UJEAS

UNIZIK JOURNAL OF ENGINEERING AND APPLIED SCIENCES

UNIZIK Journal of Engineering and Applied Sciences 2(1), June 2023, 177-186
Journal homepage: https://journals.unizik.edu.ng/index.php/ujeas
PRINT ISSN: 2992-4383 || ONLINE ISSN: 2992-4391

User-Driven Approach to Preventing Unsanctioned Profile Modifications and Deletions in Cloud-Based Multi-Tenant Infrastructures

Azubuike I. Erike[1*], Austin C. Azubogu[2] and Yusuf U. Mshelia[1]
[1]Department of Software Engineering, Federal University of Technology, Owerri, Imo State, Nigeria
[2]Department of Electronic and Computer Engineering, Nnamdi Azikiwe University, Awka, Anambra State, Nigeria
[*]Corresponding Author's E-mail: azubuike.erike@futo.edu.ng

Abstract
This study introduces a novel user-driven approach to counter unauthorized profile alteration and deletion in multi-tenant cloud environments. The researchers contend that conventional access control mechanisms are inadequate in mitigating insider threats and account hijackings, which can result from legitimate or unauthorized access to a cloud platform, with subsequent intentional or accidental modifications or deletions of data. To mitigate these threats, the researchers advocate for a user-driven approach that equips users with the ability to regulate access to their profiles utilizing the Serpentine Multifactor Authentication Technique (SeMFAT). The approach has two major components: the registration by validation process for registering authentication vectors and the authentication by validation procedure for authenticating the authentication vectors. The latter is activated when a user-secured action is triggered, based on a profile audit trail. The trail tracks all actions taken on a user's profile and activates the authentication by validation action to ensure that only users with verified privileges are granted the right to certain actions on their profiles. The authors assessed the efficacy of their approach by implementing a prototype on a multi-tenant cloud platform. 98% delivery success was recorded for SMS and emails response delivery, while a 100% success on preventing unauthorized profile alterations and deletions was recorded for all delivered messages. Overall, this study underscores the value of user-centric security measures in multi-tenant cloud settings, providing a feasible approach to thwarting both internal and external attacks since it is difficult to compromise all the user's authentication vectors within a limited authentication session.

Keywords: Authentication, cybersecurity, account hijacking, social engineering, Authentication Technique

1. Introduction

Recent advances in technology have seen an explosion in the rate of cybercrimes, especially as it concerns profile alteration and deletion in a multi-tenant cloud environment, with a particular emphasis on the social media space. Most attacks on the social media space can as well be traced back to the victim's domain in the social media space as its origin. This is because people's actions and lifestyles largely leave behind them a path that an attacker can use to trail the unsuspecting victim. Largely, these attacks come in the form of social engineering – which is a method used by hackers to obtain unauthorized access to systems by manipulating flaws in a behaviour known as mental preconceptions (Duarte et al., 2021). In the context of cybersecurity, social engineering is the practice of taking advantage of human weaknesses through manipulation to accomplish a malicious goal(Aldawood & Skinner, 2020). In a broader sense, the term is used as an umbrella term for a broad spectrum of computer exploitations that employ a variety of attack vectors and strategies to psychologically manipulate a user (Heartfield & Loukas, 2015). It involves the use of social skills to obtain usernames, passwords, and credit card data, or to compromise or alter the information and systems of an entity(Greavu Serban & Serban, 2014). Most attacks on the multi-tenant cloud environment seek to deny the user access to the domain perpetually. This is called hijacking – a situation where a user is ripped off of his account without the user having the chance to recover the account. Research conducted by (Shay et al., 2014) shows that about 30% of respondents have had their email or social networking accounts accessed by unauthorized persons.

The rather alarming increase in this crime was tightly related to the Single Sign-On Technology which brought a tighter coupling of web services – hence, at a breach of one account, most of the user's accounts are compromised (Ghasemisharif et al., 2018) – A sought of putting all of one's egg in one basket.

According to (Mirian et al., 2019), one of the reasons for the continual rise in cybercrime – as it relates to account hijacking, is because of the monetary gain that is associated with it - with prices commonly over $300 for each account successfully hijacked. According to the 2020 IBM study of data breaches, the average cost of a data breach in the healthcare industry alone was seven million, one hundred and thirty thousand dollars ($7.13 million) with an average cost of $150 per record (Security, 2020). In addition to the monetary gain achieved from successfully compromising each account, when a user's account is compromised, it becomes a potential threat to other accounts associated with such user account. This can ultimately lead to a complete network compromise through impersonation. So, the gravity of this crime qualifies it for the list of cybercrimes listed by Kaspersky (Kaspersky, 2021). Businesses of varying sizes are attacked daily. In a 2021 survey by the Department of Digital Culture, Media, And Sport, 39% of the business, and 26% of charities were attacked within the last twelve months about the time of reporting(Department for Digital Culture Media and Sport, 2021). This, therefore, calls for an urgent research response to avert the perpetuation of any attack on the user's profile should a user's account be compromised.

Hence, in cloud-based multi-tenant infrastructures, the security of user profiles is of utmost importance. Unauthorized profile modifications and deletions emanating from account hijackings pose significant threats to data integrity and user privacy. Traditional access control mechanisms have proven inadequate in mitigating these insider threats and account hijackings, which can lead to intentional or accidental unauthorized changes to user profiles. This research aims to develop a model to prevent the alteration and or deletion of data within a user's profile by locking such privileges using the distributed Serpentine Multi-Factor Authentication Technique SeMFAT. By definition, a multi-tenant environment is an ecosystem that is hosts different personalities with different virtues, characters, and values. The cloud environment is hence a digital ecosystem hosting business, organizations, communities, etc of varying sizes and having different characteristics and norms. An ecosystem exists because some occupants and data are the live wire of such an ecosystem. Research has been on the increase to digitally protect businesses in the ecosystem given the continual rise and the economic importance of the data in this age. This section presents a brief review of some works of literature sectioned in three different formats, basically focused on the commonest authentication handle - passwords. The rest of the paper is organized as follows. Section two presents the methodology for implementation. In section three, the results of the research are discussed, while section four concludes the research with future work.

1.1 Password strengthening

Password strengthening techniques are implemented to ensure that user passwords pass the minimum-security criteria to ensure that passwords are robust against cracking attacks. One of the ways to make passwords secure is through hashing. Several hashing algorithms have been developed to ensure robustness. However, a study to compare the performance of different hashing algorithms in web application security presented Argon2 as an ideal hashing algorithm for use with PHP 7.2 and above (Katrandzhiev et al., 2019). Another approach to strengthening password-based systems focused on developing a low-cost real-time security system with password self-generation ability (Banerjee et al., 2019). The microcontroller-based system with motion detection ability generates and sends the authorized user a new password for authentication. The module communicates the new password to the user using the SMS technology implemented using SIM 900 TTL module. A three-step protection technique was proposed by (Soumya et al., 2021) which involves the reception of the user-supplied password, hashing of the password using a cryptographic hash function, and the transformation of the password into a negative password. After all, the output is further encrypted using the symmetric-key algorithm.

A cost asymmetric secure hash (CASH) algorithm was introduced by (Blocki & Datta, 2015). The system used a Stackelberg game model to capture the essential elements of the interaction between a defender and an offline attacker, with the motivation that a legitimate authentication server will typically run an authentication procedure for correct password authentication other than repeated guesses by an offline attacker. Hence, by using randomization, the amortized cost of running CASH to verify a correct password is made smaller than the cost of rejecting an incorrect password. A two-factor authentication involving biometrics was presented by (Anand et al., 2018) using a self-efficient secure and scalable algorithm that does not require much space and is thus economical to ensure security and privacy in cloud service providers. A system of creating honey words which are false passwords that seek to represent user passwords was presented and proposed by (Shubham Sawant et al., 2018). The procedure involves getting a character in the original password and replacing it with another character from a pool of characters. A key-stretching

algorithm, Hash Extended Key Stretcher, was proposed. The algorithm takes a salt value and passes it through a hash function. The output is used to set the parameter for linear congruential pseudorandom generator G1. Then in the process, G1 is used to form G2, a second pseudo-random number generator. The output G2 is then used to stir an array B which is the natural input block size for the selected hash algorithm.

1.2 System Protection Techniques

A dual combat technique for curbing the username enumeration attack was developed to give the user the privilege of being involved in the combat process by initiating a virtualization and de-virtualization action upon sensing a dictionary attack or brute-force password attack (Erike et al., 2015). The system was able to track an attack and alert the user through an SMS notification about an envisaged attack on the user's profile. A cryptographic hashing technique to create a protected and crack-resistant password for user authentication was used for random hash registration for each user registration (Preethika, 2016). The hashed value is then concatenated with the user-supplied password before passing both through another hash function. This technique creates a one-way high entropy password that is resistant to cracking. (Horsch et al., 2017) implemented the password synchronization and backup systems using the PALPAS and PASCO schemes. The brute force resistant password generation mechanism operates in four building blocks as follows: Password description service through the Password Requirement Markup Language, the generation of password requirements using the Password Requirement Crawler PRC. The PRC extracts the requirement for Password Requirement Distribution PRD. The PRD then helps in making available the proposed password, which is the central purpose of the password assistant. A multi-level authentication system using sound and image-based password protection was proposed by (Moyila Mounika Dev et al., 2020). The research developed a multilevel sequential technique that utilized text, audio, and image signatures for user authentication.

While many pieces of research have been done, in this regard, preventing profile alteration and deletion in a multi-tenant cloud environment in the event of password compromise remains a puzzle that this research is focused on solving. Previous works presented the one-time password OTP and two-step authentication. However, attackers engage social engineering techniques to trick users into compromising their own account. This research presents a solution to this gap in research.

2.0 Material and System Design

The proposed methodology uses four independent authentication vectors; two phones and two email addresses, as tools for design implementation. Vectors here are carriers of authentication values – what can be within the reach of the user at any point in time for use in performing multifactor authentication. The feasibility of the use of these authentication vectors as tools came from the result of the validation survey conducted over a sample population to ascertain the viability of the use of such vectors in the design of this research work. 98.2% of the respondents were found to be between the ages of 18 and 50 years old. However, 98.3% of the total respondents are recorded to be active players in the social media cloud space (Facebook, WhatsApp, Twitter, Instagram, Telegram, etc). The analysis of this survey is seen in the results section. The basic research questions addressed in the survey are:

1. Does an average user possess multiple authentication vectors needed for the proposed technique?
2. What are the user behaviours with the technology that can enhance the implementation of the technique?

Serpentine multifactor authentication technique (SeMFAT) using independent authentication vectors is the bedrock of this research.

This approach ensures that there is a sequential validation of the authentication vectors both at set-up time and at the point of use. For this research, upon completion of 75% of the authentication validation process, deletion, alteration, and deletion privileges are unlocked for a properly signed-in user into the cloud environment. Note that the percentage validation process is not a benchmark. It is rather developer-dependent.

The fixed assumptions are:

1. The user has more than one phone, whether internet-enabled or not.
2. The user has more than one email address accessed using a different email client.
3. The idea of independence lies in the fact that the user does not use the same password or the 'remember me' feature in any email client the user chooses.

2.1 Research Design and Approach

The design has two major modules – the registration and vector validation model, and the protection and recovery model.

2.1.1 The registration and vector validation model

This module implements an interlinked registration approach to ensure immediate registration and validation of all the vectors signified by the phone identity (phone number) and the email identity (email address). The interlinked registration approach uses a relay-race technique to hand over control or validation to the next process until all the registration and validation of the vectors are completed, as shown in Figure 1.

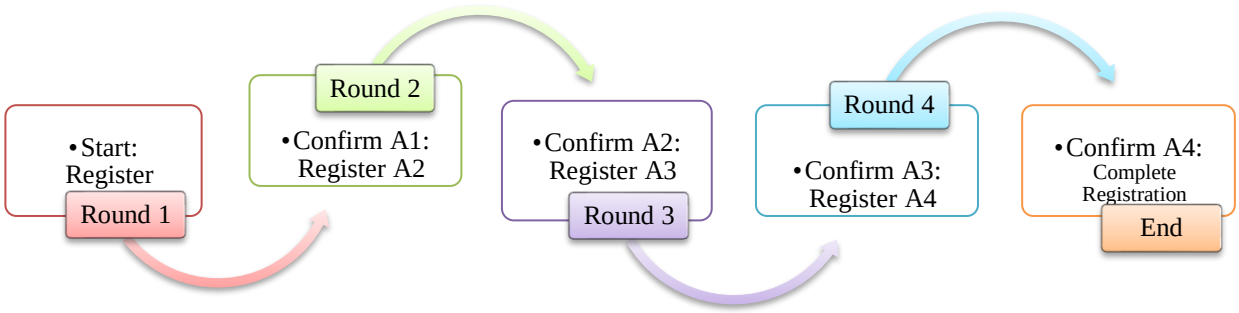

Figure 1: The interlinked registration and vector validation model.

The process depicted in Figure 1 shows that there are four independent rounds, representing the independent processes of the vector validation. A1 to A4 in the figure represent the authentication vector being validated and registered at each stage. The A1 can either be a phone number or an email address presented for validation and registration. If A1 represents a phone number, then A2 will represent an email address, and vice-versa until all the vectors are validated and registered. The first round of registration starts with the User entering the user's email address as the first vector A1. The email address will receive a validation link, which the user will click on to confirm that access to the email address is granted. Upon clicking the link, the validation link opens a link to receive the User's phone number; the second vector A2. As a way of validating the phone number, a validation code via an SMS is sent to the phone number provided by the User, and the User is directed again to the validation page that will receive the code sent to the User for A2 validation. Upon the validation and registration of the phone number, the User is redirected to a page that receives the A3 vector; the second email address. An email is sent to the provided email address, which when accessed proves the validation and registration of the A3 vector. The provision to receive the A4 vector opens upon validating the A3 vector via the link sent to the address. A code is sent to the A4 vector, and as a way of validating the input, the user is provided with a page where the sent code will be validated on the same cloud environment. Each time a vector is received, the system checks the database to ensure that the vector being validated is unique to the User. Figure 2 is a flow chart for the round 2 validation process.

At the start of the round two validation process shown in figure 2, the system checks to see if the confirmation link sent to the user-supplied email address is clicked. Upon clicking the link, an input field opens to receive the second vector labelled A2. First, a database search is made to ascertain the uniqueness of the supplied vector. If the vector has not been used before, a validation code is sent to the vector A2 (phone number) through SMS.

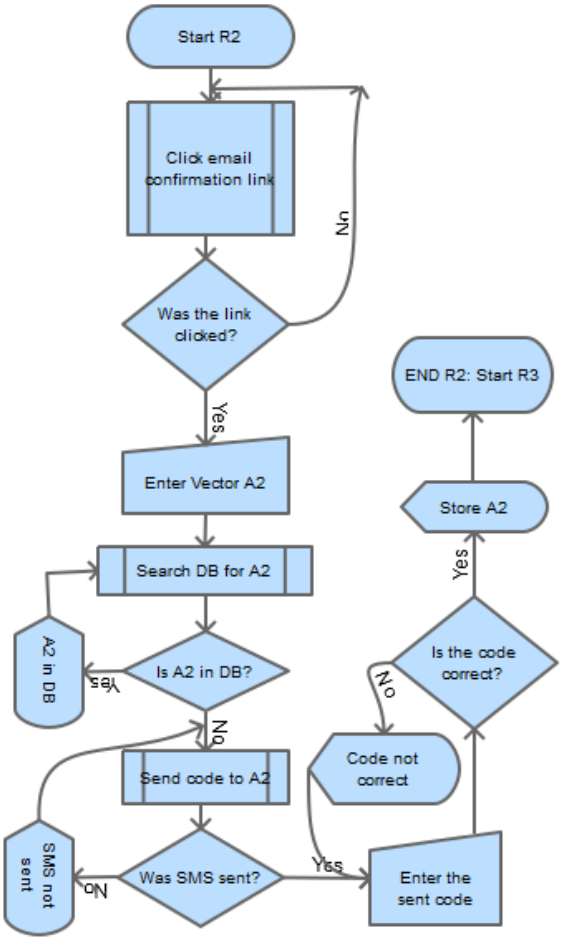

Figure 2: The excerpt of the registration and vector validation flowchart showing the round two validation process.

The user is required to supply the code sent to the phone number that the user supplied as a way of confirming the ownership of the given phone number. Upon successful validation, the vector A2 is stored, handing over to the next process. The process continues until all the vectors are validated and stored in the database.

2.1.2 The protection and recovery module

The interlinked recovery process defines when authorization is granted and when authorization is not granted. The system randomly decides without any specific criteria, which recovery process to initiate first when initiating an authentication process for the User. When a requested button with a secure privilege is clicked, the system generates a binary number. This binary number determines the validation process to be triggered. For example, if the number is 'zero,' an email validation process may be triggered. Conversely, if the number is 'one,' a phone validation process may be triggered, or vice versa. The 'Enable' signal is triggered when vector validation results become true for the first three vectors that is evaluated. Hence, authorization is granted when the authentication process proceeds to 75% correctness, irrespective of the first initiated vector validation. Note again that the 75% correctness is not a benchmark. It is used because the test bed utilized only four vectors for the research implementation.

In row 15 of the table 1, the $'\&'$ symbol in the table represents the logical AND operator while the '!' represents the logical Not operator. A1 = Email 1, A2 = Phone 1, A3 = Email 2, A4 = Phone 2

And: $(A1 \,\&\, A2 \,\&\, A3 \,\&\, !\,A4) = T_{s4}$ (1)

$\therefore P_{enable} = T_{s4}$

The protection module is enabled at state T_{s4}. State Ts4 is activated when at least the states of the first three vector validations A1, A2, A3 takes the truth value of 1 as in Eq(1). This is irrespective of the vector that serves as A1, A2,

A3, or A4. Just like the registration validation model, the authentication validation model follows a relay-race approach. The protection validation link is triggered when a click event is sensed on a protected link like the forgot password link, the edit link, or any feature that requires user-restricted action.

Table 1. The combinational logic model for protection and recovery model activation

n	A1	A2	A3	A4	Status
1	0	0	0	0	Not activated
2	0	0	0	1	Not activated
3	0	0	1	0	Not activated
4	0	0	1	1	Not activated
5	0	1	0	0	Not activated
6	0	1	0	1	Not activated
7	0	1	1	0	Not activated
8	0	1	1	1	Not activated
9	1	0	0	0	Not activated
10	1	0	0	1	Not activated
11	1	0	1	0	Not activated
12	1	0	1	1	Not activated
13	1	1	0	0	Not activated
14	1	1	0	1	Not activated
15	**1**	**1**	**1**	**0**	**Activated: (A1&A2&A3&!A4)**
16	1	1	1	1	Activated

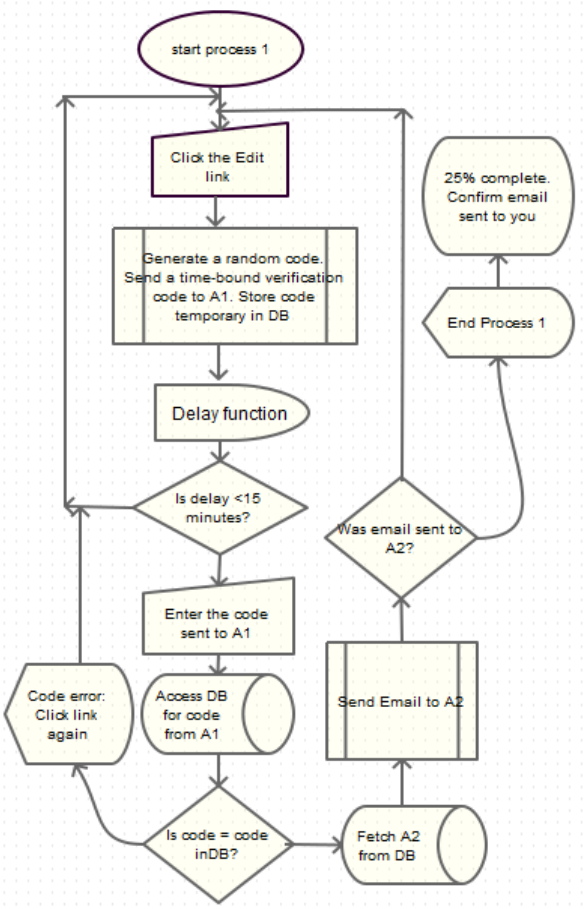

Figure 3 The excerpt of the protection and recovery model flowchart showing the process one recovery model.

The initial authentication validation process flowchart is represented in Figure 3. The process is time-based with a delay function that introduces a 15-minute delay to slow down the recovery process, so as to give the real user ample time to think about what is happening should the process be not initiated by the authorized user. This is based on the idea that a legitimate user will not be in haste when it comes to dealing with his data. At the click of the protected link, a code is sent to the vector A1. The user supplies the code to the requesting page. The system checks the supplied code to ensure it matches the code recorded against A1 in that authentication session. Upon successful verification, the system searches the corresponding vector A2 and sends a link to it, notifying the User about it. The process continues to the last point, then the locked privilege will be unlocked.

3.0 Results and Discussion

From the sample survey taken with the sole purpose of validating the use of independent vectors, it was discovered that 81.1% of respondents received SMS and 75.5% received a call from someone pretending to be from the user's bank. Coming to the response behaviour of respondents, 50.9% of respondents respond to email alerts on their device just in time, as against 73.6% that respond to SMS alerts just in time. On the assessment of the availability of authentication vectors to respondents, it was found that 84.9% of respondents have more than one email address and only about 41.5% of respondents have more than one phone. So, since the system would work when 75% of the authentication vectors have returned to a truth value of 1, this validates that the use of multiple authentication vectors as a tool to initiate multifactor authentication is feasible.

A prototype of the above design was implemented using HTML, CSS, PHP, and MySQL and was hosted on a live server. The SMS implementation was done using the SMSLive247.com gateway. The SMS functionality was tested using the three major telecom operators in Nigeria – Globacom, Airtel Nigerian, and MTN Nigeria. The time responses were measured from the time it took to initiate an email or SMS validation process to the point of delivery to the targeted client. The data in Table 2 represent different telecommunication carriers in Nigeria, and email response.

Table 2 Time responses of SMS and Email notifications using different telecommunication carriers

Freq	Glo	Airtel	MTN	Email
1	433	492	433	1013
2	500	522	492	1050
3	416	402	416	890
4	375	392	402	833
5	31291	442	30122	53492
6	402	23445	452	25219
7	389	399	398	1370
8	400	433	389	960
9	1370	1217	1317	1013
10	54416	45416	34566	84899
11	43872	399	612	49210
12	612	598	592	1050
13	399	432	722	898
14	4259	793	647	4423
15	720	647	388	820

The response chart is presented in Figure 4. For the most part, it is noticed that the SMS response is faster than that of the email. It was discovered also that the fluctuating data signal strength is a great factor that affected the notification delivery by email or by SMS. Hence, the speed of delivery was not used as a validation parameter. It is generally easier to access one's SMS notification than one's email. However, time to access may not also be used as a validation parameter. The only criteria for assessment were the workability of the technique in its application of SeMFAT to unlock a secured User-action like profile editing. For each process in the SeMFAT, the User is notified with a statement of the attending implications of the action being taken. There are some outliers in the time response data

generated as shown in table 2 and figure 4, showing that network signals were a great factor that affected the use of the technique in accessing cloud infrastructures.

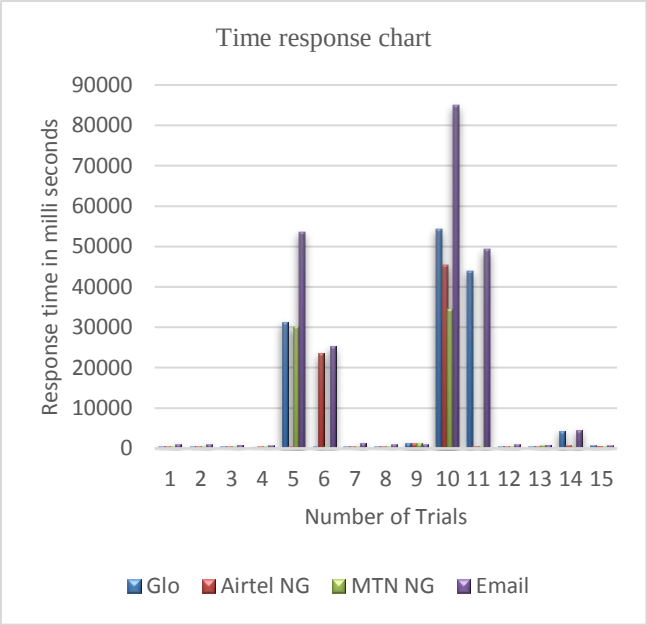

Figure 4 Time response chart of the SMS and Email-based Response.

Previous research works and implementation uses the OTP techniques and two step authentications. By this, the moment one authentication vector that is used in user validation is compromised, the entire user account is compromised. This is mostly seen as how many WhatsApp and Facebook accounts were compromised and hijacked. In contrast, the research's solution presents a multi-validation and verification of ownership using multiple independent authentication vectors which will be very difficult to be compromised at the same time. Secondly, while the previous works presents instantaneous access provision during authentication, the proposed solution introduces a user-defined time delay for user-protected actions so as to slow down the pace of an attacker. The implementation of the proposed system carries profound implications as it places a weighty burden of responsibility on the rightful owner. It demands unwavering diligence and unwavering alertness when initiating user-secured actions. Consequently, the user assumes complete and unequivocal liability for any and all modifications and deletions carried out through their account.

The application of this technique extends far beyond fortifying the security of popular social network accounts like Facebook, Twitter, and WhatsApp. It also encompasses programming systems that seek user comments, ensuring that individuals are held accountable for the comments they attribute to their identities. Furthermore, these techniques can be harnessed to bolster the security of specific transactions within online banking systems. However, a significant limitation of this research lies in the incorporation of a user-defined time delay for user-protected actions aimed at thwarting potential attackers. While this delay serves as a deterrent, it may introduce inconveniences for legitimate users who require immediate access. Consequently, striking the delicate balance between robust security measures and user convenience becomes a pivotal aspect that warrants further exploration and consideration

4.0 Conclusion and Future Work

In conclusion, the user-driven approach presents a compelling solution to address the ever-growing concerns surrounding unsanctioned profile modifications and deletions emanating from account hijackings in cloud-based multi-tenant infrastructures. By shifting the control and responsibility to users themselves, organizations like Facebook, WhatsApp, Twitter, etc can empower users to actively protect their profiles and data from unauthorized access and manipulations. The implementation of robust authentication mechanisms, with the Serpentine Multifactor Authentication Technique (SeMFAT), enables users to have a granular level of control over their profiles. Through the registration by validation process and authentication by validation procedure, users can verify their privileges and ensure that only authorized actions are performed on their profiles.

The results obtained from the prototype implementation demonstrated the effectiveness of the user-driven approach. With a 98% success rate in message delivery recorded in Table 2 and a 100% prevention of unsanctioned profile alterations and deletions, the approach showcases its potential to significantly enhance the security of cloud-based multi-tenant infrastructures. More so, by implementing multi-authentication and validation procedure, compromising user credentials as found in existing systems becomes impracticable.

So, by embracing this user-centric security approach, organizations can bolster their defence against insider threats, account hijackings, and unauthorized modifications to user profiles. The user-driven approach not only safeguards data integrity and user privacy but also instils a sense of ownership and accountability among users, fostering a culture of cybersecurity awareness and responsibility. As the adoption of cloud technologies continues to surge, it is imperative for organizations to prioritize the implementation of user-driven security measures. By empowering users and implementing robust authentication protocols, cloud-based multi-tenant infrastructures hence can be fortified against unsanctioned profile modifications and deletions, ensuring the integrity and confidentiality of user data. In conclusion, the user-driven approach represents a crucial step forward in protecting user profiles within cloud-based multi-tenant infrastructures, underscoring the significance of user-centric security measures and paving the way for a safer and more resilient cloud environment.

References

Aldawood, H., & Skinner, G. 2020. Analysis and Findings of Social Engineering Industry Experts Explorative Interviews: Perspectives on Measures, Tools, and Solutions. *IEEE Access*, *8*, 67321–67329. https://doi.org/10.1109/ACCESS.2020.2983280

Anand, S., Susila, N., & Balakrishnan, S. 2018. Challenges and issues in ensuring safe cloud based password management to enhance security. *International Journal of Pure and Applied Mathematics*, *119*(12), 1207–1215.

Banerjee, S., Chowdhury, E., Sikder, C., Sarkar, D., & Sarbadhikary, R. 2019. Arduino UNO and GSM Based Real-Time Home Security System Using Self- Generated Password Protection. *International Journal of Scientific and Research Publications (IJSRP)*, *9*(4), p8827. https://doi.org/10.29322/ijsrp.9.04.2019.p8827

Blocki, J., & Datta, A. 2015. CASH: A Cost Asymmetric Secure Hash Algorithm for Optimal Password Protection. *29th IEEE Computer Security Foundations Symposium*. https://doi.org/DOI: 10.1109/CSF.2016.33

Department for Digital Culture Media and Sport. 2021. *Cyber Security Breaches Survey 2021 Statistical Release*. www.nationalarchives.gov.uk/doc/open-government-licence/ or

Duarte, N., Coelho, N., & Guarda, T. 2021. Social Engineering: The Art of Attacks. *Communications in Computer and Information Science*, *1485 CCIS*, 474–483. https://doi.org/10.1007/978-3-030-90241-4_36

Erike, A. I., Inyiama, H. C., & Nwalozie, G. C. 2015. Securing Enterprise Information Using Dual Combat Technique. *International Journal of Computer Science and Telecommunications*, *6*(8), 12–18. www.ijcst.org

Ghasemisharif, M., Ramesh, A., Checkoway, S., Kanich, C., & Polakis, J. 2018. O single sign-off, where art thou? An empirical analysis of single sign-on account hijacking and session management on the Web. *Proceedings of the 27th USENIX Security Symposium*, 1475–1492.

Greavu Serban, V., & Serban, O. 2014. Social Engineering A General Approach. *Informatica Economica*, *18*(2/2014), 5–14. https://doi.org/10.12948/issn14531305/18.2.2014.01

Heartfield, R., & Loukas, G. 2015. A taxonomy of attacks and a survey of defence mechanisms for semantic social engineering attacks. *ACM Computing Surveys*, *48*(3), 1–38. https://doi.org/10.1145/2835375

Horsch, M., Braun, J., & Buchmann, J. 2017. Password Assistance. In *Lecture Notes in Informatics (LNI), Gesellschaft für Informatik, Bonn 2017 35*.

Kaspersky. 2021. *What is cybercrime? Types and how to protect yourself | Kaspersky*. https://www.kaspersky.com/resource-center/threats/what-is-cybercrime

Katrandzhiev, N., Hristozov, D., & Milenkov, B. 2019. A Comparison of Password Protection Methods for Web-Based Platforms Implemented with PHP and MySQL. In *International Journal on Information Technologies & Security, №* (Vol. 2).

Mirian, A., DeBlasio, J., Savage, S., Voelker, G. M., & Thomas, K. 2019. Hack for Hire: Exploring the emerging market for account hijacking. *The Web Conference 2019 - Proceedings of the World Wide Web Conference, WWW 2019*, *2*, 1279–1289. https://doi.org/10.1145/3308558.3313489

Moyila Mounika Dev, V. Sarala, & A. Durga Devi. 2020. Multi Level Authentication System Using Sound and Image Based Password Protection. *Mukt Shabd Journal*, *IX*(IV), 4767–4775.

Preethika, S. 2016. Password Protection Using Cryptographic Hash Technique. *International Journal of Emerging*

Technologies in Engineering Research (IJETER), *4*. www.ijeter.everscience.org

Security, I. 2020. *Cost of a Data Breach Report 2020*. www.ibm.com

Shay, R., Ion, I., Reeder, R. W., & Consolvo, S. 2014. "My religious aunt asked why i was trying to sell her viagra": Experiences with account hijacking. *Conference on Human Factors in Computing Systems - Proceedings*, 2657–2666. https://doi.org/10.1145/2556288.2557330

Shubham Sawant, Pratik Saptal, Kritish Lokhande, Karan Gadhave, & Randeep Kaur. 2018. Honeywords - Making Password Cracking Detectable. *International Journal of Engineering Research and Advanced Technology*, *4*(4). https://doi.org/http://dx.doi.org/10.7324/IJERAT.2018.3218

Soumya, G., Soumya, P., & Student, M. 2021. Authentication by Encrypted Negative Password. *Journal of Resource Management and Technology*, *12*(1), 437–442.