Securing Digital Transaction Using a Three-Level Authentication System

Moses Kazeem Abiodun[1], Joseph Bamidele Awotunde[2(✉)], Abidemi Emmanuel Adeniyi[1], David Ademuagun[1], and Dayo Reuben Aremu[2]

[1] Department of Computer Science, Landmark University, Omu-Aran, Nigeria
{moses.abiodun,adeniyi.emmanuel,ademuagun.david}@lmu.edu.ng
[2] Department of Computer Science, University of Ilorin, Ilorin, Nigeria
{awotunde.jb,aremu.dr}@unilorin.edu.ng

Abstract. In today's world, the rate at which people are transacting on the internet is rapidly increasing, but the majority of people are concerned with the security of the system. Shoulder-surfing, physical observation, keypad overlays, skimming attacks, etc. are the most common threats to the security of Personal Identification Number (PIN) verification. A lot of researchers have proposed several techniques for ensuring security, like Secure-PIN-Authentication-using QR Code (SPAQ), use of One-Time Password (OTP) received on a mobile phone, etc. However, we are still having hackers break into the systems. In order to overcome this threat, this study is proposing a three-level authentication system that will use PIN, OTP, and CAPTCHA at the same time. This will make it more difficult for attackers to succeed in their act and give users doing transactions online peace of mind.

Keywords: Security · CAPTCHA · Authentication · Transaction · SDG 4 · SDG 16

1 Introduction

In our world today, an authentication system is used to secure valuable things. The authentication system is used in the banking sector to secure the accounts and transactions of its customers. Through history, most of the implemented authentication systems have been hacked through. They have become vulnerable to hackers and fraudsters. A stronger authentication system is needed in our society today to strongly secure what is valuable to the people [1].

Also, according to research, people use common passwords and refuse to use complex passwords because they believe they will forget them. This makes the password they use very weak and vulnerable for an unauthorized user to break into.

What is required is a new authentication system that does not require any stressful effort from the user while also being highly secure. The method of identifying if

M. K. Abiodun and A. E. Adeniyi—Landmark University SDG 4 (Quality Education)
M. K. Abiodun—Landmark University SDG 16 (Peace and Justice, Strong Institution)
A. E. Adeniyi—Landmark University SDG 11 (Sustainable Cities and Communities)

© The Author(s), under exclusive license to Springer Nature Switzerland AG 2022
O. Gervasi et al. (Eds.): ICCSA 2022 Workshops, LNCS 13380, pp. 135–148, 2022.
https://doi.org/10.1007/978-3-031-10542-5_10

someone or something is who or what they claim to be is referred to as authentication. The technology checks if a user's data matches that in a database of legitimate users or a data authentication server to offer a user access to the system [2].

Authentication started with the password in the 1960's. In the analog world, passwords have existed for a long time, but there is a popular narrative about the first digital or computer password. Fernando Corbató, an MIT (Massachusetts Institute of Technology) researcher who later became a professor, was one of the innovators of CTSS (Compatible Time-Sharing System), used to solve the problem of keeping a file private from another user by using a password to safeguard user records on the multi-user time-sharing system. Through history, the password system became weak and could easily be hacked, so other authentication systems had to be developed like the OTP (One Time Password), biometric authentication, certificate authentication, token-based authentication and many others. This is just to properly secure the private information and property of users and customers.

In this research work, a three-level authentication system that will involve the use of CAPTCHA ("Completely Automated Public Turing Test to Tell Computers and Humans Apart") system, OTP, and PIN (personal identification number) is proposed. This method will make it easier for people to authenticate their accounts, and at the same time, it will increase the security of the users' accounts by making it more difficult for unauthorized users to gain access to them.

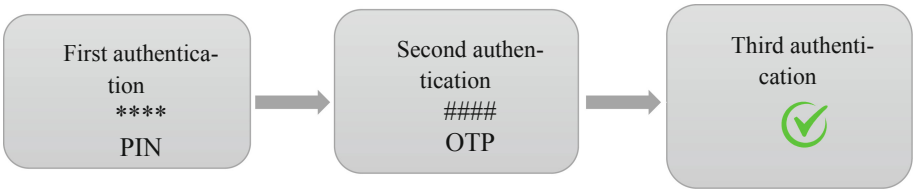

Fig. 1. Workflow diagram of the three-level authentication

Figure 1 shows the workflow diagram for the implementation of the three level authentication system.

Using a single-factor authentication system puts you at risk and is not secure enough. Thus, the use of a three level authentication system will increase the security protection against attacks. The three-level authentication system combines three different means of authentication to form a more secure system for business transactions on the internet. The rest of the sections are as follows: Sect. 2 presents the review of related literature. Section 3 discusses the methodology used in carrying out the research. Section 4 describes the implementations. Section 5 summarizes the result of the research paper.

2 Literature Review

The method of ascertaining users who seek access to a device, system, or network is referred to as authentication. It is the electronic technique that permits a natural or legal person to be identified electronically. Authentication's overall purpose is to reduce the

danger of fraud, particularly when someone deliberately misrepresents their identity or uses another person's credentials without permission. Access control is frequently used to verify a user's identification using credentials such as a username and password. Biometrics, IoT, and authentication apps are among the other technologies used to verify a user's identification [3].

Authentication has a long history that predates the first recorded writings that mention it. Since the birth of civilization, humans have utilized distinctive sounds or watchwords to "authenticate" one another. Roman troops utilized watchwords on a frequent basis. Over time, authentication has become more complicated. It's easy to verify someone's identification just by glancing at them when you know them well. As civilization became more difficult, people had to develop new techniques for authenticating strangers. Society has created personal identity numbers like Social Security numbers (SSN), passports, and other kinds of identification. Even strangers can use these analog forms of identification to verify each other's identity.

2.1 Factors of Authentication

There are four types of factors that can be utilized to verify that an internet customer is the certified owner of what he or she claims to be. These are:

What you know: these are the mental details known only to the genuine user and that should be kept secret, like the password, personal identification number (PIN), and security codes.

What you have: these are the things possessed by the genuine user, like photo ID, smart card, RFID, token, etc.

What you are: these are the distinct body features of a genuine user, like the face, palm, retina, fingerprint, Iris, and voice recognition.

Where you are: this is the data about the whereabouts of a genuine user, like the Internet Protocol (IP) address, Global Positioning System (GPS), etc.

2.2 Types of Authentication

(1) Password-based authentication.
Passwords are still the most widely used method of online authentication. This is understandable, considering that the only requirement is that everyone remember their login and password, rather than having to carry about a digital certificate, USB token, intelligent card, specialist hardware or software, and so on [4]. When it comes to password authentication, there are two parts to it. First, the suppliant will enter the username and then the password. A password can be defined as a private and secret combination of letters, numbers, or special characters known only by the supplicant. One of its strengths is that longer passwords with an accurate combination of characters are very difficult to break. But the problem is, people don't often make use of longer passwords because of fear of forgetfulness. They make use of simple passwords because they are easier to remember. Sadly, simpler passwords are weak and less reliable.

The issue with passwords is that:

(a) passwords can be forgotten if difficult to remember
(b) passwords are easily stolen if written down
(c) users may share passwords
(d) passwords are easy to guess or search if easy to remember [4]

(2) Multi-factor authentication.
To get access to a resource such as an app, an online account, or a VPN, a user must provide two or more verification factors. A good identity and access management (IAM) policy requires Multi-Factor Authentication (MFA). An MFA needs one or more extra verification criteria in addition to a login and password, which reduces the chances of a successful cyber-attack. MFA is a type of verification that entails knowing a customer through two or more approaches. Instances include programs produced by the customer's smartphone, Captcha tests, fingerprints, and facial recognition. MFA verification techniques and tools increase customer assurance by employing extra layers of security.

Although MFA offers an acceptable shield against most account hacks, it is not without errors [4, 5]. There are only three major types of authentication methods, which are:

The majority of the MFA authentication methodology is based on these three important pieces of data: The things you know (knowledge), e.g., your password or your PIN.

Things you own (possessions), such as an ID, an ATM card, or a smartphone.

The things you are (inherence), e.g. your biometrics like voice recognition or fingerprints.

(3) Certificate-based authentication.
The use of a digital certificate to identify a user, computer, or device before giving access to a resource, network, application, or other resource is known as certificate-based authentication. When it comes to user authentication, it is common practice to utilize it in conjunction with more traditional methods like username and password.

(4) Biometric authentication.
Businesses are finding it more difficult than ever to safeguard themselves and their customers from fraud and data breaches. Traditional authentication systems, such as passwords and knowledge-based authentication (KBA), are not only inconvenient but also hackable. Users who have more than 20 passwords to remember are irritated by forgotten credentials, closed accounts, and time-consuming reset processes. This frequently results in poor password hygiene. According to a PYMNTS report, almost 59 percent of users use the same password for several accounts, allowing attackers to inflict even more damage if a password is compromised. Passwords are the core cause of 80 percent of data breaches, according to the FIDO Alliance. Businesses are looking for stronger authentication methods and technology as more stories of cyber-attacks and sophisticated social engineering attempts emerge. Biometrics have the potential to improve security while also improving the user experience. According to Gartner, by 2022, 60% of major enterprises and nearly all medium-sized businesses will have reduced their reliance on passwords

by half. Biometric authentication is becoming increasingly popular. ID R & D develops best-in-class speech biometric authentication and passive voice and facial liveness detection technologies, backed by extensive knowledge and a strong R & D emphasis. Stronger security, easier personalization, enhanced fraud protection, and a better user experience are all made possible by these technologies.

Biometrics verification is a kind of security that is founded on an individual's unique bodily features. In a couple of seconds, authorized properties in a database may be compared to biological traits. When placed on gates and doors, biometric authentication can be used to regulate physical access.

The following are some of the most common biometric authentication methods:

Facial recognition: matching a person's many facial characteristics in order to gain access to a database of approved faces. When comparing faces from different perspectives or when comparing people who seem identical, such as close relatives, face recognition might be inaccurate. Spoofing is prevented by facial recognition technology.

Fingerprint scanners are devices that compare the exceptional patterns on an individual's fingerprints. Most new scanners for fingerprints can now examine the vascular outlines in people's fingers. Undoubtedly, the most frequently used biometric technology for ordinary consumers, notwithstanding their frequent errors, is fingerprint scanners. This spike in popularity can be attributed to iPhones.

Voice identification examines how a speaker's speaking patterns create distinguishing forms and sound qualities. To identify users, a voice-protected device, like a password, usually uses predefined words.

Eye scanners include technology like iris recognition and retina scanners. Iris scanners shine a bright light into the eye and examine the colored ring surrounding the pupil for different patterns. Eye-based authentication may be inaccurate if a person wears spectacles or contact lenses.

(5) Authentication using tokens.

Token-based authentication systems allow users to enter their credentials once and receive a unique encrypted string of random characters in return. You can use the token to access protected systems instead of typing in your credentials again. The digital token proves that you have been allowed access previously. The Restful APIs that are utilized by many frameworks and clients are examples of token-based authentication use cases [5, 6].

2.3 Review of Related Literature

Kumar et al. [7] authentication method is based on a one-time password (OTP) entered through a registered personal device. The client and the server begin direct communication after the OTP is verified using the registered device interface. Near Field Communication (NFC), biometrics, and PIN are used in the authentication method [8] for financial transactions. To make a transaction, a smart phone app is used to enter the money, and then the receiver's information is retrieved using NFC. A picture of the sender will be taken, and after successful verification, a four-digit PIN will be used to finalize the transaction. This scheme's limitation is user discomfort. Virgile et al. [9] generate OTP and

submit it to a cloud server using an app loaded on the phone. If the OTP comes from a trusted source, the user will be granted access by the registered MAC Address.

Ranasinghe et al. [10] described a technique in which the suggested device design functions as an RFID or NFC reader while also allowing fingerprint authentication. There are options for selecting data intake and output. Data is sent between the device and the NFC/RFID reader via RF signals after selection, although fingerprint authentication is performed first. The data exchange process can only begin after the validation step has been completed. The RFID/NFC reader has a power button, navigation buttons, a fingerprint scanner, and a display screen.

Hassan et al. [11] suggested a model called card-less in which the card is substituted by a fingerprint that utilizes a shuffling keypad method, in which a proximity sensor located on the terminal detects the user's finger and changes the keypad layout. Each time a user's finger is detected, a different layout is displayed. Mahansaria et al. [12] proposed a card-less NFC-enabled method. The mobile device connects with a terminal through NFC placed on the ATM device in this study. The user must first input his or her username and PIN. At the moment of registration, a PIN by default is created. The entered credentials are checked, and an OTP is generated if the authentication is successful. The NFC reader reads the OTP and the username, which is then certified by the server authenticating system, and lastly, a transaction is permitted after successful confirmation. In Card Emulation Mode, the provided concept works.

The authors in [13] proposed blockchain-based security and privacy in a multi-tenant environment, the proposed system was used to secured the cloud platform using Ganache and Meta-Mask schemes for creating dummy secure account for each cloud client. The proposed model revealed the importance of blockchain-based multi-tenancy in cloud computing platform. The model was able to secure the cloud environment by prevent an intruder from gaining access into the cloud database.

In [14], the authors proposed a model for the detection of intruders within the data-centric Internet of Medical Things (IoMT) environment using swarm-neural network. The model used swarm for feature selection and ANN was used for intrusion detection within the IoMT-based platform. The performance of the system was evaluated using NF-ToN-IoT dataset for IoT applications based on the telemetry, network, and operating systems data. The results of the proposed models revealed 89.0% accuracy over the ToN-IoT dataset. There are various security and privacy proposed models in various fields for the authentications and verifications of users to prevent cybersecurity and intruders' attacks within the systems [15–18].

3 System Design

The system design specifies the system's design, components, modules, interface, and data in order to meet specific criteria. There are many processes to be followed in this industry that are ensured during the design phase. The user can obtain a full grasp of how the system works thanks to the system design.

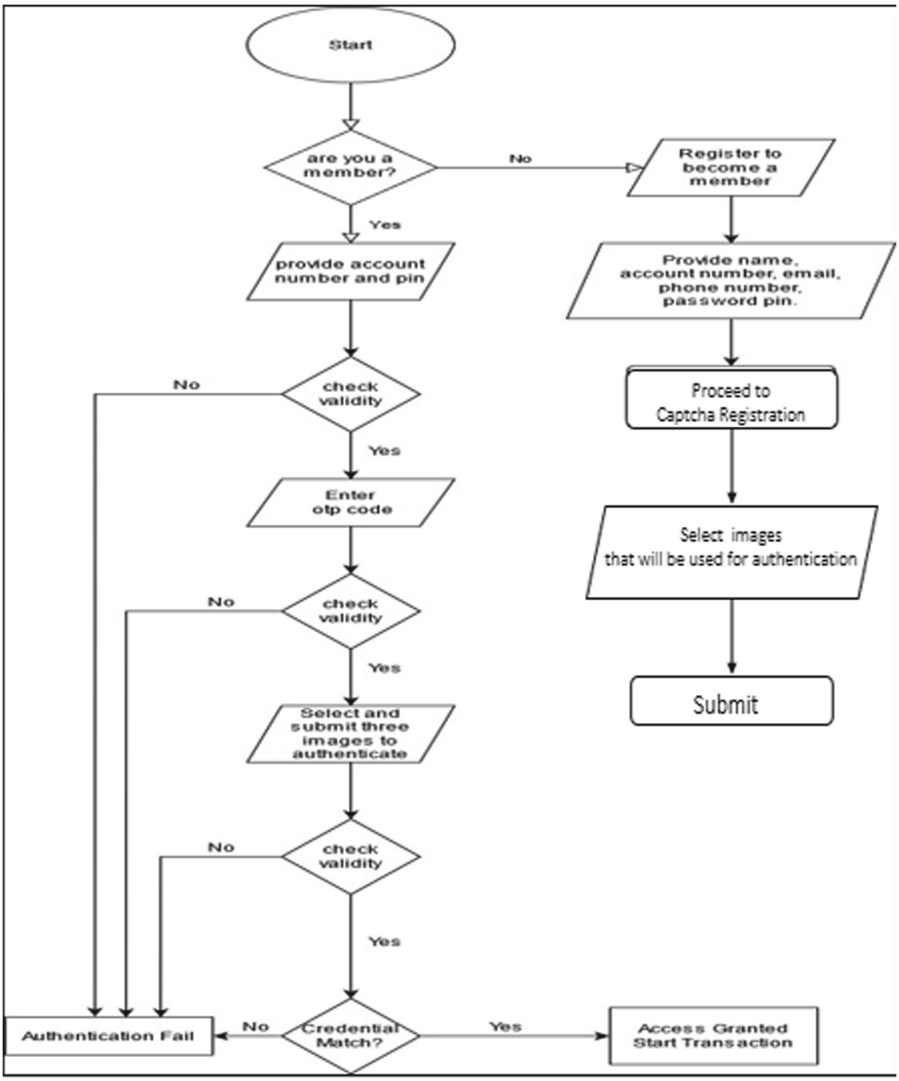

Fig. 2. The flowchart of the proposed solution

Figure 2 shows the step-by-step process of the proposed solution. The user goes to the address of the e-banking website platform, then starts the login process by entering their account number and pin. Unregistered users will have to start the registration process, in which they will have to provide their name, account number, email, phone number, pin code, and select the type of authentication they want. The registration for the 3-authentication method will be done on the registration form. After all the data has been submitted by the user, the user officially becomes a member of the e-banking platform.

As the user enters a valid account number and pin, the web browser goes through the validation phase and waits for authentication to be completed by the server. If authentication is correct, the user is led to the second authentication system, which is either the OTP or the Captcha authentication method. In the OTP authentication method, the user enters his email and then the OTP code is sent to the users email account. The code received will be used to authenticate the account. In the Captcha authentication method, the image recognition challenge will be presented to the user, and all the user has to do is to recognize and select the images chosen for verification. When the user has verified correctly, the user is granted access to his account.

When the user is verified correctly, the user will be granted access to the account and then E-transaction can start.

4 Results and Implementations

The Login Page:

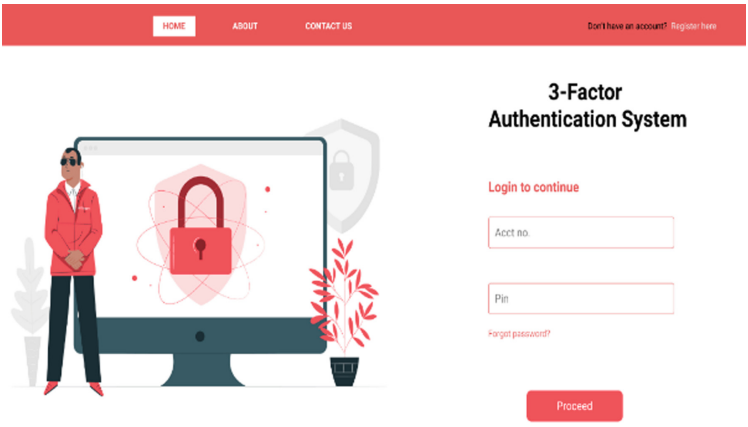

Fig. 3. The login page for customers

Figure 3 is the very first page, which is the login page. This is where an official member of the e-banking platform will enter his account number and pin in order to gain access and start a transaction. An official member that inputs the correct credential will be taken to the next level of authentication, but a user trying to authenticate who is not a member will not be granted any access because their data is not stored in the database.

Instead, he will be advised to register to become an official member of the e-banking platform. When the user clicks on the Register text, it takes the user to another page, which is the page at which the user can register to become an official member of the e-banking platform. The Register text directs the user to the registration web page.

The Registration Page (Fig. 4):

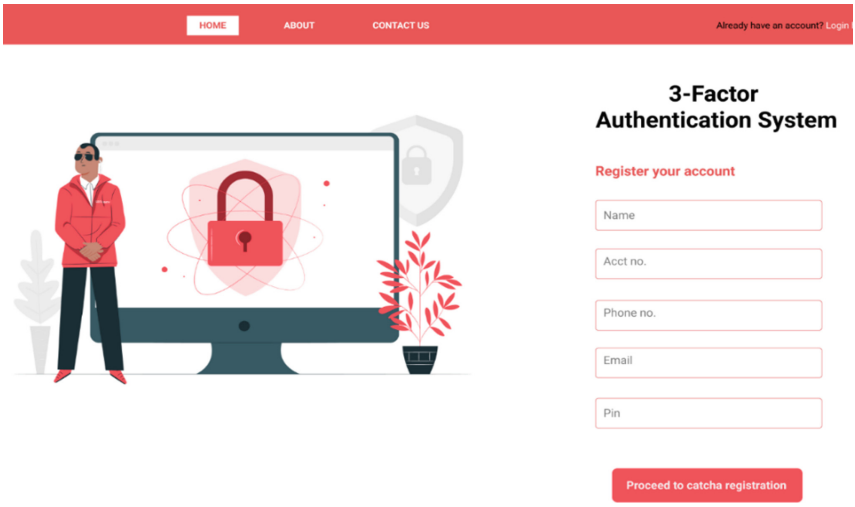

Fig. 4. The registration page

This is where a user intending to become a member of the e-banking platform can insert his data for registration. The user has to insert a username, his or her account number, email, phone number, and pin for authentication. And below all this is the option that allows the user to choose another authentication system for the security, safety, and protection of the account. When the user is done with the form, the user submits it by clicking "register", and after this, the user's data is now officially stored in the database, meaning the user has been assigned an account on the e-banking platform and can now login as an official member of the e-banking platform.

The OTP Authentication (Fig. 5):

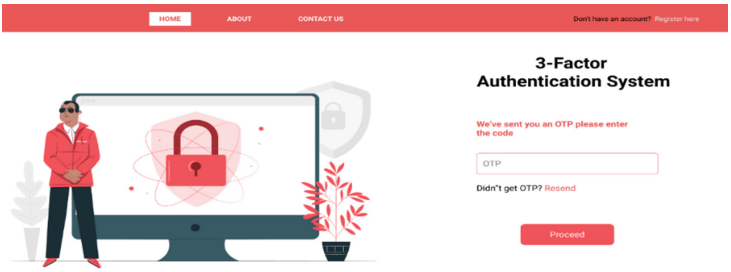

Fig. 5. A page to submit OTP code

The OTP Authentication can come with the second level of authentication. The authentication is built in such a way that all the user has to do is to enter his/her email, and activate the OTP function by clicking Send OTP. By doing this, the OTP code (5 random digits) will be sent to the user's email, so the user fetches the code by checking his/her email accounts, and inputs the code into the new OTP page that requires the user to submit the OTP code. When the user inputs the OTP code and submit it, the authentication system checks the validity of the code. If it is correct, the user is granted access to the account. If it is not, the user is denied access.

The Captcha Authentication (Fig. 6):

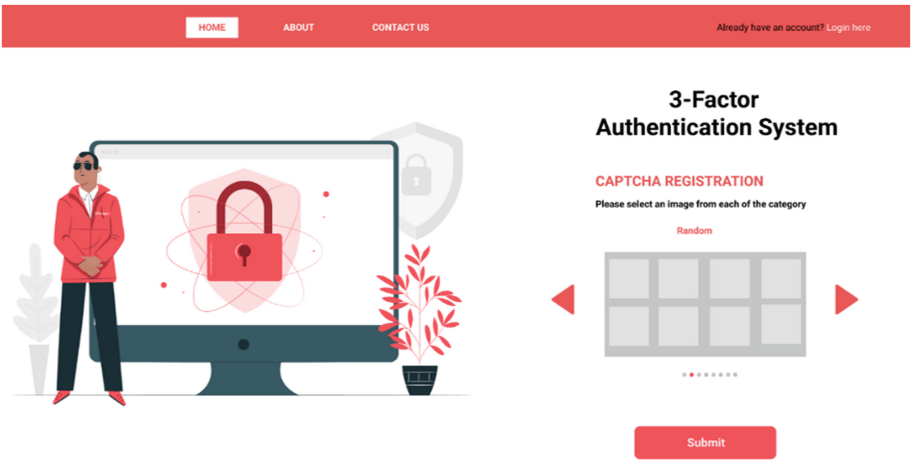

Fig. 6. The captcha authentication

The Captcha Authentication:



Fig. 7. Hobbies image dataset selected by user

Figure 7 is for the captcha authentication. A link was provided on the registration form that leads the user to select images from a different dataset of images that he or she would like to use to authenticate. It gives the user the freedom to select whichever image he or she would like in whichever dataset. The captcha authentication could also come as the second or third authentication. Therefore, during the request for captcha authentication IRC (image recognition challenge), nine random sets of images will be

presented to the user, and all the user has to do is to recognize, select, and submit three images that the user has chosen for verification; when the user is verified correctly, the user is granted access to his account and he can now start transactions. But if the user is not verified correctly, he will be denied access to the account, securing the account from unauthorized users (Fig. 8).

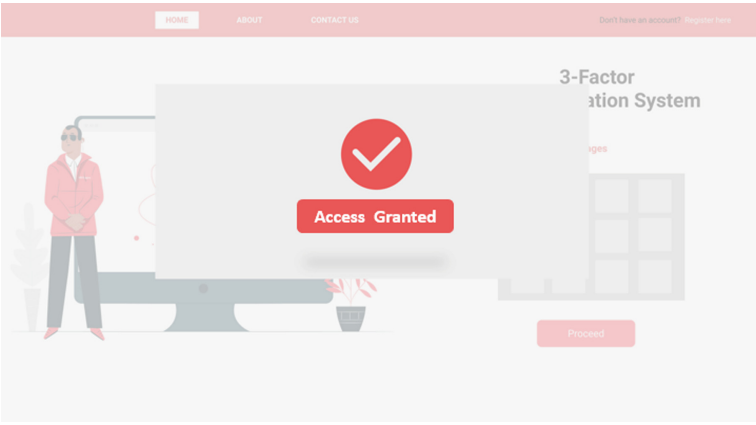

Fig. 8. Access granted alert status

5 Result

The experimental results of the 3 level authentication are found to be a bit slower in the authenticating process. However, it is also found to be more reliable in comparison to a single authentication system. The process of authentication starts with registration, where a new user must register with the system and then get authenticated before he can request a service. The first level of authentication is the PIN, followed by OTP, and then CAPTCHA. The time complexity of the result for using a single method is faster than using all three methods. The sending of OTP took some time because of the network in some cases.

6 Conclusion

Securing an e-banking transaction account with a three-level authentication system was successfully implemented. The system has been able to perform its major function of securing a user's account from an unauthorized user using the PIN, OTP, and Captcha authentication. The three level authentication makes it difficult for hackers to attack the system and steal valuable data from customers. The study could be adopted by various organizations to use in securing an individual's account. Be it an online account or a computer-offline account. This method of authentication could be developed to accommodate more options in the future. In our future research work, we intend to add biometric options to enhance the security of files on the Internet.

References

1. Jang-Jaccard, J., Nepal, S.: A survey of emerging threats in cybersecurity. J. Comput. Syst. Sci. **80**(5), 973–993 (2014)
2. Awotunde, J.B., Jimoh, R.G., Folorunso, S.O., Adeniyi, E.A., Abiodun, K.M., Banjo, O.O.: Privacy and security concerns in IoT-based healthcare systems. Internet of Things **2021**, 105–134 (2021)
3. Abiodun, M.K., Awotunde, J.B., Ogundokun, R.O., Adeniyi, E.A., Arowolo, M.O.: Security and information assurance for IoT-based big data. In: Misra, S., Tyagi, A.K. (eds.) Artificial Intelligence for Cyber Security: Methods, Issues and Possible Horizons or Opportunities. SCI, vol. 972, pp. 189–211. Springer, Cham (2021). https://doi.org/10.1007/978-3-030-72236-4_8
4. Dinesha, H.A., Agrawal, V.K.: Multi-level authentication technique for accessing cloud services. In: 2012 International Conference on Computing, Communication and Applications, pp. 1–4. IEEE (2012)
5. Rosner, G.L.: De-identification as public policy. J. Data Protection Privacy **3**(3), 250–267 (2020)
6. Hassan, M.A., Shukur, Z.: A secure multi factor user authentication framework for electronic payment system. In: 2021 3rd International Cyber Resilience Conference (CRC), pp. 1–6. IEEE (2021)
7. Kumar, S., Ganpati, A.: Multi-authentication for cloud security : a framework. Int. J. Comput. Sci. Eng. Technol. **5**(04), 295–303 (2014)
8. Adukkathayar A., Krishnan G.S., Chinchole, R.: Secure multifactor authentication payment system using NFC. In: The 10th International Conference on Computer Science & Education, pp. 349–354 (2015)
9. Virgile, K., Yu, H.: Securing cloud emails using two factor authentication based on password/apps in cloud computing. Int. J. Secur. Its Appl. **9**(3), 121–130 (2015)
10. Ranasinghe R.N.D., Yu, G.Z.: Rfid/nfc device with embedded fingerprint authentication system. In: 2017 8th IEEE International Conference on Software Engineering and Service Science (ICSESS), IEEE, pp. 266–269 (2017)
11. Hassan, A., George, L. Varghese, M.A., Sherly, K.: The biometric cardless transaction with shuffling keypad using proximity sensor. In: 2020 Second International Conference on Inventive Research in Computing Applications (ICIRCA), IEEE, pp. 505–508 (2020)
12. Mahansaria, D., Roy, U.K.: Secure authentication for atm transactions using nfc technology. In: 2019 International Carnahan Conference on Security Technology (ICCST), IEEE, pp. 1–5 (2019)
13. Adeniyi, E.A., Ogundokun, R.O., Misra, S., Awotunde, J.B., Abiodun, K.M.: Enhanced security and privacy issue in multi-tenant environment of green computing using blockchain technology. EAI/Springer Innovations Commun. Comput. **2022**, 65–83 (2022)
14. Awotunde, J.B., Abiodun, K.M., Adeniyi, E.A., Folorunso, S.O., Jimoh, R.G.: A deep learning-based intrusion detection technique for a secured IoMT system. Communications in Computer and Information Science, 2022, 1547 CCIS, pp. 50–62 (2021)
15. AbdulRaheem, M., et al.: An enhanced lightweight speck system for cloud-based smart healthcare. Communications in Computer and Information Science, 2021, 1455 CCIS, pp. 363–376 (2021)
16. Awotunde, J.B., Misra, S.: Feature extraction and artificial intelligence-based intrusion detection model for a secure internet of things networks. Lecture Notes Data Eng. Commun. Technol. **2022**(109), 21–44 (2022)

17. Awotunde, J.B., Chakraborty, C., Adeniyi, A.E.: Intrusion detection in industrial internet of things network-based on deep learning model with rule-based feature selection. Wirel. Commun. Mob. Comput. **2021**(2021), 7154587 (2021)
18. Kumari, A., Behera, R.K., Shukla, A.S., Sahoo, S.P., Misra, S., Rath, S.K.: Quantifying influential communities in granular social networks using fuzzy theory. In: International Conference on Computational Science and Its Applications, pp. 906–917. Springer, Cham (2020)