Journal of Basics and Applied Sciences Research (JOBASR)
ISSN print: 3026-9091
Volume 2(1) March 2024
DOI: https://doi.org/10.33003/jobasr-2024-v2i1-29

RatHole: Authentication Algorithm for Controling Access to Mobile Phone File Management System

Muhammad Samaila Kabir*, Oyenike Mary Olarenwaju and Abubakar Mukhtar
Department of Computer Science, Federal University Dustin-Ma
*Corresponding Author Email: samaila.makbir@gmail.com

ABSTRACT
Millions of Naira are being laundered by criminals through internet fraud, which deceives the victim with a false presentation, or hacking, which involves breaking information system security to steal financial information or data. Cybercrime, more specifically internet fraud, has become a common problem facing the world. In any case, this only occurred if the attacker was able to obtain the victim's account privileges (bank account, credit card information, or login credentials). This work presented an authentication technique that can be inexpensively implemented and used to create a secure architecture that is hard to breach. It can also reduce the amount of overhead that is placed on the authentication server during an attempt at authentication. The possibility of breaking the authentication technique was calculated using probability theory, and the mobile-based authentication algorithm was implemented using Android Studio. The result of this research shows the implementations of RatHole algorithm using android operating system which is file management android app that is being protected with RatHole algorithm and the probability of breaking down the algorithm for 1 to 10 authentication method keeps reducing by averagely 0.12. The implemented Rat-Hole on android devices also consumed 20 to 30 megabytes of data very less than memory consumption of recent research based on block chain solution which consumed 1 gigabyte to 50 gigabyte of memory.

Keywords:
Authentication,
Access control,
Algorithm,
Non-internet based

INTRODUCTION

These days, mobile devices have greatly increased our convenience by enabling us to access a variety of applications—including online shopping, Internet banking, navigation, and mobile media—at any time and from any location. Although the "Go Mobile" trend offers customers convenience and flexibility, there is a risk that their credit card number and other sensitive private information on mobile devices could be compromised. By unlocking the devices, an attacker could gain access to the private and sensitive data kept on them. Additionally, there are security risks associated with all of the user's mobile services and apps. An adversary might, for instance, exploit the user's mobile device to carry out prohibited activities (such conducting online transactions and installing malware) (Wang et al., 2020). Due to the aforementioned security concerns, authentication methods have had to be developed for both internet-based and non-internet-based systems, including web application systems and mobile devices (Zukarnain et al., 2022). The most widely used forms of authentication include biometrics, patterns, PINs, and passwords.

One modern authentication method for determining the real owner is biometric. As shown below, biometric authentication also encountered several difficulties, including: (1) Face: Variations in background illumination, shifting perspectives, and inconsistent lighting might make it challenging to identify the user's face. Due to hereditary influences and other circumstances, features derived from biometric characteristics of different individuals can be fairly similar. "Intra-class variation" refers to the situation where data collected during verification differs from data collected during enrollment due to variations in posture, facial expressions, facial hair, and spectacle wear. (2) IRIS: The user's gaze point, low central processing unit of a mobile phone, and illumination can all affect the performance of the identification process. The attention can be diverted from the top and lower eyelids by eyelashes and eyelids. The user also cannot be wearing contact lenses or spectacles as it causes the overshadowing of eye image and Iris varies throughout an individual life, thus it will be not being the same for phase of adulthood and adolescence of the user. Changes of the structures happen due to aging. Iris contains

complex pattern as it has a lot of distinctive features of the eye, such as: furrows, ridges, rings, corona, freckles and arching ligaments (3) Voice: It is unreliable when it faces age deterioration as the user's voice may change due to aging, human voices may change over time due to behavioral characteristics of each individual such as age, health, and emotion, different types of handsets, and the varying quality of telephone connection. The user also cannot wear contact lenses or spectacles as they cause the overshadowing of the eye image. Iris varies throughout an individual life, thus it will be different for phase of adulthood and adolescence of the user. Changes of the structures happen due to aging. could make the process of identification more difficult. (4) Fingerprint: Fraud is easily committed because of the ease with which it may be concealed by criminals using phony fingerprints or by mutilating fingers to evade detection by automated systems or even human specialists. This requires a significant amount of computational resources. (Ooi Yee et. al., 2016). The primary objective of an attacker is to take control of mobile devices, which are secured by authentication systems, in order to obtain access to users' personal data or carry out unauthorized operations. In order to accomplish this, the attacker must either exploit the user's identity information to pass the authentication system or employ other methods (such as compromising the remote server's database or intercepting data transmission) to go around the authentication procedure (Wang et al., 2020).

Authentication system assaults can take several forms, such as: Attacks using brute force and guesswork. Basically, the goal of a brute-force assault is to attempt a large number of identity-related data points for the authentication metrics (passwords, fingerprints, and physical addresses of mobile devices) that are needed to pass the authentication (Wang et al., 2020). Attacks by Observation. Using visual sensing technologies (e.g., video recording and photo taking) or just human vision (e.g., shoulder surfing), the attacker launches observation attacks (Wang et al., 2020). Attacks by Impersonation. By supplying identical or comparable identifying information, the impersonation attack seeks to take the identity of authentic users (Wang et al., 2020). Attacks via the side channel. In contrast to the previously described attacks, side-channel attacks seek to obtain the user's identification information by taking advantage of the au-thentication system's identify-irrelevant information leakage (Wang et al., 2020).

Researchers have developed a variety of authentication schemes to effectively defend authentication systems from the aforementioned assaults. There are three groups into which the authentication scheme can be divided: One-factor authentication (1FA), which verifies ownership by requiring a password and username, As the name implies, two factor authentication (2FA) requires two account-related factors, such as a PIN and email address, before granting access. Multi-factor authentication (MFA) calls for two or more factors.

The existing method of user authentication by entering an ID and password is likely to leak sensitive information if the server is attacked or key logged. Therefore, multi-level authentication is needed to prevent server attacks or keylogging. Methods: Biometric authentication technology has been utilized by smartphones, but it is challenging to apply in the case of a lost device because the central server does not manage biometric data. Encrypting transactions through blockchain technology makes data management more secure because blockchain technology is distributed, and there is no primary target for hackers (Kim et. al., 2022).

A blockchain-based authentication technique has been created by Kim et al. in 2022. Development of information and communication technology serves a number of industries. Particularly, omnipresent services have been made possible by the advancement of mobile technologies. That being said, security is becoming increasingly important as technology develops. The existing method of user authentication by entering an ID and password is likely to leak sensitive information if the server is attacked or key logged. For this reason, multi-level authentication is required to stop keylogging and server attacks. Smartphones have made use of biometric authentication technology, however because the biometric data is not managed by the central server, it is difficult to use in the event of a lost handset. Because blockchain technology is distributed and lacks a single point of attack for hackers, encrypting transactions using it increases the security of data management (Kim et al., 2022).

Related Work

Industries and researchers generally propose very accurate and temper-free (secured) authentication methods. Before designing the final authentication system, Zulkarnain et al, 2013. contend that the authentication process and its usability should be carefully considered. This includes not only deciding which verification technique will be most practical for users to use, but also which one should be prioritized for its effectiveness. Zulkarnain et al,.2013).

Ahmad et al.'s research effort categorized the authentication techniques and highlighted the difficulties that each technique encountered. The first category includes fingerprint authentication, which has a high accuracy but cannot be used on fingers with sweaty or dry skin. Another authentication method, facial recognition, has a medium accuracy but has drawbacks such as unpredictable facial features, wearing makeup or a hijab may cause the user's authentication to be refused, and IRIS/Eye recognition, which has a medium high accuracy but has drawbacks when the user has blind eye blinking issues or glasses that shield the recognition system from

direct eye contact. The research project helped to clarify the difficulties that the existing authentication techniques are facing. The study also suggests using mobile GPS and SIM cards for geolocation authentication, as well as fingerprint authentication. However, due to varying policies and regulations, the need for end devices, and changes in user data, these suggested techniques are not feasible to put into practice (Ahmad et al., 2022). Purkayastha et al.'s paper compares three alternative authentication systems to examine people's perceptions of each one, whereas the majority of previous research examines the usefulness of a single authentication system. The comparative analysis demonstrates that fingerprints are more widely used and accurate than other forms of authentication. A survey is included in a different study to gauge Brigham Young University users' perceptions of Duo Two-Factor Authentication (2FA) (Dutson et al., 2019). Both qualitative and quantitative data were collected through the survey questions (Purkayasth et al., 2020).

The best biometric authentication method for mobile phones would be the iris authentication method, followed by the fingerprint authentication method and the face authentication method. This authentication method will be the least acceptable authentication technique to be utilized in mobile phones until some new invention is made to raise the accuracy rate of voice authentication as well as lower the processing time and RAM memory utilization. The evaluation of user authentication techniques reveals that many biometric authentication methods are resource-intensive, consuming a lot of memory, processing time, and power. Some biometric authentication techniques, like face, voice, and fingerprint, are also unsuitable for implementation on mobile devices. However, among these techniques, iris biometric authentication is the most appropriate due to its high accuracy and low memory usage. (Yee Ooi et al., 2016). Following the development of the widely used biometric authentication method, a second method known as two-factor authentication emerged. This approach involves sending the user a one-time password, which they must successfully enter within a set amount of time to gain access to the system or devices. The user must provide their password, user name, and OTP in order to utilize Google Authenticator OTP. Google built a two-factor authentication method, however it is susceptible to brute force and relay attacks. (Wermelin & Persson, 2017).

A multifactor authentication method that authenticate user even if some of the input factors are missing by requesting them from a cloud storage, the sensor compute with a results of its measurements and probabilistic characteristics. furthermore utilizing neural networks for the next-generation biometrics (face,iris, and fingerprint) is the most likely best way to use due to the current high levels of the analysis difficulties. (Ometove et. al., 2018).

According to Li's findings, 3.42% of users in the 12306 dataset use their birthday as a password. Furthermore, male users are more likely than female users to include personal information in their passwords. Y. Li went on to provide new variables and a methodology for accurately gauging the connection between a password and personal data. Furthermore, the findings of the coverage-based measurement demonstrate the severe use of private information when creating passwords, making the user more susceptible to attacks. By combining PCFG with additional semantic patterns, Y. Li created a Personal-PCFG that could be used to crack passwords. By using personal information in the guessing processes, Personal-PCFG creates tailored password guesses on a regular basis. Their empirical findings demonstrate that Personal-PCFG minimizes the likelihood of encountering online attacks and cracks passwords far more quickly than PCFG. Finally, Li suggested employing a distortion system to stop people from using weaker passwords that included user personal data. Li's proof that the implementation of a distortion scheme can stop the creation of passwords using personal information. Li claims that the only password keeper that supports password availability while decentralizing password vault storage to prevent centralization failure is one that sends decryption keys to distant servers. Li used Google Chrome and Android to create a prototype password-storing server. According to evaluation, a user would typically encounter a password retrieval latency of 0.2 seconds on a normal range. Additionally, the password storing server uses 1% of the electric energy during 10 hours of regular use on a mobile device. Y. Li shows that BluePass (Password storage server) does encourage users to establish stronger passwords and are less likely to re-create current passwords by using a user survey with 31 testers (Li, 2019).

A variety of attacks were made against different forms of authentication, including the Playback/Replay assault, which involved the use of a fingerprint and a face, the Mimic attack, which involved the use of a face, a keystroke, and a touch. Attack on sensors: fingerprint, face, retina, and iris, in that order facial authentication is vulnerable to facial spoofing attacks (Silasai et. al., 2020). Ullah et al.'s work helps simulate authentication threats by utilizing the AOM profile, security profile, and mal sequence diagram. Second, by employing the developed approach, it helped to mathematically verify the aspect-oriented mal (AOM) sequence woven model's correctness and completeness. This allowed for the accurate elimination of the dispersing and tangling problem from the initial sequence diagram during the design stage, utilizing all of the actual aspect-oriented (AOM) scheme concepts. Their study aimed to determine the rate at which difficulty, time, and modeling effort would decrease in subsequent projects. (Ullah et al., 2022). An additional study presented a multi-factor approach in

which different authentication techniques are applied in a random order. There is no chance of tampering or forgery because the stored authentication information in both approaches is documented on the blockchain. Another benefit is that although user data is exposed on the blockchain, it is secure since it has been changed and is unchangeable by a hash function. Users may authenticate and obtain services with confidence as a result. However, the solution is energy-intensive due to its usage of blockchain technology and isn't suitable for many offline authentication processes. (Kim et al., 2022).

All forms of authentication can generally be divided into three categories:

(1) Single factor authentication, or 1FA, is simply the standard login and password pair. The only component in this instance is something you already know; the primary problems with 1FA are shoulder surfing and brute force.

(2) 2FA is exactly what it sounds like: rather of requiring only one proof of identity, two are needed. Compared to the previous method, this one offered greater security. For instance, your ATM card can serve as the first factor and your PIN can serve as the second, requiring the PIN to access your account even in the event that your card is lost.

(3) MFA employed two or more factors for authentication. (2018, Nath).

The work of S. Kim et al., which presented Multi-Factor Authentication with Randomly Selected Authentication Methods with DID on a Random Terminal, is the most recent study among the previously evaluated literatures. The research highlights the potential of blockchain technology to establish faster, more secure, and immutable authentication systems. However, a significant limitation of the work is the high cost of integrating blockchain technology into building authentication system, which is limited to smart devices capable of internet-based communication. A safe authentication mechanism, such as one-factor authentication (1FA), two-factor authentication (2FA), or multi-factor authentication (MFA), is the subject of other study. Research on developing multifactor authentication algorithms for software and devices that are not internet-based has not yet been conducted.

.

This research focus on developing a highly secured authentication scheme that is applicable to both internet nased and non-internet based system and can be use in both 1FA, 2FA and MFA by confusion or diverting the attention of attackers who is attempting to authenticate using either brute force attack, dictionary attack, shoulder surfing or relay attack.

MATERIALS AND METHODS

Methodology go over any equipment or processes that are required to complete this research project. The tools section explains the tools needed, whether they are software or hardware; the models and techniques section explains any models or techniques used in this research project.

Probability

Using probability theory, determine the likelihood that brute force attacks can be used to break the algorithm. $\alpha_D = \sum_{i=1}^{n} x_i$ (1)

Where:

α_D is the Total difficulty of the entire algorithm
x_1 is the difficulty of authentication scheme 1
x_2 is the difficulty of authentication scheme 2
x_3 is the difficulty of authentication scheme 3
x_n is the difficulty of authentication scheme n.
x represent the authentication scheme

$$\gamma = \frac{1}{\sum x} \quad (2)$$

γ is the probability of breaking the strength of the algorithm

The probability test for a range of positive integers, from 3 to 10. The values in this range indicate how many authentication methods the algorithm uses.

$\gamma = \frac{1}{3} = 0.333$
$\gamma = \frac{1}{4} = 0.250$
$\gamma = \frac{1}{5} = 0.200$
$\gamma = \frac{1}{6} = 0.166$
$\gamma = \frac{1}{7} = 0.142$
$\gamma = \frac{1}{8} = 0.125$
$\gamma = \frac{1}{9} = 0.111$
$\gamma = \frac{1}{10} = 0.100$

As the number of authentication methods increased, the likelihood of breaching the algorithm decreased.

RathHole Scenario

The scenario where rats evade predators. When a predator pursues a rat with the intention of killing it, the rodent has already established several burrows on the ground, usually in areas that are camouflaged (such as areas with fallen leaves). If the predator does not pay close attention to the rat when it spots it, the rat will enter one of its holes, confusing the predator as to which one the rat has entered! In order for the predator to locate the correct hole, it must inspect each one, and the number of holes the rat dug will determine how long it takes to inspect them all.

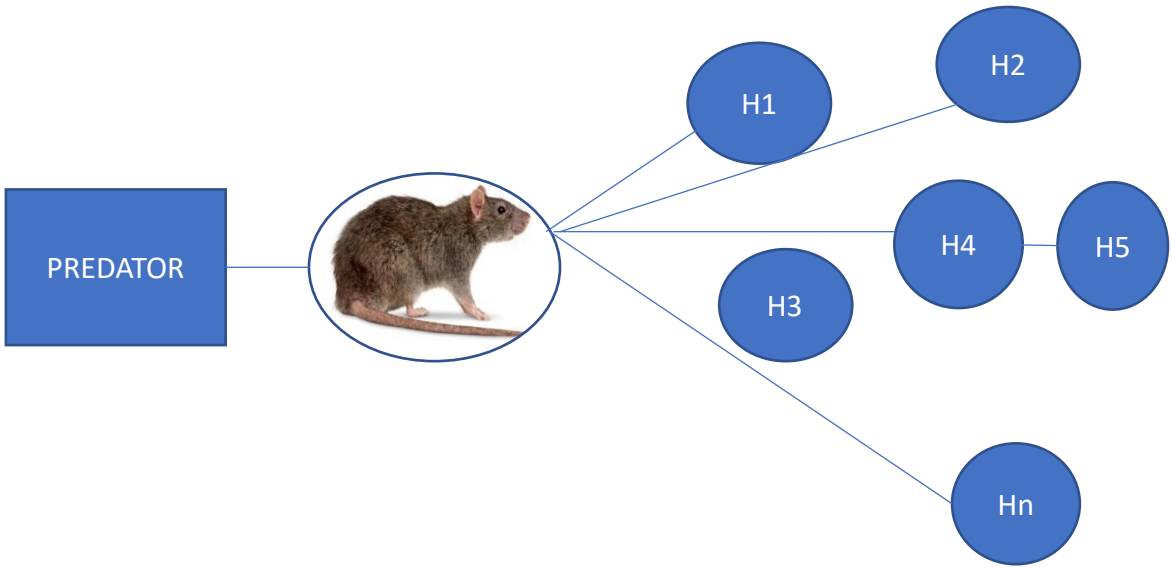

Figure 1: Rat scenario

From the above we depicted three entities. The first one is the predator chasing the rat, The second entity is the rat itself that is being chased by the attacker, and the third entity is the holes where the rat is trying to reach.

Transforming the Rat Scenario into an Algorithm for Authentication

Now the rat survival scenario is turn into an algorithm with potential applications in computer science. During the authentication process, the user is asked to provide information that will help identify him as the legitimate owner of the account, device, or system. If the user provides accurate information, access to the account, device, or system is automatically granted; if the user provides inaccurate information, access to the system may be denied.

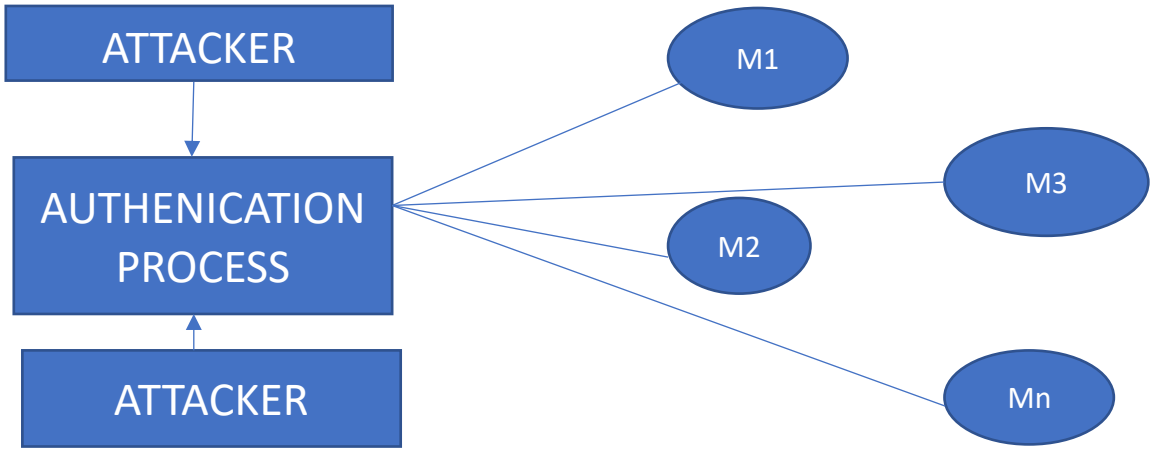

Figure 2: Translating the Rat scenario into an algorithm for authentication

The three entities in the above image are similar to those in a real-life rat scenario, but computer terminology have been used in their place. In a rat scenario, M is the hole that the rats built. The attacker is the predator attempting to gain access to the account, device, or system through deceptive presentation. The user is the rat attempting to fend off the attacker's attacks. The algorithm example uses the following various forms of authentication techniques: Pin authentication is represented by M1, Thump print authentication by M2, and pattern authentication by M3. Mn stands for alternative kinds of authentication techniques.

The time it takes to break the method example pin is represented by the depth of the holes here. The more methods the algorithm implement to uses to get access to a device, account, or system, the longer it takes them to succeed.

PROPOSED RatHole ALGORITHM

1. Initialize user_password=password
2. Initialize string auth_type []=9
3. Compute screen area=lenghthXbreath
4. Position (P_i)=Area/9
5. Assign each P_i to each one of auth_type element
6. Store each authentication type in one element of type[];
7. input password
8. input_password ⟵ password
9. Input type
10. Input_type ⟵ type
11. Initialize Boolean real
12. For each element of auth_type compare input_ type and auth_type
13. If input_type=auth_type
14. real=true
15. Else real=false
16. If real=false
17. Redirect to fake authentication channel
18. Else if real=true and input password=user_password
19. Grant access

Tools used for the research work

Any hardware or software item required for experimentation, analysis, and report creation during the course of the research project is referred to as a tool. Table 1 shows the list of software tools along with their names, descriptions, and an explanation of their uses; Table 2 shows the list of hardware tools information.

Table 1: Software tools

S/N	Name	Description	Use for
1	Android studio	Tool used for developing android apps	Implementation of RatHole Algorithm
2	Microsoft word	Word editor	Writing work reports.
3	Operating System	Windows 8	Computer OS

Table 2: Hardwares tools

S/N	Name	Description	Use for
1	Computer System	1. Processor of 1.30GHz 2. Install Memory (RAM) 2.00GB, 32 or 64 bit Operating system.	1. Running OS 2. Running MATLAB
2	A smart mobile phone	1. Processor 1.5ghz	1. Running android OS 2. Running Our case study systems.

Table. 3: Adopted techniques

S/N	Name	Description	Use for
1	Mathematical probability theory.	The probability of an event is the number that show how likely an event can happen.	Here we will use probability to check how likely to break the authentication system

RESULT AND DISCUSSION

An android-based application that protect memory access using the RatHole technique was implemented using the Android operating system.

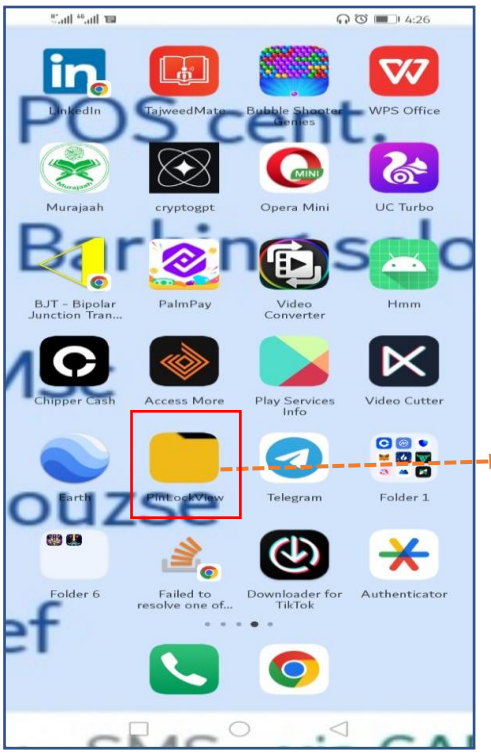

Figure 3: entry position

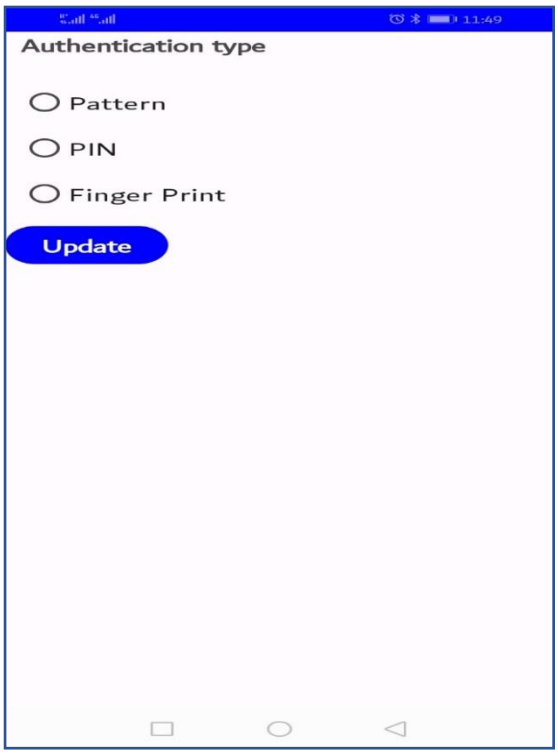

Figure 4: entry position

Figure 3 show the menu icon of the file management app that RatHole algorithm was implemented at the first time launch by clicking the icon the next view is Figure 4. The view in Figure 4 show where the user can set its correct authentication method which indicated correct entry holes for rat scenario.

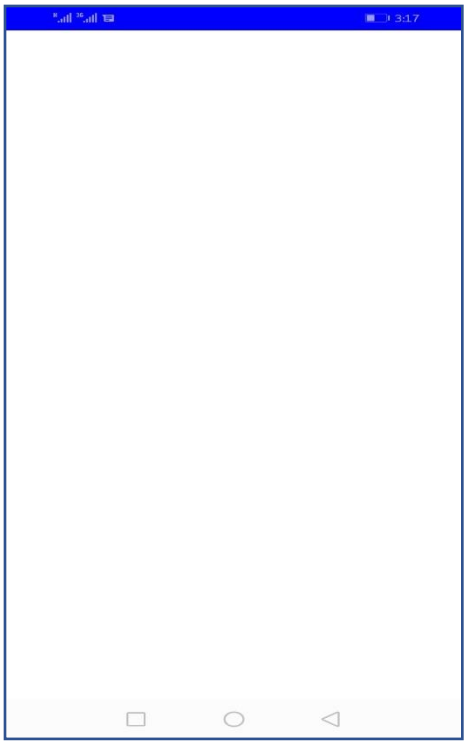

Figure 5: Rat-Hole entry position

Figure 5 show the real life entry positions of RatHole algorithm in android app where the entries are placed into various position of the screen but are hidden which means it's the only original real user know the correct entry like in the case of rat hole where most of the time rat created its house with multiple hole and under a covered ground like place where there is fallen tree leaves, the holes to the entry of the rat house are many and only one is correct and the rest are fake. Another good idea that rat apply is that it makes all the holes (Correct and fake) in a camouflage environment if possible making it more difficult for predator to first locate the holes and then guess the original correct hole. In figure 6 the screen is not plane empty, but contains some entry position in the case of this research the top right corner hold entry to pattern authentication where the user can be authenticated using 9-digit pattern, the center of the screen hold pin authentication where the user is authenticated using 9 digit numerical numbers and the bottom left corner of the screen hold fingerprint authentication method where the user is authenticated using fingerprint sensor of the device. The placement of the entry position formed a diagonal pattern from top-right to center to bottom left-corner, but this three method are used in this research and it's very important to note that more than 3 three authentication method can be implemented placing them in various positions.

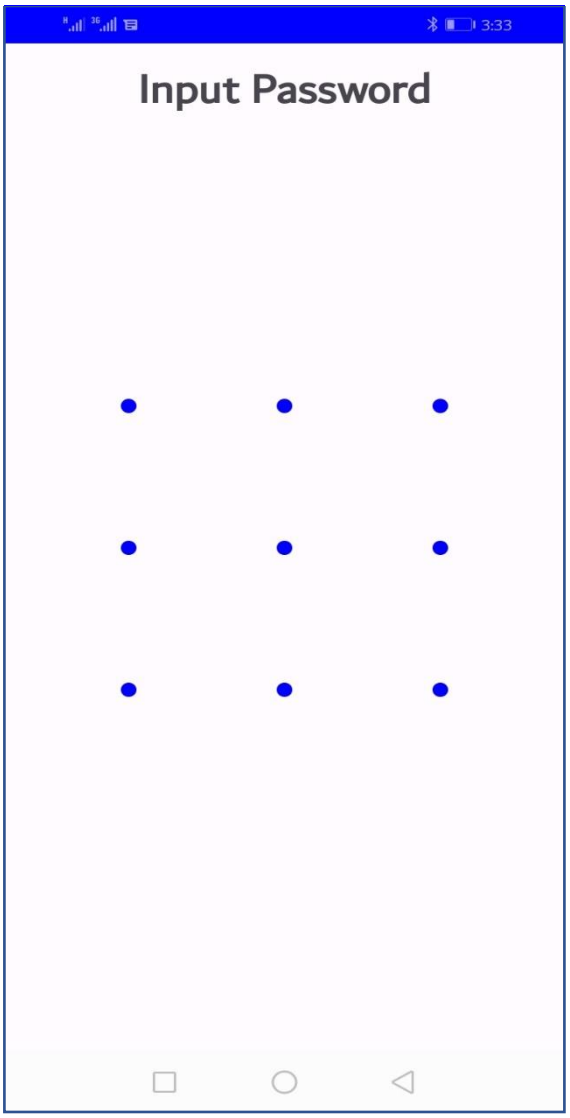

Figure 6: Pattern entry position

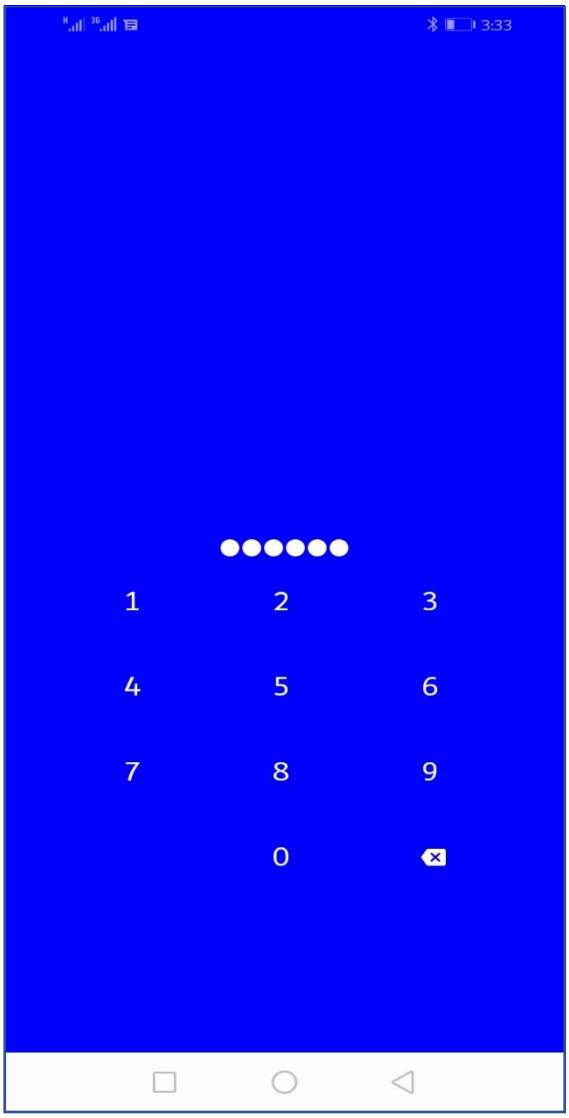

Figure 7: Pin entry position

Figure 6 and 7 shows that one of the method was selected now the algorithm check if the method selected was correct the input to supplied by the user are check with the stored valued otherwise the user is fake and will be channel to the fake method where the supplied input are not tested against the sored values.

Figure 8: fingerprint entry position

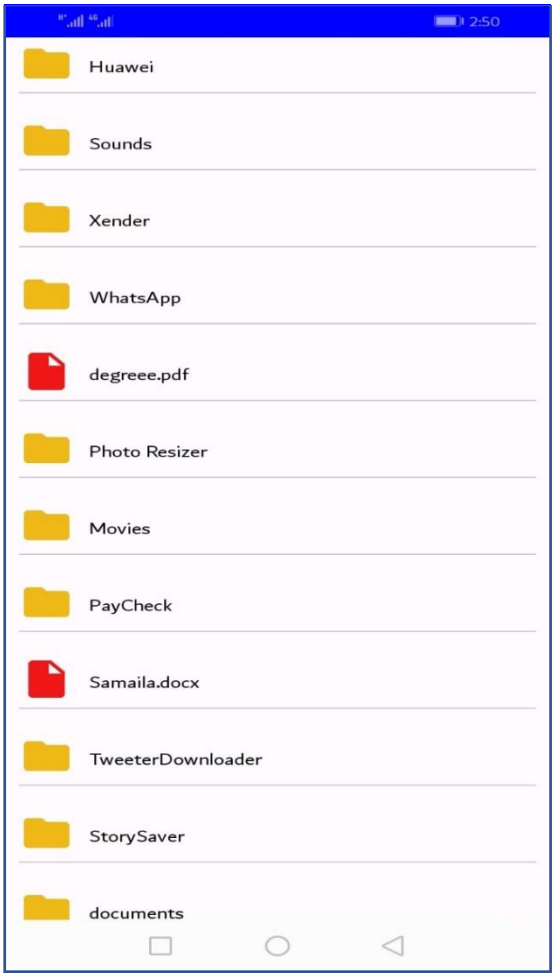

Figure 9: Folders

Figure 6 and 7 shows that one of the method was selected and the algorithm check if the method selected was correct the input to supplied by the user are check with the stored value otherwise the user is fake and will be channel to the fake method where the supplied input is not tested against the stored values. Figure 9 shows that the authentication method selected was correct and the user details supplied was correct and finally access was granted; now the user can open any file in the phones memory. This research attempted to safeguard a basic file management application in the solution, which mostly retrieves every file from the mobile device's memory. The RatHole authentication technique must be successfully completed before the user is able to read every file stored in the phone's memory. If this is not the case, the user will be sent to a phony authentication process that will never end.

Discussion

Recent authentication research is built on blockchain technologies, where user data is stored across multiple servers, creating a decentralized system that requires an attacker to compromise the majority of servers in order to access user data. Despite the development of a highly secure user authentication technique, the solution still had to overcome some obstacles, such as: Scalability: it's not applicable to be implemented to non-internet based system like video game software and device which need to provide privacy, but does not support internet.

The proposed RatHole algorithm built a simple authentication mechanism that can be apply on both internet and non-internet based systems. Some basic privacy protection and authentication software, such as Screen Lock and app lock are very important and required less time to process Implementing block chain technologies on the app lock will take a long time to open a mobile application. When this research is compared with the recent research by Kim et al., it shows that this research reduced the amount of memory and data consumed in performing authentication process for light weight system and device and also reduced the cost of development because it required only one devices to perform authentication but blockchain based required multiple devices.

Table 4: Comparison between RatHole and Blockchain based solution

Characteristics	RatHole	Blockchain
Memory	20-50 MB	1GB-500GB
Device	Single	Multiple
Non internet based system	Applicable	Not-Applicable
Decentralization	No	Yes
Cost of Implementation	Low	High
Cost of maintenances	Low	High

CONCLUSION

Non-internet based applications like file management need to be protected with a simple but secured authentication algorithm that does not required consumption of computational resources such as memory and power like bock chain based authentication method. The proposed authentication algorithm was implemented with simple tools (Android studio) into 1FA, 2FA and MFA. In future work the difficulty of each authentication method is required to be calculated explicitly.

REFERENCES

Aloul, F., Zahidi, S., & W. E.-H. (2009, March 25). Multi Factor Authentication Using Mobile Phones. *International Journal of Mathematics and Computer Science*, 65–80. Retrieved from http://ijmcs.future-in-tech.net

Hui, D. O., Yuen, K. K., Zahor, B. A., & al., e. (2016). An assessment of user authentication methods in mobile phones. Universiti Sains Malaysia, 11800 USM, Pulau Pinang: AIP Publishing. doi:10.1063/1.5055518

Ibrahim, T. M., Abdulhamid, S. M., & Alarood, A. A. (2019, September). Recent Advances in Mobile Touch Screen Security Authentication Methods: A Systematic Literature Review. *African Scholars Journal of pure and Applied Science (JPAS-9), VOL. 15*(NO. 9).

Idrus, S. Z., Cherrier, E., Rosenberger, C., & Schwartzmann, J.-J. (2013, December 10). A Review on Authentication Methods. *Journal of Basic and Applied Sciences*, pp.95-107. Retrieved from https://hal.science/hal-00912435

Kim, S., Mun, H.-J., & Sunghyuck Hong 3,. (2022, 2 22). Multi-Factor Authentication with Randomly Selected Authentication Methods with DID on a Random Terminal. (L. J. Villalba, Ed.) *journal of applied science*. doi:10.3390/app12052301

Li, Y. (2019). *On Enhancing Security of Password-Based Authentication.* William & Mar y - Ar ts & Sciences , Department of Computer Science. W&M ScholarWorks. doi:DOI:10.21220/s2-j1wq-4306

Nath, A. (2016, January). Issues and Challenges in Two Factor Authentication Algorithms. *International Journal of Latest Trends In engineering and Technology (IJLTET), 6*(3).

Ometov, A., Bezzateev, S., Mäkitalo, N., Andreev, S., Mikkonen, T., & 1, Y. K. (2018, 2 1). Multi-Factor Authentication: A Survey. *journal of cryptography*. doi:10.3390/cryptography2010001

Persson, O., & Wermelin, E. (n.d.). *A Theoretical Proposal of Two-Factor Authentication in Smartphones.* Faculty of Computing Blekinge Institute of Technology SE–371 79 Karlskrona, Sweden, Department of Computer Science.

Pin Shen Teh Ning Zhang, S.-Y. Q. (2020). Strengthen user authentication on mobile devices by using user's touch dynamics pattern. *Journal of Ambient Intelligence and Humanized Computing (2020) 11:4019–4039* , 1-2.

Roy, I., Hossain, A., & Rumee, S. T. (2021, December). Attacks on Graphical Password: A Study on Defense Mechanisms and Limitations. *International Journal of Information Technology and Applied Sciences, 3*(4). doi:DOI: 10.52502/ijitas.v3i4.201

Seung-hwanJu, Hee-sukSeo, Sung-hyuHan, Jae-cheolRyou, & JinKwak. (n.d.). A Study on User Authentication Methodology Using Numeric Password and Fingerprint Biometric Information. *BioMed ResearchInternational , Volume 2013*. doi:10.1155/2013/427542

Silasai, O., & Khowfa, W. (2020, 05 18). The Study on Using Biometric Authentication on Mobile Device. *International Journal of Science 2020; 17(1) : 90-110*.

TADE, O. (2013). A SPIRITUAL DIMENSION TO CYBERCRIME IN NIGERIA: THE 'YAHOO PLUS'

PHENOMENON. *HUMAN AFFAIRS , 23*, 689–705. doi:DOI: 10.2478/s13374-013-0158-9

Ullah, U., Faiz, R. B., & Haleem, M. (2022, July 6). Modeling and verification of authentication threats mitigation in aspect-oriented mal sequence woven model. doi:DOI:10.1371/journal.pone.0270702

Wang, C., Wang, Y., Chen, Y., Hongbo, L., & Jian, L. (2020). User Authentication on Mobile Devices: Approaches, Threats and Trends. *journal of Computer Network, Volume 170*. doi:10.1016/j.comnet.2020.107118

Zukarnain, Z. A., Muneer, A., & Aziz, M. K. (2022, April 14). Authentication Securing Methods for Mobile Identity: Issues, Solutions and Challenges. *journal of symmatry*. doi:10.3390/sym14040821