International Journal of Science and Research (IJSR)
ISSN: 2319-7064
Impact Factor 2024: 7.101

A Novel Three-Tier Multi Stage Verification System for Protection of Medical Records Over the Cloud Environment

Dr. J. Vinothkumar[1], Dr. S. Sutha[2]

Assistant Professor, Department of Computer Applications, Rajiv Gandhi Arts and Science College, Puducherry, India
Email: *jaivinothkumar. mca[at]gmail.com*

Assistant Professor, Department of Computer Applications, Rajiv Gandhi Arts and Science College, Puducherry, India
Email: *ssutha1612[at]gmail.com*

Abstract: ***This study aims to provide a multi-level authentication strategy that is secure, affordable, and easy to use. It leverages many factors to grant rights to resources on unreliable environment and facilitates money exchanges. The proposed research is predicated on the idea that an authentication scheme becomes more resilient to various sorts of assaults and harder to breach when it incorporates several tiers and multiple elements. This study aims to implement a technique known as Three Tier Multi-Stage Verification (TTMSV), which uses various factors to carry out the authentication procedure in three stages. Outside of Band (OOB) verification is another feature of the method that provides reliable defense from Man-In-The-Middle (MIM) attacks. Double encryption is used for the username and password in the first level. The second level employs Outside of Band (OOB) verification with email ID and mobile number for OTP verification. The third level involves the user interacting with a graphical interface by clicking on preset numbers of buttons and graphics and choosing preset numbers of menu items. The suggested system's security is dependent on user involvement on a graphical user interface that employs probability combinations of different integers, Outside of Band verification using OTP, and double encryption using SHA-1 and AES-128-CBC (Cipher Block Chaining).***

Keywords: One Time Password (OTP), Outside of Band 1verification (OOBV), SHA-1 and AES-128-CBC, Three-Tier Multi-Stage 1vaerification (TTMSV), Graphical User Interface

1. Introduction

Cloud computing (CC) is a booming platform that has advanced quickly in the modern era. It was made available to the public by two significant computing behemoths, IBM and Google. By offering on-demand services for software, servers, networking, storage, and databases, it completely changed the data industry. CC is described as "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources" by the National Institute of Standards and Technology (NIST) [1-2]. The terms IaaS, PaaS, and SaaS are used to describe the cloud computing services. In IaaS, cloud providers lend users access to servers, virtual machines, storage, networks, and operating systems. PaaS offers its clients an environment for creating, testing, distributing, and overseeing software platform. SaaS gives users access to software programs, but they never have any control over the operating system, hardware, or network. In cloud computing, there are four distinct implementation models.

- **Private Cloud:** The CC infrastructure is devoted to a single company, which may have several users. It is not disseminated to other institutions. Usually, a third party or the same entity is in charge of it. It's regarded as the most costly, yet insecure option.
- **Public Cloud:** The cloud service holder provides the infrastructure, which the broader public can use. The Internet is used to provide the services. It is thought to be the most unsecured and open to intrusions.
- **Community Cloud:** Organizations within the same category share the infrastructure. Either the firm or a cloud service holder may own and run it.
- **Hybrid cloud:** This type of cloud combines free and paid cloud resources.

Security and privacy are the two main challenges with cloud computing. As data is dispersed across numerous machines worldwide, it becomes increasingly crucial. The Cloud Security Alliance (CSA) named "The Notorious Nine"—nine significant cloud security threats. These problems include loss of data, service traffic hijacking, denial of service, malicious insiders, cloud abuse, inadequate due diligence, unsecured interfaces and APIs, and most importantly, shared technology. In addition to these problems, inadequate authentication procedures and methods for gaining access to the resource provide a further risk to data kept in the cloud. Since confirming a user's identity is one of the first stages in ensuring security, authentication plays a crucial role in cloud security [3-5].

We have presented a revolutionary three-tiered multi-stage verification technique for CC in this work. The program is dependent on a number of variables, including the amount of mouse clicks on different GUI elements on a monitor, an encrypted password, a One Time Password, a mail ID, and a mobile number.

2. Literature Survey

Singh, A. (2024) examined the system, which explores the theoretical foundations of SHA-3 and AES+ChaCha20. It assesses the system's fit for cloud-based applications by taking into account aspects like computational efficiency, encryption strength, and resilience to cryptographic attacks [6]. Kumar, R et. al (2017) suggested in their paper with the

goals of achieving dynamicity, protecting user identity, and maintaining data privacy. Additionally, it offers full public auditability for hybrid clouds. The confidentiality of data anduser uniqueness is maintained, and it is preserved from both internal and external adversaries. Virtual Machines (VM) and the Tri Degree Coalition (TDC) Architecture are used to accomplish this. The system seeks to offer the following features: extensive auditing, uniqueness, dynamicity, trackability, unpredictability, shared data privacy, and user identity. Additionally, the system's effectiveness is preserved [7]. To authenticate cloud users, the One Time Password (OTP) approach is suggested by Kyaw Swar Hlaing et al (2019). To increase security for cloud user authentication, the auto-produced OTP is encrypted using RSA public key encryption. Therefore, in their paper, the irrelevent party is not obliged to generate OTP. Their paper can assist in resolving the issue with user authentication in cloud environments [8] [9].

V. Venkatachalapathy. K. J. K. (2020) suggested conducting research to identify different types of attacks and proposed system to eliminating them by introducing a three-phase system with optimization objectives including energy preservation, load monitoring, and security using different algorithms [10] [11] [12]. A system that uses a USBdevice and the combination encryption process of Rivest-Shamir-Adleman (RSA) and Advanced Encryption Standard (AES) was proposed by Pitchay, S. A. et al. (2016). Even though the files are accessible through the cloud, they will all stay encrypted as long as the USB device is not removed from the node. The goal of using this technique is to completely secure the files rather than relying just on one password. The user won't be able to fully memorize the extremely complex combinations of the randomly generatedpasskeys. The USB drive containing the personal key needed to download files from the cloud was identified by their system [13].

Wang and et. al (2013) introduced a private-maintaining public auditing system that is secure in the cloud. They expanded on their findings to give the TPA the ability to effectively and concurrently audit numerous users. The suggested schemes are shown to be highly efficient and provably safe through extensive security and evaluation analysis. The quick performance of the design is further demonstrated by their initial experiment, which was carried out on an Amazon EC2 instance [14]. As stated by Mahmoodet. al (2019) Before storing the stego image in the cloud, a hash value is generated for the image using the Secure Hash Algorithm 2 (SHA-2). This ensures data integrity. Once the picture has been downloaded from the cloud, the same algorithm (i. e. e. SHA-2). The secret image is then obtained checking the hash values to see if the data stored in the cloud is varying. An extensive security and performance analysis has demonstrated the protection and high efficiency [15] [16-18].

3. Proposed Multi-Stage Verification Scheme

The OOB verification with a One Time Password and double encryption are the foundations of the proposed Three-Tier multi-Stage Verification scheme (TTMSV). Additionally, users interact with the graphical screen by pre-registering clicks on buttons, menu items, and images. In a multi-part scheme, even if one level is bypassed, an attacker will still need to proceed through additional levels to gain access to the target.

3.1 Phases in Authentication Scheme

The three stages of the scheme's operation are registration, authentication, and password changes.

3.1.1Registration Phase

A user enrolls them in the registration process by providing their email address and mobile number in addition to their username and password. Furthermore, in the first level of verification, the client is prompted to enter a phrase that will serve as a key for the double encryption procedure utilizing open SSL AES-128-ECB. During the third level of authentication, the client is additionally asked to enter the number of pictures to click, buttons to click, and menu items to select on a GUI screen. The registration form's details are displayed in Fig.1.

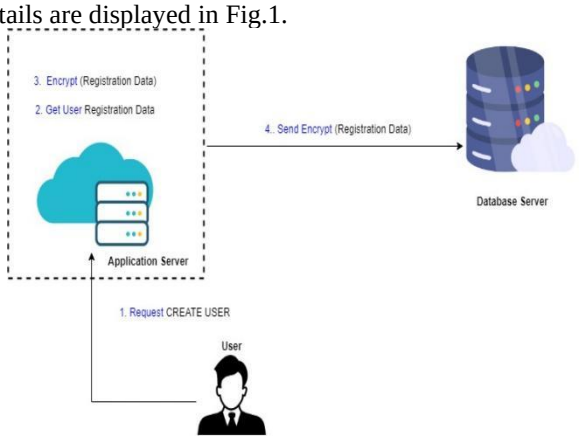

Figure 1: User Registration

3.1.2 Verification Stage

To reach the target, a client must successfully complete three levels of verification: double encryption-decryption with user credentials, OOB Verification using a time-limited One Time Password, and GUI screen interaction with a predetermined number of button, picture, and menu option clicks. The user enters an alphanumeric password and their username on a screen in the first level. The first level login screen is displayed in Figure 2.

The user's registered email address receives a random 6-digit message generated by the server in the next level after the username and password have been successfully verified by the database. The client must use his registered mobile number to send this OTP message back to the server through SMS.

Upon confirming the OTP, the client progresses to the last stage of verification. Here, they encounter a visual interface with a menu bar, various menu options, multiple buttons in distinct shapes and hues, and a 6x5 grid of images. To surmount this security level, the user must press a prearranged number of images within the grid, press a prearranged number of buttons, and choose a prearranged number of menu items. The figures must correspond to the choices made during registration

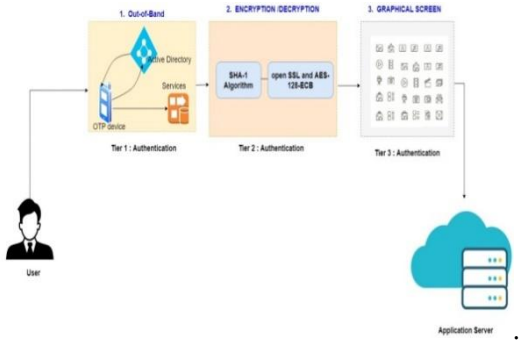

Figure 2: User Authentication

3.1.3 Password Change Phase

An option for the user to change their password has been included in the authentication scheme to make it more user-friendly. The user must pass all three authentication levels in order to access this option. Thus, a user can only modify their password following a successful login. The client can provide all of the info. he entered during registration on the screen that appears when he chooses to change his password. Here, a client can modify his alphabet and numeric mixture as password, adds a new key phrase for SHA-1 password encryption, and update his/her mail ID or mobile number. The client can also customize the number of buttons, pictures, and menu items they wish to click on in a graphical user interface for the last stage of Verification.

3.2 First Stage of Verification

Double encryption/decryption is the basis for the username/password scheme used in the first stage of verification. The password of the client is encrypted twice, once with SHA1 and once with AES-128-CBC. The user must select an alphanumeric password that is at least eight characters long. There must be capital, lowercase, digits, and special characters in the password. In order to generate a 40-digit hexadecimal output, this password is first encrypted using the SHA-1 algorithm.40 digits make up this hexadecimal output. E. Using an open SSL AES-128-CBC key that the client supplied during registration, the encrypted password is further encrypted. The password is stored in the server's database as the result of double encryption, as opposed to in hashed form, which is the output of SHA-1 encryption. This is the unique feature of the suggested work's enhanced security. E. the end result of AES-128 encryption.

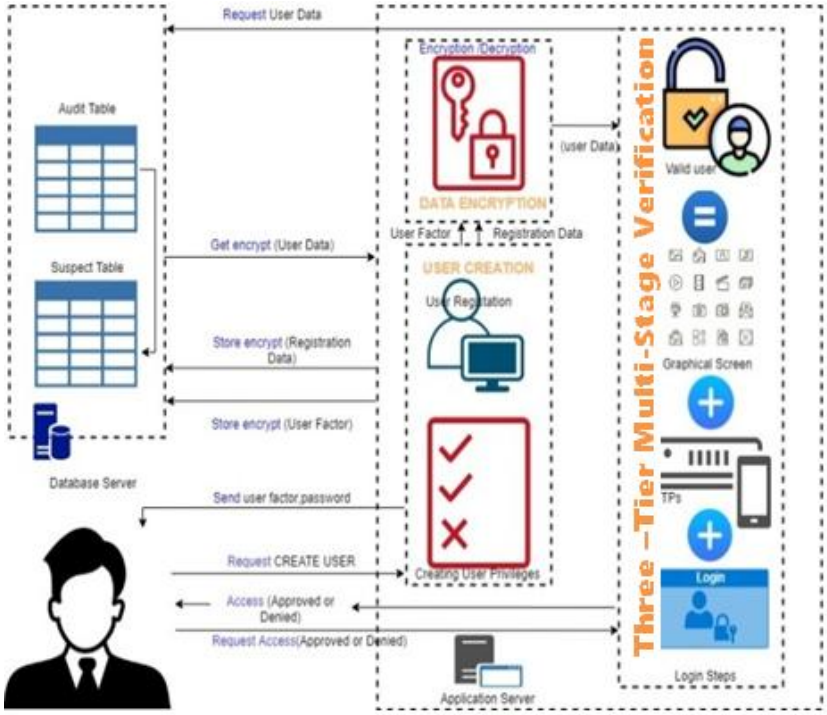

Figure 3: Proposed Architecture

During the authentication phase, the server retrieves the key from one table and the doubly encrypted password from another table in order to decrypt the password, which is then checked against the client's new password. If both passwords match, the client moves on to the next stage of verification. Our scheme offers enhanced security at this level by employing double encryption and preserving the key for the second encryption in a separate grid from the one containing the encrypted password. This degree of verification improves security and prevents insider attacks by using double encryption and decryption.

3.3 Second Stage of Verification

The second level of verification employs the OOBV technique. After successful username-password verification, the server crates a random 6-digit OTP and sends it to the client's registered mail ID. In the meanwhile, a screen that starts a backwards-counting timer is shown to the user. The maximum setting for this timer is 300 seconds. Within this time frame, the client must access his registered mail ID and receive the random code. To send this code to the server through SMS, the client needs to use the registered mobile number. If a client fails to send SMS to the server within the allotted 300 seconds, the session

will be expired and access will be blocked. A comparison will be made between the 6-digit random code that the client sent and the code that was sent to their registered mail ID. Furthermore, the server will verify with the database that the OTP was simultaneously sent from the registered number. If both of the components, i. e. The user's OTP and mobile number are sent to the third level of authentication once they have been confirmed to be correct. This level of verification in the recommended schemes provides an extra layer of security in terms of OOB verification because the OTP is transmitted and received over two separate, unrelated channels. OOB verification stops man-in-the-middle attacks from happening in the system. A malicious user must follow stringent time restrictions in order to steal or collapse the communication because the OTP in the proposed scheme is time-based. Because the OTP can only be verified from the registered mobile number, it is tougher for a malicious user to simultaneously access a client's mail ID address and mobile number.

3.4 Third Stage of Verification

The third stage of verification uses a GUI screen, and the client has to use a mouse to interact with the objects on the screen. Neither recognition nor recall are the foundations of this graphical password system. As a result, it does not cognitively tax the user's memory. After the OTP has been validated, our workloads a screen with a grid of six by five images, a menu bar with several menu options, and a variety of color and shape based buttons. To be verified at this stage, a client must select a predefined number of menu items from a variety of menu options and click on a predetermined number of buttons and images. Both the count of menu items chosen and the count of buttons and images clicked should be matched the count the client chose when registering. When these three numbers are accurately entered, the user's identity is verified. If any one of the numbers in the combination is off, access is prohibited.

The suggested plan requires a client to select three different menu items from various menus and click buttons and images at least three times. To deter hackers and enhance protection, the images in the 6 x 5 grid alternate at random each time a user logs in. Every login also has a different set of button labels, colors, and locations. The various menu options are constantly changing, even for the same user. Additionally, selecting or clicking on the same image, button, or menu item twice is prohibited by this level of authentication.

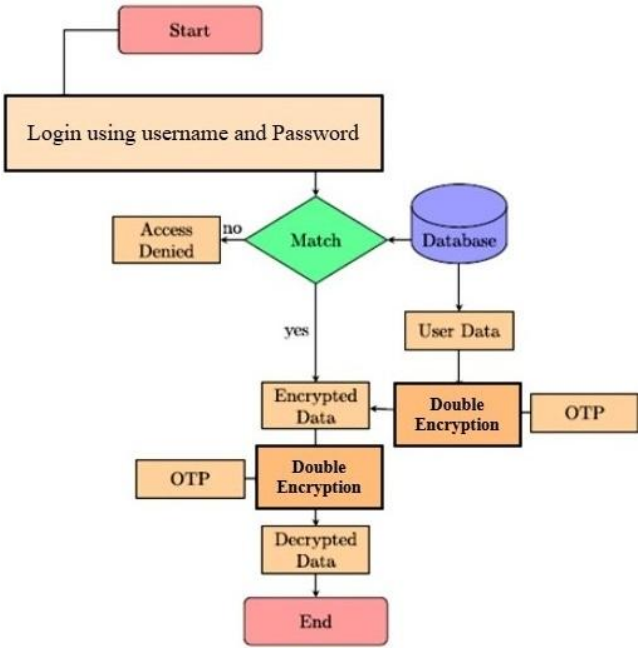

Figure 4: Working of Double Encryption

This level of authentication's security is determined using a probability model. The user of our proposed work must interact with the graphical screen based on three criteria, namely, buttons pressed count, menu items selected count and clicked images count in a grid. Thus, the formula provides the likelihood that the third level of authentication is secure:

$$S_{Third\ level} = 1 - (p1 * p2 * p3) \quad (1)$$

where p1 represents the possibility of correctly predicting the number of menu items chosen, p2 represents the possibility of correctly predicting the number of button clicks, and p3 represents the possibility of correctly predicting the number of image clicks. The third level's probability of security is represented by $S_{Thirdlevel}$ Level. For instance, the probability of this stage being secure is 90% if p1 = 1, p=20.6, and p3 = 0.5. Additionally, the user is only given one chance to choose the right combination. Other graphical elements, like sliders, checkboxes, and radio buttons, can be added to raise the number of clicks in order to enhance improvement of system protection. This will raise the possibility of a more secure system.

At the third stage of verification, the suggested scheme provides a lot of password space. The interfusion of the number of interactive items (i) and the key space size increases. E. buttons, menu options, screen graphics, and the quantity of items that are selected. If one is to click on q images from p, s buttons from r, and u menu items from the total of t, then the password space created by these three combinations is

$$p_{C_q + r_{C_s} + t_{C_u}} \quad (2)$$

Audit Table: All completed transactions are recorded in the audit table, starting with the login phase and concluding with access control. The audit table records each action a user takes with the application data. The audit table gives users a summary of all alarms raised so that future countermeasures can be increased.

Suspected Table: This table was made to keep track of all suspicious users who have overreached their authority.

3.5 Pseudo code for Three-Tier Multi-Stage Verification

The steps listed below represent how the TTMSV scheme operates.

Begin TTMSV

1) The user enters their login credentials, which include their username, password, email address, mobile number, key phrase, the number of buttons and pictures they want to click, and the number of menu items they want to select.
2) In step 2, Login option requires the username and password to be filled by the client.
3) In order to decrypt the SHA-1 password and verify user credentials from the database, the server uses the phrase that the user supplied as a key. Both open SSL and AES-128 CBC are used for this decryption.
4) If the user credential gets match in the database, the server sends a dynamic 6-digit OTP to the user's registered email address; if not, access is restricted. The server simultaneously shows a screen that starts a countdown of 300 seconds.
5) Using this 6-digit OTP that receives retrieves through email, the client sends a SMS to the server through registered mobile number.
6) If this OTP is not sent within the 300 seconds given, the login time expires and access is blocked. The server confirms that the 6-digit code is accurate and that the user's registered mobile number was used to send the OTP after receiving one from the user.
7) If both the OTP and the mobile number are correct, the server displays a GUI screen with a 6 x 5 grid of images, a number of buttons of different shapes and colors, and extensive menu items.
8) In order to proceed, the user must click on a set number of images in a grid, press buttons, and choose menu items with the same count as those chosen during registration.
9) The exact amount of each of the three actions, specifically. To access a specific resource, the user must click on buttons, menu items, and pictures.

End TTMSV

4. Results & Discussion

The dataset used in this section is shown in Table. Access roles, multi-level authentication, and intrusion detection were all included in the proposed access procedures to assess their effectiveness. To further improve efficiency, an extra authentication process ($AUTH_{ADD}$) was also added. The overall Detection Rate (DR), False Negative (FN) alarm rate, and False Positive (FP) alarm rate are measured to assess the effectiveness of the suggested access procedures. Tab 2. Describes the definition of the dataset taken in our experimental results and a classification of the clients types—normal clients or intruders.

Table 1: Experimental Details

Normal clients		Intruders			
3000		900			
70 clients	15 clients	Insider	Outsider	Insider	Outsider
-2.30%	-0.50%	18 clients (2%)	0 clients (0%)	18 clients (2%)	9 clients (1%)
FP rate		DR & FN Rates			

The False Positive (FP) alerts make reference to the potential for benign users to be mistakenly classified as dangerous users. Formula (3) illustrates this.

$$FP = \frac{N_f}{N} \times 100\% \quad (3)$$

As depicted in Fig.5. In the absence of ($AUTH_{ADD}$), 2.3 % of regular users are deemed intruders and added to the suspected table. To lower the FP rate, the ($AUTH_{ADD}$) process was combined with the login steps. We consider that the clients are regular clients who attempt to use the application.

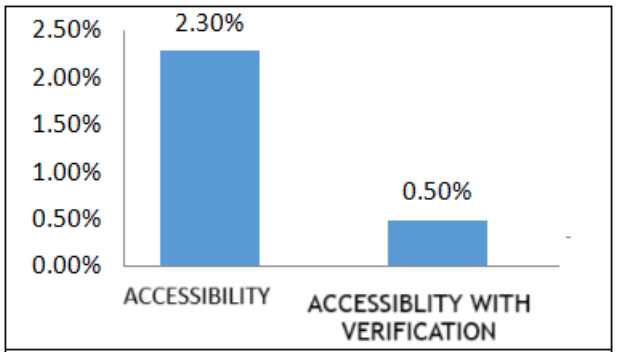

Figure 5: False Positive alert

By dividing the total number of detected clients (Nd) by the total number of clients (N), Detection Rate (DR) displays the ratio of intrusion actions detected. Formula (4) illustrates this.

$$DR = \frac{N_d}{N} \times 100\% \quad (4)$$

As depicted in Fig.6, the detection rate is high, at 98%, based on the use of multistage verification and intrusion detection. However, we have observed that the integration of the access and ($AUTH_{ADD}$) steps may facilitate an intruder's access to the application, lowering the Detection Rate (DR) to 97%.

The number of malicious users who successfully complete the login processes is indicated by the False Negative (FN) alarms. The number of malicious users who pass (Np) divided by the total number of users examined (N) yields the ratio. As can be seen in formula (5).

$$FN = \frac{N_P}{N} \times 100\% \quad (5)$$

As depicted in Fig.7, FN logs low numbers. Insider intruders account for the remaining 2.0% of the FN. They attempt to carry out malicious activations without utilizing the ($AUTH_{ADD}$) feature, which restricts access to the application to insiders only. The percentage of the FN increased to 3.0% because an outsider intruder may use the

($AUTH_{ADD}$) to access the application after using it. After examining the audit table, we discovered that a client should not use the ($AUTH_{ADD}$) more than twice.

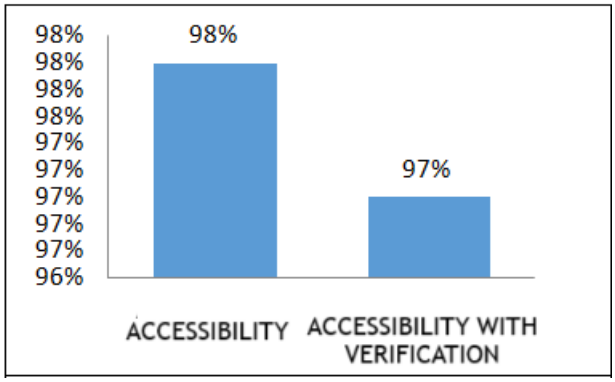

Figure 6: Overall DR

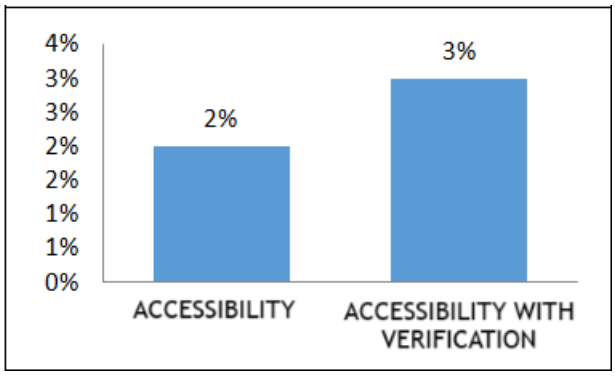

Figure 7: FN alert

5. Conclusion & Future Work

The first, second, and third levels of the three-tiered multi-stage verification method was proposed in this paper include outside-of-band verification, double encryption, and client interaction on a graphical screen. Based on open source GUI technologies, the proposed system allows users to verify for secure online transactions. Numerous security threats, such as dictionary, MIM, insider, and stolen credential attacks, are unable to get past the plan. Because, at the third stage of verification, the client only needs to remember a predetermined number of clicks rather than the kinds of images and the sequence in which they should be clicked, the scheme requires less cognitive load than recognition and recall based GUI password schemes.

To evaluate the usability of the suggested model and verify the system's resistance to different types of attacks, an empirical study is necessary. Future research will compare the security to evaluate whether the proposed plan is effective for different cloud applications, counter the shoulder surfing attack, and trade off user login time. Further investigation is necessary to determine the feasibility of the proposed touch-based screen design. Experimental results show that the suggested method achieved high detection rates with low false positive alert, demonstrating the accuracy and efficacy.

References

[1] Aalam, Z., Kumar, V., and Gour, S, "A review paper on hypervisor and virtual machine security", Journal of Physics: Conference Series, 1950 (1) (2021).
[2] Al Refai, H., Batiha, K., and Al-Refai, A. M, "An Enhanced User Authentication Framework in Cloud Computing", International Journal of Network Security & Its Applications, 12 (2), pp.59–75 (2020).
[3] Chen, L., Xian, M., Liu, J., and Wang, H, "Research on Virtualization Security in Cloud Computing", IOP Conference Series: Materials Science and Engineering, 806 (1) (2020).
[4] Gudimetla, S. R, "Multi-Factor Authentication for Cloud", International Research Journal of Modernization in Engineering Technology and Science, 03, pp.4341–4343 (2024).
[5] Hossain, M. A., and Al Hasan, M. A, "Improving cloud data security through hybrid verification technique based on biometrics and encryption system", International Journal of Computers and Applications, 44 (5), pp.455–464 (2022).
[6] Singh. A, "An Enhanced Three Layer Cryptographic Algorithm for Cloud Information Security", International Journal of Intelligent Systems and Applications in Engineering IJISAE, 2024 (17s), pp.615–627 (2024).
[7] Kumar, R. G. S., Nalini, T., and Saranya, V, "A Complete Public Auditing for Data Sharing in Hybrid Cloud using Tri Degree Coalition (TDC) architecture", 117 (21), pp.925–929 (2017).
[8] Kyaw Swar Hlaing and Nay Aung Aung, "Secure One Time Password OTP Generation for user Authentication in Cloud Environment", International Journal of Trend in Scientific Research and Development, 3 (6), pp.89–92 (2019).
[9] Venkatachalapathy, V. K. J. K, "A Security System for Electronic Medical Records using Three Phase Efficiency Model on Cloud", 29 (7), pp.4844–4860 (2020).
[10] Jaikumar, V., and Venkatachalapathy, K, "Integrative optimization with QoS using multi-level security in medical cloud", Journal of Ambient Intelligence and Humanized Computing (2021).
[11] Vinothkumar, J., & Venkatachalapathy, K, "Protection of Medical Records Using Block Chain Technology".9 (4) (2021).
[12] Pitchay, S. A., Alhiagem, W. A. A., Ridzuan, F., and Saudi, M. M, "A Proposed System Concept on Enhancing the Encryption and Decryption Method for Cloud Computing", Proceedings-UKSim-AMSS 17th International Conference on Computer Modelling and Simulation, UKSim 2015, pp.201–205 (2015).
[13] Wang, C., Chow, S. S. M., Wang, Q., Ren, K., and Lou, W, "Privacy-preserving public auditing for secure cloud storage", IEEE Transactions on Computers, 62 (2), pp.362–375 (2013).
[14] Mahmood, G., Sabeeh Mahmood, G., Jun Huang, D., and Abdulrahman Jaleel, B, "Achieving an Effective, Confidentiality and Integrity of Data in Cloud Computing", International Journal of Network Security, 21 (2), 326 (2019).

[15] Sun, J., Zeng, Y., Shi, G., Li, W., and Li, Z, "The Research for Virtualization Network Security on Cloud Computing", 146 (ICAITA), pp.145–148 (2018).
[16] Sun, W., Cai, Z., Li, Y., Liu, F., Fang, S., and Wang, G. "Security and Privacy in the Medical Internet of Things: A Review", Security and Communication Networks (2018).
[17] Liu, J., Huang, X., and Liu, J. K, "Secure sharing of Personal Health Records in cloud computing: Ciphertext-Policy Attribute-Based Signcryption", Future Generation Computer Systems, 52 (October), pp.67–76 (2015).
[18] M. Javaid, A. Haleem, R. P. Singh, and R. Suman, "5G technology for healthcare: Features, serviceable pillars, and applications, " Intell. Pharm., vol.1, no.1, pp.2–10 (2023).
[19] T. Althobaiti, Y. Sanjalawe, and N. Ramzan, "Securing Cloud Computing from Flash Crowd Attack Using Ensemble Intrusion Detection System, " Comput. Syst. Sci. Eng., vol.47, no.1, pp.453–469 (2023).
[20] D. H. Devi et al., "5G Technology in Healthcare and Wearable Devices: A Review, " Sensors, vol.23, no.5 (2023).
[21] J. Okwuibe, M. Liyanage, I. Ahmad, and M. Ylianttila, "Cloud and MEC security, " A Compr. Guid. to 5G Secur., no. October, pp.373–397 (2018).
[22] Ullah, H. Aznaoui, C. B. Şahin, M. Sadie, O. B. Dinler, and L. Imane, "Cloud computing and 5G challenges and open issues, " Int. J. Adv. Appl. Sci., vol.11, no.3, pp.187–193 (2022).
[23] K. Kim, H. Yang, J. Lee, and W. G. Lee, "Metaverse Wearables for Immersive Digital Healthcare: A Review, " Adv. Sci., vol.2303234, pp.1–24 (2023).
[24] D. F. T. Morais, G. Fernandes, G. D. Lima, and J. J. P. C. Rodrigues, "IoT-Based Wearable and Smart Health Device Solutions for Capnography: Analysis and Perspectives, " Electron., vol.12, no.5 (2023).
[25] J. Palomares, E. Coronado, C. Cervelló-Pastor, and S. Siddiqui, "Enabling Intelligence Inclusiveness in Edge to Cloud Continuum: Challenges and Opportunities, " in 2023 IEEE 9th International Conference on Network Softwarization (NetSoft), 2023, pp.362–365 (2023).
[26] S. Jung, H. Kim, X. Zhang, and S. Dey, "GaMiCO: Game-slicing based multi-interface computation offloading in 5G vehicular networks, " J. Commun. Networks, vol.25, no.4, pp.491–506 (2023).
[27] Alnoman, "How Artificial Intelligence Helped the Humanity During the COVID-19 Pandemic: A Review, " IEEE Trans. Artif. Intell., pp.1–10 (2023).
[28] M. Fahim, V. Sharma, T.-V. Cao, B. Canberk, and T. Q. Duong, "Machine Learning-Based Digital Twin for Predictive Modeling in Wind Turbines, " IEEE Access, vol.10, pp.14184–14194 (2022).
[29] J. Chen, C. Yi, S. D. Okegbile, J. Cai, and X. S. Shen, "Networking Architecture and Key Supporting Technologies for Human Digital Twin in Personalized Healthcare: A Comprehensive Survey, " IEEE Commun. Surv. Tutorials, p.1 (2023).
[30] Z. xia Lu et al., "Application of AI and IoT in Clinical Medicine: Summary and Challenges, " Curr. Med. Sci., vol.41, no.6, pp.1134–1150 (2021).
[31] K. M. Hosny, A. I. Awad, M. M. Khashaba, M. M. Fouda, M. Guizani, and E. R. Mohamed, "Enhanced multi-objective gorilla troops optimizer for real-time multi-user dependent tasks offloading in edge-cloud computing, " J. Netw. Comput. Appl., vol.218, p.103702 (2023).