

Article

Strengthening Cloud Security: An Innovative Multi-Factor Multi-Layer Authentication Framework for Cloud User Authentication

Ayman Mohamed Mostafa ^{1,*}, Mohamed Ezz ², Murtada K. Elbashir ¹, Meshrif Alruily ², Eslam Hamouda ², Mohamed Alsarhani ² and Wael Said ^{3,4}

¹ Department of Information Systems, College of Computer and Information Sciences, Jouf University, Sakaka 72388, Saudi Arabia; mkelfaki@ju.edu.sa

² Department of Computer Science, College of Computer and Information Sciences, Jouf University, Sakaka 72388, Saudi Arabia; maismail@ju.edu.sa (M.E.); mfalruily@ju.edu.sa (M.A.); efhamouda@ju.edu.sa (E.H.); 431100004@ju.edu.sa (M.A.)

³ Computer Science Department, Faculty of Computers and Informatics, Zagazig University, Zagazig 44511, Egypt; wmmohamed@taibahu.edu.sa

⁴ Computer Science Department, College of Computer Science and Engineering, Taibah University, Medina 42353, Saudi Arabia

* Correspondence: amhassane@ju.edu.sa

Abstract: Cloud multi-factor authentication is a critical security measure that helps strengthen cloud security from unauthorized access and data breaches. Multi-factor authentication verifies that authentic cloud users are only authorized to access cloud apps, data, services, and resources, making it more secure for enterprises and less inconvenient for users. The number of authentication factors varies based on the security framework's architecture and the required security level. Therefore, implementing a secured multi-factor authentication framework in a cloud platform is a challenging process. In this paper, we developed an adaptive multi-factor multi-layer authentication framework that embeds an access control and intrusion detection mechanisms with an automated selection of authentication methods. The core objective is to enhance a secured cloud platform with low false positive alarms that makes it more difficult for intruders to access the cloud system. To enhance the authentication mechanism and reduce false alarms, multiple authentication factors that include the length, validity, and value of the user factor is implemented with a user's geolocation and user's browser confirmation method that increase the identity verification of cloud users. An additional AES-based encryption component is applied to data, which are protected from being disclosed. The AES encryption mechanism is implemented to conceal the login information on the directory provider of the cloud. The proposed framework demonstrated excellent performance in identifying potentially malicious users and intruders, thereby effectively preventing any intentional attacks on the cloud services and data.

Keywords: cloud authentication; multi-factor authentication; authentication factors; cloud intrusion detection; user behavior



Citation: Mostafa, A.M.; Ezz, M.; Elbashir, M.K.; Alruily, M.; Hamouda, E.; Alsarhani, M.; Said, W. Strengthening Cloud Security: An Innovative Multi-Factor Multi-Layer Authentication Framework for Cloud User Authentication. *Appl. Sci.* **2023**, *13*, 10871. <https://doi.org/10.3390/app131910871>

Academic Editors: Liangyin Chen, Pengpeng Chen and Yanru Chen

Received: 3 September 2023

Revised: 25 September 2023

Accepted: 28 September 2023

Published: 30 September 2023



Copyright: © 2023 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

Cloud authentication verifies user identities across a cloud platform to determine whether the user is trusted to access cloud applications, data, services, and resources by ensuring access rights and privileges. The lack of strong and appropriate cloud authentication techniques leads to the occurrence of some cloud security threats and attacks. Some of the most common cloud threats are information disclosure, Denial-of-Service (DoS), spoofing identity, data tampering, repudiation, account hijacking, and the elevation of privilege [1,2]. Cloud-based authentication attacks include DoS attacks, Man-in-the-Middle (MITM) attacks, Replay attacks, Cloud Malware Injection attacks, Password Discovery

attacks, Reflection attacks, Customer Fraud attacks, Insider attacks, and Known Session-Specific Temporary Information (KSSTI) attacks [3,4].

Indeed, various possible authentication techniques are the first barrier of defense against various attacks that prevent unauthorized access to applications, data, services, and resources. Some such techniques include password-based authentication, Single Sign-On (SSO) [5], token authentication, graphical password authentication, biometric authentication, third-party authentication [6], certificate-based authentication [7], digital device authentication, two-factor authentication, and multi-factor authentication (MFA) [8–10]. More recently, organizations have implemented and used MFA in cloud applications to increase security and productivity, reduce the risk of compromised passwords, improve regulatory compliance, and enable enterprise mobility [11].

MFA in cloud computing primarily relies on electronic or digital authentication techniques in which a cloud user is allowed to access either data, application, service, or resource only after two or more factors have been successfully submitted [12]. In the literature, these factors are categorized into knowledge factors, possession factors, inheritance factors, location factors, time factors, behavior factors, processing factors, and personal knowledge factors [13]. The knowledge factors are the already known things such as the personal identification number (PIN), password, security question, one-time code, and passphrase. The possession factors, referred to also as token-based factors, are the owned things such as identity cards, SIM cards, memory cards, smartcards, Fast Identity Online (FIDO) security keys, one-time password tokens, and smartphones with an OTP app. The inheritance factors are the integral elements of a person in the form of biometric data such as iris scans, fingerprint scans, and voice recognition. The location factors are those factors that determine where a person is supposed to be located, such as IP addresses and MAC addresses. Time factors are those factors that are used to detect the presence of a person at a scheduled time of day or within a scheduled time interval. The behavior factors are the actions by which a person can be identified and authorized, such as keystroke rhythm, gait, and mouse usage [11,14]. Processing factors are factors that depend on the level of human perception to perform or memorize a mathematical or logical operation. Personal knowledge factors are implemented based on a person's social relationships by asking someone how much they know the person being asked for validation. When using MFA, in case one factor is compromised by an unauthorized user, the chances of another factor being compromised are low. Therefore, MFA represents a higher degree of assurance about a user's identity. Further information regarding the convenience and importance of MFA for ensuring secure access to the cloud can be found in [15]. In this paper, we proposed a multi-factor multi-layer authentication framework with a variety of user authentication choices to achieve the following contributions.

1. Providing a concise survey that clarifies the existence of various cloud MFA authentication techniques using multiple numbers of factors.
2. Proposing a multi-factor multi-layer authentication framework for the cloud computing environment.
3. Proposing the authentication method selector (AMS) technique for improving the authentication process by selecting the appropriate authentication method based on user behavior.
4. Providing interactive response to users' behaviors based on users' location and default used web browser information for increasing and enforcing the intrusion detection security steps.
5. Obtaining experimental results to demonstrate and validate the performance of the proposed framework.

The rest of this paper can be browsed as follows: a literature review of different numbers of MFA factors and techniques in cloud-based environments is discussed in Section 2. The proposed cloud multi-factor multi-layer authentication framework is presented in Section 3. Section 4 provides a threat model for a set of security issues to evaluate the proposed authentication framework. Section 5 provides a security analysis for the proposed

MFA model to explore the major assets and vulnerabilities, and explore how to mitigate these threats by developing MFA. The implementation and results of the authentication algorithm are provided in Section 6. The conclusions are outlined in Section 7.

2. Literature Review

Unauthorized access is one of the most common cloud application security threats. The MFA method, one of the most popular methods of authenticating cloud users, is used to minimize the risk of unauthorized access to cloud applications, data, services, and resources. In MFA, the number of authentication factors varies according to the design of security frameworks and the level of security requirements. Indeed, MFA provides more secure access to organizations and less inconvenience to users. According to our survey of authentication methods in the literature, there are three levels of authentication factors: single-factor authentication (SFA), two-factor authentication (2FA), and multi-factor authentication (MFA). SFA uses a single factor to authenticate a user, while 2FA uses two factors [16–18], and MFA uses three or more factors. In general, the more factors that are used, the more secure the authentication scheme will be. MFA is becoming increasingly common as organizations look to improve the security of their systems [19–22].

In zero-factor authentication, there is no requirement for the user to take any action, as it relies upon user signals and user passive biometric behavior. Device, network, and location signals are all examples of user signals. By multi-factor, we mean using two or more factors. According to existing research articles, MFA could be categorized as two-factor authentication (2FA or TFA) [23–25], three-factor authentication (3FA) [26], four-factor authentication (4FA or FFA) [27–30], and five-factor authentication (5FA) [31].

The primary study areas for MFA are mutual authentication, biometric authentication, transaction authentication, multi-factor protocol authentication, multi-factor user behavior authentication, and graphical password authentication. Furthermore, new recent research trends in MFA are emerging on the horizon. These trends include blockchain-based multi-factor authentication [32,33], password-less multi-factor authentication [34], and machine/deep learning-based multi-factor authentication [35,36]. In this paper, we applied multi-factor remote user behavior authentication for cloud computing environments.

In [37], a bibliometric survey was performed based on Web of Science data for research publications on the topic of MFA. Furthermore, we summarize the use of MFA through a different number of factors for cloud computing environments in Table 1. These cloud-based environments include general cloud computing architecture [38–41], cloud storage [42–45], multi-cloud [46], cloud-based logistics information systems [47], cloud-based OTP services [48], multiple-agent cloud-based search engines [49], cloud health care [50,51], financial transactions [52], private cloud [53], and cloud-based web services [54]. Other non-cloud environments include cryptocurrency [55], websites and mobile apps [56], electronic payments [57,58], electronic voting systems [59–62], mobile voting systems [63], wireless networks [64], non-internet based applications [65], electronic document management systems [66], IoT networks [67–69], RFID infrastructure [70], wearable and virtual reality (VR) platforms with a gesture input interface [71], ATM systems [72], public multi-touch displays [73], blockchain [74], attendance record management systems (ARMSs) [75], question-based authentication systems [76], the Internet of Medical Things (IoMT) [77], human-computer interaction (HCI) [78], ATM transactions [79], and electronic healthcare systems [80].

Table 1. MFA different number of factors and techniques in cloud-based environments.

Ref.	Authentication Technique	Security Factors	Factor Classification	Environment
[38]	MFA + SHA 1 + AES-128-CBC	Encrypted Password, OTP based on OOB, Email Account, Mobile Number, Count of mouse clicks	SYK + SYH	Cloud Computing
[39]	MFA	PIN/Password, Biometrics, SMS OTP	SYH + SYA	Cloud Computing
[40]	MFA	Username-Password, Email Account, Mobile Number, PIN, OTP	SYK + SYH	Cloud Computing
[41]	MFA	Secret-splitting key, OTP, IMEI number	SYH	Cloud Computing
[42]	MFA + CP-ABE	Username—Password, QR Code-based OTP	SYK + SYH	Private Cloud Storage
[43]	MFA + CP-ABE	Username—Password, QR Code-based OTP	SYK + SYH	Private Cloud Storage
[44]	MFA + VGG face model	Username—Password, Security Questions, Mobile OTP, Face image	SYK + SYH + SYA	Cloud Storage
[45]	MFA	Username—Password, OTP, Fingerprints	SYK + SYH + SYA	Cloud Storage in Smart Banking
[46]	MFA + SSO	SMS OTP, Call on Phone, App approval	SYH	User's Metadata in a Multi-Cloud
[47]	MFA	Face Verification, NFC Card Authentication, Geofence Location, Temporal Data Verification	SYH + SYA	Cloud-based Logistics IS
[48]	2FA + PSK	Username—Password, OTP	SYK + SYH	Cloud-based OTP Services
[49]	MFA	Username—Password, Secret key to AES technique, Biometrics	SYK + SYH + SYA	Multiple Agents Cloud-based Search Engine
[50]	MFA + RSA + Hash Func	Contextual, Sign encryption, Iris Biometric	SYH + SYA	Cloud Health Care
[51]	MFA + Hash Func	Username and Password, Biometrics, Timestamp, Random number nonce	SYK + SYH + SYA	Cloud-based SDN Health Care
[52]	MFA + ECC	Username and Low Entropy, Password, Fingerprints, Voice print, IMSI identity	SYK + SYH + SYA	Cloud-based Financial Transactions
[53]	2FA	Username and Password, TOTP	SYK + SYH	Private Cloud
[54]	2FA	OTP, IoT Token	SYH	Cloud-based Web Services

As presented in [81], CMAF-IIoT is built on the ASCON authenticated encryption (AE) system, which combines encryption and decryption with authentication to provide secrecy, integrity, and authenticity. As a result, designing an authentication framework requires fewer cryptographic procedures. As presented in [82], ESCI-AKA was applied using a Scyther tool with the use of a random oracle model and informal security analysis. Furthermore, the analysis of ESCI-AKA and other renowned security systems demonstrates that it has minimal computational and communication overhead, while offering strong security issues. As presented in Table 1, a variety of authentication techniques and factors that can be used to protect accounts and data are presented. Some of the most common techniques include multi-factor authentication (MFA), which requires users to provide two or more factors to authenticate, and encryption, which can protect data from unauthorized access.

The factors used for authentication can be divided into three classes: something you know, something you have, and something you are. Something you know (SYK) could be a password, PIN, or secret question. Something you have (SYH) could be a physical object, such as a security key or smartphone, or a digital object, such as a one-time password (OTP). Something you are (SYA) could be a biometric factor, such as a fingerprint or facial scan.

The environment in which authentication takes place can also be a factor. Some of the environments mentioned in the table include cloud computing, private cloud storage, cloud storage in smart banking, users' metadata in a multi-cloud, cloud-based logistics IS, cloud-based OTP services, multiple agents cloud-based search engines, cloud health care, cloud-based SDN health care, and cloud-based financial transactions.

MFA is especially important in cloud computing, where data and applications are often hosted by third-party providers. When using MFA, cloud environment can reduce the risk of unauthorized access to their cloud resources, even if an attacker is able to obtain a user's password. Organizations can choose to implement MFA for all cloud users or only users, such as those with access to sensitive data. MFA can be implemented at the cloud provider level or at the application level. Some of the benefits of using MFA in cloud computing are presented as follows.

- Reduced risk of data breaches: MFA makes it much more difficult for attackers to gain access to cloud resources, even if they have compromised a user's password.
- Improved compliance: Many industry regulations require organizations to implement MFA for certain types of data and applications.
- Enhanced user experience: MFA can be implemented in a way that is convenient for users, such as by using push notifications or smartphone apps.

Therefore, MFA is an essential security measure for cloud computing environments. When using MFA, the risk of data breaches will reduce, improve compliance, and enhance the user experience.

According to our survey, the MFA either used as 2FA, 3FA, or more. It is used either beside other techniques such as cipher text-policy attribute-based encryption (CP-ABE) [42,43], SSO [46], RSA algorithm and hash functions [50], SHA 1 and AES-128-CBC [38], AES 256 [74], pre-shared secret keys (PSK) [48], deep learning and leap motion controllers [83], enhanced Feistel block ciphers [59,60], Blockchain [61,63,65], VGG face models [44], CNN-LSTM-based classifiers, [70], and semantic ambient media frameworks (SAMF), which is an authoritative interface between smartphones and public displays [73]. A different number of factors are used, ranging from two to five. The most used factors are Username and Password, OTP, and Biometrics of the user. These biometrics include fingerprints, face verification, and iris. Other factors include location confirmation and temporal data confirmation [47], security questions [65], graphical passwords [67,68], motion signals of in-air-handwriting [71], the geometry of the hand skeleton [71], keystroke rhythm [72], hand gestures [83], and image recognition with user-established relations [84].

In this paper, we proposed an interactive, flexible, and secure multi-factor multi-layer authentication framework by designing an authentication method selector (AMS) and interactive intrusion detection steps. AMS is based on a pool that contains a variety of authentication techniques and knowledge of previous user authentication information. Depending on the needs of the organization, the administrator will be able to add the proper authentication mechanism. The administrator will select an authentication method from the pool and activate it in accordance with these specifications. The proposed framework provides interactive intrusion detection steps via the inspection of user behavior based on the user's previously used location and web browser. This framework provides a flexible and inexpensive authentication method based on the AMS technique and intrusion detection systems.

3. Proposed Framework for Cloud Multi-Factor Multi-Layer Authentication

As presented in Figure 1, the proposed cloud multi-factor multi-layer authentication framework is based on three main layers with an additional embedded layer for encrypting and decrypting user parameters and authorizations.

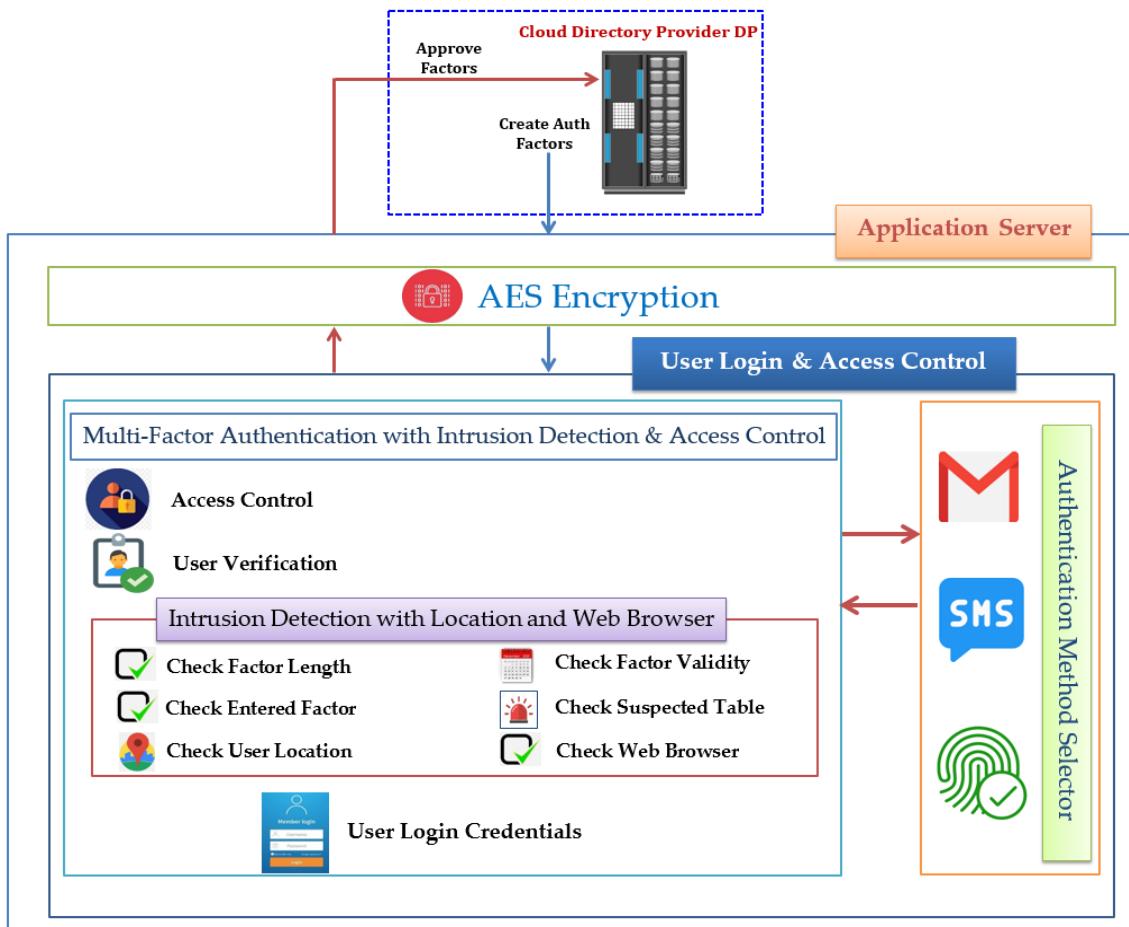


Figure 1. Proposed cloud multi-factor authentication framework.

Using IAM is considered a central solution for managing user access to cloud resources. Cloud-based IAM solutions can provide a centralized and scalable way to manage user access, and can support features such as multi-factor authentication and single sign-on. This framework provides a single sign-on (SSO) solution for cloud users, allowing them to authenticate and register for cloud resources using a single identity. The central authority for maintaining user data, producing authentication parameters, and producing identity tokens within the system is a directory provider (DP). The first layer is based on the selection of authentication methods for users based on different priority parameters. The authentication methods are selected based on a priority table that recommends the next appropriate method for user access. By using the priority table, different authentication parameters can be added or modified to the requirements of the organization. The second layer is based on detecting user behavior on the cloud system or platform using different multi-factor authentication parameters. The third layer proposes an algorithm for manipulating the behavior of users based on defined cloud multi-factor authentication methods. The three layers are connected to an additional layer for encrypting user credentials and authentication parameters to prevent any probable disclosure of user information and cloud computing sensitive data.

Multi-factor authentication makes it more difficult for intruders to gain access to the system, even if they have stolen one of the user's authentication factors [85]. This is because the intruder would also need to have access to the user's other authentication factors, such as their geolocation or browser name. By using multiple authentication factors, the framework can help to reduce the number of false alarms. This is because it is less likely that an intruder will be able to provide all of the required authentication factors. The user experience can be also improved provide their authentication factors once, when they first log in to the system. After that, they can access the system without having to provide their authentication factors again. This can save users time and hassle. The rationales for designing the cloud multi-factor multi-layer authentication framework are as follows.

- To enhance the security of cloud platforms and reduce false alarms.
- To make it more difficult for intruders to gain access to the system, even if they have stolen one of the user's authentication factors.
- To reduce the number of false alarms by using multiple authentication factors.
- To improve the user experience by only requiring users to provide their authentication factors once, when they first log in to the system.

The framework uses a variety of authentication factors:

- The length, validity, and value of the authentication factor;
- The suspected table;
- The user's geolocation;
- The user's browser name.

By checking all of these factors, the framework can help to verify that only authorized users can access the cloud system.

3.1. Authentication Method Selector (AMS)

The AMS manages the authentication technique to be applied primarily to user behavior prediction. Various authentication techniques can be used or added according to business needs and according to the regulations of the organization. Some organizations can provide fingerprint authentication, while others can provide security tokens. The selection process for any technique depends on the role of the organization, the tools available, and the sensitivity degree through which different multi-factor methods are adapted and applied to secure confidential data. The application administrators are responsible for adding and choosing the authentication techniques used. This paper provides additional authentication methods like SMS, security token via email, and biometric authentication using fingerprint. Assume a $user_k$ wants to access the cloud application and forget her/his username-password credentials, s/he will be authenticated using her/his email for the first time of authentication. For the next login process on the cloud application platform, s/he must be authenticated using a different method like SMS or fingerprint authentication to ensure the user's identity in case of email disclosure. The process of selecting an authentication method is based on three main steps. These steps are the user's last authentication method, authentication method priority, and the authentication process status.

In the user's last authentication method step, three methods of authentication are selected: security token via email, SMS, and fingerprint authentication. Before authenticating the user, a request is directed to the cloud database server to obtain the last authentication method that was used in the last authentication process. The second step defines the applied authentication method, where a priority table is defined to determine the usage priority for each authentication method. Each method is assigned a number that defines its priority. The priority of the authentication mechanism increases with the number, and vice versa. Changes to the requirements and organizational regulations can easily be made to this priority. The authentication method is selected depending on the percentage of usage. This percentage is calculated by dividing the number of usage times of each authentication method by the sum of all authentication times. The priority in the authentication method table can be changed according to the security measures of the organization. Further-

more, additional authentication methods can be added to the priority-level table. Table 2 represents the priority table for the proposed authentication method.

Table 2. Priority-level table.

Authentication Method	Priority
	3
	2
	1

The third step for defining the authentication is implemented by using the status step for the user authentication process. After selecting the authentication method, the first authentication layer using security token via email is applied. Based on the result of the first authentication process, an additional authentication layer is added. If the first layer is true, the user will be authentic and will have the privileges to access cloud services. Otherwise, the SMS is selected to be the next authentication method. The mechanism will continue until the last layer of authentication.

As shown in Table 3, the selection of the authentication method is based on the importance of the method in the priority table. Based the authentication methods applied to $user_i$, the security token via email have 38.46% while the SMS and fingerprint authentication both have percentage usage of 30.77%. Therefore, the next authentication method will be selected between SMS and fingerprint authentication. Due to the high priority of SMS over fingerprint authentication based on the priority table, the next authentication method will be SMS. The authentication method for $user_j$ contains 35.71% for both security tokens via email and SMS, while fingerprint authentication has 30.77% usage. Therefore, the next authentication method will apply fingerprint, as it contains the lowest percentage of usage. If the $user_k$ has equal usage percentage as explained in Table 3, the next authentication method will apply the priority table to select a security token via email as an authentication method.

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 Algorithm for Intrusion Detection

In this section, an enhanced MFA framework and algorithm for detecting intrusions in cloud platforms are implemented. The main methodology is based on applying different layers of authentications to verify cloud users and reduce false alarms. Furthermore, different methods must be applied to check cloud user identity and maintain the secrecy of

data. The key threats in different cloud computing applications and environments include data loss, hijacking of accounts, malicious users, and leakage of data [86]. The intrusion detection element is responsible for verifying user validity, checking a suspected table that contains pre-detected suspicious users, and issuing an alert as soon as suspicious user activities are discovered.

When a $user_x$ logs in to the cloud platform using her/his credentials, the cloud database server sends a user factor that contains the authentications and privileges of the user to the cloud. In the proposed framework, an audit table and a suspected table are created. The audit table is applied for verifying users whether are authentic or not, and records all user actions, while the suspected table stores and retrieves malicious users who try to disclose confidential information from the cloud. The audit table sends a one-time pad (OTP) key using one of the three authentication methods that have been proposed in the authentication method selector (AMS). The audit table is responsible for recording all user actions performed on the application data and summarizing all raised alerts for the users to maximize the rate of future countermeasures. The suspected table archives all suspected users who have violated the granted privileges.

As presented in Figure 2, the proposed intrusion detection framework is based on multi-layer factors for authenticating users based on four subsequent steps: check factor length, check factor validity, check factor value, and check suspected table. These steps are used to identify intruders and work as a second level of authentication after the AMS methodology. Additional authentication steps are added to complete the process of identifying the intruders based on the stored location of the user and the browser name. The geolocation of the user is stored for the next time the user accesses the cloud application, while the user's web browser name is added and stored in the cloud web server. The MFA intrusion detection steps start with the first four steps, and if all steps are successfully passed, the user geolocation and user's default browser are checked as final security confirmation. If both user's geolocation and the default browser are different, the user account is blocked and the user is added to the suspected table.

To summarize the authentication factors, the intrusion detection framework described in the text uses a variety of authentication factors to maintain the system security. The first four steps of the framework check the length, validity, value, and suspected table of the authentication factor. If all of these steps are passed, the user is authenticated and allowed access to the system. However, if any of the steps fail, the user is blocked and added to the suspected table. In addition to these four steps, the framework also verifies the user's geolocation and browser name. If the user's geolocation and browser name do not match the values stored in the system, the user is blocked and added to the suspected table. The use of multiple authentication factors makes it more difficult for intruders to access to the system. By checking the length, validity, value, suspected table, geolocation, and browser name of the authentication factor, the framework can help to maintain that only authorized users can access the system.

The objective of integrating multi-factor authentication methods on cloud is to enhance the security of cloud platforms and reduce false alarms. By using multiple authentication factors, it is more difficult for intruders to violate the system. The framework described in the abstract uses a variety of authentication factors, including the length, validity, value, suspected table, geolocation, and browser name of the authentication factor. By checking all of these factors, the framework can help to maintain that only authorized users can access the system.

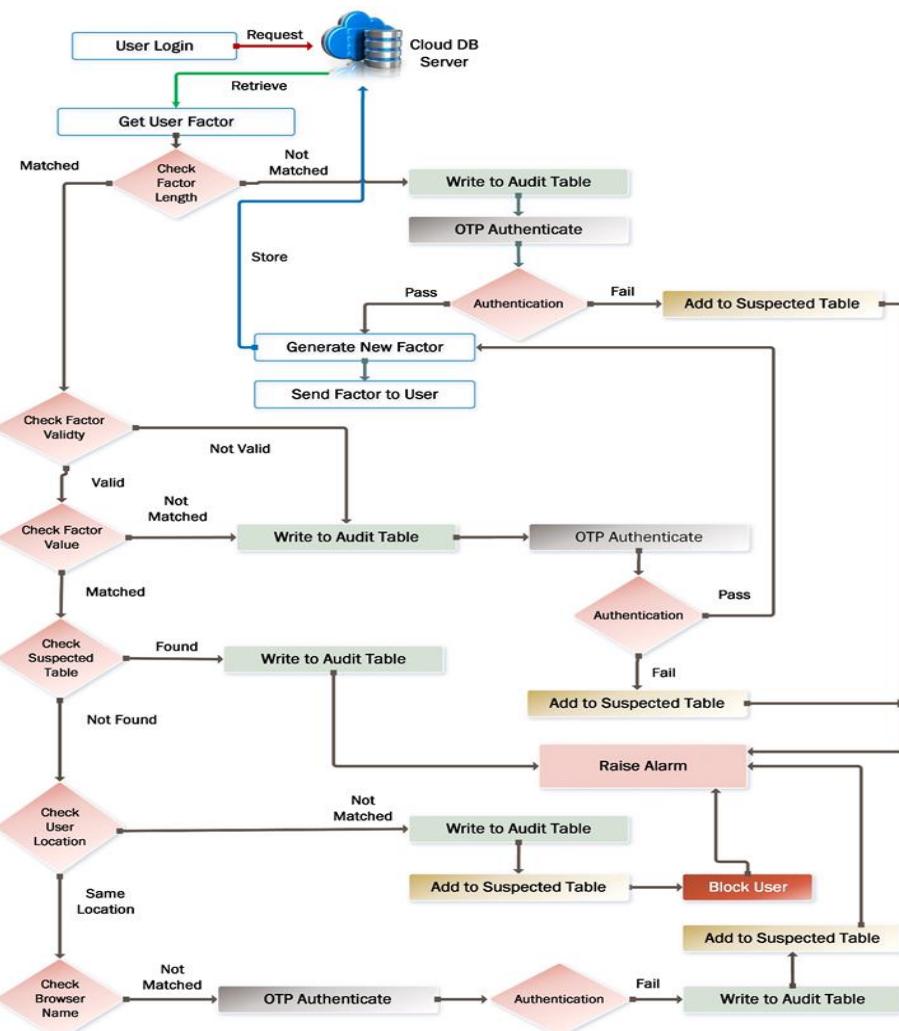


Figure 2. MFA layers for cloud computing platform.

Using a combination of different security approaches is the optimal way to secure the systems and data from attack. This is because no single security approach is perfect, and attackers are constantly developing new ways to exploit vulnerabilities. By using a combination of approaches, the attackers and malicious users will find it more difficult to access cloud computing resources. The best way to detect malicious users and intruders is to use a combination of different approaches. By using multiple authentication factors and monitoring user activity, the system can make it more difficult for attackers to access the system and disclose data. The best combination of security approaches for your organization will depend on your specific needs and risks. The major benefits of integrating multi-factor authentication methods on cloud are as follows.

1. Increased security: multi-factor authentication makes it more difficult for intruders to access the system, even if they have stolen one of the user's authentication factors.
2. Reduced false alarms: By using multiple authentication factors, the framework can help to reduce the number of false alarms. This is because it is less likely that an intruder will be able to provide all of the required authentication factors.
3. Improved user experience: Multi-factor authentication can also improve the user experience. This is because users only need to provide their authentication factors once, when they first log in to the system. After that, they can access the system without having to provide their authentication factors again.

4. Improved security posture: by using a combination of different security approaches, you can create a more layered security posture that is more difficult for attackers to penetrate.
5. Reduced risk of data breaches: A combination of security approaches can help to reduce the risk of data breaches by making it more difficult for attackers to gain access to your systems and data.
6. Improved compliance: Many industry regulations require organizations to implement a combination of security approaches. By using a combination of approaches, you can help to ensure that your organization is compliant with all applicable regulations.

Overall, the integration of multi-factor authentication methods in the cloud can provide a number of benefits, including increased security, reduced false alarms, and improved user experience. Different research methodologies are used to limit data access and provide provable security measures. As presented in [87], the authors proposed a new method for fine-grained data access control in mobile cloud computing (MCC)-based healthcare applications. The method is designed to be provably secure and to provide fine-grained control over data access, while also being efficient and scalable. As presented in [88], a new three-factor authentication, and key agreement protocol (CT-AKA) for cloud-assisted vehicles is proposed. The paper begins by discussing the security challenges of cloud-assisted AVs. These challenges include the need to protect the privacy of AV users, the need to ensure the security of AV communications, and the need to prevent malicious attacks on AVs. The paper then presents the proposed CT-AKA protocol, which is based on a combination of three-factor authentication, fuzzy vault cryptography, and key agreement. As presented in [89], a 3FA protocol is applied to provide secure, efficient, and practical for mobile lightweight devices. The extended chaotic maps component of the protocol is used to generate random numbers. The fuzzy verifier's component of the protocol is used to verify the users' identity.

Algorithm 1 explores the main security layers that are embedded together to create multi-factor methods for authenticating, verifying, securing, and maintaining the privacy of cloud users who are connected to the cloud platform services. As explained, the algorithm initiates the user factor UFP of $user_x$ that contains the authentications and privileges of the user on the cloud. Furthermore, both the validity and value for each user factor UFP are defined as Boolean variables with false values at the beginning of the verification method. After passing the first two layers of authentication that include access control and AMS that manipulates user access using email, SMS, and biometric authentication, the MFA is initiated, wherein a request from $user_x$ is sent to the cloud server to login into the cloud platform. Once the user factor UFP_i is sent to the user, the first layer of MFA is to check the length of the factor. If the factor length is not correct, the factor UFP_i is stored in the audit table, and the second layer of authentication is initiated, wherein the cloud server verifies the validity of the factor. If the factor UFP_i is not valid, an alarm will be raised to prevent the user access, and the factor UFP_i will be stored in the suspected table. A new authentication factor UFP_j is generated and stored in the cloud server to be sent to $user_x$.

If the validity of the factor UFP_i is true, the factor is stored in the audit table; otherwise, the $user_x$ is classified as suspicious, and the factor UFP_i is stored in the suspected table, and an alarm will be raised. The next authentication parameter is initiated by verifying the value of each privilege in the factor UFP_i . Each value in the factor UFP_i represents a specified authorization on the cloud platform services. If the factor value is true and matched, the suspected table is checked first before giving the user permission to login into the cloud services. If the factor has existed in the suspected table, the factor UFP_i will be stored in the audit table, and an alarm will be raised. If the factor UFP_i does not exist in the suspected table, this means that the $user_x$ is mostly viewed as a normal user.

In order to reduce the false positive (FP) percentage of normal users, the location and browser name of $user_x$ are verified. Both the location and browser name are stored during user registration to the cloud service provider, then the user location is checked against the stored location in the cloud server. If the location does not match the stored one, the

$User_x$ will be stored in the suspected table, and an alarm will be raised. If the location is correct, the browser name will be checked as a final countermeasure. An OTP is applied for verification in this step, as the user can use another browser during registration to the cloud. Therefore, an OTP is raised to ensure the validity of the user. If the verification is not correct, the $User_x$ will be stored in the suspected table and an alarm will be raised. Otherwise, the user will login to the cloud platform to manipulate its services.

Algorithm 1: User Behavior Authentication

```

1   Initialize User Factor Privilege UFP
2   Initialize Boolean Value for UFP validity = false
3   Initialize Boolean Value for UFP value = false
4   Request UFPi from Cloud DB Server
5   GET UFPi
6   IF UFPi. length ≠ Matched THEN
7       Store UFPi in Audit_Table
8       Apply AUTH2 Layer
9       IF AUTH2 = Valid THEN
10          Generate New UFPj
11          Store UFPj into Cloud DB Server
12          Send UFPj to Userx
13      ELSE
14          Add UFPi to Suspected_Table
15          Raise Alarm
16      END IF
17  ELSE
18      Check UFPi validity
19      IF UFPi_valid = false THEN
20          Store UFPi in Audit_Table
21          Apply AUTH2 Layer
22          IF AUTH2 = Valid THEN
23              Generate New UFPj
24              Store UFPj into Cloud DB Server
25              Send UFPj to Userx
26          ELSE
27              Add UFPi to Suspected_Table
28              Raise Alarm
29          END IF
30      ELSE //UFPi_valid = true
31          Check UFPi for Auth Parameters
32      END IF
33      IF UFPi_value = false THEN
34          Store UFPi in Audit_Table
35          Apply AUTH2 Layer
36          IF AUTH2 = Valid THEN
37              Generate New UFPj
38              Store UFPj into Cloud DB Server
39              Send UFPj to Userx
40          ELSE
41              Add UFPi to Suspected_Table
42              Raise Alarm
43          END IF
44      ELSE //UFPi_value = true
45          Check Suspected_Table
46  END IF

```

Algorithm 1: Cont.

```

47      IF  $UFP_i = UFP_S$  THEN
48          Add  $UFP_i$  to Suspected_Table
49          Raise Alarm
50      ELSE
51          Check  $User_x$  Location  $UL$ 
52      END IF
53      IF  $UL_k \neq valid$  THEN
54          Add  $UL_k$  to Suspected_Table
55          Block  $UFP_i$ 
56          Raise Alarm
57      ELSE
58          Check  $User_x$  Browser  $UB$ 
59      END IF
60      IF  $UB_n \neq valid$  THEN
61          Add  $UB_n$  to Suspected_Table
62          Block  $UFP_i$ 
63          Raise Alarm
64      ELSE
65          Block  $UFP_i$ 
66      END IF
67  END IF

```

4. Threat Model

Cloud computing environments are often attractive targets for attackers because they offer potential victims and a wide range of sensitive data. In addition, cloud-computing infrastructures can be complex and difficult to secure, which can make them more vulnerable to attack. Different factors can be defined for explaining failures in multi-factor authentication (MFA). One of these factors is the incomplete definition of an adversary, in which the capabilities and goals of an attacker and difficulties in defining cryptographic primitives must be defined. In addition, the provided MFA frameworks may be complex or unable to identify vulnerabilities. These factors are checked with eight proof failures to examine vulnerabilities [90].

Another methodology for securing authentication in critical applications is provided in [91], wherein a two-factor authentication is provided to overcome quantum attacks. The method is based on generating a smart card with a password authentication scheme for preventing key exchange. The following are a set of security issues that the attacker can perform to compromise the data from the cloud platform.

- Data loss: The framework stores user credentials and authentication parameters in an encrypted format, but there is always a risk that these data could be compromised. If an attacker were to gain access to these data, they could use them to impersonate users and gain unauthorized access to cloud resources.
- Account hijacking: The framework uses a variety of methods to detect suspicious user activity. Once an attacker has hijacked an account, they could use it to access sensitive data or to make unauthorized changes to cloud resources.
- Data leakage: The framework uses a variety of methods to protect user data, but there is always a risk that data could be leaked. For example, an attacker could exploit a vulnerability in the framework to steal data, or could gain access to data by compromising a cloud service provider.
- Brute force attack: in this attack, the attacker tries different possible keys until he obtains an intelligible secret key.
- Monitoring for suspicious activity: when suspicious activity is detected, it is important to verify the activity and perform a suitable action to prevent the suspicious user from attacking the cloud services.

To mitigate these threats, the proposed MFA layer framework and the algorithm of user behavior authentication implement the following security measures:

- Using strong authentication: the provided MFA authentication is based on defense-in-depth multi-layers, which authenticate, verify, secure, and maintain the privacy of cloud users who are connected to the cloud platform services.
- Encrypting data: we use strong encryption to protect user credentials and authentication parameters.
- We implement robust security controls to detect and prevent unauthorized access to user data.
- We train users with recommended security practices, such as using secure passwords and staying away from fraudulent websites.

5. Security Analysis for the Proposed MFA Model

Security analysis plays a critical role in cloud computing by helping organizations to identify, assess, and mitigate security risks. A security analysis of major attacks on cloud infrastructure is defined based on a set of steps. These steps are listed below.

5.1. Identify Assets and Vulnerabilities

The first step in cloud security analysis is to identify all of the assets in the cloud environment, such as servers, storage, and databases. Once the assets have been identified, the next step is to identify any vulnerabilities that exist in those assets. The major assets and vulnerabilities of the cloud platform can be defined as follows.

Assets:

- Cloud applications;
- Cloud data;
- Provided cloud services;
- Cloud main resources.

Vulnerabilities:

- Unauthorized access;
- Data breaches;
- Brute force attacks.

5.2. Assess Threats

The next step is to assess the threats to the cloud environment. This includes identifying the potential attackers, their motivations, and their capabilities. The threat assessment should also consider the likelihood of each threat occurring. The major threats and vulnerabilities during the authentication of users on cloud are as follows.

- Weak passwords: Passwords are common forms of authentication, but they are also one of the weakest. Attackers can use different techniques, such as brute-force attacks and password cracking tools, to guess or steal passwords.
- Phishing attacks, which aim to deceive users into disclosing private data like passwords and credit card details. Attackers frequently send emails that look like they are coming from reputable businesses or organizations.
- Malware attacks: Malware is harmful software that can be secretly placed on a user's device. Malware can be used to steal passwords, intercept communications, and launch other attacks.

5.3. Analyze Risks

Once the assets, vulnerabilities, and threats have been identified, the next step is to analyze the risks to the cloud environment. In each cloud environment, potential risks can be analyzed based on the following issues.

- Complexity: the proposed cloud framework should be easy to implement and manage.
- Security risks: the framework should introduce and identify major security risks and identify a proposed intrusion detection method for preventing these risks.
- Privacy risks: the framework must preserve the privacy and sensitivity of users in factors such as location and web browser information.
- Time: the execution time for detecting any malicious attacks depends on the complexity of authentication methods, number of authentication factors, number of manipulating users on the cloud, and the performance of the hardware/software used to implement the framework.

5.4. Develop MFA

The final step is to develop an enhanced framework for mitigating the risks to the cloud environment. The proposed framework in this paper should mitigate the analyzed risks based on the following parameters:

- Complexity: Although the proposed framework contains multi-factor with multi-layer authentication parameters, the framework and its proposed algorithm provide efficient integration of three main layers with an additional embedded layer for encrypting and decrypting user parameters and authorizations. The first layer is responsible for selecting authentication methods for users based on different priority parameters. The second layer is responsible for detecting user behavior on the cloud system or platform using different multi-factor authentication parameters. The third layer proposes an algorithm for manipulating the behavior of users based on the defined cloud multi-factor authentication methods. The three layers are connected to an additional layer for encrypting user credentials and authentication parameters to prevent any probable disclosure of user information and cloud computing-sensitive data.
- Security risks: The proposed framework introduces new security risks, such as vulnerabilities in the authentication method selector (AMS) technique or the intrusion detection component. Additionally, the framework collects sensitive user data, such as location and web browser information, which could be misused if compromised.
- Privacy risks: The proposed framework collects sensitive user data, such as location and web browser information. These data could be misused if compromised. Additionally, the framework uses these data to manipulate user behavior, which could be seen as an invasion of privacy. To mitigate these privacy risks, the framework can be designed to collect only the information that is necessary for its operation, and this information should be protected using appropriate security measures. Additionally, users should be given the option to opt out of having their data used to manipulate their behavior.
- Execution time: although the proposed framework contains different authentication factors, the overall time complexity is considered relatively low with the increasing number of cloud users.

MFA can be used to boost the security of cloud computing environments by adding an extra layer of protection to the authentication process. In doing so, you can defend yourself from several types of assaults, such as phishing attacks, password attacks, and brute-force attacks [92].

There are varieties of different MFA methods that can be used in cloud computing environments. Some common MFA methods include the following.

- One-time passwords (OTPs): OTPs are generated by a separate device, such as a smartphone app or a hardware token.
- Location-based authentication: Location-based authentication methods use the user's location to authenticate them. For example, a user can enter a code that is sent to their smartphone when they are trying to log in to a cloud application from a new location.

Security analysis can be used to assess the security of MFA implementations in cloud computing environments [93]. This analysis can help to identify and mitigate any potential security risks. Some of the key areas of security analysis for MFA in cloud computing include the following.

- The strength of the authentication factors used: The authentication factors used should be strong and resistant to attack. For example, passwords should be complex and unique, and OTPs should be generated using a secure algorithm.
- The implementation of the MFA method: The MFA method should be implemented correctly and securely. For example, OTPs should be transmitted and stored securely.
- The management of MFA users and devices: MFA users and devices should be managed securely. For example, users should be required to change their passwords regularly, and devices should be improved with the latest security patches.

There are a number of benefits to using proposed MFA in cloud computing environments, including the following.

- Improved security: the MFA framework makes it more difficult for attackers to gain unauthorized access to cloud systems and applications.
- Reduced risk of data breaches: the MFA framework can help to reduce the risk of data breaches by making it more difficult for attackers to steal user credentials.
- Increased compliance: many organizations are subject to industry-specific regulations that require them to implement MFA.
- Improved user confidence: customers are more likely to trust organizations that can demonstrate that they are taking steps to protect their data.

Generally, the proposed framework is designed to improve the security of cloud platforms and reduce false alarms by using a variety of authentication factors and by monitoring user behavior.

6. Implementation and Results for Authentication Algorithm

This section explains how the planned MFA layers will be implemented on the cloud-computing platform along with the user authentication method that goes with it. The percentages of false-positive and false-negative rates during the manipulation of the MFA layers are used to calculate the outcomes, together with the execution duration of the generated multi-factor layers.

6.1. Execution Time for Multi-Factor Authentication Layer

In this stage, authentication layers using the nested multi-factor methods are developed and implemented. The goal of this step is to measure the overall execution time for verifying cloud computing users based on the six major layers: factor length checking, validity of factor, factor value, checking the suspected table, user location, and browser name checking. The execution time is measured per millisecond for a different number of users per each experiment. As shown in Figure 3, the execution time for the first factor that checks the factor length increases linearly with the increasing number of users. The execution time was 218 ms with 50 users, while the time was 278 ms with 1000 users. The checking factor validity method recorded a non-linear execution time of 174 ms with 50 users, and the time increased at 100 users to 196 ms. The execution time showed a minimal decrease at 200 and 300 users, at 194 ms and 193 ms, respectively. The change in execution time in this method is due to the checking procedure with a Boolean variable (whether it is yes or no), as proposed in user behavior authentication. The two factors of check value and suspected table increased linearly when the execution time increased with the increase in the number of users. For the check factor value, the time recorded was 186 ms with 50 users, 224 ms with 500 users, and 252 ms with 1000 users. When checking the suspected table, the execution times increased linearly from 50 users to 800 users, while the time relatively decreased for 900 users, with 231 ms, and then the time increased again to 243 ms with 1000 users. The last two factors of user location and browser name checking

also showed a linear increase from 50 users to 500 users. After 500 users, the time relatively decreased, then increased again, and recorded 263 ms and 237 ms for 1000 users for both user location and browser name factors.

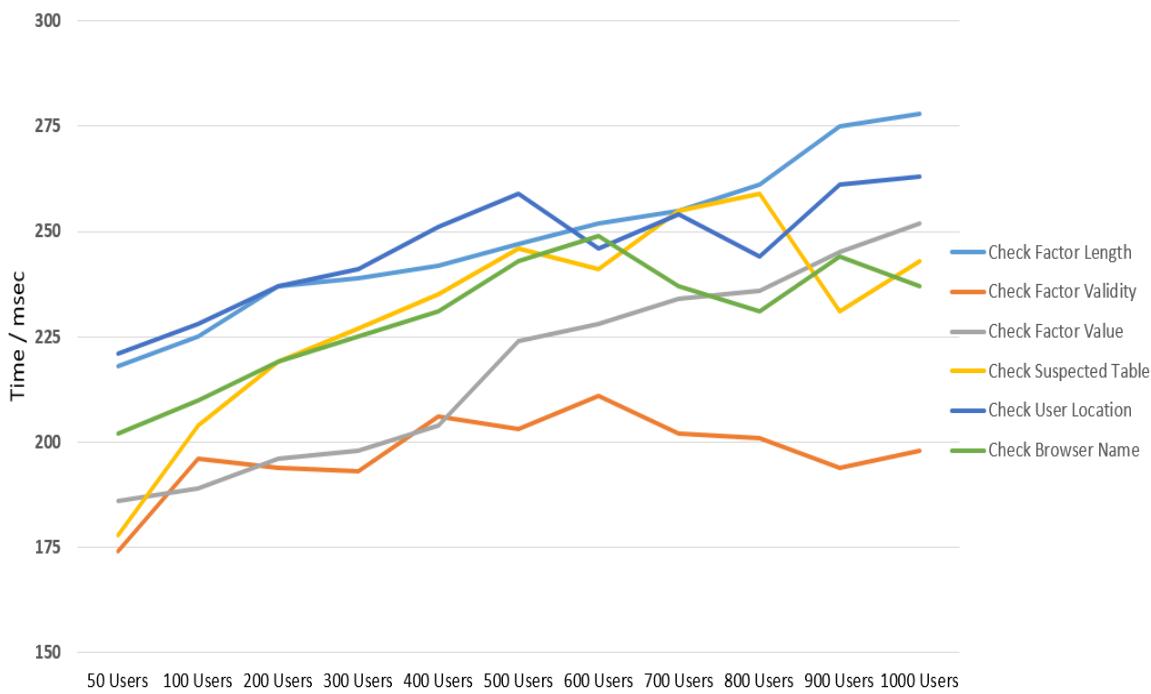


Figure 3. Time performance for multi-factor authentication layers.

6.2. Detection Performance

For most security applications and methodologies that apply different methods of protection and authentication, the measurement of detection performance is considered a major reference and guide for the efficiency of the proposed algorithms. In this section, the false-positive (FP) and false-negative (FN) rates are measured, where the false-positive rate reflects the percentage of detecting normal users as intruders, while the false-negative rate reflects the percentage of intrusions that succeed in penetrating the cloud computing services for disclosing confidential information from the cloud service platform. As presented in Figure 4, the user location and browser name recorded 2% FP for 50 users, while the remaining factors recorded 0% false alarms. With a number of 100 users, the FP percentage recorded only 1% for both factor length and factor validity. This is due to the incorrect detection of location and browser names for the users. These factors still recorded FP alarms when the number of users increased from 50 to 1000 users. For 500 users, the user location check recorded 0% FP, while the browser name recorded 0.4% FP. When the number of users increased from 600 to 1000 users, the FP rate recorded false alarms from 0.1% to a maximum of 1%. This is due to the efficiency and flexibility of the MFA methods that can correctly verify normal users.

As presented in Figure 5, the false-negative (FN) percentage refers to the successful attack percentage that succeeds in disclosing secret information from the cloud service platform. As explained, the FN rate was 0% with all MFA methods for 50 users. When the number of users increased to 100, the FN rate was 0% for the four factors: factor length, factor validity, suspected table, and user location, while the FN was 1% for the factor value and browser name. For 500 users, the accuracy of the MFA methodology showed a low FN rate, with 0.4%, 0.2%, 0.8%, 0.2%, 0.2%, and 0.2% for all authentication factors. For 800 users, the accuracy also showed a low FN rate, with 0.63%, 0.25%, 0.38%, 0.25%, 0.13%, and 0.75% for all authentication factors. The remaining experiment recorded a low rate of FN for 900 and 1000 users, with the highest FN of 0.78% for the browser name check and 0.7 with the factor length check. In general, the proposed methodology and algorithm using

MFA methods achieved high performance in detecting suspicious users and intruders to prevent any intentional attacks on the cloud server or cloud services.

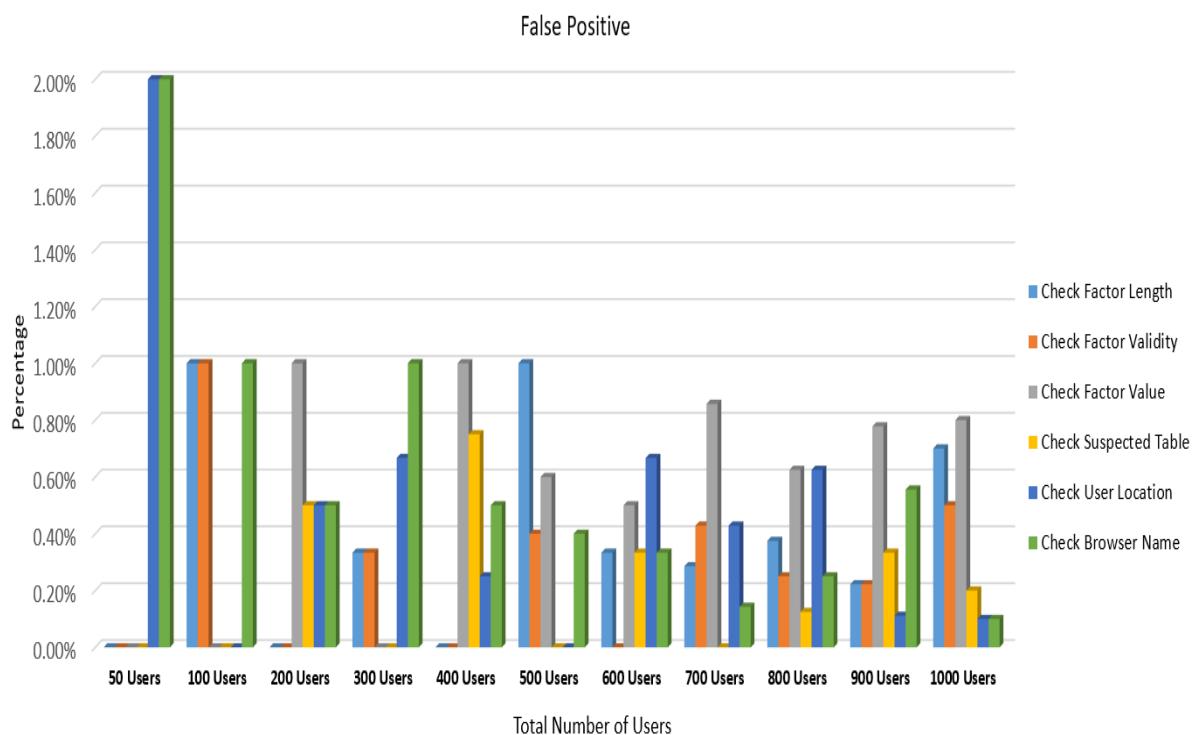


Figure 4. FP users on multi-factor authentication layers.

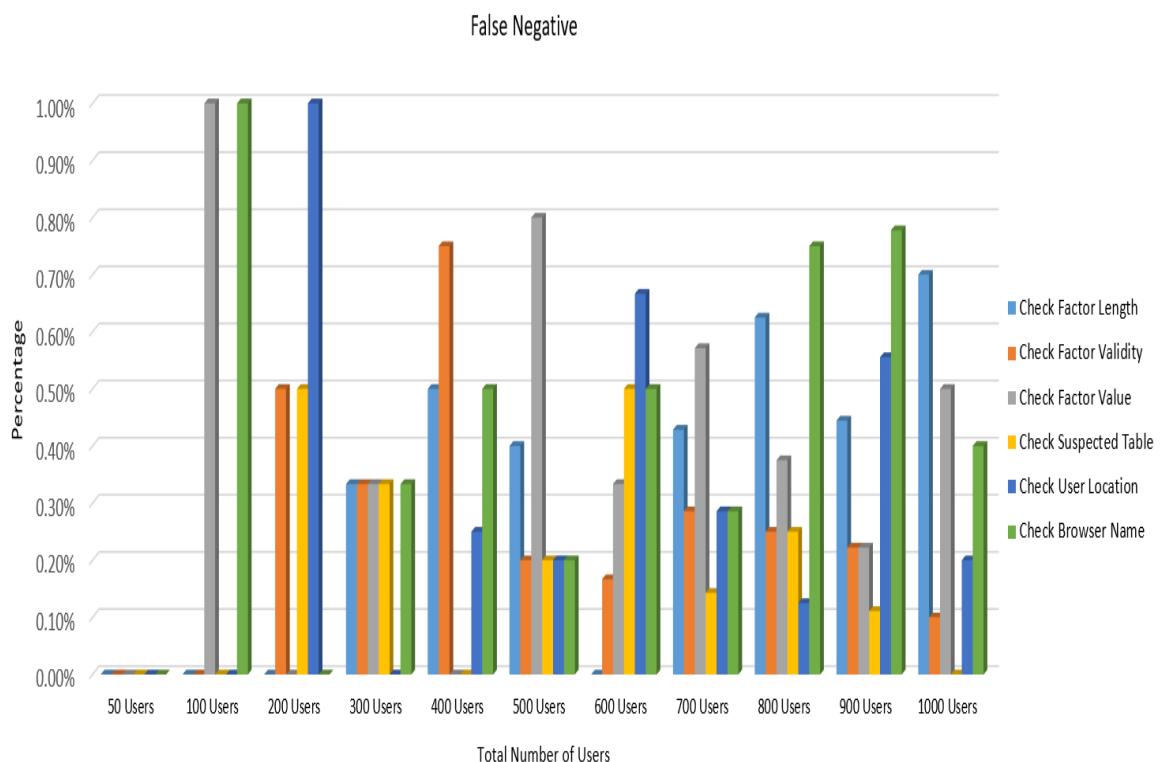


Figure 5. FN users on multi-factor authentication layers.

The performance evaluation of the proposed MFA framework and algorithm are conducted based on quantitative and qualitative measures to assess the success rate of attack prevention. Regarding quantitative measures, false-positive (FP) and false-negative (FN) rates are measured to identify the overall performance of the proposed MFA framework and algorithm. In addition to these quantitative metrics, Table 4 shows the following qualitative factors.

- Usability testing: Usability testing can be conducted to observe users as they interact with the MFA system. This can help to identify any areas where the system is confusing or difficult to use.
- Scalability: The system should be able to scale to meet the needs of a growing organization.
- Flexibility: The system should be flexible enough to accommodate different security requirements.
- Affordability: The system should be affordable for the organization.

Table 4. Authentication method selection.

Ref.	Usability Testing	Scalability	Flexibility	Affordability
[92]	Moderate	Effective	Effective	Effective
[93]	Effective	Effective	Effective	Moderate
[94]	Moderate	Effective	Moderate	Moderate
[95]	Moderate	Effective	Effective	Moderate
[96]	Minimal	Moderate	Effective	Minimal
Proposed MFA	Effective	Effective	Effective	Effective

7. Conclusions

Cloud authentication is an indispensable process of ensuring user identity to maintain the security of data, applications, services, and resources. It is most commonly performed in the PaaS layer. One challenge of using PaaS authentication is achieving a balance of ease of use and security. In this paper, we proposed a flexible multi-factor framework for user authentication to secure access to data and applications in the PaaS environment. In the proposed framework, multi-factor authentication is performed in conjunction with an intrusion detection system, access control policies, and an encryption/decryption algorithm. By using multi-factor authentication, organizations have the ability to provide stronger authentication options to their users. On the other hand, users have the ability to use PaaS without compromising their privacy. By using an intrusion detection system, the users' identities are insured. By using access control policies, the users' identities are verified and users' access times are controlled. By using the AES encryption algorithm, data are protected from being disclosed.

The flexibility feature in the proposed framework is gained by providing the authentication method selector (AMS). By using AMS, an organization has the ability to select various authentication techniques. We used email, SMS, and biometric authentication as examples; any other combination of methods can be used without losing generality. By using the user's geolocation and the web browser feature that is commonly used with other factors in the intrusion detection process, the proposed framework achieves increased security using six factors. Indeed, by utilizing the proposed framework, we are capable to verify the proper application is being used by the right user, with specific data. Moreover, we are able to guarantee the integrity and confidentiality of the data. The experimental results were obtained to measure the false-negative alarm rate and the false-positive alarm rate. The false-negative rate greatly decreased, and the false-positive rate greatly increased for different numbers of users. In future work, the framework can be further improved upon by incorporating additional security features, such as risk-based authentication and

adaptive authentication. The framework can also be evaluated with a larger number of users and a wider range of attack scenarios. Finally, the framework can be made more user-friendly by providing a more intuitive user interface.

Author Contributions: Data curation, A.M.M.; formal analysis, M.K.E. and M.E.; investigation, M.A. (Meshrif Alruily), M.A. (Mohamed Alsarhani) and E.H.; supervision, W.S.; writing—original draft, A.M.M. and M.E.; writing—review and editing, A.M.M., M.A. (Mohamed Alsarhani) and W.S. All authors have read and agreed to the published version of the manuscript.

Funding: This work was funded by the Deanship of Scientific Research at Jouf University under Grant No. (DSR2022-RG-0104).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Published upon request.

Acknowledgments: The authors acknowledge the Deanship of Scientific research at Jouf University.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Tabrizchi, H.; Kuchaki Rafsanjani, M. A survey on security challenges in cloud computing: Issues, threats, and solutions. *J. Supercomp.* **2020**, *76*, 9493–9532. [[CrossRef](#)]
2. Yeng, P.K.; Wulthusen, S.D.; Yang, B. Comparative analysis of threat modeling methods for cloud computing towards healthcare security practice. *Int. J. Adv. Comp. Sci. Appl. (IJACSA)* **2020**, *11*, 772–784. [[CrossRef](#)]
3. Panda, D.R.; Behera, S.K.; Jena, D. *A Survey on Cloud Computing Security Issues, Attacks and Countermeasures. Advances in Machine Learning and Computational Intelligence*; Patnaik, X.-S., Yang, I.K., Sethi, S., Eds.; Springer: Singapore, 2021; pp. 513–524. [[CrossRef](#)]
4. Sumitra, B.; Pethuru, C.; Misbahuddin, M. A survey of cloud authentication attacks and solution approaches. *Int. J. Innov. Res. Comp. Commun. Eng. (IJIRCCE)* **2014**, *2*, 6245–6253.
5. Ghasemisharif, M.; Kanich, C.; Polakis, J. Towards automated auditing for account and session management flaws in single sign-on deployments. In Proceedings of the IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA, 20–26 May 2022; pp. 1774–1790. [[CrossRef](#)]
6. Wang, C.; Wang, D.; Duan, Y.; Tao, X. Secure and lightweight user authentication scheme for cloud-assisted internet of things. *IEEE Trans. Inf. Forensics Secur.* **2023**, *18*, 2961–2976. [[CrossRef](#)]
7. Li, Z.; Wang, D.; Morais, E. Quantum-safe round-optimal password authentication for mobile devices. *IEEE Trans. Dependable Secur. Comp.* **2020**, *19*, 1885–1899. [[CrossRef](#)]
8. Balaram, V.S. Cloud computing authentication techniques: A survey. *Int. J. Sci. Eng. Technol. IJSETR* **2017**, *6*, 458–464.
9. Sudha, S.; Manikandasaran, S. A survey on different authentication schemes in cloud computing environment. *Int. J. Manag. IT Eng.* **2019**, *9*, 359–375.
10. Li, Y.; Luo, J.; Deng, S.; Zhou, G. SearchAuth: Neural architecture search based continuous authentication using auto augmentation search. *ACM Trans. Sensor Networks* **2023**, *19*, 1–23. [[CrossRef](#)]
11. Ometov, A.; Bezzateev, S.; Mäkitalo, N.; Andreev, S.; Mikkonen, T.; Koucheryavy, Y. Multi-factor authentication: A survey. *Cryptography* **2018**, *2*, 1. [[CrossRef](#)]
12. ALSaleem, B.O.; Alshoshan, A.I. Multi-factor authentication to systems login. In Proceedings of the National Computing Colleges Conference (NCCC), Taif, Saudi Arabia, 27–28 March 2021; pp. 1–4. [[CrossRef](#)]
13. AlQahtani, A.A.S.; El-Awadi, Z.; Min, M. A survey on user authentication factors. In Proceedings of the IEEE 12th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON), Vancouver, BC, Canada, 27–30 October 2021; pp. 323–328. [[CrossRef](#)]
14. Dasgupta, D.; Roy, A.; Nag, A. *Multi-Factor Authentication. Advances in User Authentication*; Dasgupta, D., Roy, A., Nag, A., Eds.; Infosys Science Foundation; Springer International Publishing: Cham, Switzerland, 2017; pp. 185–233.
15. Singh, C.; Kaur, R. *Relevance of Multifactor Authentication for Secure Cloud Access. Big Data, Cloud Computing and IoT: Tools and Applications*, 1st ed.; Sita Rani, P.B., Aman, K., Khang, A., Kumar Sivaraman, A., Eds.; Chapman and Hall/CRC: London, UK, 2023; Chapter 10.
16. Andrés, S. Zero factor authentication: A four-year study of simple password-less website security via one-time emailed tokens. *J. Inf. Secur. Appl.* **2015**, *1*–11.
17. Gunson, N.; Marshall, D.; Morton, H.; Jack, M. User perceptions of security and usability of single-factor and two-factor authentication in automated telephone banking. *Comput. Secur.* **2011**, *30*, 208–220. [[CrossRef](#)]

18. Bruun, A.; Jensen, K.; Kristensen, D. *Usability of Single- and Multi-Factor Authentication Methods on Tabletops: A Vomparative Study*. *Human-Centered Software Engineering*; Sauer, S., Bogdan, C., Forbrig, P., Bernhaupt, R., Winckler, M., Eds.; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 2014; Volume 8742, pp. 299–306. [[CrossRef](#)]
19. Said, W.; Mostafa, S.; Hassan, M.M.; Mostafa, A.M. A multi-factor authentication-based framework for identity management in cloud applications. *Comput. Mater. Contin.* **2022**, *71*, 3193–3209. [[CrossRef](#)]
20. Mupila, F.K.; Gupta, H. A multi-factor approach for cloud security. Innovations in Computer Science and Engineering. In *Lecture Notes in Networks and Systems*; Saini, H.S., Sayal, R., Govardhan, A., Buyya, R., Eds.; Springer: Singapore, 2013; Volume 171, pp. 437–445. [[CrossRef](#)]
21. Neware, R.; Shrawankar, U.; Mangulkar, P.; Khune, S. Review on multi-factor authentication (mfa) sources and operation challenges. *Int. J. Smart Secur. Technol. IJSST* **2020**, *7*, 62–67. [[CrossRef](#)]
22. Boonkrong, S. *Multi-Factor Authentication. Authentication and Access Control: Practical Cryptography Methods and Tools*; Boonkrong, S., Ed.; Apress: Berkeley, CA, USA, 2021; Chapter 6; pp. 133–162.
23. Tirfe, D.; Anand, V.K. *A Survey on Trends of Two-Factor Authentication. Contemporary Issues in Communication, Cloud and Big Data Analytics*; Sarma, H.K.D., Balas, V.E., Bhuyan, B., Dutta, N., Eds.; Lecture Notes in Networks and Systems; Springer: Singapore, 2022; Volume 281, pp. 285–296. [[CrossRef](#)]
24. Wang, P.; Baskerville, R. The Case for Two-Factor Authentication- Evidence from a Systematic Literature Review. In Proceedings of the Pacific Asia Conference on Information Systems (PACIS 2019) Proceedings, X’ian, China, 8–12 July 2019.
25. Archana, B.S.; Chandrashekhar, A.; Bangi, A.G.; Sanjana, B.M.; Akram, S. Survey on usable and secure two-factor authentication. In Proceedings of the IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT), Bangalore, India, 19–20 May 2017; pp. 842–846. [[CrossRef](#)]
26. Lee, H.; Kang, D.; Lee, Y.; Won, D. Secure three-factor anonymous user authentication scheme for cloud computing environment. *Wirel. Commun. Mob. Comput.* **2021**, *2021*, 1–20. [[CrossRef](#)]
27. Jain, S.; Gautam, R.; Sharma, S.; Tomar, R.; Choudhury, T. *Four-Factor Authentication with Emerging Cybersecurity for Mobile Transactions*. *Innovations in Cyber Physical Systems*; Singh, J., Kumar, S., Choudhury, U., Eds.; Lecture Notes in Electrical Engineering; Springer: Singapore, 2021; Volume 788, pp. 391–399. [[CrossRef](#)]
28. Brainard, J.; Juels, A.; Rivest, R.L.; Szydlo, M.; Yung, M. Fourth-factor authentication: Somebody you know. In Proceedings of the 13th ACM conference on Computer and communications security, Alexandria, VA, USA, 30 October–3 November 2006. [[CrossRef](#)]
29. Sharmila, K.; Janaki, V. Necessity of fourth factor authentication with multiple variations as enhanced user authentication technique. In Proceedings of the Third International Conference on Computational Intelligence and Informatics, Singapore, 28–29 December 2018; Raju, K.S., Govardhan, A., Rani, B.P., Sridevi, R., Murty, M.R., Eds.; Advances in Intelligent Systems and Computing. Springer: Singapore, 2020; Volume 1090, pp. 491–500. [[CrossRef](#)]
30. Edwards, J.; Aparicio-Navarro, F.J.; Maglaras, L.; Douligeris, C. FFDA: A novel four-factor distributed authentication mechanism. In Proceedings of the IEEE International Conference on Cyber Security and Resilience (CSR), Rhodes, Greece, 27–29 July 2022; pp. 376–381. [[CrossRef](#)]
31. Hemamalini, S.; Manuel, M. A fuzzy implementation of biometrics with five factor authentication system for secured banking. *Int. J. Smart Sens. Adhoc Netw.* **2012**, *1*, 238–242. [[CrossRef](#)]
32. Mukhin, V.E. Multifactor authentication as a protection mechanism in computer networks. *Cybern. Syst. Anal.* **1999**, *35*, 832–835. [[CrossRef](#)]
33. Ahmad, M.O. A Blockchain-based multi-factor authentication mechanism for securing smart cities. *Sensors* **2023**, *23*, 2757. [[CrossRef](#)]
34. Sethuraman, S.C.; Mitra, A.; Ghosh, A.; Galada, G.; Subramanian, A. MetaSecure: A passwordless authentication for the metaverse. *arXiv* **2023**, arXiv:2301.01770.
35. Albuquerque, S.L.; Miosso, C.J.; da Rocha, A.F.; Gondim, P.R. Multi-factor authentication protocol based on electrocardiography signals for a mobile cloud computing environment. In *Mobile Computing Solutions for Healthcare Systems*; Bentham Science: Sharjah, United Arab Emirates, 2023; Chapter 5; pp. 62–88.
36. Zaenchkovski, A.; Lazarev, A.; Masyutin, S. Multi-factor authentication in innovative business systems of industrial clusters. In *Advances in Automation IV*; Springer International Publishing: Berlin/Heidelberg, Germany, 2023; pp. 271–281.
37. Saqib, R.M.; Khan, A.S.; Javed, Y.; Ahmad, S.; Nisar, K.; Abbasi, I.A.; Haque, M.R.; Julaihi, A.A. Analysis and Intellectual structure of the multi-factor authentication in information security. *Intell. Autom. Soft Comput.* **2022**, *32*, 1633–1647. [[CrossRef](#)]
38. Singh, C.; Singh, T.D. A 3-level multifactor authentication scheme for cloud computing. *Int. J. Comput. Eng. Technol. IJCET* **2019**, *10*, 184–195. [[CrossRef](#)]
39. Patel, S.C.; Jaiswal, S.; Singh, R.S.; Chauhan, J. Access control framework using multi-factor authentication in cloud computing. *Int. J. Green Comput. IJGC* **2018**, *9*, 1–15. [[CrossRef](#)]
40. Kaleem, M.; Arshad, M.J. A customizable client authentication framework (ccaf) based on multi-factor for cloud computing application. *Int. J. Comput. Sci. Telecommun. IJCST* **2017**, *8*, 18–25.
41. Banyal, R.K.; Jain, P.; Jain, V.K. Multi-factor authentication framework for cloud computing. In Proceedings of the Fifth International Conference on Computational Intelligence, Modelling and Simulation (CSSIM), Seoul, Korea, 24–25 September 2013; pp. 105–110. [[CrossRef](#)]

42. Patil, D.H.; Asbe, V.S.; Chavan, M.S.; Birajdar, P.L.; Joshi, G.A. A survey on private cloud storage security using multifactor authentication. *J. Archit. Technol.* **2019**, *XI*, 7–11.
43. Nikam, R.; Potey, M. Cloud storage security using multi-factor authentication. In Proceedings of the 2016 International Conference on Recent Advances and Innovations in Engineering (ICRAIE), Jaipur, India, 23–25 December 2016; pp. 1–7. [CrossRef]
44. Priya, K.D.; Sumalatha, L. Trusted hybrid multifactor authentication for cloud users. *i-Manager's J. Cloud Comp.* **2020**, *7*, 12–20. [CrossRef]
45. Monaswarnalakshmi, S.R.; Sai Aravindhan, C.P. Multifactor authentication in iot devices for ensuring secure cloud storage in smart banking. *Int. Res. J. Eng. Technol. IRJET* **2018**, *5*, 1307–1311.
46. Hussain, M.I.; He, J.; Zhu, N.; Sabah, F.; Zardari, Z.A.; Hussain, S.; Razque, F. AAAA: SSO and MFA implementation in multi-cloud to mitigate rising threats and concerns related to user metadata. *Appl. Sci.* **2021**, *11*, 3012. [CrossRef]
47. Karabulut, Z.E.; Kasapbaşı, M.C. Cloud computing integrated multi-factor authentication framework application in logistics information systems. *J. Int. Trade Logist. Law JITAL* **2018**, *3*, 50–57.
48. Erdem, E.; Sandikkaya, M.T. OTPaaS—One time password as a service. *IEEE Trans. Infor. Forensics Secur.* **2019**, *14*, 743–756. [CrossRef]
49. Dhanasekaran, S.; Murugan, B.S.; Vasudevan, V. A reliable agent system for cloud service discovery using mfa technique. *Int. J. Recent Technol. Eng. IJRTE* **2019**, *8*, 682–685. [CrossRef]
50. Meena, S.; Gayathri, V. Securing personal health records using advanced multi-factor authentication in cloud computing. *Int. J. Recent Technol. Eng. IJRTE* **2020**, *8*, 5133–5140. [CrossRef]
51. Midha, S.; Verma, S.; Kavita; Mittal, M.; Jhanjhi, N.; Masud, M.; AlZain, M.A. A secure multi-factor authentication protocol for healthcare services using cloud-based sdn. *Comput. Mater. Contin.* **2023**, *74*, 3711–3726.
52. Prabakaran, D.; Ramachandran, S. Multi-factor authentication for secured financial transactions in cloud environment. *Comput. Mater. Contin.* **2022**, *70*, 1781–1798. [CrossRef]
53. Gordin, I.; Graur, A.; Potorac, A. Two-factor authentication framework for private cloud. In Proceedings of the 23rd International Conference on System Theory, Control and Computing (ICSTCC), Sinaia, Romania, 9–11 October 2019; pp. 255–259. [CrossRef]
54. Kambou, S.; Bouabdallah, A. A strong authentication method for web/mobile services. In Proceedings of the 2019 6th IEEE International Conference on Cyber Security and Cloud Computing (CSCloud)/2019 5th IEEE International Conference on Edge Computing and Scalable Cloud (EdgeCom), Paris, France, 21–23 June 2019; pp. 124–129. [CrossRef]
55. Taher, K.A.; Nahar, T.; Hossain, S.A. Enhanced Cryptocurrency Security by Time-Based Token Multi-Factor Authentication Algorithm. In Proceedings of the 2019 International Conference on Robotics, Electrical and Signal Processing Techniques (ICREST), Dhaka, Bangladesh, 10–12 January 2019; pp. 308–312. [CrossRef]
56. Kennedy, W.; Olmsted, A. Three factor authentication. In Proceedings of the 2017 12th International Conference for Internet Technology and Secured Transactions (ICITST), Cambridge, UK, 11–14 December 2017; pp. 212–213. [CrossRef]
57. Hassan, M.A.; Shukur, Z. A secure multi factor user authentication framework for electronic payment system. In Proceedings of the 3rd International Cyber Resilience Conference (CRC), Langkawi Island, Malaysia, 29–31 January 2021; pp. 1–6. [CrossRef]
58. Hassan, M.A.; Shukur, Z.; Hasan, M.K. *Enhancing multi-factor user authentication for electronic payments*. *Inventive Computation and Information Technologie*; Smys, S., Balas, V.E., Kamel, K.A., Lafata, P., Eds.; Lecture Notes in Networks and Systems; Springer: Singapore, 2021; Volume 173. [CrossRef]
59. Oke, B.A.; Olaniyi, O.M.; Aboaba, A.A.; Arulogun, O.T. Multifactor authentication technique for a secure electronic voting system. *Electron. Gov. Int. J. EG* **2021**, *17*, 312–338. [CrossRef]
60. Oke, B.A.; Olaniyi, O.M.; Aboaba, A.A.; Arulogun, O.T. Developing multifactor authentication technique for secure electronic voting system. In Proceedings of the 2017 International Conference on Computing Networking and Informatics (ICCNI), Lagos, Nigeria, 29–31 October 2017; pp. 1–6. [CrossRef]
61. Olaniyi, O.M.; Dogo, E.M.; Nuhu, B.K.; Treiblmaier, H.; Abdulsalam, Y.S.; Folawiyo, Z. *A Secure Electronic Voting System Using Multifactor Authentication and Blockchain Technologies*. *Blockchain Applications in the Smart Era*; Misra, S., Kumar Tyagi, A., Eds.; Springer International Publishing: Cham, Switzerland, 2022; pp. 41–63.
62. Olaniyi, O.M.; Arulogun, O.T.; Omidiola, E.O.; Oludotun, A. Design of secure electronic voting system using multifactor authentication and cryptographic hash functions. *Int. J. Comp. Inf. Technol.* **2013**, *2*, 1122–1130.
63. Abayomi-Zannu, T.P.; Odun-Ayo, I.A.; Barka, T.F. A proposed mobile voting framework utilizing blockchain technology and multi-factor authentication. *J. Phys. Conf. Ser. JPCS* **2019**, *1378*, 032104. [CrossRef]
64. Rusdan, M.; Manurung, D.T. Designing of user authentication based on multi-factor authentication on wireless networks. *J. Adv. Res. Dynam. Control Syst. JARDCS* **2020**, *12*, 201–209. [CrossRef]
65. Kinai, A.; Otieno, F.; Bore, N.; Weldemariam, K. Multi-factor authentication for users of non-internet based applications of blockchain-based platforms. In Proceedings of the IEEE International Conference on Blockchain (Blockchain), Rhodes, Greece, 2–6 November 2020; pp. 525–531. [CrossRef]
66. Lee, K. A study on user access control method using multi-factor authentication for EDMS. *Int. J. Secur. Its Appl. IJSIA* **2013**, *7*, 327–334. [CrossRef]
67. Santhi, S.G.; Kameswara Rao, M. Multifactor user authentication mechanism using internet of things. In Proceedings of the Second International Conference on Computer Networks and Communication Technologies, 15–16 June 2019; Smys, S., Senju, T., Lafata, P., Eds.;

- Lecture Notes on Data Engineering and Communications Technologies; Springer International Publishing: Cham, Switzerland, 2020; Volume 44, pp. 496–502. [CrossRef]
68. Rao, M.K.; Santhi, S.G.; Hussain, M.A. Multi factor user authentication mechanism using internet of things. In Proceedings of the Third International Conference on Advanced Informatics for Computing Research, Shimla, India; 2019.
69. Chen, Z.; Cheng, Z.; Luo, W.; Ao, J.; Liu, Y.; Sheng, K.; Chen, L. FSMFA: Efficient firmware-secure multi-factor authentication protocol for IoT devices. *Internet Things* **2023**, *21*, 100685. [CrossRef]
70. Liu, J.; Zou, X.; Han, J.; Lin, F.; Ren, K. BioDraw: Reliable multi-factor user authentication with one single finger swipe. In Proceedings of the IEEE/ACM 28th International Symposium on Quality of Service (IWQoS), Hang Zhou, China, 15–17 June 2020; pp. 1–10. [CrossRef]
71. Lu, D.; Huang, D.; Deng, Y.; Alshamrani, A. Multifactor user authentication with in-air-handwriting and hand geometry. In Proceedings of the International Conference on Biometrics (ICB), 20–23 February 2018; pp. 255–262. [CrossRef]
72. Abiew, N.A.K.; Jnr, M.D.; Banning, S.O. Design and implementation of cost effective multi-factor authentication framework for ATM systems. *Asian J. Res. Comp. Sci. (AJRCoS)* **2020**, *5*, 7–20. [CrossRef]
73. Bouck-Standen, D.; Kipke, J. Multi-factor authentication for public displays using the semantic ambient media framework. In Proceedings of the ADVCOMP 2019: The Thirteenth International Conference on Advanced Engineering Computing and Applications in Sciences, Porto, Portugal, 22–26 September 2019; Rückemann, C.-P., Münster, W.-U., Eds.; International Academy, Research and Industry Association (IARIA): Athens, Greece, 2019; pp. 30–35.
74. Şahan, S.; Ekici, A.F.; Bahtiyar, Ş. A multi-factor authentication framework for secure access to blockchain. In Proceedings of the 2019 5th International Conference on Computer and Technology Applications (ICCTA 2019), Istanbul, Turkey, 16–17 April 2019.
75. Zin, M.Z.M.; Saidi, R.M.; Sappar, F.; Arshad, M.A. Multi-factor authentication to authorizing access to an application: A conceptual framework. *J. Adv. Res. Comp. Appl.* **2019**, *16*, 1–9.
76. Al-Shqeerat, K.H.A. Securing a question-based multi-factor authentication system using LSB steganography technique. In *Explore Business, Technology Opportunities and Challenges After the COVID-19 Pandemic*; Springer International Publishing: Cham, Switzerland, 2023; pp. 1118–1128.
77. Chunka, C.; Banerjee, S.; Sachin Kumar, G. A secure communication using multifactor authentication and key agreement techniques in internet of medical things for COVID-19 patients. *Concurr. Comp. Pract. Exp.* **2023**, *35*, e7602. [CrossRef]
78. Asani, E.O.; Longe, O.B.; Balla, A.J.; Ogundokun, R.O.; Adeniyi, E.A. *Secure Human-Computer Interaction: A Multi-Factor Authentication CAPTCHA Scheme. Handbook of Research on the Role of Human Factors in IT Project Management*; Misra, S., Adewumi, A., Eds.; IGI Global: Hershey, PA, USA, 2020; pp. 149–163.
79. Lala, O.G.; Aworinde, H.O.; Ekpe, S.I. Towards A secured financial transaction: A multi-factor authentication model. In Proceedings of the 25th iSTEAMS Trans-Atlantic Multidisciplinary Virtual Conference, Laboratoire Jean Kuntzmann, Universite Laboratoire Jean Kuntzmann, Universite Grenoble, Alpes, France; 2020; pp. 139–146.
80. Alghamdi, A.A. A verification system for multi-factor authentication for e-healthcare architectures. *Arab J. Sci. Publ. (AJSP)* **2021**, *31*, 1–44.
81. Tanveer, M.; Badshah, A.; Khan, A.; Alasmary, H.; Chaudhry, S. CMAF-IIoT: Chaotic map-based authentication framework for industrial internet of things. *Internet Things* **2023**, *23*, 100902. [CrossRef]
82. Alasmary, H.; Tanveer, M. ESCI-AKA: Enabling secure communication in an iot-enabled smart home environment using authenticated key agreement framework. *Mathematics* **2023**, *11*, 3450. [CrossRef]
83. Aleluya, E.R.M.; Vicente, C.T. Faceture ID: Face and hand gesture multi-factor authentication using deep learning. *Procedia Comput. Sci.* **2018**, *135*, 147–154. [CrossRef]
84. Carrillo-Torres, D.; Pérez-Díaz, J.A.; Cantoral-Ceballos, J.A.; Vargas-Rosales, C. A novel multi-factor authentication algorithm based on image recognition and user established relations. *Appl. Sci.* **2023**, *13*, 1374. [CrossRef]
85. 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. [CrossRef]
86. 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. [CrossRef]
87. Roy, S.; Das, A.K.; Chatterjee, S.; Kumar, N.; Chattopadhyay, S.; Rodrigues, J. Provably secure fine-grained data access control over multiple cloud servers in mobile cloud computing based healthcare applications. *IEEE Trans. Ind. Inf.* **2019**, *1*, 457–468. [CrossRef]
88. 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. [CrossRef]
89. 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. [CrossRef]
90. 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. [CrossRef]
91. 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. [CrossRef]
92. Kaur, S.; Kaur, G.; Shabaz, M. A Secure two-factor authentication framework in cloud computing. *Secur. Commun. Netw.* **2022**, *2022*, 7540891. [CrossRef]

93. Otta, S.; Panda, S.; Gupta, M.; Hota, C. A Systematic survey of multi-factor authentication for cloud infrastructure. *Future Internet MDPI* **2023**, *15*, 146. [[CrossRef](#)]
94. Lee, J.; Kim, M.; Yu, S.; Park, K.; Park, Y. A secure multi-factor remote user authentication scheme for cloud-IOT applications. In Proceedings of the International Conference on Computer Communication and Networks (ICCCN), Valencia, Spain, 29 July–1 August 2019. [[CrossRef](#)]
95. Babu, R.; Badirova, A.; Moghaddam, F.; Wieder, P.; Yahyapour, R. Authentication and access control in cloud-based systems. In Proceedings of the Fourteenth International Conference on Ubiquitous and Future Networks (ICUFN), Paris, France, 4–7 July 2023. [[CrossRef](#)]
96. Gordin, I.; Graur, A.; Vlad, S. Adomnitei, Moving forward passwordless authentication: Challenges and implementations for the private cloud. In Proceedings of the 20th RoEduNet Conference: Networking in Education and Research (RoEduNet), Iasi, Romania, 4–6 November 2021. [[CrossRef](#)]

Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.