

Enhancing Cloud Data Storage Security Through Multi-Factor Authentication

^{1*} Manchikatla Srikanth, ² Syed Shabbeer Ahmad

¹Research Scholar, Department of CSE, UCE, Osmania University, Hyderabad, India. Email Id: srikanth_m@vnrvjiet.in

² Professor, Department of CSE, MJCET, Hyderabad, India, Email Id: shabbeer.ahmad@mjcollege.ac.in

*Corresponding author: srikanth_m@vnrvjiet.in

Abstract: Cloud multi-factor authentication provides robust security measures to prevent unauthorized access and mitigate the risk of data breaches. Multi-factor authentication enhances the security of cloud applications, data, services, and resources by allowing only legitimate users to access them, hence improving safety for enterprises and convenience for individuals. The security level and architecture of the framework dictate how many authentication factors are needed. Deploying a robust multi-factor authentication system in a cloud platform poses significant challenges. This study introduces an advanced authentication system that incorporates several factors and layers, and includes features such as access control, intrusion detection, and automatic method selection for authentication. Developing a highly secure cloud platform with a minimal number of false positive alerts increases the difficulty for unauthorized individuals to gain access. The cloud user identity verification process is enhanced and false alarms are minimized by combining multiple authentication elements such as length, validity, together with geolocation and browser confirmation. Data that has not been revealed is encrypted using the Advanced Encryption Standard (AES). The cloud directory provider obfuscates login information using AES encryption. The proposed architecture effectively detected and thwarted unauthorized users and intrusions, effectively safeguarding cloud services and data from intentional attacks.

Keywords: Cloud Data security; multi-factor authentication; security challenges

1. Introduction

As the initial line of protection against illegal entry, the authentication technique is one of the most crucial components of the security system [1]. Authentication is the process of confirming a person's identity who is permitted to access a system or device in order to give them permission to use it legally. A legitimate user must provide necessary details during registration, including their email address, password, and username. The process of authentication starts with this. Every single piece of information is kept on the server and is verified multiple times during the login procedure. The most widely used forms of authentication are biometrics [4], Personal Identification Numbers (PIN) [3], and text passwords [2]. Consequently, having a suitable, trustworthy, and robust authentication framework is essential to guaranteeing the security of a system [5].

Single-factor authentication, often known as SFA, is the most common authentication method that users employ and is widely utilized. However, due to the fact that it only offers the most fundamental security protections, SFA is vulnerable to cyberattacks. According to the findings of recent research, it is essential to implement multi-factor authentication (MFA)

to improve the level of security that is associated with the user's access to a variety of systems and applications. Several multi-factor authentication (MFA) frameworks have been proposed as potential solutions to the challenges of assuring authentication security. A single structure is unable to handle all of them, which is a regrettable situation. Because of this, the purpose of this study was to carry out an in-depth analysis of the existing MFA framework as well as the proposed solution.

As a result of its ease of use and scalability, cloud storage has emerged as an essential component of data management and business operations in the modern world. Significant concerns regarding security have been raised as a result of the growing use of Internet of Things devices, particularly with regard to the susceptibility of users' private information to unauthorized access and hacking. There has been a growing demand for robust security in cloud systems, which has led to an increase in concerns over the safety of digital data [1, 2]. This desire has been identified in recent research. Multi-Factor Authentication, also known as MFA, is a potent defensive technique that transcends the limitations of traditional password-based systems. Not only does it

safeguard the cloud, but it also offers protection on every level simultaneously. It is a response to the growing complexity of cyber threats [3], which has led to the development of sophisticated malware and attack methodologies that are utilized by hackers. This strategy is a response to this emerging threat. There is a point of view concerning the linkages in technological growth that may be achieved by connecting cloud-based systems with intelligent malware detection systems located at the edge [4, 5]. The outstanding adaptability of cloud security services is demonstrated by the presentation of the most recent advancements in cybersecurity technologies that have been implemented within the realm of cloud computing. Within the realm of cloud storage, the implementation of multi-factor authentication (MFA) is investigated in this article. In addition to presenting the most recent research and knowledge from cyber security practitioners and academics, it focuses on the challenges and methods involved in adopting MFA. This is done with the intention of supplying the region with information and direction.

2. Related Work

Numerous distinct authentication techniques have been put up as prospective remedies for the problem of inadequate authentication throughout study. There are benefits and drawbacks to every MFA framework that has been created. Leslie Lamport introduced the first remote authentication technology in 1981. It consisted of three parts: an encryption method, a password lookup table, and a one-way hash encryption process. Nonetheless, even though the suggested authentication method is especially user-friendly, handling password databases still necessitates a large hashing capacity as well as an extra storage capacity. Consequently, some studies focus on the use of smart cards as a potential fix for the vulnerabilities that have been discovered. [6] offered a method that combines a third-party app and an intelligent device to perform cloud-based universal sign-on authentication. This approach was given as an illustration. The research literature has offered a variety of smartcard or smart device solutions, particularly [6] and [7].

Despite this, a sizable portion of the recommended authentication techniques call for extra equipment to complete the authentication process. Among other things, this has a biometric scanner and a smart card reader. The second category of authentication techniques is represented by the digitalized method of multi-factor authentication. RSA encryption is a part of the recommended authentication mechanism for the digital signature and One-Time Password (OTP). Moreover, RSA and asymmetric digital signatures are both used by the architecture's second component [8]. The initial configuration, the user registration procedure, and the

authentication verification process are the three main stages that comprise the proposed design. As a result, hardware like a token device, a smart card system card reader, and a physiological biometrics scanner are no longer required with the suggested authentication framework [9].

Concerns about NFC hacking, stolen accounts and devices, unsecured access points, and other security and authentication issues with cloud-based or on-premises systems and applications can be eased by using suitable authentication. It is quite easy for these sorts of attacks to compromise user privacy because the authentication data is stored on a server.

The traditional authentication mechanism, which uses a password and username combination to secure the system, is no longer adequate or dependable when it comes to cloud computing. As a result, the implementation of Two-Factor Authentication, or 2FA, makes sense because it merges the aspect of individual possession with the identifiable information. A phone or smartcard are two instances of these components. The smartcard device adds an additional layer of authentication that helps to improve security.

A framework for two-factor authentication has been established because of previous study on the level of security offered by SFA [2][10][11][12]. The security method known as two-factor authentication, or 2FA, was created to shield users against phishing attempts and password disclosures made without authorization [13]. However, there is now an examination and further research being done on the usage of two-factor authentication (2FA), which limits the device to the secondary authentication protocol [14], [15], and [16]. Compared to single sign-on (SSO) and two-factor authentication (2FA) systems, multi-factor authentication (MFA) and two-factor authentication (MFA) both offer considerable security precautions for the system environment [17].

As a result, a Multi-Factor Authentication (MFA) system protects the system and the data environment. This action was taken to tackle the difficulties that arose in the process of ensuring authentication security. A sequential authentication process is created by combining many authentication procedures with multi-factor authentication (MFA). To establish a link between the user and the previous credentials, MFA required three components:

- Factor of information
- Ownership factor
- Biometric factor

Because of this, the multi-factor authentication (MFA) framework was put into place to strengthen the security measures of a system and simplify the process of continuously protecting computer devices and systems from

unauthorized access. It is important to have a minimum of two authentication techniques that offer possession, knowledge, and uniqueness to construct a multi-factor authentication (MFA) framework [18], [19]. As part of the multi-factor authentication (MFA) framework, the two most common methods of authentication are usernames and passwords, as well as biometrics, which are frequently complemented by other authentication measures [15]. There are three methods of authentication: text passwords, one-time passwords (OTP), and two-factor combinations. that are most frequently used, according to professionals in the industry. The fact that they were suitable for the application's continued development was the primary factor that led to their selection [17].

Furthermore, a variety of sectors, such as cloud computing, cryptography, wireless sensor networks, healthcare and telecare, mobile environments, the multi-factor authentication architecture is essential to cloud computing and remote authentication. Consequently, the multi-factor authentication system improved security by employing a time-based one-time password (TOTP) mechanism [20]. The Time-based One-Time Password (TOTP) system that was being built required both a password and a login at the beginning. Subsequently, the user must possess the MFA token to create a virtual TOTP. It was determined that the suggested authentication mechanism offers a high degree of security for the transactions being conducted.

Single authentication, a crucial security measure that is also user-friendly, is built on a password-based authentication method. Automated Teller Machines (ATMs), Database Management Systems (DBMS), and Personal Digital Assistants (PDAs) all employ password-based authentication techniques. Nevertheless, the password-providing mechanism has two fundamental problems [21]. Initially, database systems save passwords and personal identification numbers (PINs) in their unencrypted, original form. This makes it simple for the administrator to access the PINs and passwords. Additionally, the attacker may pose as a valid user by gaining access to the user ID and password that are stored in the database. The attacker can now access the database as a result of this.

Consequently, MFA is seen as the answer to the several issues that were previously covered. The vulnerabilities that are present in SFA are mitigated by MFA through the utilization of a multi-tiered authentication system. These vulnerabilities include unauthorized entry into trusted devices and modifications to the data architecture. The majority of the previous research on multi-factor authentication (MFA) concentrated on improving authentication technology and

restricting user access control in order to reduce vulnerabilities in a variety of domains.

In spite of this, there is still a lack of clarity on the extent to which technology is being utilized, the degree to which it is user-friendly, and the degree to which it is in accordance with the users' sense of risk [22]. Even though the focus of current research has been on studying novel authentication systems, previous studies have also extensively evaluated the performance of multi-factor authentication (MFA) frameworks that are already in place. There have been studies carried out [23] [24] [25] that have been undertaken about the speed, ease of user activities, and user-side authentication error rates. Nevertheless, the feasibility of high-contact and low-technology approaches continues to provide issues [22].

Only a small fraction of studies, precisely 2.4%, have specifically evaluated the adoption of MFA (Multi-Factor Authentication) in businesses [22]. This is even though the industry is a large provider of jobs and data storage. Due to the data regulations of the sector, the lack of involvement by organizations, and the challenges in recruiting technical professionals, the ramifications for the industry are generally disregarded.

A thorough summary of several studies conducted between 2016 and 2022 is provided in Table 1, which includes the study that specifically looks at the suggested MFA framework.

Table 1 Summary of MFA Frameworks

No	Authentication Method	Author(s), year
1	Text Password	[26]
2	Graphical Password	[27]
3	Biometric	[28] [29]
4	One Time Password (OTP)	[30] [31]
5	Token	[32]
6	Card Reader	[33]
7	Time-based One Time Password (TOTP)	[34]

OBJECTIVES

1. To enhance Cloud Security through Multi-Factor Authentication
2. To develop an Adaptive Authentication Mechanism for Data Security.

3. Proposed Framework

The suggested cloud multi-factor multi-layer authentication system is shown in Figure 1. It consists of three primary layers as well as an embedded layer that encrypts and decrypts user parameters and authorizations.

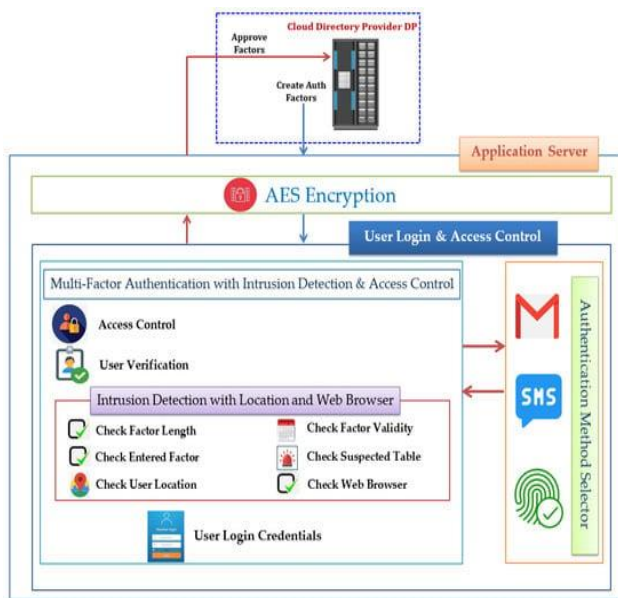


Figure 1 Proposed framework.

Identity and Access Management, or IAM, is a key component of cloud resource access control. User access can be effectively and centrally managed by cloud-based Identity and Access Management (IAM) solutions. Since these systems are scalable, a big number of users and resources can be handled by them. They also offer multi-factor authentication, which requires multiple forms of verification and adds an additional degree of security. They also facilitate single sign-on, which gives users access to numerous programs and services using only one set of login credentials. With the help of this framework, cloud users can register for resources and authenticate with a single identity. Identity tokens, authentication parameters, and user data are managed by directory providers. The choice of user authentication techniques is given top priority in the first layer.

Priority tables provide a clear indication of the most suitable authentication mechanism for user access. Utilize the priority table to incorporate or alter authentication configurations in order to fulfill the organization's requirements. The second layer employs multi-factor authentication settings to identify and monitor user activities on the cloud system or platform. The third layer introduces a strategy for manipulating user behavior based on cloud multi-factor authentication. An additional layer is added to the three existing layers to encrypt user credentials and authentication settings, ensuring the protection of both user data and important data related to cloud computing.

Multi-factor authentication increases the difficulty of gaining system access, even if an intruder manages to steal one of the components used for user authentication [37]. The hacker would also want the user's browser name or geolocation. Implementing several authentication mechanisms can

effectively minimize the occurrence of false alarms inside the framework. Given the limited probability that an intruder can provide all the necessary authentication components. Providing users with their authentication factors upon logging in could potentially enhance the user experience. Subsequently, they can gain entry to the system without having to reenter their verification details. This has the potential to reduce both time and effort. The following are the justifications for constructing the cloud-based architecture that incorporates multiple factors and layers of authentication.




- Improving cloud platform security and reducing the frequency of false alarms.
- To improve system security against unauthorized access, especially when an attacker has obtained one of the components used for user authentication.
- Using a multi-factor authentication method is intended to lower the number of false alarms.
- To enhance the user experience by establishing a single authentication procedure for users at first login, thereby eliminating the need for them to submit their authentication factors many times.
- The framework makes use of several authentication factors, including the user, the suspected table, the user's browser name, geolocation, the length, validity, and value of the authentication factor, and so on.
- To guarantee that only authorized users may access the cloud system, the framework assesses each of these factors.

3.1 Selector for Authentication Methods (AMS)

Predicting user behavior is the main authentication technique used by the AMS. Several authentication techniques can be put into place or changed as necessary to satisfy the company's needs and adhere to legal requirements. While some businesses use security tokens, others use fingerprint authentication. Organizational function, available resources, and the level of sensitivity of the secret data must be considered when selecting a strategy for implementing multi-factor authentication. Administrators of applications can choose and include many forms of authentication. This page includes new features such as fingerprint biometric authentication, security tokens sent by email, and SMS. For the first time, an email will be used for authentication in the event that a user forgets both their login and password for a cloud service. Any subsequent logins to cloud application platforms will need the user to provide additional authentication, such as a fingerprint scan or an SMS, in the event of an email breach. There is a three-step process to choose an authentication method. Past authentication methods, priorities, and statuses are all part of the process. The user can choose email security token, SMS authentication, or fingerprint authentication at the final end.

The last authentication method is requested from the server hosting the cloud database before the user is authenticated. The second step uses a priority table to rank the order of importance for each authentication method. There is a priority number for each approach. An increased number corresponds to an increased significance for the authentication technique, and vice versa. Organizational rules and guidelines could change quickly, affecting this priority. The percentage of usage determines the type of authentication. This percentage is calculated by dividing the total number of authentications by the total number of times each authentication method was used. The organization's security protocols can be followed while modifying the authentication method table priority. The priority-level table can have additional authentication techniques added to it. The recommended authentication mechanism's priority is shown in Table 2.







Table 2 Table of priorities

Method of Authentication	Priority
	3
	2
	1

In the third phase, authentication is defined by looking at the user authentication status. After you choose a method, the first layer of authentication uses email security tokens. The first authentication process is used to add further authentication. Users are able to access cloud services if layer 1 is true. In any case, the subsequent authentication mechanism is SMS. This will be maintained all the way up to the last layer of verification. According to Table 3, the authentication mechanism is determined by the priority table. Among the various authentication methods utilized by *abefi*, 30.77% use fingerprint authentication, 38.46% use email security tokens, and 30% use SMS. The subsequent step is to select either fingerprint or SMS authentication. Due to its higher importance in the priority table than fingerprint authentication, short message service (SMS) will replace it as the next authentication method. Email and SMS security tokens account for 35.71% of *byefb*'s authentication methods, while fingerprint authentication accounts for 30.77%. Next, we'll employ fingerprint authentication, which is the least common method currently in use. If Table 3 shows that the percentage of *abefk* usage is equal, the following

authentication method will select a security token by email using the priority table.

Table 3 Authentication method selection

Method Selector	Authentication Method			Next Auth Method	Priority Reason
User Name					
User _i	5	4	4		Higher Priority
Percentage	38.46%	30.77%	30.77%		
User _j	5	5	4		Lower Usage
Percentage	35.71%	35.71%	28.58%		
User _k	5	5	5		Higher Priority
Percentage	33.33%	33.33%	33.33%		

3.2 Cloud MFA Intrusion Detection Algorithm

An upgraded multi-factor authentication (MFA) architecture and technique for cloud platform intrusion detection are presented in this section. The primary method uses a multi-layered authentication system to confirm cloud users and cut down on false alerts. Moreover, the cloud demands the adoption of many methods for user identity authentication and data protection. Threats to cloud computing apps and settings include data loss, account takeover, malevolent users, and data leaking [38]. The intrusion detection part verifies the identity of suspicious users, looks up suspicious users in a database, and raises an alarm if it detects unusual conduct.

When a user logs into the platform, the cloud database server sends their credentials together with their authentication and rights as a user factor. The suggested approach creates audit and suspect tables. Any fraudulent users attempting to leak cloud data are saved and retrieved from the suspicious table. All user behavior is tracked and audited in the database. The audit table sends a one-time password (OTP) using each of the three accessible authentication methods. For the most effective follow-up mitigation, the audit table logs all user activities on application data and aggregates alarms. All of the people who are thought to have breached privileges are included in the suspected table. The suggested intrusion detection framework uses multi-layer factors, including check factor length, validity, value, and suspected table. Figure 2 shows the four-step method for user authentication. These approaches identify intruders as a supplementary authentication step following AMS. Additional authentication procedures are conducted depending on the browser name and location that the user has logged in order to detect phony users. For later use, the user's location and browser name are stored by the cloud web server. After the initial four phases of multi-factor authentication (MFA) intrusion detection are

finished, the user's preferred browser and geolocation are used for final security validation. The user's account will be blocked and placed to the suspect database if their chosen browser and geolocation do not match.

In summary, the intrusion detection framework employs many authentication elements to ensure system security. In the first four phases, the framework verifies the length, validity, value, and suspicious table of the authentication factor. The user gets validated and granted access to the system once everything has been completed appropriately. The user is blocked and added to the suspicious table if any step fails. The framework also confirms the user's geolocation and browser name during these four steps. Users are banned and put to the suspect database if their browser name and geolocation do not match the system data. The many authentication methods make it more difficult for unauthorized users to access the system. To prevent unwanted access, the framework checks the authentication factor's validity, length, value, suspicious table, geolocation, and browser name.

validity, value, suspicious table, and length. By verifying each of these characteristics, the framework ensures that only authorized users are able to access the system.

Multiple layers of protection are the most effective strategy for protecting systems and data. Because cybercriminals are continuously inventing new vulnerabilities, no security measure can be guaranteed to be foolproof. Attackers and malicious individuals will have a hard time obtaining cloud computing resources due to the multiple ways used. It is best to utilize a combination of strategies when trying to identify hostile users or intruders. It can be more challenging for hackers to acquire and reveal data if user activity is monitored and several authentication mechanisms are used. The needs and risks of your business will determine the best security plan to implement.

Here are some of the most important advantages of using cloud multi-factor authentication.

1. Enhanced security: Even if an attacker manages to steal just one factor, the use of multi-factor authentication will make it far more difficult for them to get access to the system.
2. Reduced false alarms: The framework's use of several authentication factors helps reduce false alerts. Since it is highly improbable that an attacker could supply every component of authentication.
3. Improved user experience: Adding a second layer of security to authentication can improve user experience. since consumers only need to input their authentication factors once. They won't need to reenter their login information after that in order to access the system.
4. Improved security posture: Make your security measures more layered and hence more difficult to penetrate by using a variety of security methods.
5. Reduced risk of data breaches: A Data breaches are less likely when a combination of security measures is used to make it harder for hackers to access your systems and data.
6. Improved compliance: Organizations must use a variety of security measures in accordance with industry laws. There are several methods you may assist your company in following all rules.

Security, false alarms, and user experience can all be enhanced with cloud multi-factor authentication. Security is proved by the use of many research methodologies, and data access is limited. In [87], the authors detailed a novel approach to data access management with fine-grained parameters for healthcare applications built on mobile cloud computing (MCC). With this method, you may manage data access at a finer level while yet maintaining efficiency and scalability. As stated in [39], a new method It is recommended that three-factor authentication and key agreement (CT-AKA) be used for cloud-assisted automobiles. Security risks using cloud-assisted AV are covered in the study's opening section.

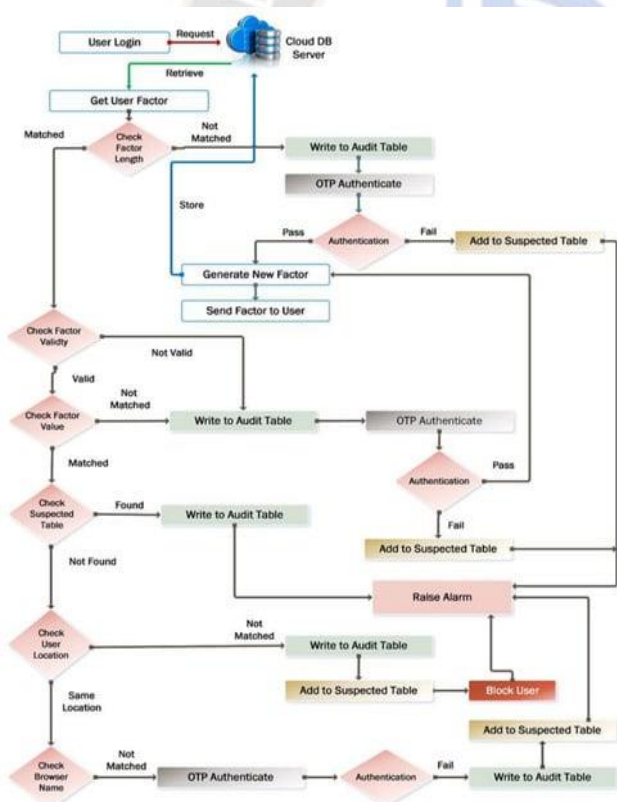


Figure 2 Cloud computing platform MFA layers.

Improved security and fewer false alarms are the results of using multi-factor authentication with cloud systems. It is more difficult to penetrate a system that uses many authentication factors. The abstract's framework employs the following authentication factors: browser name, geolocation,

Among these, safeguarding AV communications, avoiding hostile attacks on AVs, and preserving users' privacy are important. The CT-AKA approach, which incorporates key agreement, fuzzy vault cryptography, and three-factor authentication, is subsequently suggested by the study. Mobile lightweight devices that use three-factor authentication are safe, efficient, and practical, according to [40]. Using extended chaotic maps, the methodology creates random numbers. User identification is checked via the protocol's fuzzy verifier.

4. Threat Model

The abundance of sensitive data and the possibility of victims make cloud computing infrastructures an attractive target for attackers. In addition to being more vulnerable to attacks, complex cloud-computing infrastructures might be more difficult to secure. Failures in multi-factor authentication can occur due to a variety of factors. One of these problems is the faulty opponent characterization, which encompasses the attacker's capabilities, objectives, and the difficulties associated with cryptographic primitive definition. Additionally, MFA frameworks may fail to detect flaws or be too complicated. Eight proof failures are used to analyze the weaknesses in these areas [41].

Protecting mission-critical apps from quantum attacks is the goal of two-factor authentication, as discussed in [42]. To avoid key duplication, the approach employs a smart card that requires authentication via password. These security holes allow an attacker to gain access to sensitive cloud data.

- Data loss: User credentials and authentication settings are susceptible to compromise even though the framework encrypts them. An attacker might use this information to pretend to be a genuine user and get entry to cloud-based resources.
- Hijacking an account: The framework employs several methods to identify anomalous user activity. Once an attacker has access to an account, they could be able to modify cloud resources or go through confidential data.
- Data leakage: Despite the system's best efforts, data leaks are still conceivable. By breaching a cloud provider or taking advantage of a vulnerability in the framework, a malicious actor could potentially steal data.
- Brute force attack: The goal of this attack is to discover a secret key that can be deciphered by trying several keys.
- Monitoring for suspicious activity: To stop the user from harming cloud services, verify suspicious activities and act accordingly.

Risk mitigation is possible with the help of the suggested multi-factor authentication (MFA) layer architecture and algorithm for user behavior authentication:

Making use of robust authentication: User authentication, verification, security, and protection for cloud platform services are all handled by multi-factor authentication, which employs defense-in-depth multi-layers.

- Encrypting data: Strong encryption protects user credentials and authentication settings.
- We have robust security measures in place to stop unwanted access to user information.
- We educate consumers on security habits, including password security and avoiding bogus websites.
- Security Evaluation of the Suggested MFA Framework Finding, evaluating, and fixing security flaws in cloud computing is the job of security analysts. The procedures outline an analysis of security flaws in major cloud infrastructure attacks. Listed below are the steps.

4.1. Determine Your Assets and Weaknesses

To begin examining cloud security, one must first list all cloud resources, such as servers, databases, and storage. The next step, after identifying assets, is to identify vulnerabilities. Here are the key advantages and disadvantages of the cloud platform.

Resources:

- Apps for the cloud;
- Cloud information
- Offered cloud-based services;
- Primary cloud resources.

Deficiencies:

- Unapproved entry.
- Breach of data.
- Use of force in assaults.

4.2. Evaluate Dangers

Next, the hazards associated with the cloud need to be evaluated. This involves identifying potential assailants, as well as their abilities, goals, and objectives. Every potential danger needs to have its probability evaluated. Here are the most significant vulnerabilities and risks related to cloud authentication.

- Poor password security: Common types of authentications, such as passwords, are not safe. Hackers can guess or take credentials using brute-force assaults and password cracking software.
- Phishing attacks, which trick users into divulging personal information like passwords and credit card details by deception. Attackers regularly send emails posing as legitimate businesses or organizations.
- Attacks via malware: Hackers can covertly access a user's device. Malware is one type of threat that may attack, intercept messages, and steal login credentials.

4.3. Examine the Risks

Conducting a risk analysis for the cloud environment comes next, after the identification of assets, vulnerabilities, and threats. By addressing these concerns, we can evaluate the security of any cloud infrastructure.

- **Intricacy:** It should be easy to set up and maintain this cloud infrastructure.
- **Risks to security:** An intrusion detection system should be available within the framework, and it should be able to detect critical security issues.
- **Privacy risks:** Web browser and user location data must be securely protected by the framework.
- **Time:** The time it takes for the framework to execute in order to identify malicious attacks is affected by the complexity of the authentication procedures, the amount of authentication elements, the number of manipulating cloud users, and the performance of the hardware and software.

4.4. Develop MFA

Enhancing cloud risk mitigation is the focus of the third stage. To manage the assessed risks, this study suggests the following framework:

- **Complexity:** While the suggested architecture does include multi-factor authentication with many layers of parameters, the algorithm and framework effectively combine three main levels, one of which is an integrated layer for the encryption and decryption of user parameters and authorizations. The priority of user authentication methods is determined by the first layer. The second layer employs multi-factor authentication settings to identify user activity on cloud systems or platforms. The third layer introduces a method for manipulating user behavior that is based on cloud multi-factor authentication. An additional layer that encrypts authentication settings and user credentials is linked with the three levels to safeguard sensitive data stored in the cloud as well as user data.
- **Security risks:** Intrusion detection vulnerabilities and an authentication method selector (AMS) are presented in the suggested framework. It is possible for the framework to abuse the data it collects from users, which includes information about their location and web browser.
- **Privacy risks:** Location and browser information are among the sensitive user data collected by the proposed system. It is possible to misuse compromised data. Furthermore, the framework may jeopardize privacy by using this data to regulate user behavior. One way to build the framework to protect user privacy is to ensure that it only collects the data that is necessary for its operation. Users must have the option to desist from having their data altered as well.

- **Execution time:** Due to the increasing number of cloud users, the proposed system has a low time complexity despite multiple authentication elements.

Multi-factor authentication (MFA) strengthens the authentication process in cloud computing. This will prevent brute-force, phishing, and password attacks [43].

Cloud computing makes use of a wide variety of MFA techniques. Some typical methods for MFA are as follows.

- **OTPs, or one-time passwords:** One-time passwords are generated by an external device, which could be a hardware token or an app on a smartphone (OTPs).
- **Authentication based on location:** The user's current position is sought for the purpose of location-based authentication. When logging in from a remote location, users of certain cloud services may be required to enter a code that has been delivered to their smartphone.

Security analysis can be used to evaluate cloud MFA deployments [44]. Identifying and reducing security risks is possible with this analysis. When it comes to cloud computing, these are the most important areas for MFA security assessments.

- It is important that authentication elements are robust and secure. Strong one-time passwords and secure one-time passwords are examples.
- The MFA mechanism must be implemented in a secure and appropriate manner. Secure transmission and storage of one-time passwords (OTPs) is essential.
- Manage MFA users and devices securely. Regular password changes and device updates with all available security patches are essential.

The following are only a few of the numerous advantages of the proposed MFA in cloud computing settings.

- **Improved security:** Using MFA makes it more difficult for attackers to access cloud apps and infrastructure.
- **Lower chance of data breaches:** MFA increases the difficulty of obtaining user credentials for attackers, hence reducing the frequency of data breaches.
- **Increased compliance:** MFA implementation is mandated by numerous organizations due to industry-specific legislation.
- **Improved user confidence:** Businesses that show they are protecting their consumers' data are more likely to earn their trust.

The proposed method attempts to reduce false alarms and improve cloud platform security by analyzing user activity and utilizing several authentication factors.

Authentication Algorithm Implementation and Outcomes

- In this case, we outline the user authentication procedure as well as the expected MFA levels for the cloud computing platform. The results, which need altering the MFA layer, are determined by calculating the duration of the multi-factor

layer's execution and the percentages of false-positive and false-negative rates.

4.5. Multi-Factor Authentication Layer Execution Time

Nested layers for multi-factor authentication are now developed and put into use. To track execution time, cloud computing employs six main steps of user verification: factor length checking, factor validity, factor value, suspicious table validation, and user location. Every trial counts the number of users whose execution duration is measured in milliseconds.

The first factor that verifies factor length has an execution time that grows linearly with the number of users, as shown in Figure 3. For 50 users, the execution time was 218 milliseconds, and for 1000 users, it was 278 milliseconds. The factor validity method is checked in 174 milliseconds for 50 users and 196 milliseconds for 100 users. At 200 and 300 users, the execution times were 194 and 193 milliseconds, respectively. This approach takes longer to execute since the variable being verified by user behavior authentication is Boolean in nature.

The check value and suspect table rose linearly when the execution time increased in proportion to the number of users. The check factor value was 186 ms for 50 users, 224 ms for 500 users, and 252 ms for 1000 users. Execution times increased linearly from 50 to 800 users, then decreased to 231 ms for 900 users, and then increased to 243 ms for 1000 users again when the suspect table was examined. From 50 to 500, there was a linear growth in the number of users as well as the rate of location and browser name checks. The length started to get shorter at 500 users, but it later got longer, reaching 263 ms for user location and 237 ms for browser name factors at 1000 users.

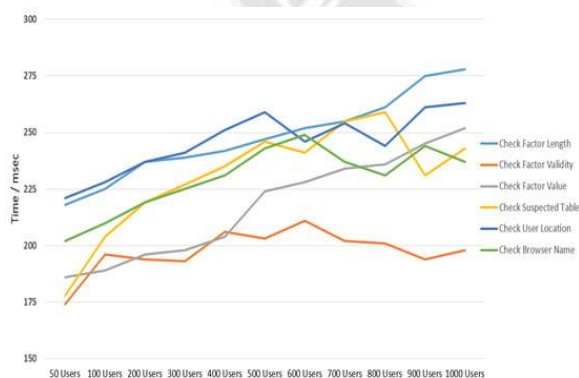


Figure 3 Time-effectiveness of multi-factor authentication levels.

5. Performance of Detection

Detection performance metrics are used by many security applications and strategies, which employ a range of authentication and protection measures, to inform algorithm

efficiency. In this part, we compute the false-positive (FP) and false-negative (FN) rates. The false-positive rate is the proportion of legitimate users who are mistakenly categorized as invaders. The false-negative rate is the proportion of incursions that compromise cloud computing services and expose personal data. As illustrated in Figure 4, there was 2% FP for the locations and browser names of 50 users and 0% for the remaining users.

The FP rate was 1% when factor length and validity were tested on 100 users. Users' browser names and inaccurate location identification are to blame for this. When the user base grew from 50 to 1000, these criteria continued to record the FP alarms. For 500 users, there was no FP for location check, but 0.4% for browser name.

The percentage of false alerts increased from 0.1% to 1% as There were 1000 users instead of just 600. Multiple factor authentication (MFA) techniques are effective and flexible enough to reliably authenticate regular users.

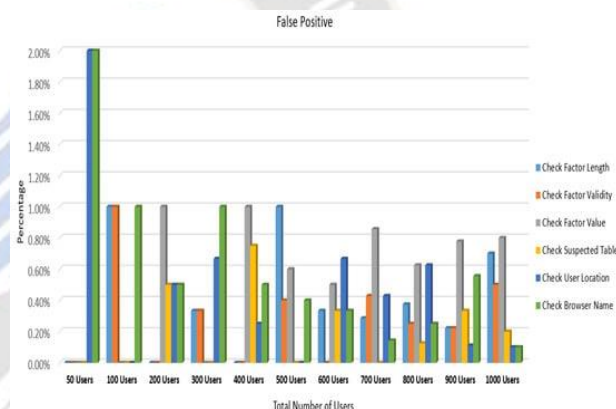


Figure 4 Users of FP on tiers of multi-factor authentication.

The percentage of assaults that reveal secrets of cloud service platforms in the false-negative (FN) category is shown in Figure 5. For fifty users, no MFA method resulted in FN. Factor value and browser name had a 1% FN rate, but suspicious table, user location, factor length, and validity all had a 0% FN rate when 100 users were considered.

For 500 users, MFA had a low FN rate across all authentication factors: 0.4%, 0.2%, 0.8%, 0.2%, and 0.2%. On all authentication criteria, 800 users had low FN rates ranging from 0.63% to 0.75%. Maximum FN rates for browser name check and factor length check in the remaining experiment were 0.78% and 0.7, respectively, for 900 and 1000 participants.

In order to avoid assaults on cloud servers or services, the suggested method and algorithm that use MFA techniques were successful in identifying suspicious users and intruders.

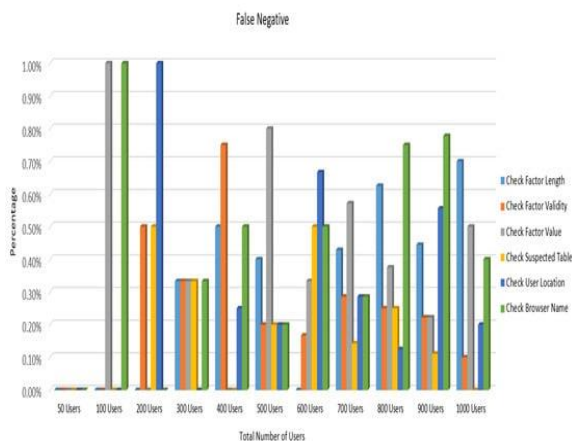


Figure 5 FN users enrolled in multi-factor authentication levels.

Two methods are used to evaluate how well the suggested MFA design and algorithm work to stop attacks: quantitative and qualitative methods. The suggested MFA architecture and algorithm can be assessed using quantitative measures such as rates of false-negative (FN) and false-positive (FP) events.

6. Conclusion

User identity is critical to apps, services, and resources in the cloud. It's handled by PaaS by default. For PaaS authentication to work, security and usability must be balanced. We developed a versatile multi-factor authentication system as part of this study to grant users access to PaaS data and apps. Intrusion detection, multi-factor authentication, access control, and encryption/decryption are all used in the proposed design. Businesses can offer even more protection to their customers by implementing multi-factor authentication. PaaS users don't have to worry about their privacy being violated when using it. An intrusion detection system protects users' identities. There are regulations in place to limit who has access to what and how long. AES-256 encryption is used for all data.

The suggested structure is adaptable thanks to the selection of authentication methods. With AMS, a company may select among several authentication methods. You can use any combination of methods, such as email, SMS, and biometric authentication, and it will still be applicable generally. The proposed design tightens security in six ways: by leveraging the user's geolocation and a browser feature in conjunction with other intrusion detection attributes. We can confirm that the correct user is accessing the correct application with the correct data using the proposed framework. Furthermore, we promise that all information will remain private and undeleted. Results from the experiment indicated the rates of false-positive and false-negative alarms. For different numbers of users, While the false-negative rate dropped, the false-positive rate rose. The system can be enhanced in the

future to include risk-based and adaptive authentication. It is possible to test the framework with additional users and other attack scenarios. For the framework to be truly user-friendly, it needs an intuitive user interface.

References

- [1] Al Harbi, S., Halabi, T. and Bellaiche, M. (2020) "Fog Computing Security Assessment for Device Authentication in the Internet of Things", in Proceedings - 2020 IEEE 22nd International Conference on High Performance Computing and Communications, IEEE 18th International Conference on Smart City and IEEE 6th International Conference on Data Science and Systems, HPCC-SmartCity-DSS. Institute of Electrical and Electronics Engineers Inc., pp. 1219–1224.
- [2] Reese, K., Smith, T., Dutson, J., Armknecht, J., Cameron, J. and Seamons, K. (2019) "A Usability Study of Five Two-Factor Authentication Methods", Fifteenth Symposium on Usable Privacy and Security.
- [3] Guerar, M., Migliardi, M., Palmieri, F., Verderame, L. and Merlo, A. (2020) "Securing PIN-based authentication in smartwatches with just two gestures", Concurrency and Computation: Practice and Experience. John Wiley and Sons Ltd, 32(18).
- [4] Alizadeh, M., Dowlatshah, K., Ahmadzadeh Raji, M. and Nabil Alkhanak, E. (2020) "Coding theory View project User Privacy of Internet of Things View project A secure and robust smart card-based remote user authentication scheme", Article in International Journal of Internet Technology and Secured Transactions, 10(3), pp. 255–267.
- [5] Prabhanjan Yadav, B., Shiva Sai Prasad, C., Padmaja, C., Naik Korra, S. and Sudarshan, E. (2020) "A Coherent and Privacy-Protecting Biometric Authentication Strategy in Cloud Computing", IOP Conf. Series: Materials Science and Engineering, 981.
- [6] Karthigaiveni, M. and Indrani, B. (2019) "An efficient two-factor authentication scheme with key agreement for IoT based E-health care application using smart card", Journal of Ambient Intelligence and Humanized Computing. Springer Verlag.
- [7] Bouchaala, M., Ghazel, C. and Saidane, L. A. (2022) "Enhancing security and efficiency in cloud computing authentication and key agreement scheme based on smart card", Journal of Supercomputing. Springer, 78(1), pp. 497–522
- [8] Sarna, S. and Czerwinski, R. (2022) "Small prime divisors attack and countermeasure against the rsa-otp algorithm", Electronics (Switzerland) MDPI AG. MDPI, 11(1).

- [9] R. Madhusudhan and M. Hegde (2019) "Smart Card Based Remote User Authentication Scheme for Cloud Computing", in IEEE 10th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON), pp. 905–910.
- [10] J. Colnago et al., "'It's Not Actually That Horrible': Exploring Adoption of Two-Factor Authentication at a University," in Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems, 2018, pp. 1–11, doi: 10.1145/3173574.3174030.
- [11] Li, S., Xu, C., Zhang, Y. and Zhou, J. (2022) 'A Secure Two-Factor Authentication Scheme From Password-Protected Hardware Tokens', IEEE Transactions on Information Forensics and Security, 17, pp. 3525–3538.
- [12] M. N. Aman, M. H. Basheer, and B. Sikdar, "Two-Factor Authentication for IoT With Location Information," IEEE Internet Things J., vol. 6, no. 2, pp. 3335–3351, 2019, doi: 10.1109/IJOT.2018.2882610.
- [13] T. Petsas, G. Tsirantonakis, E. Athanasopoulos, and S. Ioannidis, "TwoFactor Authentication: Is the World Ready? Quantifying 2FA Adoption," 2015, doi: 10.1145/2751323.2751327.
- [14] Ometov, A., Bezzateev, S., Mäkitalo, N., Andreev, S., Mikkonen, T. and Koucheryavy, Y. (2018) 'Multi-Factor Authentication: A Survey', in Cryptography, pp. 1–31.
- [15] Velásquez, I. (2021) 'Framework for the Comparison and Selection of Schemes for Multi-Factor Authentication', in CLEI ELECTRONIC JOURNAL.
- [16] B. W. Kwon, P. K. Sharma, and J. H. Park, "CCTV-based multi-factor authentication system," J. Inf. Process. Syst., vol. 15, no. 4, pp. 904–919, 2019, doi: 10.3745/JIPS.03.0127.
- [17] Velásquez, I., Caro, A. and Rodríguez, A. (2018) 'Authentication schemes and methods: A systematic literature review', Information and Software Technology. Elsevier, 94, pp. 30–37.
- [18] Singh, C. and Singh, T. (2019) 'A 3-Level Multi-factor Authentication Scheme for Cloud Computing', International Journal of Computer Engineering & Technology (IJCET), 10(1), pp. 184–195.
- [19] Karie, N. M., Kebande, V. R., Ikuesan, R. A., Sookhak, M. and Venter, H. S. (2020) 'Hardening SAML by Integrating SSO and Multi-Factor Authentication (MFA) in the Cloud', PervasiveHealth: Pervasive Computing Technologies for Healthcare. ICST.
- [20] Taher, K. A. , Nahar, T. , and Hossain, S. A. , (2019) 'Enhanced Cryptocurrency Security by Time-Based Token Multi-Factor Authentication Algorithm', in International Conference on Robotics,Electrical and Signal Processing Techniques (ICREST). IEEE, pp. 308–312.
- [21] Rajasekar, V., Jayapaul, P., Krishnamoorthi, S. and Saračević, M. (2021) Secure Remote User Authentication Scheme on Health Care, IoT and Cloud Applications: A Multi-layer Systematic Survey, Acta Polytechnica Hungarica.
- [22] Das, S., Wang, B., Tingle, Z. and Camp, L. J. (2019) Evaluating User Perception of Multi-Factor Authentication A Systematic Review.
- [23] Xiong, W., Zhou, F., Wang, R., Lan, R., Sun, X. and Luo, X. (2018) 'An Efficient and Secure Two-Factor Password Authentication Scheme with Card Reader (Terminal) Verification', IEEE Access. Institute of Electrical and Electronics Engineers Inc., 6, pp. 70707–70719.
- [24] Nag, S., Chiat, S., Torgerson, C. & Snowling, M. J. (2014).Literacy, foundation learning and assess-ment in developing countries: final report. (London, EPPI-Centre, Social Science Research Unit,University of London)
- [25] Abo-Zahhad, Mohammed, Sabah M. Ahmed, and Sherif N. Abbas. "A new multi-level approach to EEG based human authentication using eye blinking." Pattern Recognition Letters 82 (2016): 216-225.
- [26] Bong, J., Suh, Y. and Shin, Y. (2016) 'Fast user authentication method considering mobility in multi clouds', in 2016 International Conference on Information Networking (ICOIN), pp. 445–448.
- [27] Meng, W., Zhu, L., Li, W., Han, J. and Li, Y. (2019) Enhancing the security of FinTech applications with map-based graphical password authentication, Future Generation Computing Systems.
- [28] Neha and Chatterjee, K. (2019) 'Biometric re-authentication: an approach towards achieving transparency in user authentication', Multimedia Tools and Applications. Springer New York LLC, 78(6), pp. 6679–6700.
- [29] Prabhu, D., S. Vijay Bhanu, and S. Suthir. "Privacy preserving steganography based biometric authentication system for cloud computing environment." Measurement: Sensors 24 (2022): 100511.
- [30] Ma, S., Feng, R., Li, J., Liu, Y., Nepal, S., Ostry, D., Bertino, E., Deng, R. H., Ma, Z. and Jha, S. (2019) 'An empirical study of SMS one-time password authentication in android apps', in ACM International Conference Proceeding Series. Association for Computing Machinery, pp. 339–354.
- [31] Gosavi, S. S., & Shyam, G. K. (2021). A novel approach of OTP generation using time-based OTP and randomization techniques. In Data Science and

- Security: Proceedings of IDSCS 2020 (pp. 159-167). Springer.
- [32] Li, S., Xu, C., Zhang, Y. and Zhou, J. (2022) 'A Secure Two-Factor Authentication Scheme From Password-Protected Hardware Tokens', *IEEE Transactions on Information Forensics and Security*, 17, pp. 3525–3538.
- [33] Xiong, W., Zhou, F., Wang, R., Lan, R., Sun, X. and Luo, X. (2018) 'An Efficient and Secure Two-Factor Password Authentication Scheme with Card Reader (Terminal) Verification', *IEEE Access. Institute of Electrical and Electronics Engineers Inc.*, 6, pp. 70707–70719.
- [34] V. A. Cunha, D. Corujo, J. P. Barraca, and R. L. Aguiar, "TOTP Moving Target Defense for sensitive network services," *Pervasive Mob. Comput.*, vol. 74, pp. 0–18, 2021, doi: 10.1016/j.pmcj.2021.101412.
- [35] Kitchenham, B., Pretorius, R., Budgen, D., Brereton, O. P., Turner, M., Niazi, M., & Linkman, S. (2010). Systematic literature reviews in software engineering—a tertiary study. *Information and software technology*, 52(8), 792-805.
- [36] Hafiza Razami, H. and Ibrahim, R. (2022) 'Models and constructs to predict students' digital educational games acceptance: A systematic literature review', *Telematics and Informatics*. Elsevier Ltd, 73.
- [37] Wang, D.; Wang, P.; Wang, C. Efficient multi-factor user authentication protocol with forward secrecy for real-time data access in WSNs. *ACM Trans. Cyber-Physical Syst.* 2020, 1, 1–25.
- [38] Alsirhani, A.; Ezz, M.; Mostafa, A.M. advanced authentication mechanisms for identity and access management in cloud computing. *Comp. Syst. Sci. Eng.* 2022, 43, 967–984.
- [39] Jiang, Q.; Zhang, N.; Ni, J.; Ma, J.; Ma, X.; Choo, K. Unified biometric privacy preserving three-factor authentication and key agreement for cloud-assisted autonomous vehicles. *IEEE Trans. Veh. Technol.* 2020, 69, 9390–9401
- [40] Qui, S.; Wang, D.; Xu, G.; Kumari, S. Practical and provably secure three-factor authentication protocol based on extended chaotic maps for mobile lightweight devices. *IEEE Trans. Dependable Secur. Comp.* 2022, 20, 1338–1351.
- [41] Wang, Q.; Wang, D. Understanding failures in security proofs of multi-factor authentication for mobile devices. *IEEE Trans. Infor. Forensics Secur.* 2022, 18, 597–612.
- [42] Wang, Q.; Wang, D.; Cheng, C.; He, D. Quantum2FA: Efficient quantum-resistant two-factor authentication scheme for mobile devices. *IEEE Trans. Dependable Secur. Comp.* 2021, 20, 193–208.
- [43] Kaur, S.; Kaur, G.; Shabaz, M. A Secure two-factor authentication framework in cloud computing. *Secur. Commun. Netw.* 2022, 2022, 7540891.
- [44] Otta, S.; Panda, S.; Gupta, M.; Hota, C. A Systematic survey of multi-factor authentication for cloud infrastructure. *Future Internet MDPI* 2023, 15, 146.