An Interactive Multi-Factor User Authentication Framework in Cloud Computing

Elsayed Mostafa[1*], M.M. Hassan[1], Wael Said[1]
[1]Faculty of Computers and Informatics, Zagazig University, Zagazig 44519, Egypt
[*]Corresponding Author :

Abstract
Identity and access management in cloud computing is one of the leading significant issues that require various security countermeasures to preserve user privacy. An authentication mechanism is a leading solution to authenticate and verify the identities of cloud users while accessing cloud applications. Building a secured and flexible authentication mechanism in a cloud computing platform is challenging. Authentication techniques can be combined with other security techniques such as intrusion detection systems to maintain a verifiable layer of security. In this paper, we provide an interactive, flexible, and reliable multi-factor authentication mechanisms that are primarily based on a proposed Authentication Method Selector (AMS) technique. The basic idea of AMS is to rely on the user's previous authentication information and user behavior which can be embedded with additional authentication methods according to the organization's requirements. In AMS, the administrator has the ability to add the appropriate authentication method based on the requirements of the organization. Based on these requirements, the administrator will activate and initialize the authentication method that has been added to the authentication pool. An intrusion detection component has been added to apply the users' location and users' default web browser feature. The AMS and intrusion detection components provide a security enhancement to increase the accuracy and efficiency of cloud user identity verification.

Keywords:
Cloud authentication, multi-factor authentication, authentication factors, cloud intrusion detection, and user behavior.

1. Introduction

Cloud authentication is the process of verifying 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]. The cloud-based authentication attacks include the 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 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 of such techniques include password-based authentication, Single Sign-On (SSO), token authentication, graphical password authentication, biometric authentication, third-party authentication, certificate-based authentication, digital device authentication, two-factor authentication, as well as multi-factor authentication [5, 6]. More recently, organizations have implemented and used multi-factor authentication in cloud applications to increase security and productivity, reduce the risk of compromised passwords, improve regulatory compliance, and enable enterprise mobility [7]. Multi-factor authentication 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 [8]. 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 [9]. The knowledge factors are the already known things such as personal identification number (PIN), password, security question, one-time code, and passphrase. The possession factors; referred also as token-based factors, are the owned things such as identity card, SIM Card, memory card, smartcard, Fast Identity Online (FIDO) security key, one-time password token, and a smartphone 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 [7, 10]. Processing factors are factors that depend on the level of human perception to perform or memorize a mathematical or logical operation. Personal

Manuscript received August 5, 2023
Manuscript revised August 20, 2023
https://doi.org/10.22937/IJCSNS.2023.23.8.8

knowledge factors are implemented based on a person's social relationships by asking someone how much they know the person with whom to ask for validation. By using multi-factor authentication, in case of one factor is compromised by an unauthorized user, the chances of another factor being compromised are low. Therefore, multi-factor authentication represents a higher level of assurance about a user's identity.

1. Traditional authentication methods can be merged with other security techniques like intrusion detection, access control, and encryption to form security authentication layers. The contribution of our research is presented as follows: Provides a concise survey that clarifies the existence of various cloud authentication techniques in different environments using multiple numbers of factors.
2. Proposing the AMS technique for improving the authentication process that has been presented in [11] for selecting the appropriate authentication method based on user behavior.
3. 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 in [11].
4. Conducting the experimental results to demonstrate and validate the accuracy and performance of the proposed framework.

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 minify 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, we could classify authentication based on the number of factors into three main categories, namely; Zero-Factor Authentication (ZFA or 0FA) [12], Single-Factor Authentication (SFA) or One-Factor Authentication (1FA) [13, 14], and Multi-Factors Authentication (MFA) [11, 15-17]. By multi-factor, it means using two or more factors. According to existing research articles, MFA could be categorized into Two-Factor Authentication (2FA or TFA) [18-20], Three-Factor Authentication (3FA) [21], Four-Factor Authentication (4FA or FFA) [22-24], and Five-Factor Authentication (5FA) [25]. Fig.1 shows the classification of authentication factors based on the number of factors.

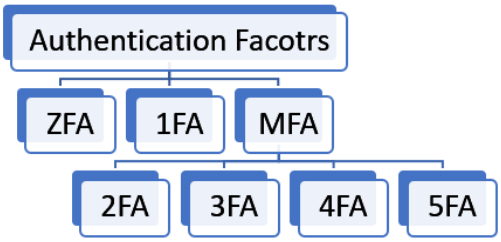

Fig. 1 Classification of Authentication Factors.

As presented in Fig.2, the number of publications per year of research articles interested in multi-factor authentication is presented. It indicates the rate of increase, especially in the last three years. The graph is based on a collected 914 diverse scientific materials by using the keywords "multifactor/ multi-factor/multi-factor authentication" that appeared in the title. These materials include Journal Articles, Proceedings Articles Conference Papers, Patents, Dissertations, Book Chapters, and Reports. The search process is done using:

- ACM Digital Library (https://dl.acm.org)
- Elsevier (www.sciencedirect.com)
- Emerald (www.emeraldinsight.com)
- Google Scholar (https://scholar.google.com)
- John Wiley (http://onlinelibrary.wiley.com)
- Microsoft Academic (https://academic.microsoft.com/home)
- Online IEEE Xplore Library (http://ieeexplore.ieee.org)
- Open Access Theses and Dissertations (https://oatd.org)
- Scopus Document Search (https://www.scopus.com)
- Springer Link (https://link.springer.com)
- Taylor and Francis (http://tandfonline.com)

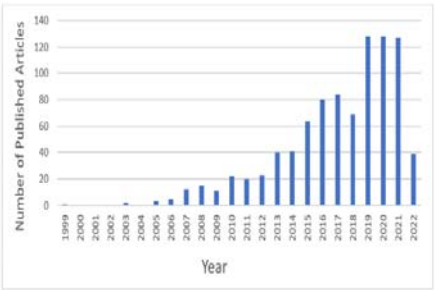

Fig. 2 Number of MFA Researches per Year.

As shown in Fig.2, there has been a growing interest in MFA by researchers in the past three years. The main research directions for MFA are multi-factor user authentication, multi-factor protocol authentication, multi-factor mutual authentication, multi-factor remote user authentication, multi-factor biometrics authentication, and multi-factor graphical password authentication. In this paper, we are interested in multi-factor user authentication for cloud computing environments. In [26], a bibliometric survey is performed based on Web of Science data for research publications on the topic of MFA. Furthermore, we summarize the use of MFA by a different number of factors in various environments in Table 1 and Table 2. In Table 1 the different cloud-based areas are represented while Table 2 denotes the non-cloud different environments.

Table 1: MFA Different Number of Factors in Cloud-based Environments

Reference	***Authentication Technique***	***Factors***	***Environment***
[27]	MFA + CP-ABE	• Username and Password • QR Code-based OTP	Private Cloud Storage
[28]	MFA + SSO	• SMS OTP • Call on Phone • App approval	User's Metadata in a Multi-Cloud
[29]	MFA + RSA+Hash Func	• Contextual • Sign encryption • Iris Biometric	Cloud Health Care
[30]	MFA	• Username and Password • Secret key to AES technique • Biometrics	Multiple Agents Cloud-based Search Engine
[31]	MFA	• Username and Password • OTP • Fingerprints	Cloud Storage in Smart Banking
[32]	MFA + VGG face model	• Username and Password • Security Questions • Mobile OTP • Face image	Cloud Storage
[33]	MFA + SHA 1 + AES-128-CBC	• Encrypted Password • OTP based on OOB • Email Account • Mobile Number • Count of mouse clicks on different graphical elements on a screen	Cloud Computing
[34]	MFA	• PIN/Password • Biometrics • SMS OTP	Cloud Computing
[35]	MFA	• Username and Password • Email Account • Mobile Number • PIN • OTP	Cloud Computing
[36]	MFA	• Secret-splitting key • OTP • IMEI number	Cloud Computing

[37]	MFA	• Face Verification • NFC Card Authentication • Geofence Location • Temporal Data Verification	Cloud-based Logistics IS
[38]	MFA + CP-ABE	• Username and Password • OTP based on QR code	Private Cloud Storage
[39]	2FA + PSK	• Username and Password • OTP	Cloud-based OTP Services
[40]	2FA	• Username and Password • TOTP	Cryptocurrency
[41]	2FA	• Username and Password • TOTP	Private Cloud
[42]	2FA	• OTP • IoT Token	Cloud-based Web Services

The MFA is used in various environments either cloud-based; Table 1, or non-cloud ones; Table 2. The cloud-based environments include general cloud computing architecture [33-36], cloud storage [27, 32, 38], multi-cloud [28], Cloud-based Logistics Information Systems [37], Cloud-based OTP services [39], multiple agents cloud-based search engine [30], cloud health care [29], and Cloud-based web Services [42]. The other environments include Cryptocurrency [40], websites and mobile apps [43], Electronic Payments [44, 45], electronic voting systems [46-49], mobile voting systems [50], Wireless Networks [51], non-internet based applications [52], electronic document management system [53], IoT network [54, 55], RFID infrastructure [56], wearable and virtual reality (VR) platforms with gesture input interface [57], ATM systems [58], public multi-touch displays [59], blockchain [60], and attendance record management system (ARMS) [61].

Table 2: MFA Different Number of Factors in Non-Cloud Environments

Reference	***Authentication Technique***	***Factors***	***Environment***
[62]	MFA + Deep Learning + Leap Motion Controller	• Face Verification • OTP	-
[43]	3FA	• Username and Password • Face Verification • Microsoft Cognitive Service	Websites and Mobile Apps
[44]	MFA	• Username and Password • Fingerprints • OTP	Electronic Payments
[45]	MFA	• Username and Password • Fingerprints	Electronic Payments
[46, 47]	MFA + enhanced Feistel block cipher	• Fingerprints • Sart card	Electronic Voting Systems
[48]	2FA + Blockchain	• Face verification • RFID authentication	Electronic Voting Systems
[49]	MFA + SHA256	• One Time Short Message Service • Grid Card	Electronic Voting Systems
[50]	MFA + Blockchain	• Voter's ID (VIN) • PIN • OTP	Mobile Voting Systems

[51]	MFA	• Username and Password • OTP • Face image	Wireless Networks
[52]	MFA + Block chain	• Security questions based on past blockchain transactions	Non-internet based Applications
[53]	2FA	• Username and Password • OTP	Electronic Document Management System
[56]	MFA + CNN-LSTM-based Classifier	• Pattern-based password • Four Biometrics of human hand	RFID Infrastructure
[54, 55]	2FA	• Graphical passwords • IoT Device	IoT Network
[57]	MFA	• In-air-handwriting based motion signal • Hand skeleton based geometry	Wearable and VR Platforms
[63]	MFA + CAPTCHA	• Face verification • Real-time functionality	Human-Computer Interaction
[64]	2FA	• PIN • Facial recognition	ATM transactions
[65]	MFA + AES 256	• Username and Password • Dynamically generated NFC code • Face verification	Electronic Healthcare Systems
[58]	3FA	• PIN • Bank Card • Keystroke Dynamics	ATM Systems
[59]	MFA + SAM.F	• Smartphone • Username and Password • Geofence Location	Public Multi-touch Displays
[60]	MFA + AES256	• Username and Password • Fingerprints • Security questions	Blockchain
[61]	MFA	• Mobile MAC address • Geofence Location • Fingerprints	Attendance Record Management System

According to Table 1 and Table 2, the MFA either used as 2FA, 3FA, or more. It is use either beside other techniques such as cipher text-policy attribute-based encryption (CP-ABE) [27, 38], SSO [28], RSA algorithm and hash function [29], SHA 1 and AES-128-CBC [33], AES 256 [60], pre-shared secret key (PSK) [39], Deep learning and leap motion controller [62], enhanced Feistel block cipher [46, 47], Blockchain [48, 50, 52], VGG face model [32], CNN-LSTM-based classifier [56], and semantic ambient media framework (SAM.F); an authoritative interface between smartphones and public displays [59]. 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 hand gesture [62], location confirmation and temporal data confirmation [37], security questions [52], graphical passwords [54, 55], motion signal of in-air-handwriting [57], geometry of hand skeleton [57], and keystroke rhythm [58].

In this paper, we proposed an interactive, flexible, and secure multi-factor 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. The administrator will have the ability to add the appropriate authentication method based on the requirements of the organization. Based on these requirements, the administrator will activate and initialize the authentication method from the pool. The proposed framework provides interactive intrusion detection steps by 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 that have been proposed in [11].

3. Proposed Framework for Cloud Intrusion Detection

As presented in [11], the framework consists of three main phases. These phases include the user creation phase, granting access phase, and encryption and decryption phase. In the first phase, the necessary procedure to create a user account is initialized and the required characteristics for a user to access the application are generated. The user creation phase consists of two foremost stages; It is the stage of user registration and the stage of creating user privileges. In the user registration stage, the user enters his/her personal secret attributes and selects a contingency authentication method such as email account, mobile, etc. In the creating user privileges stage, the privileges allocated to each user are realized. In the granting access phase, the needed procedures to grant a user accessibility to the application are specified. Multi-factor authentication, intrusion detection, auditing table, and suspect table are four elements that come together to form this phase. The multi-factor authentication element authenticates a user through three different levels. These level include the user name and password, user factor, and OTP based on email. The intrusion detection element is responsible for verifying the user factor, checking the suspected table, and issuing an alert as soon as suspicious activities of users are discovered. The user verification step is performed by checking the user factor length, checking user factor validity, comparing the entered user factor value, and check suspected table. The auditing table element is responsible for recording all user actions performed on the application data and summarizing all raised alerts for the users in order to maximize the rate of future countermeasures. The suspect table element archives all suspicious users who have violated their granted privileges. The login steps are also relies on the $AUTH_{ADD}$ which is an additional authentication process. The $AUTH_{ADD}$ is activated if a user is suspicious. In the encryption and decryption phase, the application data are encrypted/decrypted using AES algorithm in/from the database server.

In this paper, we consider the granting access phase to be our primary objective. We add some security features that make our proposed framework more flexible and secure to ensure user identity and prevent intruders. The flexibility feature is gained by using the Authentication Method Selector (AMS). By using AMS, an organization has the ability to select various authentication techniques, not just email as in [11]. We used email, SMS, and WhatsApp as examples, any other combination of methods can be used without losing generality. By using the user's geolocation and user's usually used web browser as other factors in the intrusion detection process, our proposed framework achieves more security by using six factors instead of four as in [11]. The overall components of the proposed framework are depicted in Fig.3.

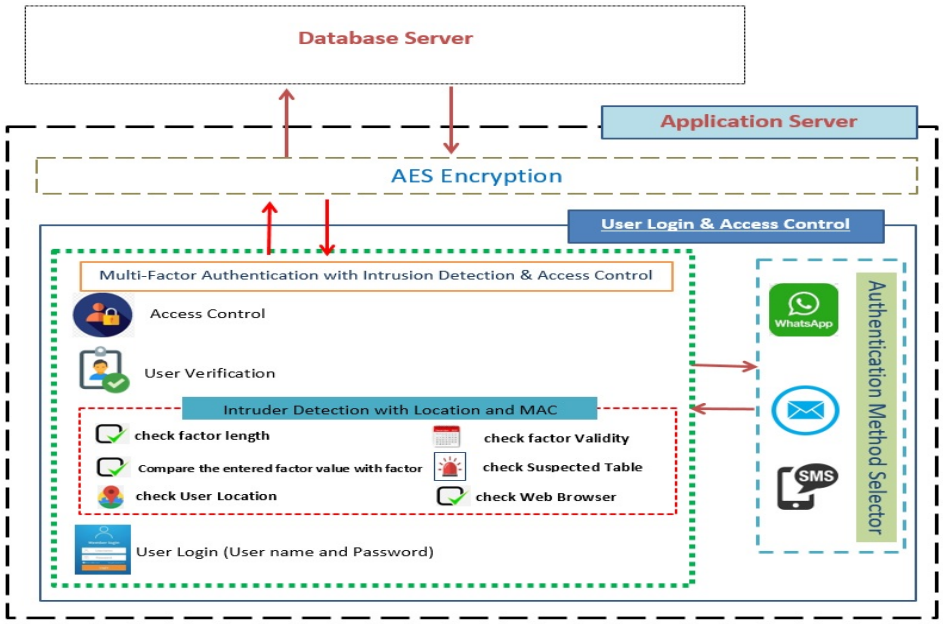

Fig. 3 Overall Proposed Framework Components.

3.1 Authentication Method Selector (AMS)

AMS is our proposed technique which is used to manage the choice of authentication technique to be used based primarily on user behavior. It defines the next authentication technique that will be used in the current authentication process. Various multiple 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 other organizations can provide security tokens [66]. The selection process for any technique depends on the ability of the organization and the tools available. The application admins are responsible for adding and choosing the authentication techniques that will be used. As discussed in [11], the authentication is based on just email authentication. In this paper, additional authentication methods were added like WhatsApp messages, SMS, or any authentication method selected by the admins.

Assume a $user_k$ wants to access the application and forget his/her password, s/he will be authenticated throw email for the first time of authentication. Assuming that the user forgets his/her factor, s/he must be authenticated using a different way like WhatsApp messages or SMS to ensure the user identity in case of email disclosure. The main components of the AMS technique are shown in Fig. 4. These components include:

- Authentication Technique Selection Process, presented in Section 3.1.1
- Authentication Techniques Pool, presented in Section 3.1.2

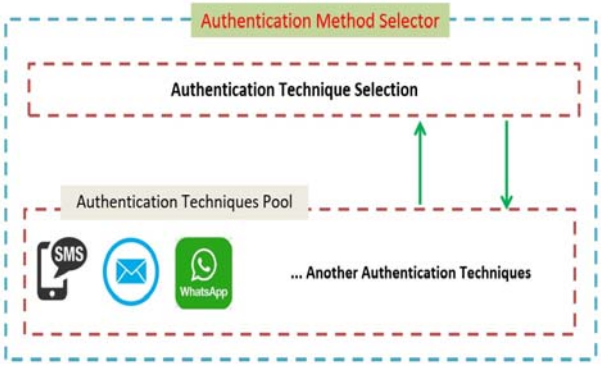

Fig. 4 Authentication Method Selector.

3.1.1 Authentication Technique Selection Process

The process automatically determines the authentication technique that will be applied in the recent authentication process. The authentication technique selection is presented in Fig. 5.

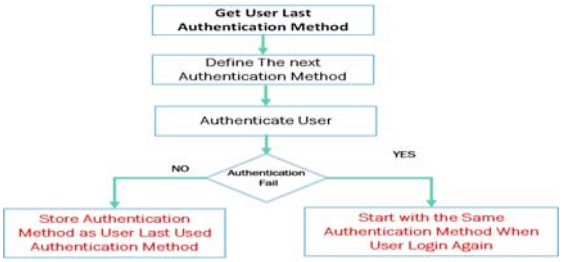

Fig. 5 Authentication Technique Selection Process.

As presented in Fig. 5 the process of selecting an authentication method is based on three main steps. These steps are the user's last authentication method, define authentication method, and user authentication process status. In the user's last authentication method step, we selected only three methods of authentication: email, WhatsApp messages, and SMS Messages. Before authenticating the user, a request is directed to the database server to obtain the last authentication method that was used in the last authentication process.

In the second step, define the authentication method, we provide an authentication method priority table to determine the usage priority for each authentication method. Each method is assigned a number that defines its priority. The higher the number, the higher the priority of the authentication method. The authentication method is selected depending on the percentage of usage. This percentage is calculated by dividing the number of uses of the authentication method by the sum of all authentication times. Table 3 represents the proposed Authentication Method Priority Table.

Table 3: Authentication Method Priority Table

Authentication Method	***Priority***
Email	3
SMS	2
WhatsApp	1

In the User Authentication Process Status step, after selecting the authentication method, the first authentication layer using 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 4 and Table 5, the authentication methods are applied by $user_k$ and the percentage of usage for each authentication method is represented. In case two authentication methods have the same percentage, Table 3 will determine which priority will be applied.

Table 4: Authentication Method Selection Example 1

	Authentication Method		
User name	Email	WhatsApp	SMS
$user_k$	5	4	5
Percentage	0.357	0.285	0.357

The last authentication method is SMS.
Email percent = 5 ÷ (5 + 3 + 4) = 0.357
WhatsApp percent = 4 ÷ (5 + 3 + 4) = 0.285
SMS percent = 4 ÷ (5 + 3 + 4) = 0.357
The next authentication method will be WhatsApp because it has the lowest percent

Table 5: Authentication Method Selection Example 2

	Authentication Method		
User name	Email	WhatsApp	SMS
$user_k$	5	5	5
Percentage	0.333	0.333	0.333

The last authentication method is WhatsApp.
Email percent = 5 ÷ (5 + 3 + 4) = 0.333
WhatsApp percent = 4 ÷ (5 + 3 + 4) = 0.333
SMS percent = 4 ÷ (5 + 3 + 4) = 0.333
The next authentication method will be Email. All methods had the same percentage but the last authentication method was WhatsApp. Both Email and SMS had the same percentage but according to the authentication method, priority table Email had high priority.

3.1.2 Authentication Techniques Pool

The Authentication Techniques Pool is a shared pool that contains a group of authentication techniques. It provides the ability to add any required authentication techniques, just implement authentication techniques, add them to the pool, then add them to the priority table to be used.

3.2 Intrusion Detection with User Behavior Factors

As discussed in [11], the intrusion detection component is based on the user factor that paths through four 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. Additional steps are added to complete the process of identifying the intruders based on the user behavior. After the user registration process for the first time, s/he starts logging into the application. The location of the user is stored for the next time the user accesses the application. Also, the user's usually used web browser is stored. The intrusion detection steps start with the first four steps which depend on the user factor after the user passes the steps successfully the user geolocation is checked if the location is different than the user's default browser is also checked. In this case, both user's geolocation and the default browser are different the user account is blocked and the user is added to the suspected table. In case one of them is not the same as previously stored the $AUTH_{ADD}$ is fired to authenticate the user. In case of $AUTH_{ADD}$ failure the user is added to the suspected table and the user account is blocked until the admin user ensures the user identity. The all-intrusion detection steps with behavioral factors were shown in Fig. 6.

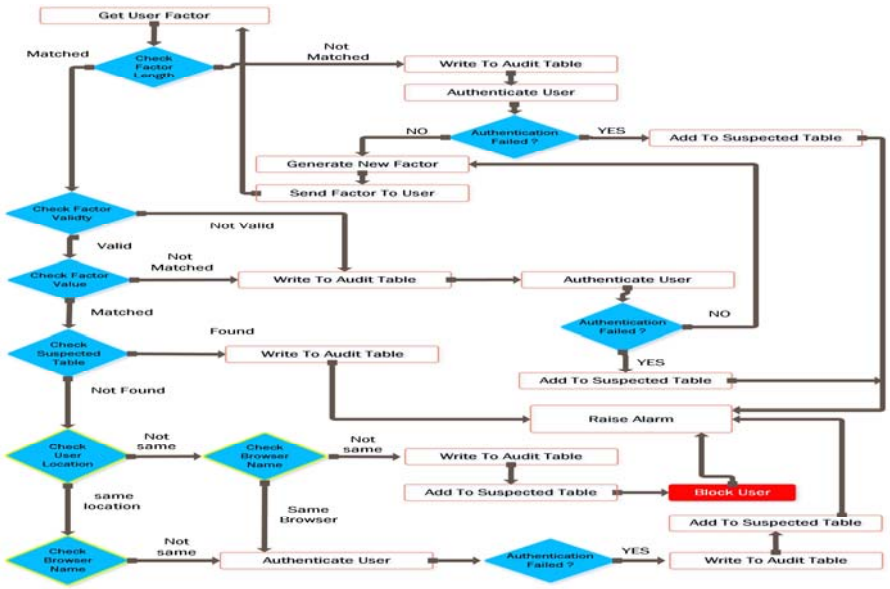

Fig. 6 Intrusion Detection Steps with User Behavior Factors

3.3 Proposed Framework Login Procedures

After applying the AMS and the behavioral factors to the intrusion detection steps to the framework in [11]. The complete access steps and intrusion detection processes are depicted in Fig. 7.

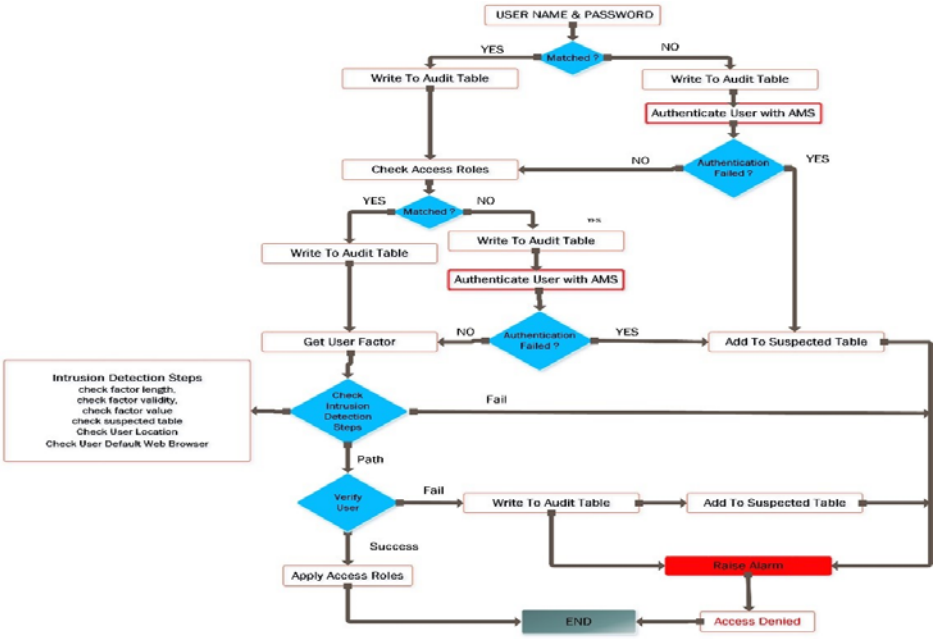

Fig. 7 Overall access steps in conjunction with intrusion detection.

As presented in Fig. 7, the overall access procedures are mainly relying on three factors of authentication. The first authentication factor (username and password) is applied with access rules. The second authentication factor is the user access factor that was created earlier in the user creation stage. It is used in intrusion detection steps to verify the following:

- User factor length
- User factor validity
- Entered user factor value
- Suspected table
- User location
- User default web browser

The third authentication factor is the user verification OTP is sent based on AMS and authorization rules that are applied.

4. Experimental Results

A data set of 3900 cases was generated according to the possible test scenarios that can be applied to the proposed framework. The data set is divided into two main parts. The first part represents normal users with 3000 cases that are used to calculate the false positive alert (FP) rate. Part Two with 900 cases representing intruders is used to calculate the detection rate (DR) and the false negative alert rate (FN). Intruders are also categorized into two groups insiders and outside hackers. Experimental results are based on the proposed access mechanism that involves access rules, multi-factor authentication, intrusion detection, and AMS for the proposed framework. These results are calculated based on the login steps and applied to the two frameworks. Table 6 shows the comparison of calculated percentages between both frameworks.

Table 6: FP, DR, and FN Comparison

	Framework in [11]	***Proposed Framework***
FP	0.5 %	0.8 %
DR	97.0 %	99.0 %
FN	3.0 %	1.0 %

4.1 False Positive (FP) Alarms

As shown in Table 6 and Fig. 8, after applying the AMS and behavioral factors to the intrusion detection process. The percentage of normal users who are considered

intruders as indicated by the FP rate has increased from 0.5% to 0.8% in the new framework. The FP rate is calculated by dividing the number of normal users who are considered intruders (N_f) by the total number of normal users (N) as shown in Formula (1).

$$FP = \frac{N_f}{N} \times 100\% \quad (1)$$

The increase in the FP rate is due to users who try to access the application from a different location or use a different web browser or due to the failure of $AUTH_{ADD}$.

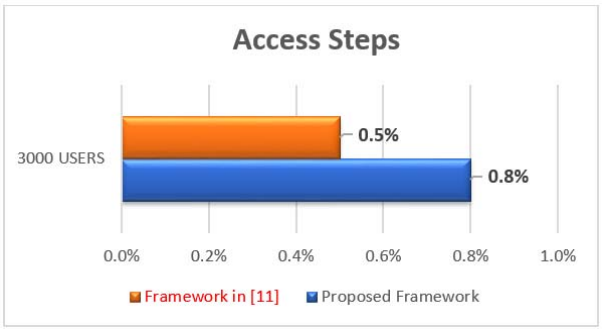

Fig. 8 FP Alarms.

4.2 Detection Rate (DR)

As shown in Table 6 and Fig. 9, the DR is increased from 97% to 99% in the new framework after applying the AMS and behavioral factors to the intrusion detection process. The DR is calculated by dividing the whole number of detected users (N_d) by the total number of users (N). This is shown in Formula (2).

$$DR = \frac{N_d}{N} \times 100\% \quad (2)$$

The DR records a higher percentage due to AMS which prevents intruders who succeed to steal one of the authentication methods. Assume an intruder steals the user's name and email, at first s/he will be authenticated using email but the OTP which is the third authentication factor will be sent to another authentication method like WhatsApp or SMS. While the framework in [11] just relies on email authentication which increases the intruder opportunities to access the application in case of email disclosure. Also, the behavioral factors will detect the intruder in case of s/he login from a different location or uses a different web browser. Therefore, the intruder will be blocked and an alarm will be raised.

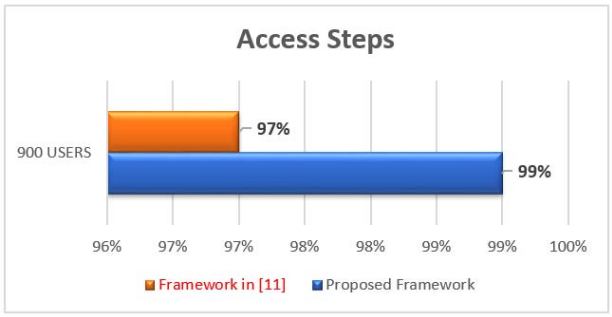

Fig. 9 Overall DR

4.3 False Negative (FN) Alarms

As shown in Table 6 and Fig. 10, the FN rate decreased from 3.0% to 1.0% in the new framework. This rate indicates the percentage of intruders who successfully routed their login steps after applying AMS and behavioral factors to intrusion detection. FN is calculated by dividing the number of passing malignant users (N_p) by the total number of examined users (N). It appears in Formula (3).

$$FN = \frac{N_p}{N} \times 100\% \quad (3).$$

The FN rate has decreased due to higher detection ratios. FN originates from internal intruders who already have access to the application as normal users and are trying to perform malevolent actions.

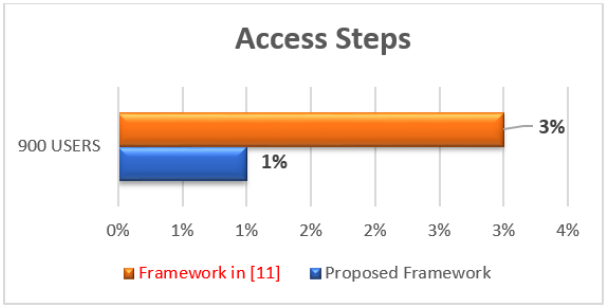

Fig. 10 FN alarms.

5. 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 the achievement of balancing ease of use with 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 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 WhatsApp 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 as other factors in the intrusion detection process, the proposed framework achieves increased security by 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. Experimental results are performed to measure the detection rate, false negative alarm rate, and false positive alarm rate. The detection rate increased from 97% to 99%. The false negative rate decreased from 3.0% to 1.0%. The false positive rate is increased by 60 %.

References

[1] H. Tabrizchi and M. Kuchaki Rafsanjani, "A Survey on Security Challenges in Cloud Computing: Issues, Threats, and Solutions," The Journal of Supercomputing, vol. 76, no. 12, pp. 9493-9532, 2020, doi: https://doi.org/10.1007/s11227-020-03213-1.

[2] P. K. Yeng, S. D. Wulthusen, and B. Yang, "Comparative Analysis of Threat Modeling Methods for Cloud Computing towards Healthcare Security Practice," International Journal of Advanced Computer Science and Applications (IJACSA), vol. 11, no. 11, pp. 772-784, 2020, doi: http://dx.doi.org/10.14569/IJACSA.2020.0111194.

[3] D. R. Panda, S. K. Behera, and D. Jena, "A Survey on Cloud Computing Security Issues, Attacks and Countermeasures," in Advances in Machine Learning and Computational Intelligence, Singapore, S. Patnaik, X.-S. Yang, and I. K. Sethi, Eds., 2021: Springer Singapore, pp. 513-524, doi: https://doi.org/10.1007/978-981-15-5243-4_47.

[4] B. Sumitra, C. Pethuru, and M. Misbahuddin, "A Survey of Cloud Authentication Attacks and Solution Approaches," International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE), vol. 2, no. 10, pp. 6245-6253, 2014.

[5] V. V. S. S. S. BALARAM, "Cloud Computing Authentication Techniques: A Survey," International Journal of Scientific Engineering and Technology Research (IJSETR), vol. 6, no. 3, pp. 458-464, 2017.

[6] S. Sudha and S. S. Manikandasaran, "A Survey on Different Authentication Schemes in Cloud Computing Environment," International Journal of Management, IT and Engineering, vol. 9, no. 1, pp. 359-375, 2019.

[7] A. Ometov, S. Bezzateev, N. Mäkitalo, S. Andreev, T. Mikkonen, and Y. Koucheryavy, "Multi-Factor Authentication: A Survey," Cryptography, vol. 2, no. 1, 2018, doi: https://doi.org/10.3390/cryptography2010001.

[8] B. O. ALSaleem and A. I. Alshoshan, "Multi-Factor Authentication to Systems Login," in 2021 National Computing Colleges Conference (NCCC), 27-28 March 2021 2021, pp. 1-4, doi: https://doi.org/10.1109/NCCC49330.2021.9428806.

[9] A. A. S. AlQahtani, Z. El-Awadi, and M. Min, "A Survey on User Authentication Factors," in 2021 IEEE 12th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON), Vancouver, BC, Canada, 27-30 Oct 2021, pp. 0323-0328, doi: https://doi.org/10.1109/IEMCON53756.2021.9623159.

[10] D. Dasgupta, A. Roy, and A. Nag, "Multi-Factor Authentication," in Advances in User Authentication, D. Dasgupta, A. Roy, and A. Nag Eds., (Infosys Science Foundation. Cham: Springer International Publishing, 2017, pp. 185-233.

[11] W. Said, E. Mostafa, M. M. Hassan, and A. M. Mostafa, "A Multi-Factor Authentication-Based Framework for Identity Management in Cloud Applications," Computers, Materials & Continua, vol. 71, no. 2, pp. 3193--3209, 2022, doi: https://doi.org/10.32604/cmc.2022.023554

[12] S. Andrés, "Zero Factor Authentication: A Four-Year Study of Simple Password-less Website Security via One-Time Emailed Tokens," Journal of Information Security and Applications, 2015.

[13] N. Gunson, D. Marshall, H. Morton, and M. Jack, "User Perceptions of Security and Usability of Single-Factor and Two-Factor Authentication in Automated Telephone Banking," Computers & Security, vol. 30, no. 4, pp. 208-220, 2011, doi: https://doi.org/10.1016/j.cose.2010.12.001.

[14] A. Bruun, K. Jensen, and D. Kristensen, "Usability of Single- and Multi-factor Authentication Methods on Tabletops: A Comparative Study," in Human-Centered Software Engineering, Berlin, Heidelberg, S. Sauer, C. Bogdan, P. Forbrig, R. Bernhaupt, and M. Winckler, Eds., 2014, vol. 8742: Springer Berlin Heidelberg, in Lecture Notes in Computer Science, pp. 299-306.

[15] F. K. Mupila and H. Gupta, "A Multi-factor Approach for Cloud Security," in Innovations in Computer Science and Engineering, Singapore, H. S. Saini, R. Sayal, A. Govardhan, and R. Buyya, Eds., 2021, vol. 171: Springer Singapore, in Lecture Notes in Networks and Systems, pp. 437-445.

[16] R. Neware, U. Shrawankar, P. Mangulkar, and S. Khune, "Review on Multi-Factor Authentication (MFA) Sources and Operation Challenges," International Journal of Smart Security Technologies (IJSST), vol. 7, no. 2, 2020, doi: https://doi.org/10.4018/IJSST.2020070104.

[17] S. Boonkrong, "Multi-Factor Authentication," in Authentication and Access Control: Practical Cryptography Methods and Tools, S. Boonkrong Ed. Berkeley, Apress, 2021, ch. 6, pp. 133-162.

[18] D. Tirfe and V. K. Anand, "A Survey on Trends of Two-Factor Authentication," in Contemporary Issues in Communication, Cloud and Big Data Analytics, Singapore, H. K. D. Sarma, V. E. Balas, B. Bhuyan, and N. Dutta, Eds., 2022, vol. 281: Springer Singapore, in Lecture Notes in Networks and Systems, pp. 285-296, doi: https://doi.org/10.1007/978-981-16-4244-9_23.

[19] P. Wang and R. Baskerville, "The Case for Two-Factor Authentication- Evidence from a Systematic Literature Review," in Pacific Asia Conference on Information Systems (PACIS 2019) Proceedings, X'ian, China, D. Xu, J. Jiang, and H.-W. Kim, Eds., 8-12 July 2019

[20] B. S. Archana, A. Chandrashekar, A. G. Bangi, B. M. Sanjana, and S. Akram, "Survey on Usable and Secure Two-Factor Authentication," in 2017 2nd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT), 19-20 May 2017, pp. 842-846, doi: https://doi.org/10.1109/RTEICT.2017.8256716.

[21] H. Lee, D. Kang, Y. Lee, and D. Won, "Secure Three-Factor Anonymous User Authentication Scheme for Cloud Computing Environment," Wireless Communications and Mobile Computing, vol. 2021, pp. 1-20, 2021, doi: https://doi.org/10.1155/2021/2098530.

[22] S. Jain, R. Gautam, S. Sharma, R. Tomar, and T. Choudhury, "Four-Factor Authentication with Emerging Cybersecurity for Mobile Transactions," in Innovations in Cyber Physical Systems, Singapore, J. Singh, S. Kumar, and U. Choudhury, Eds., 2021, vol. 788: Springer Singapore, in Lecture Notes in Electrical Engineering, pp. 391-399, doi: https://doi.org/10.1007/978-981-16-4149-7_35.

[23] J. Brainard, A. Juels, R. L. Rivest, M. Szydlo, and M. Yung, "Fourth-Factor Authentication: Somebody You Know," presented at the Proceedings of the 13th ACM conference on Computer and communications security, Alexandria, Virginia, USA, 2006. [Online]. Available: https://doi.org/10.1145/1180405.1180427.

[24] K. Sharmila and V. Janaki, "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, K. S. Raju, A. Govardhan, B. P. Rani, R. Sridevi, and M. R. Murty, Eds., 2020, vol. 1090: Springer Singapore, in Advances in Intelligent Systems and Computing, pp. 491-500, doi: https://doi.org/10.1007/978-981-15-1480-7_41.

[25] S. Hemamalini and M. L. A. E. Manuel, "A Fuzzy Implementation of Biometrics With Five Factor Authentication System For Secured Banking," International Journal of Smart Sensor and Adhoc Network, vol. 1, no. 4, pp. 238-242, 2012, doi: https://doi.org/10.47893/IJSSAN.2012.1070.

[26] R. M. Saqib et al., "Analysis and Intellectual Structure of the Multi-Factor Authentication in Information Security," Intelligent Automation & Soft Computing, vol. 32, no. 3, pp. 1633-1647, 2022, doi: https://doi.org/10.32604/iasc.2022.021786.

[27] D. H. Patil, V. S. Asbe, M. S. Chavan, P. L. Birajdar, and G. A. Joshi, "A Survey on Private Cloud Storage Security using Multifactor Authentication," Journal of Architecture & Technology, vol. XI, no. VIII, pp. 7-11, 2019.

[28] M. I. Hussain et al., "AAAA: SSO and MFA Implementation in Multi-Cloud to Mitigate Rising Threats and Concerns Related to User Metadata," Applied Sciences, vol. 11, no. 7, 2021, doi: https://doi.org/10.3390/app11073012.

[29] Meena.S and V.Gayathri, "Securing Personal Health Records using Advanced Multi-Factor Authentication in Cloud Computing," International Journal of Recent Technology and Engineering (IJRTE), vol. 8, no. 6, pp. 5133-5140, 2020, doi: https://doi.org/10.35940/ijrte.F9724.038620.

[30] S. Dhanasekaran, B. S. Murugan, and V. Vasudevan, "A Reliable Agent System for Cloud Service Discovery using MFA Technique," International Journal of Recent Technology and Engineering (IJRTE), vol. 8, no. 4S2, pp. 682-685, doi: https://doi.org/10.35940/ijrte.D1110.1284S219.

[31] S. R. Monaswarnalakshmi and C. P. Sai Aravindhan, "Multifactor Authentication in IoT Devices for Ensuring Secure Cloud Storage in Smart Banking," International Research Journal of Engineering and Technology (IRJET), vol. 5, no. 3, pp. 1307-1311, 2018.

[32] K. D. Priya and L. Sumalatha, "Trusted Hybrid Multifactor Authentication for Cloud Users," i-manager's Journal on Cloud Computing, vol. 7, no. 1, pp. 12-20, 2020, doi: https://doi.org/10.26634/jcc.7.1.16670.

[33] C. Singh and T. D. Singh, "A 3-Level Multifactor Authentication Scheme for Cloud Computing," International Journal of Computer Engineering & Technology (IJCET), vol. 10, no. 1, pp. 184-195, 2019.

[34] S. C. Patel, S. Jaiswal, R. S. Singh, and J. Chauhan, "Access Control Framework Using Multi-Factor Authentication in Cloud Computing," International Journal of Green Computing (IJGC) vol. 9, no. 2, 2018, doi: https://doi.org/10.4018/IJGC.2018070101.

[35] M. Kaleem and M. J. Arshad, "A Customizable Client Authentication Framework (CCAF) Based on Multi-Factor for Cloud Computing Application," International Journal of Computer Science and Telecommunications (IJCST), vol. 8, no. 3, pp. 18-25, 2017.

[36] R. K. Banyal, P. Jain, and V. K. Jain, "Multi-Factor Authentication Framework for Cloud Computing," in 2013 Fifth International Conference on Computational Intelligence, Modelling and Simulation (CSSIM), Seoul, Korea (South), 24-25 Sept. 2013, pp. 105-110, doi: https://doi.org/10.1109/CIMSim.2013.25.

[37] Z. E. Karabulut and M. C. Kasapbaşı, "Cloud Computing Integrated Multi-Factor Authentication Framework Application in Logistics Information Systems," Journal of International Trade, Logistics and Law (JITAL), vol. 3, no. 2, pp. 50-57, 2018. [Online]. Available: http://www.jital.org/index.php/jital/article/view/66.

[38] R. Nikam and M. Potey, "Cloud storage security using Multi-Factor Authentication," in 2016 International Conference on Recent Advances and Innovations in Engineering (ICRAIE), 23-25 Dec. 2016, pp. 1-7, doi: https://doi.org/10.1109/ICRAIE.2016.7939528.

[39] E. Erdem and M. T. Sandıkkaya, "OTPaaS—One Time Password as a Service," IEEE Transactions on Information Forensics and Security, vol. 14, no. 3, pp. 743-756, 2019, doi: https://doi.org/10.1109/TIFS.2018.2866025.

[40] K. A. Taher, T. Nahar, and S. A. Hossain, "Enhanced Cryptocurrency Security by Time-Based Token Multi-Factor

Authentication Algorithm," in 2019 International Conference on Robotics,Electrical and Signal Processing Techniques (ICREST), 10-12 Jan. 2019, pp. 308-312, doi: https://doi.org/10.1109/ICREST.2019.8644084.

[41] I. Gordin, A. Graur, and A. Potorac, "Two-Factor Authentication Framework for Private Cloud," in 2019 23rd International Conference on System Theory, Control and Computing (ICSTCC), 9-11 Oct. 2019, pp. 255-259, doi: https://doi.org/10.1109/ICSTCC.2019.8885460.

[42] S. Kambou and A. Bouabdallah, "A Strong Authentication Method for Web/Mobile Services," in 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, doi: https://doi.org/10.1109/CSCloud/EdgeCom.2019.000-8.

[43] W. Kennedy and A. Olmsted, "Three Factor Authentication," in 2017 12th International Conference for Internet Technology and Secured Transactions (ICITST), Cambridge, UK, 11-14 Dec. 2017, pp. 212-213, doi: https://doi.org/10.23919/ICITST.2017.8356384.

[44] M. A. Hassan and Z. Shukur, "A Secure Multi Factor User Authentication Framework for Electronic Payment System," in 2021 3rd International Cyber Resilience Conference (CRC), Langkawi Island, Malaysia, 29-31 Jan. 2021, pp. 1-6, doi: https://doi.org/10.1109/CRC50527.2021.9392564.

[45] M. A. Hassan, Z. Shukur, and M. K. Hasan, "Enhancing Multi-Factor User Authentication for Electronic Payments," in Inventive Computation and Information Technologies, Singapore, S. Smys, V. E. Balas, K. A. Kamel, and P. Lafata, Eds., 2021, vol. 173: Springer Singapore, in Lecture Notes in Networks and Systems, pp. 869-882, doi: https://doi.org/10.1007/978-981-33-4305-4_63.

[46] B. A. Oke, O. M. Olaniyi, A. A. Aboaba, and O. T. Arulogun, "Multifactor Authentication Technique for a Secure Electronic Voting System," Electronic Government, an International Journal (EG), vol. 17, no. 3, pp. 312-338, 2021, doi: https://doi.org/10.1504/EG.2021.115999.

[47] B. A. Oke, O. M. Olaniyi, A. A. Aboaba, and O. T. Arulogun, "Developing Multifactor Authentication Technique for Secure Electronic Voting System," in 2017 International Conference on Computing Networking and Informatics (ICCNI), Lagos, Nigeria, 29-31 Oct. 2017, pp. 1-6, doi: https://doi.org/10.1109/ICCNI.2017.8123773.

[48] O. M. Olaniyi, E. M. Dogo, B. K. Nuhu, H. Treiblmaier, Y. S. Abdulsalam, and Z. Folawiyo, "A Secure Electronic Voting System Using Multifactor Authentication and Blockchain Technologies," in Blockchain Applications in the Smart Era, S. Misra and A. Kumar Tyagi Eds., (EAI/Springer Innovations in Communication and Computing. Cham: Springer, 2022, pp. 41-63.

[49] O. M. Olaniyi, O. T. Arulogun, E. O. Omidiora, and A. Oludotun, "Design of Secure Electronic Voting System using Multifactor Authentication and Cryptographic Hash Functions," International Journal of Computer and Information Technology, vol. 2, no. 6, pp. 1122-1130, 2013. [Online]. Available: http://www.ijcit.com/archives/volume2/issue6/Paper020618.pdf.

[50] T. P. Abayomi-Zannu, I. A. Odun-Ayo, and T. F. Barka, "A Proposed Mobile Voting Framework Utilizing Blockchain Technology and Multi-Factor Authentication," Journal of Physics: Conference Series (JPCS), vol. 1378, no. 3, p. 032104, 2019, doi: https://doi.org/10.1088/1742-6596/1378/3/032104.

[51] M. Rusdan and D. T. Manurung, "Designing of User Authentication Based on Multi-factor Authentication on Wireless Networks," Journal of Advanced Research in Dynamical and Control Systems (JARDCS), vol. 12, no. 1, 2020, doi: https://doi.org/10.5373/JARDCS/V12I1/20201030.

[52] A. Kinai, F. Otieno, N. Bore, and K. Weldemariam, "Multi-Factor Authentication for Users of Non-Internet based Applications of Blockchain-based Platforms," in 2020 IEEE International Conference on Blockchain (Blockchain), Rhodes, Greece, 2-6 Nov. 2020, pp. 525-531, doi: https://doi.org/10.1109/Blockchain50366.2020.00076.

[53] K. Lee, "A Study on User Access Control Method using Multi-Factor Authentication for EDMS," International Journal of Security and Its Applications (IJSIA), vol. 7, no. 6, pp. 327-334, 2013, doi: http://dx.doi.org/10.14257/ijsia.2013.7.6.33.

[54] S. G. Santhi and M. Kameswara Rao, "Multifactor User Authentication Mechanism Using Internet of Things," in Second International Conference on Computer Networks and Communication Technologies, Cham, S. Smys, T. Senjyu, and P. Lafata, Eds., 2020, vol. 44: Springer International Publishing, in Lecture Notes on Data Engineering and Communications Technologies, pp. 496-502, doi: https://doi.org/10.1007/978-3-030-37051-0_56.

[55] M. K. Rao, S. G. Santhi, and M. A. Hussain, "Multi Factor User Authentication Mechanism using Internet of Things," presented at the Proceedings of the Third International Conference on Advanc ed Informatics for Computing Research, Shimla, India, 2019.

[56] J. Liu, X. Zou, J. Han, F. Lin, and K. Ren, "BioDraw: Reliable Multi-Factor User Authentication with One Single Finger Swipe," in 2020 IEEE/ACM 28th International Symposium on Quality of Service (IWQoS), Hang Zhou, China, 15-17 June 2020, pp. 1-10, doi: https://doi.org/10.1109/IWQoS49365.2020.9212855.

[57] D. Lu, D. Huang, Y. Deng, and A. Alshamrani, "Multifactor User Authentication with In-Air-Handwriting and Hand Geometry," in 2018 International Conference on Biometrics (ICB), 20-23 Feb. 2018, pp. 255-262, doi: https://doi.org/10.1109/ICB2018.2018.00046.

[58] N. A. K. Abiew, M. D. Jnr., and S. O. Banning, "Design and Implementation of Cost Effective Multi-factor Authentication Framework for ATM Systems," Asian Journal of Research in Computer Science (AJRCoS), vol. 5, no. 3, pp. 7-20, 2020, doi: https://doi.org/10.9734/ajrcos/2020/v5i330135.

[59] D. Bouck-Standen and J. Kipke, "Multi-Factor Authentication for Public Displays using the Semantic Ambient Media Framework," in ADVCOMP 2019 : the Thirteenth International Conference on Advanced Engineering Computing and Applications in Sciences, Porto, Portugal, C.-P. Rückemann and W.-U. Münster, Eds., 22-26 Sep 2019: International Academy, Research and Industry Association (IARIA), pp. 30-35.

[60] S. Şahan, A. F. Ekici, and Ş. Bahtiyar, "A Multi-Factor Authentication Framework for Secure Access to

Blockchain," presented at the Proceedings of the 2019 5th International Conference on Computer and Technology Applications (ICCTA 2019), Istanbul, Turkey, 16-17 April, 2019.

[61] M. Z. M. Zin, R. M. Saidi, F. Sappar, and M. A. Arshad, "Multi-factor Authentication to Authorizing Access to an Application: A Conceptual Framework," Journal of Advanced Research in Computing and Applications, vol. 16, no. 1, pp. 1-9, 2019.

[62] E. R. M. Aleluya and C. T. Vicente, "Faceture ID: Face and Hand Gesture Multi-Factor Authentication Using Deep Learning," Procedia Computer Science, vol. 135, pp. 147-154, 2018, doi: https://doi.org/10.1016/j.procs.2018.08.160.

[63] E. O. Asani, O. B. Longe, A. J. Balla, R. O. Ogundokun, and E. A. Adeniyi, "Secure Human-Computer Interaction: A Multi-Factor Authentication CAPTCHA Scheme," in Handbook of Research on the Role of Human Factors in IT Project Management, S. Misra and A. Adewumi Eds. Hershey, PA, USA: IGI Global, 2020, pp. 149-163.

[64] O. G. Lala, H. O. Aworinde, and S. I. Ekpe, "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.

[65] A. A. Alghamdi, "A Verification System for Multi-Factor Authentication for E-Healthcare Architectures," Arab Journal for Scientific Publishing (AJSP), vol. 31, 2021.

[66] G. J. W. Kathrine, "A Secure Framework for Enhancing User Authentication in Cloud Environment using Biometrics," in 2017 International Conference on Signal Processing and Communication (ICSPC), Coimbatore, India, 28-29 July 2017, pp. 283-287, doi: https://doi.org/10.1109/CSPC.2017.8305854.