protocol. The protocol eliminated replay attacks and man-in-the-middle attacks and offered untraceability and anonymity to users, thereby mitigating the vulnerabilities of the preceding protocol. Burrows-Abadi-Needham (BAN) logic was used to demonstrate the protocol's security. Phases of the protocol included initialization, registration, login, authentication, revocation, re-registration, password updates, and biometric updates.

Prabha et al. [19] introduced a Schmidt-Samoa Cryptography (SKMA-SC) technique that addresses security and privacy concerns in cloud computing data access based on

Suppressed K-Anonymity MFA. Data access, authentication, and registration were all involved. It then used conditional characteristics, a one-time token, and multifactor authentication. The method was evaluated using the following metrics: privacy-preserving rate, computational complexity, and accuracy of authentication. The SKMA-SC method improved cloud data access authentication accuracy, decreased computing complexity, and preserved privacy.

Hossain et al. [20] utilized an algorithm for minutiae extraction to feature extraction and biometric sample collecting from the user. For authentication, the extracted template was compared to the template that was saved in the cloud database. The cloud authentication server utilized distinct characters to construct a One-Time Password (OTP), encrypted user data using the AES technique and delivered the encrypted data to the client side. An HTTP gateway was employed to provide the user with the OTP, which was needed to decrypt the encrypted data.

Alsahlani et al. [21] presented an LMAAS-IoT-based simple MFA and authentication mechanism for instantaneous data access in Internet of Things cloud settings. For security, bitwise XOR operations and cryptographic hash purposes were employed in the approach. Lightweight authentication systems are necessary in Internet of Things environments, as previous research has demonstrated, and security weaknesses exist in current schemes. This system used fuzzy extractors, hash functions, and XOR operations to provide efficient real-time data access, common authentication, and user anonymity.

Kebande et al. [22] presented a Cloud-enabled Internet of Vehicles (IoV) MFA approach built on blockchain technology. For a connected edge-to-cloud ecosystem, it incorporated Single Sign-On (SSO) and Security Assertion Markup Language (SAML). By utilizing an embedded digital signature and a probabilistic polynomial-time algorithm (ePPTA), this concept improved security. Utilizing the Dolev-Yao adversarial model as a basis, the strategy attempted to protect Confidentiality, Integrity, and Availability (CIA) in the face of significant adversarial threats in an IoV-centred environment. By establishing a security layer, it improved the integrity, secrecy, and trustworthiness of Proof-of-Work (PoW) in blockchain transactions.

Midha et al. [23] introduced an efficient hash function-based multi-factor authentication scheme. For security validation, this method is examined using the AVISPA program. Analyze the comparative performance analysis in terms of security parameters and computational charge compared to the current ones.

DeviPriya et al. [24] introduced an authentication mechanism that entails the Cloud Server (CS) and Cloud User (CU) verifying digital signatures and certificates. A shared one-time session key is generated by the protocol and shared by CU and CS. The authentication approach involves the use of strategies that include symmetric encryption and key decryption. GNY belief logic is used in logical analysis to accomplish the authentication protocol's intended goals.

Bouchaala et al. [25] presented an expansion of a key agreement and authentication system based on smart cards to improve cloud computing security. Elliptic Curve Cryptography, fuzzy verifier, and two-factor authentication are some of its features. The solution is designed to survive multiple types of assaults, including replay, privileged insider, and impersonation attacks. The security of the system under CDH and ECDL problems is demonstrated by both informal and rigorous validation utilizing the Scyther tool.

3. Methodology

There are three primary phases to the proposed framework. The process of creating a user, allowing access, and encrypting and decrypting data are some of these phases. The initial phase involves initiating the process required to establish an account and generating the essential attributes for a user to access the program. The registration phase and the privilege creation phase are the two primary phases of the user creation phase. An alternate form of authentication, like a mobile device or email account, is chosen by the user together with his or her secret qualities during the registration stage. The honours granted to each user are realized during the creating user honours stage. The necessary steps to provide a user with accessibility to the application are provided in the access-giving phase. Four components join to constitute this phase: intrusion detection, multi-factor authentication, auditing tables, and suspect tables. A user is authenticated across three levels by the multifactor authentication element. These levels consist of the email-based OTP, the user factor, and the username and password. The objective of the intrusion detection component is to confirm the user factor, examine the distrusted table, and send out an alert as soon as it finds evidence of unusual user activity. In the user verification stage, the user's byte size is verified, the user factor validity is checked, the entered user byte size is compared, and the distrusted table is checked. Preserving track of every action the user does on the program data and providing a summary of all alarms produced for the users is the responsibility of the auditing table element. It enables to exploitation of the rate at which impending countermeasures are implemented. All suspected users who have overridden their authorized privileges are archived in the suspect table element. The AUTH, an extra authentication procedure, is also necessary for the login procedures. The AUTH is activated if a user is suspicious. A CP-ABHE algorithm is employed to encrypt and decrypt application data in and out of the database server throughout the encryption and decryption phase.

In this research, we deliberate the access-granting phase as our main goal. To guarantee user identity and deter intrusions, we incorporate security measures that enhance the

flexibility and security of our suggested framework. Using the Sorter authentication mechanism yields the flexibility feature (ASS). A company can choose from a variety of authentication methods, not just email, by utilizing ASS. While we utilized IMEI numbers, emails, and thermal image identification as instances, any other amalgamation of techniques may be applied without sacrificing generality. Our suggested framework employs five factors to detect intrusions more securely by utilizing the user's IP address and geolocation as additional factors. The suggested framework's general elements are shown in Figure 1.

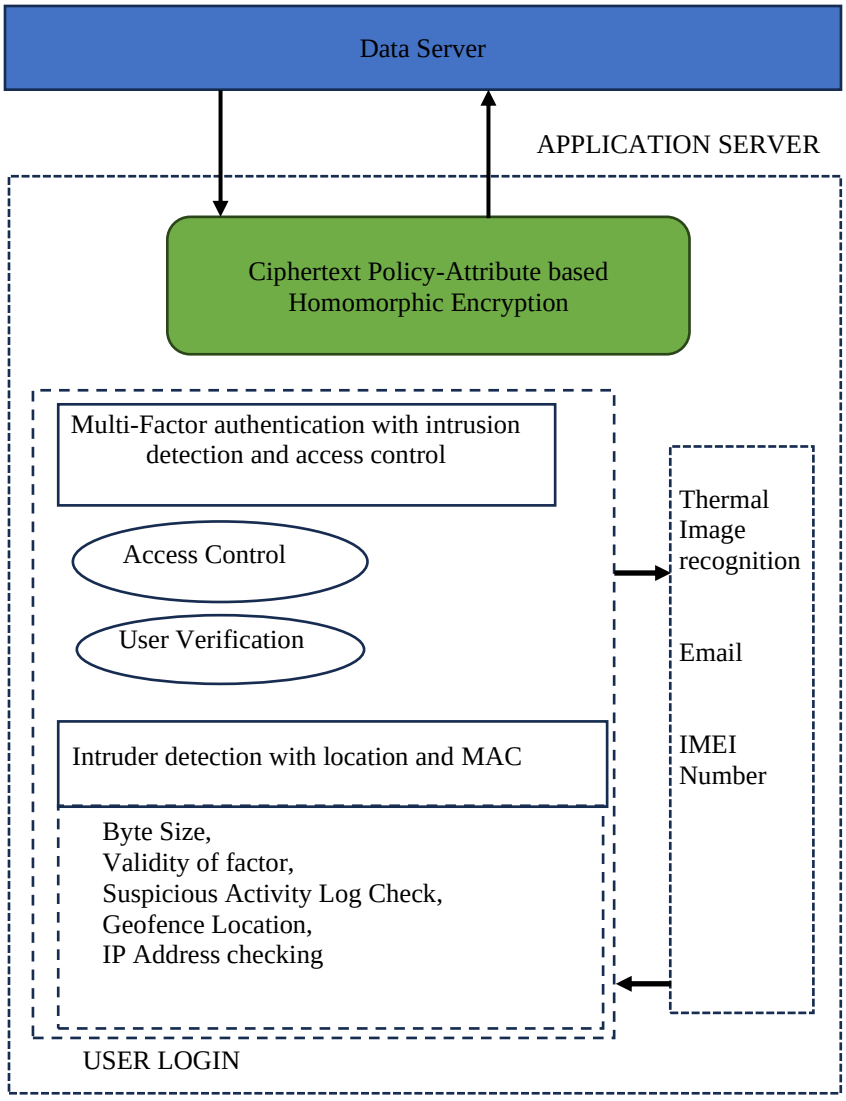

Fig. 1 The overall components of the proposed framework

3.1. Ciphertext Policy-Attribute-based Homomorphic Encryption (CP-ABHE)

A cryptographic method called CP-ABHE is used to improve cloud system security. This is accomplished by extending the scope of messages that can be handled and delivered securely [26-28]. Here is a more thorough breakdown of how it operates: CP-ABHE expresses messages as polynomials over certain mathematical structures identified as rings. There are specific requirements that these polynomials' integer coefficients must follow. Messages encoded as polynomials with each coefficient being an integer less than a predetermined value are employed in non-circuit-based CP-ABHE schemes. To recover the original message, decoding entails evaluating these polynomials. Conventional methods involve bit-by-bit computations and binary representation of integers. Processing complexity is decreased by CP-ABHE, which simplifies this procedure by encoding complete messages as single polynomials. CP-ABHE maintains the homomorphic characteristics required for safe computations on encrypted data. This implies that ciphertexts can be directly subjected to operations like addition and multiplication without requiring initial decryption.

Setup: Initializes the cryptographic parameters and key generation structures.

Encrypt: Encodes plaintext messages into encrypted form (ciphertexts) using polynomial representations.

Evaluate: Performs homomorphic operations on ciphertexts to compute results without revealing underlying plaintexts.

KeyGen: Generates secret keys for authorized users or entities to decrypt and access data.

Decrypt: Recovers plaintext messages from encrypted ciphertexts using appropriate secret keys.

3.2. Authentication Strategy Sorter

ASS manages the selection of the authentication method and is mostly dependent on user behavior. ASS is responsible for managing the authentication method selection, which is primarily based on user behavior. Several authentication approaches can be introduced or employed based on the needs of the business and the organization's regulations. While security tokens are available from certain organizations, fingerprint authentication is available from other organizations. The organization's capacity and the resources at hand determine the procedure for selecting any technique. The selection and addition of authentication methods fall under the purview of the application administrators. Additional authentication techniques, including IMEI numbers, thermal image recognition, and any other technique decided upon by the administrators, have been added to this paper. Whenever a user first logs in using an email address, they will be authenticated using email if they want to access the program but forgot their password. Suppose the user loses track of their factor. In that case, they will need to be verified using an alternative method, such as their IMEI number or Thermal Image Recognition, to protect their identity if their email is leaked. The Authentication technology Selection Process and the Authentication Techniques Pool are both primary parts of the AMS technology.

3.3. Authentication Technique Selection Process

The authentication method assortment is illustrated in Figure 2, and the procedure automatically decides which authentication method will be utilized in the most current authentication progression.

Selecting an authentication technique involves three primary processes, illustrated in Fig. 2.

The phases include the user's most recent authentication process, the authentication method definition, and the state of the user's authentication process. Only three authentication methods were chosen by the user in the last step of the authentication process: email, IMEI number, and thermal image recognition. An application is sent to the database server to retrieve the most recent authentication technique utilized in the previous authentication procedure before authenticating the user. To ascertain the usage priority for every authentication method, we present an authentication method priority table in the second step, identifying the authentication process. A number designating each method's priority is assigned to it. The authentication process's priority increases with increasing numbers. The selection of the authentication mechanism is contingent upon the usage percentage. By splitting the entire quantity of authentication attempts by the number of uses of the authentication method, this percentage is determined.

The suggested Priority Table for Authentication Systems is represented by Table 1.

Table 1. Authentication process priority table

Authentication method	Priority
Thermal image recognition	3
Email	2
IMEI number	1

Thermal image recognition is utilized as the initial authentication layer in the User Authentication Progression Status step, following the selection of the authentication system. A further level of authentication is applied based on the conclusion of the initial authentication procedure. The user will have legitimate and approved access to cloud services if the first layer is verified. If not, the Email is selected as the subsequent authentication method. The process continues until the final authentication layer.

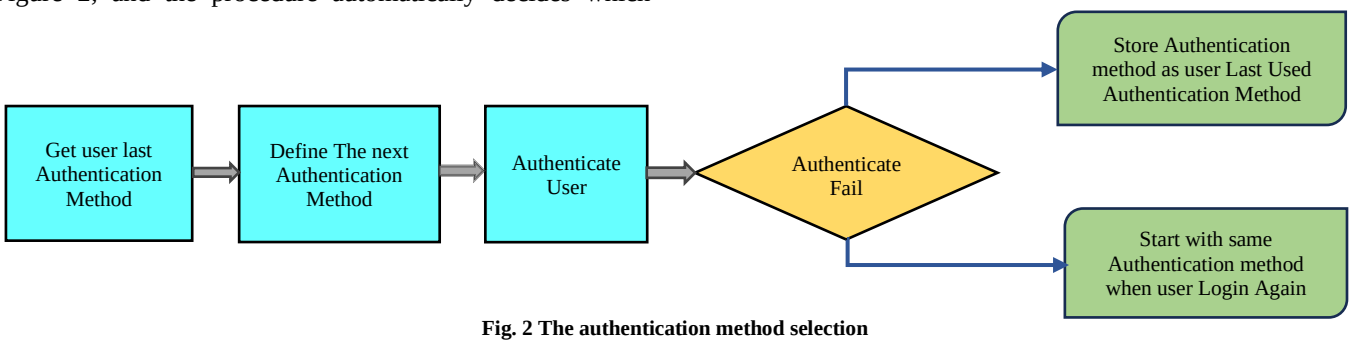

Fig. 2 The authentication method selection

The authentication methods are applied by $user$ A, as indicated in Tables 2 and 3, and the utilization percentage for each authentication method is displayed. Table 1 will decide which priority will be used if the percentages of the two authentication methods are equal.

Table 2. Authentication process selection illustration 1

	Authentication system		
Username	**Thermal image recognition**	**Email**	**IMEI number**
User A	5	4	5
Percentage	0.357	0.285	0.357

IMEI numbers are the last means of authentication. Email is 0.285, IMEI number is 0.357, and thermal image recognition is 0.357 percent. Email will be the next authentication method since its percentage is the nethermost.

Table 3. Authentication method selection illustration2

	Authentication method		
Username	**Thermal image recognition**	**Email**	**IMEI number**
User A	5	5	5
Percentage	0.333	0.333	0.333

The IMEI number is the last form of authentication. The percentages for thermal image recognition, email, and IMEI numbers are all 0.333. Thermal image recognition will be the next authentication technique because its percentage is the same as that of the other techniques. IMEI numbers were the last authentication method. The percentages for email and thermal image recognition were equal. However, thermal image recognition was given more priority in the authentication method's priority table.

3.3.1. Authentication Techniques Pool

Methods of Authentication techniques are gathered into a shared pool termed pool. The feature allows for the addition of any necessary authentication procedures; simply put them into practice, add them to the pool, and arrange them in the order of priority for usage.

3.4. Intrusion Detection with User Behaviour Factors

The intrusion detection constituent is predicated on the user factor that proceeds via three stages: byte size verification, factor validity verification, and suspicious activity log verification.

These procedures serve as a second degree of authentication and are used to identify intruders. To finish the process of recognizing the invaders based on user behavior, more steps are implemented. The user begins logging into the application after completing the registration process for the first time. The user saves their location so they can use the application again later.

It also stores the web browser that the user typically uses. The initial four phases of the intrusion detection process are user-dependent and begin with the user's location. If the user's location differs from that of their preferred browser, extra steps are added after the user completes the steps. The user account is congested in this instance, and the user is supplementary to the distrusted table since the user's geolocation and IP address differ. The POST is triggered to authenticate the user if any of them differ from the previously stored ones. A user's account is blocked, and the admin user verifies their identity until they are verified in the event of a HASN failure.

3.5. Proposed Framework Login Procedures

After the application of the ASS and behavioral factors to the framework's intrusion detection processes, figure 3 shows the entire intrusion detection and access phases procedure. Three authentication factors constitute the mainstay of the entire access procedure, as shown in Figure 3. Access rules are used in conjunction with the initial authentication factor, which is a username and password. The user access factor, which was developed earlier during the user creation phase, serves as the second authentication factor. It is used to confirm the IP address verification, geofence location, suspicious activity log check, byte size verification, and factor validity in intrusion detection processes. The user verification OTP, which is issued by the authorization rules and AMS, serves as the third authentication factor.

4. Results and Discussion

This section discusses the way the intended cloud computing platform will have MFA layers installed and how the associated user authentication technique will function. The computation of results considers the fractions of FP and FN rates that are experienced during the handling of the MFA layers in accumulation to the length of time that the resulting multi-layers take to execute.

4.1. Execution Time for MFA Layer

This phase involves the development and implementation of authentication layers that utilize the use of layered multi-factor techniques. Measurement of the entire accomplishment time for cloud computing user verification founded on the five major levels is the aim of this step: Verifying the byte size, factor validity, geofence location, suspicious activity log, and IP address. For every experiment, the accomplishment time is expressed in milliseconds for a variable number of users. The first factor that verifies the byte size has an execution time that grows linearly with the number of users, as seen in Figure 4.

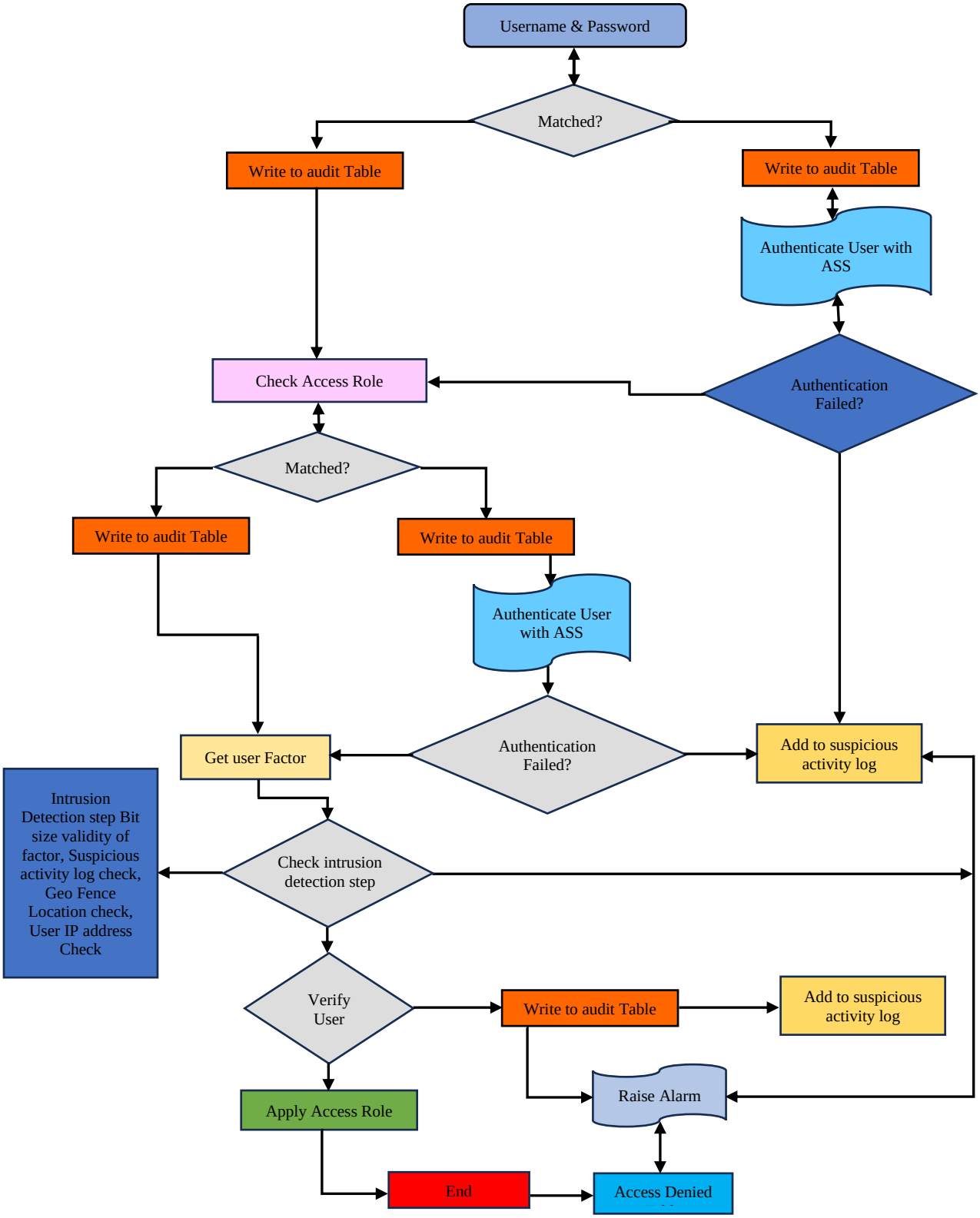

Fig. 3 Complete access steps and intrusion detection process

The execution time for 50 users was 218 ms, whilst the time for 1000 users was 278 ms. When 50 users were involved, at 100 users, the non-linear execution time increased to 196 ms, according to the checking factor validity technique. The execution time decreased somewhat to 194 ms for 200 users and 193 ms for 300 users. This method's variation in execution time can be attributed to the usage of a Boolean variable to check whether a statement is true or false, as suggested by user behavior authentication. When the execution duration grew in tandem with the rise in user count, the components of the suspicious activity log increased linearly [29–31]. Examining the suspicious activity log revealed that the execution times rose linearly from 50 to 800 users, then comparatively fell to 231 ms for 900 users, and again surged to 243 ms for 1000 users. There was a linear increase in both the user geofence location and IP address checking factors from 50 to 500 users. The time exhibited a relative drop after 500 users, followed by a rise once again, with reported times of 263 ms and 237 ms for 1000 users for both the user locality and browser name components.

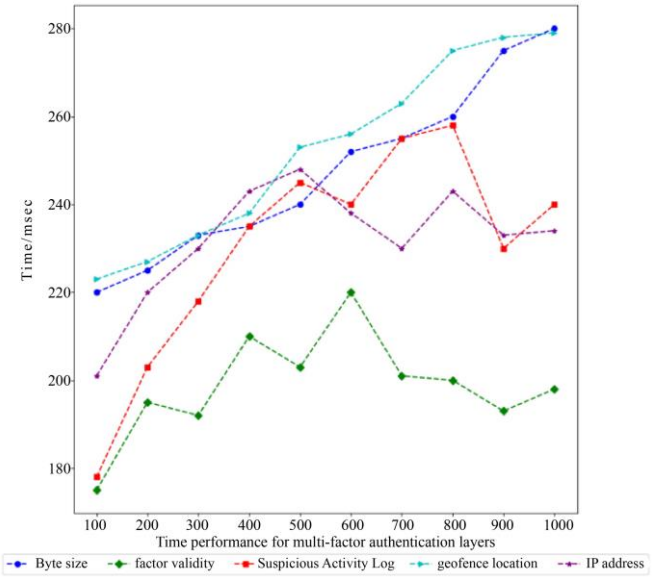

Fig. 4 Time performance for MFA layers

4.2. Detection Performance

The assessment of detection performance is widely regarded as a crucial point of orientation and a director for the effectiveness of suggested algorithms in security applications and approaches that utilize diverse authentication and protection techniques. The fraction of normal users that are detected as intruders is represented by the false-positive rate (FP) in this section, while the percentage of intrusions that are successful in breaching cloud computing services to reveal private data from the cloud service platform is represented by the false-negative rate (FN) [32–33]. Figure 4 illustrates that for 50 users, the geofence location and IP address checks reported 2% false positives (FP), while the remaining components recorded 0% false positives. For both byte size and factor validity, the FP percentage with 100 users was only 1%. This results from users' browser names and locations being incorrectly detected. When the user count rose from 50 to 1000, these factors continued to record FP alarms. The IP address recorded 0.4% FP, while the user geofence location check recorded 0% FP for 500 users. False alarms ranged in the FP rate from 0.1% to a high of 1%. When the number of users climbed from 600 to 1000, this is because MFA systems, which can accurately validate regular users, are efficient and flexible. The fraction of successful attacks that manage to extract confidential data from the cloud service platform is known as the false-negative (FN) percentage, as shown in Figure 5. The FN rate for 50 users was 0% across all MFA techniques, as previously mentioned. The FN rates for the four factors byte size, factor validity, suspicious activity log, and user geofence location were 0%, 1%, and 1%, respectively, when the user count reached 100. The MFA methodology's accuracy for 500 users revealed a low false negative rate (FN rate) of 0.4%, 0.2%, 0.8%, 0.2%, 0.2%, and 0.2% for each authentication factor. The accuracy for 800 users also revealed a low false positive rate (FN rate), 0.25%, 0.38%, 0.13%, 0.75%, 0.63%, and 0.25% for each authentication factor. The residual experiment found that the FN rate for users 900 and 1000 was modest, with the highest FN of 0.78% for the IP address check and 0.7 for the factor length check. To prevent any intentional assaults on the cloud server or its services, the suggested methodology and algorithm utilizing MFA techniques often produced a good presentation in recognizing suspicious users and interlopers.

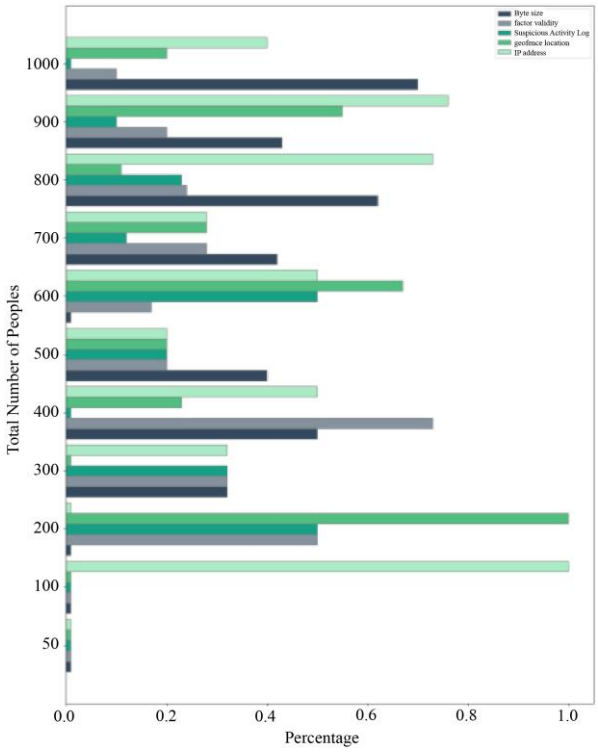

Fig. 5 FP users on MFA layers

Table 4. Shows the following qualitative factors

Ref	Usability	Accessibility	Cost effectivity	Adaptability	Versatility
[34]	Moderate	Effective	Moderate	Effective	Effective
[35]	Effective	Moderate	Effective	Moderate	Effective
[36]	Effective	Moderate	Moderate	Effective	Effective
[37]	Moderate	Effective	Moderate	Effective	Moderate
Proposed MFA model	Effective	Effective	Effective	Effective	Effective

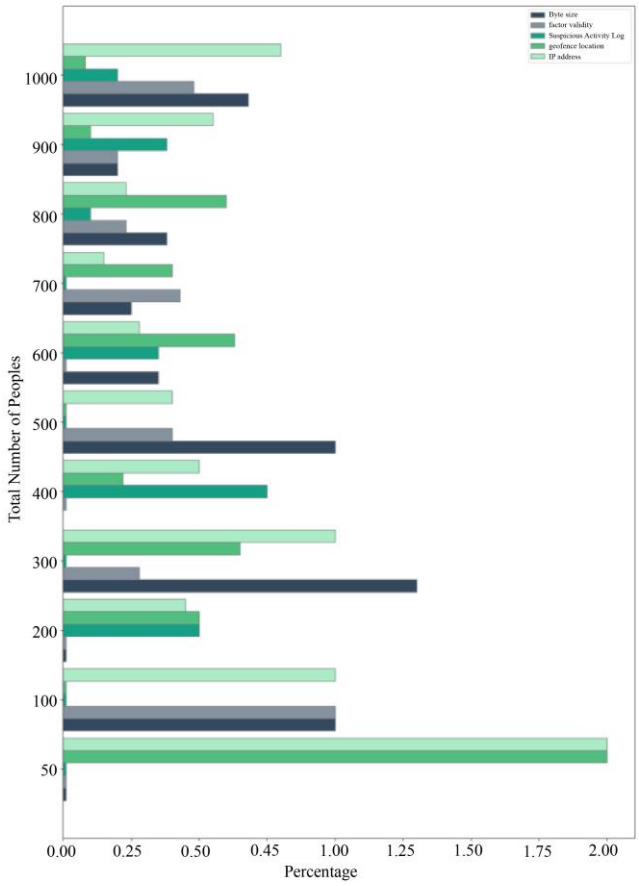

Fig. 6 FN users on MFA layers

4.2.1. Comparative Analysis

The effectiveness of attack prevention is evaluated using both quantitative and qualitative metrics in the performance assessment of the suggested MFA structure. To assess the overall effectiveness of the suggested MFA architecture and algorithm, quantifiable metrics such as FP and FN rates are calculated. Qualitative indicators are equally significant in addition to these quantitative ones. The qualitative characteristics are compared with previous works in Table 4 below.

5. Conclusion

To preserve the refuge of data, apps, services, and properties, cloud authentication is an essential procedure for verifying user identification. In the PaaS layer, it is most frequently executed. Achieving a balance between usability and security is a difficulty when utilizing PaaS authentication. Our paper presents a versatile multi-factor authentication architecture designed to provide secure application and data access within a PaaS environment. The suggested structure combines an encryption/decryption method, access control policies, and an intrusion detection system with MFA. Employing MFA enables companies to provide their users with more robust authentication possibilities. However, consumers can make use of PaaS without jeopardizing their privacy. The users' individualities are protected by employing an IDS. Users' identities are confirmed, and their access periods are managed using access control policies. Data protection is achieved by employing the Homomorphic Encryption algorithm, which is based on the Ciphertext Policy-Attribute ciphertext.

Providing the Authentication Strategy Sorter (ASS) provides the proposed framework to gain flexibility. An organization can choose from several different authentication methods by employing ASS. We demonstrated these points with thermal image recognition, email, and IMEI number authentication; different combinations of techniques can be applied without compromising generality. Using five elements, the suggested framework increases security by utilizing the user's geofence position and a web browser capability that is frequently utilized with other intrusion detection process components. We can confirm that the correct application is being utilized by the appropriate user with the relevant data by employing the suggested framework.

Additionally, we can ensure that the data is secret and of high integrity. The FN and FN alarm rates were calculated using the experimental data. At varying user counts, the FN rate significantly climbed, and the FN rate significantly dropped. By including further security features like the structure for risk-based and adaptive authentication can be further enhanced in subsequent work. A broader range of attack scenarios and a higher number of users can be used to test the structure. Finally, by providing a more user-friendly interface, the framework can be made more approachable.

References

[1] Dharmesh Dhabliya, "Cloud Computing Security Optimization via Algorithm Implementation," *International Journal of New Practices in Management and Engineering*, vol. 10, no. 1, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[2] Satwinder Singh Rupra, and Amos Omamo, "A Cloud Computing Security Assessment Framework for Small and Medium Enterprises," *Journal of Information Security*, vol. 11, no. 4, pp. 201-224, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[3] Zhiying Wang et al., "An Empirical Study on Business Analytics Affordances Enhancing the Management of Cloud Computing Data Security," *International Journal of Information Management*, vol. 50, pp. 387-394, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[4] A. Shaji George, and S. Sagayarajan, "Securing Cloud Application Infrastructure: Understanding the Penetration Testing Challenges of IaaS, PaaS, and SaaS Environments," *Partners Universal International Research Journal*, vol. 2, no. 1, pp. 24-34, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[5] Praveen Kumar et al., "An Analytical Evaluation of Cloud Computing Service Model IaaS&PaaS using Market Prospective," *2021 International Conference on Technological Advancements and Innovations (ICTAI)*, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[6] Sandeep Kaur, Gaganpreet Kaur, and Mohammad Shabaz, "A Secure Two-factor Authentication Framework in Cloud Computing," *Security and Communication Networks*, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[7] Naveed Khan, Jianbiao Zhang, and Saeed Ullah Jan, "A Robust and Privacy-preserving Anonymous user Authentication Scheme for Public Cloud Server," *Security and Communication Networks*, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[8] J. Stanly Jayaprakash et al., "Cloud Data Encryption and Authentication based on Enhanced Merkle Hash Tree Method," *Computers, Materials & Continua*, vol. 72, no. 1, pp. 519-534, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[9] Ghulam Mustafa Khaskheli, Marina Sherbaz, and Umair Ramzan Shaikh, "A Comparative Usability Study of Single-factor and Two-factor Authentication," *Tropical Scientific Journal*, vol. 1, no. 1, pp. 17-27, 2022. [Google Scholar] [Publisher Link]

[10] Qingxuan Wang et al., "Quantum2FA: Efficient Quantum-resistant Two-factor Authentication Scheme for Mobile Devices," *IEEE Transactions on Dependable and Secure Computing*, vol. 20, no. 1, pp. 193-208, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[11] Abdelouahid Derhab et al., "Two-factor Mutual Authentication Offloading for Mobile Cloud Computing," *IEEE Access*, vol. 8, pp. 28956-28969, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[12] Shivangi Shukla, and Sankita J. Patel, "A Design of Provably Secure Multi-factor ECC-based Authentication Protocol in Multi-server Cloud Architecture," *Cluster Computing*, vol. 27, pp. 1559-1580, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[13] Geeta Sharma, and Sheetal Kalra, "Advanced Lightweight Multi-factor Remote user Authentication Scheme for Cloud-IoT Applications," *Journal of Ambient Intelligence and Humanized Computing*, vol. 11, pp. 1771-1794, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[14] K. Devi Priya, and L. Sumalatha, "Trusted Hybrid Multifactor Authentication for Cloud Users," *I-Manager's Journal on Cloud Computing*, vol. 7, no. 1, p. 12, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[15] Sara Ahmed AlAnsary, Rabia Latif, and Tanzila Saba, "Multi Factor Authentication as a Service (MFAaaS) for Federated Cloud Environments," *Proceedings of the Second International Conference on Innovations in Computing Research (ICR'23)*, pp. 225-236, 2023. Cham: Springer Nature Switzerland. [CrossRef] [Google Scholar] [Publisher Link]

[16] Wael Said et al., "A Multi-Factor Authentication-based Framework for Identity Management in Cloud Applications," *Computers, Materials & Continua*, vol. 71, no. 2, pp. 3193-3209, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[17] Marius Lulian Mihailescu, and Stefania Loredana Nita, "A Searchable Encryption Scheme with Biometric Authentication and Authorization for Cloud Environments," *Cryptography*, vol. 6, no. 1, p. 8, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[18] Yulei Chen, and Jianhua Chen, "A Secure Three-factor-based Authentication with Key Agreement Protocol for e-Health Clouds," *The Journal of Supercomputing*, vol. 77, pp. 3359-3380, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[19] K. Mohana Prabha, and P. Vidhya Saraswathi, "Suppressed K-anonymity Multi-factor Authentication based Schmidt-samoa Cryptography for Privacy Preserved Data Access in Cloud Computing," *Computer Communications*, vol. 158, pp. 85-94, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[20] Alamgir Hossain, and Abdullah Al Hasan, "Improving Cloud Data Security through Hybrid Verification Technique Based on Biometrics and Encryption System," *International Journal of Computers and Applications*, vol. 44, no. 5, pp. 455-464, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[21] Ahmed Yaser Fahad Alsahlani, and Alexandru Popa, "LMAAS-IoT: Lightweight Multi-factor Authentication and Authorization Scheme for Real-time Data Access in IoT Cloud-based Environment," *Journal of Network and Computer Applications*, vol. 192, p. 103177, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[22] Victor R. Kebande et al., "A Blockchain-based Multi-factor Authentication Model for a Cloud-enabled Internet of Vehicles," *Sensors*, vol. 21, no. 18, p. 6018, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[23] Sugandhi Midha et al., "A Secure Multi-factor Authentication Protocol for Healthcare Services Using Cloud-based SDN," *Computers, Materials & Continua*, vol. 74, no. 2, pp. 3711-3726, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[24] K. DeviPriya, and Sumalatha Lingamgunta, "Multi Factor Two-way Hash-based Authentication in Cloud Computing," *International Journal of Cloud Applications and Computing (IJCAC)*, vol. 10, no. 2, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[25] Mariem Bouchaala, Cherif Ghazel, and Leila Azouz Saidane, "Enhancing Security and Efficiency in Cloud Computing Authentication and Key Agreement Scheme based on Smart Card," *The Journal of Supercomputing*, vol. 78, pp. 497-522, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[26] Zengpeng Li et al., "Ciphertext-policy Attribute-based Proxy Re-Encryption Via Constrained PRFs," *Science China, Information Sciences*, vol. 64, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[27] Hang Li et al., "An Efficient Ciphertext-policy Weighted Attribute-based Encryption for the Internet of Health Things," *IEEE Journal of Biomedical and Health Informatics*, vol. 26, no. 5, pp. 1949-1960, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[28] Yong Wang et al., "Efficient and Secure Ciphertext-policy Attribute-based Encryption without Pairing for Cloud-assisted Smart Grid," *IEEE Access*, vol. 8, pp. 40704-40713, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[29] Leandro Loffi et al., "Mutual Authentication with Multi-factor in IoT-Fog-Cloud Environment," *Journal of Network and Computer Applications*, vol. 176, p. 102932, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[30] Ayman Mohamed Mostafa et al., "Strengthening Cloud Security: An Innovative Multi-Factor Multi-Layer Authentication Framework for Cloud User Authentication," *Applied Sciences*, vol. 13, no. 19, p. 10871, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[31] Marco Pernpruner et al., "An Automated Multi-Layered Methodology to Assist the Secure and Risk-Aware Design of Multi-Factor Authentication Protocols," *IEEE Transactions on Dependable and Secure Computing*, pp. 1-16, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[32] Noor Afiza Mohd Ariffin et al., "Vulnerabilities Detection using Attack Recognition Technique in Multi-factor Authentication," *TELKOMNIKA (Telecommunication Computing Electronics and Control)*, vol. 18, no. 4, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[33] Emanuela Marasco et al., "Biometric Multi-factor Authentication: On the Usability of the FingerPIN Scheme," *Security and Privacy*, vol. 6, no. 1, p. e261, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[34] Sandeep Kaur, Gaganpreet Kaur, and Mohammad Shabaz, "A Secure Two-factor Authentication Framework in Cloud Computing," *Security and Communication Networks*, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[35] Soumya Otta et al., "A Systematic Survey of Multi-factor Authentication for Cloud Infrastructure," *Future Internet*, vol. 15, no. 4, p. 146, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[36] Joon Young Lee et al., "A Secure Multi-factor Remote user Authentication Scheme for Cloud-IOT Applications," *Proceedings of the International Conference on Computer Communication and Networks (ICCCN)*, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[37] Rajeshwari Gadathas Krishna Babu et al., "Authentication and Access Control in Cloud-based Systems," *Proceedings of the Fourteenth International Conference on Ubiquitous and Future Networks (ICUFN)*, 2023. [CrossRef] [Google Scholar] [Publisher Link]