Computer Engineering and Intelligent Systems
ISSN 2222-1719 (Paper) ISSN 2222-2863 (Online)
Vol.13, No.3, 2022

An Enhanced Mobile Financial Security System using Facial Recognition and Resident Token generator

Olufunmilola Adunni Ogunyolu Oludele Awodele
Department of Computer Science, Babcock University, Ilishan-Remo, Ogun State, Nigeria
* E-mail of the corresponding author: ogunyolu0363@pg.babcock.edu.ng

Abstract
A mobile application has been embraced over the years by various sectors of the economy for its ease and controlling power in communication, academics, social platforms, shopping, and financial services like banking. It has also been used to control residential gadgets connected through home networks from mobile smartphones. In the medical sector, it is being used for the retrieval of patient history to make medical resolutions. However, this developed application also poses a threat when not properly implemented or built, as interesting as it seems, it also has its cons, particularly in the financial industry that has embraced mobile banking. The challenges of the mobile app include having a single device with single authentication and authorization poses security issues and can be porous to attacks while some use SMS for token information which is also susceptible to spoofing attacks. The study aims to develop a facial recognition enabled mobile app authentication during the process of logging on a single device using a resident token generator enabled for authorization of transactions on the same banking app. The implementation of the token resident generator icon will be resident on the mobile app where Pin and generated token are used for approvals of banking transactions.
Keywords: Authorization, Authentication, Financial security, Two-factor authentication, Resident Token generator, Facial recognition, Mobile app
DOI: 10.7176/CEIS/13-3-02
Publication date: May 31st 2022

1. Introduction

Financial Institutions provide various means for new and existing customers to transact business through technological means without having to visit bank branches. There are various ways in which services are made available to these customers via the internet of things and USSD (Unstructured supplementary data). Among these services are Point of sale (POS), Internet banking, Atm, and mobile banking. Mobile banking services are downloaded on smartphones or tablets and are readily available 24 hours daily. The banking mobile app provides services based on the features built by the financial institutions and the very common features include Airtime purchase, bill paymentVirtual Savings, transfers (own, Same bank, other banks, and foreign transfers). Based on the work of (Borowski-Beszta & Kiermas, 2019) it was explained that the number of customers that embraced mobile banking as an alternative to other banking services between 2014 to 2018 increased to 11.2m as of 2018. Other general features included in the bank's available products and services are the request for bank statements, Loans, Cheque book requests, flight booking, hotel placement, and car rentals among others. Every mobile application has a home page that houses all available services as well as the important information of the applicant, transaction history, statement of account, etc. hence it is important to ensure security, ease, and seamlessness.

Financial institutions, Banks, and Fintechs have all adopted mobile banking applications as a means to reach both the banked and the unbanked, there are several means of logging into mobile banking applications including the use of biometrics (finger, iris among others), passwords as well as the use of software and hardware token. This login authentication mode has its Pros and Cons. According to (Clark, 2021) the use of mobile phones for banking transactions increased to 95% in the United States while the percentage of mobile apps embrace grew by over a Billion worldwide during the year 2017 and based on the work of (Ashibani & Mahmoud, 2020) it was mentioned that known dependent means of authentication and authorization using pin and password is weak especially if the process does not terminate its session on time and can lead to loss of funds and exposure of confidential credentials and information. According to (Shankar & Rishi, 2020) the essence of developing mobile banking is for transaction ease and other researchers (Singh & Srivastava, 2018) aside ease is for self-learning technology literacy, safety, and peer influence. In his work (Phan, 2020) mentioned that one of the challenges of using mobile banking which is unique for each financial Institution is privacy, convenience, ease, and minimizing security risk. Other researchers like (Wang, Wang, Chen, Liu, & Liu, 2020) mentioned that authentication on mobile devices is expected to block unauthorized users based on knowledge-based information like password and lock patterns, biometrics like fingerprint, and Iris as well as behavioral biometrics like hand gesture.

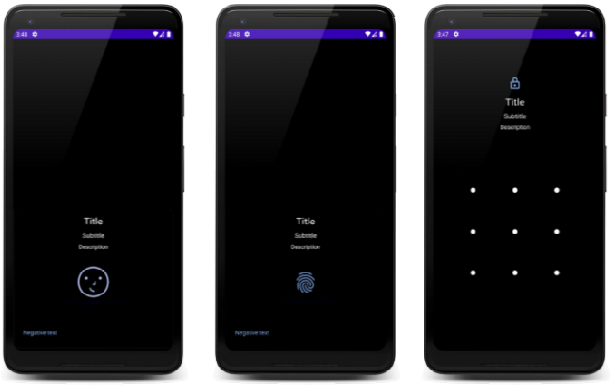


Figure 1 Authentication approvals: shows biometric, Pin, and pattern authentication methods(Husayn, 2020) which grant safe authentication in android smart mobiles.

1.1 Contribution to knowledge

The aim is to design and develop an enhanced mobile financial security system that will provide a seamless and secure authentication and authorization banking service in financial institutions and banks. The Objectives of the study are to design a mobile application that houses a resident Two-factor authorization token generator using Dart Programming language. To develop a biometric system using facial recognition on the mobile app for authentication. To also develop a mobile application that aims in providing transaction ease. This study covers the various implementation of mobile apps and diverse authorization and authentication means of providing services to customers and also identified works of literature by researchers, its gaps, and proffer solutions to achieve the specific goal.

1.2 Related Work

Based on the work of (Omotosho, 2021) both quantitative and qualitative data were used to analyze the experiences of bank customers that have embraced the use of a mobile app for banking transactions, and based on sentiment analysis where 17.8% received and embraced mobile apps while 7.75% rejected the idea due to the fear of insecurity attached to it. In the work of (Habibur Rahman, Al-Amin, & Sharmin Lipy, 2020) it was identified that mobile banking is one of the services banks chunked out to customers however customers were reluctant to embrace it due to the inability to believe the security attached to this service. The study also identified performance metrics for mobile banking having mentioned only perceiving trust (PT) and inherent risk and security (IRS) but failed to mention other threats, mobile banking can experience. (Hayikader, Hadi, & Ibrahim, 2016) mentioned that 70% of IOS mobile banking apps between 2005 to 2014 were hacked and for android, an estimated 95% as a result of malware attacks and it was suggested that various security measures like encryption, password, and minimizing active screen time can be used, however, the gap noted here is that weak password is also susceptible to hacking if not properly configured. Biometrics has been an essential tool embraced by financial institutions and banks for transacting business using smart devices with front or back cameras as well as sensors, however it also has its limitations when used as only authentication means. Financial institutions provide customers with services through diverse technological means among which is mobile banking application with authentication like single-factor authentication (user name and password) and two-factor authentication which grants better security by adding a second level of safety than a single factor. Banks have software and hardware tokens for users which generates a one time passcode for authorization of financial transactions valid only for few seconds, these was introduced to avoid data breaches that might arise from the use of username and password.

However, the hardware token is an extra burden being carried around by any user which can get lost easily, can be stolen, and it's costly while the software token is believed to have a better advantage over the hardware token since it cannot get missing, easily upgraded and can be implemented in any part of the world however it has a burden of moving in between apps for authentication and authorization of a transaction. Blockchain-enabled mobile banking application was also mentioned by (Awotunde, Ogundokun, Misra, Adeniyi, & Sharma, 2021) by providing safe transaction processes based on two-factor authentication rules to generate one-time passwords for transfers. According to (Patrick Ajibade, Mutula, & Ajibade, 2020) it was discussed that mobile banking acceptance was limited due to technological infrastructure like lack of adequate internet services, low power supply for charging phones, cost of smartphones is high among others, it was also mentioned that clients usually travel a lot of distance before getting to banks for financial services however a mobile banking app could easily have solved this.

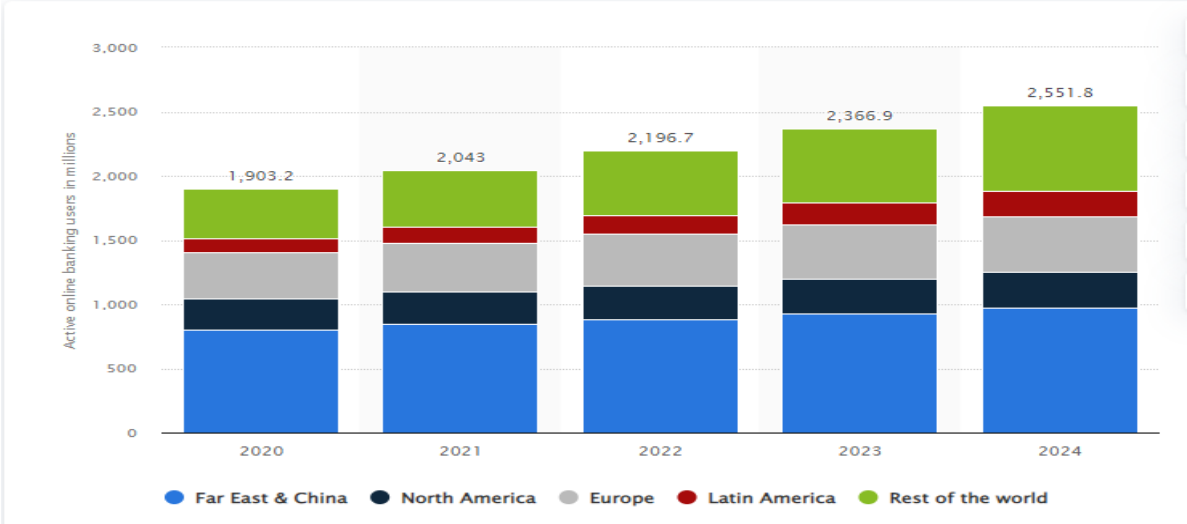


Figure 2. Mobile banking app users globally: shows the present and future adoption of mobile banking. According to (Norrestad, 2022) mobile and online financial app users are expected to rise tremendously yearly.

2. Literature Review

According to (Gerami & Ghiasvand, 2016) many instances of authentication and authorization are called Two-factor authentication based on a one time password and software token through the use of SMS which does not require any device but SMS sent to a phone, however, this procedure requires a shift from the mobile device to retrieve the one time password before proceeding back to a mobile app which lacks ease, convenience and SMS can be hacked. Another researcher (Sharma & Mathuria, 2018) mentioned that authentication procedure for mobile banking using fingerprint-based on Java-enabled application was used to simulate entry to mobile app for login and payment option and derived 100% security as well as transaction ease but limited by attacks based on data theft and finger disabilities can cause the process not to identify the registered traits. Another researcher (Haupert & Müller, 2018) explained Malware is a threat that affects mobile banking applications if two-factor authentication is not enabled on a device and the study used an application Photo TAN for authorization and authentication on two devices having a method of authentication as a two device authentication, two-app authentication and it implemented a design photo Tan based on matrix code. The result explained that the application called Photo TAN uses keys for authentication of process successfully providing security against malware attacks using photo app initialization and the Gap noticed is that the method of authentication and authorization is cumbersome and stressful having to migrate between two apps. Several researchers have tried to mention diverse methods of ensuring secure, seamless, and reliable transactions. According to (Basar, Alptekin, Volaka, Isbilen, & Incel, 2019), Mobile banking application requires the consumption of resources during implementation which is not cost-effective based on behavioral metrics and the objective of the study is to determine the efficiency of behavioral metrics concerning the consumption of resources, having its method of authentication using a Touch screen. The study used sensors created by an accelerometer, gyroscope, magnetometer, and the use of mobile touch screen, The outcome showed the effect on CPU was 5%, 39% power was utilized while touchscreen was 3% consumption. The study did not carry out the making of magnetometer and gyroscope inactivity to reduce consumption when not in use. Based on the work of (Maček et al., 2019) it was indicated that iris biometrics can be also used for authentication into mobile banking applications using phones with front cameras while others use finger biometrics as an alternative for signing in. As mentioned by (Hammood et al., 2020) online banking transactions should be carried out with a safe authentication process to prevent fraud on accounts having reviewed present mobile platforms adopted by users. The means of access popularly used are passwords, PIN, and biometrics but suggested digital watermarking, SMS as alternative means of authentication however, SMS is susceptible to impersonation, interception,

smishing, hacking during process reset, and the high cumulative cost of message alerts. It was also identified by (Ali, Dida, & Sam, 2020) that mobile money faces several attacks hence the need for countermeasures against them using a two-factor authentication scheme based on cryptography and PIN, however, a drawback of cryptography is the inability to guide against threats associated with poor design. Furthermore, there is a need to minimize continuous approval during transaction sessions when biometrics is used as indicated in the work of (Incel et al., 2021) by using data collection from touchscreen and sensors like accelerometer, gyroscope, and magnetometer for building biometric model however also susceptible to cyber-attacks. Another attack possible on mobile banking apps as mentioned by (Thakur & Yoshiura, 2021) is phishing and suggested an anti-phishing model called Simple Promela interpretation but can only work well with

simulation else it can't be effective for verification. Another means of transaction authentication and authorization is the use of hardware tokens also prone to theft and loss, it is a two-factor authentication requiring pin and token digits, However, carrying hardware token around also lacks ease and if it gets missing it can also be hacked using the information behind the hardware token. Financial Institution is expected to provide financial transaction safety and seamlessly banking processes for their users. In as much as mobile banking is increasingly adopted worldwide, it also has its challenges like device battery life, and storage capacity, it was mentioned by (Oludele & Oluwabukola, 2016) that mobile gadgets however can provide authentication and authorization by relying on information stored in the database and further explained that mobile application also exists through mobile cloud computing in areas like mobile commerce, mobile banking, and mobile healthcare among others. This work will provide an easy and safer means of transacting on a mobile app based on the Two-factor authentication principle implemented using Dart programming language powered by google flutter wave for the development of a token resident generator embedded in the mobile app and a biometric facial recognition for signing into the app.

3 Research methodology and Design:

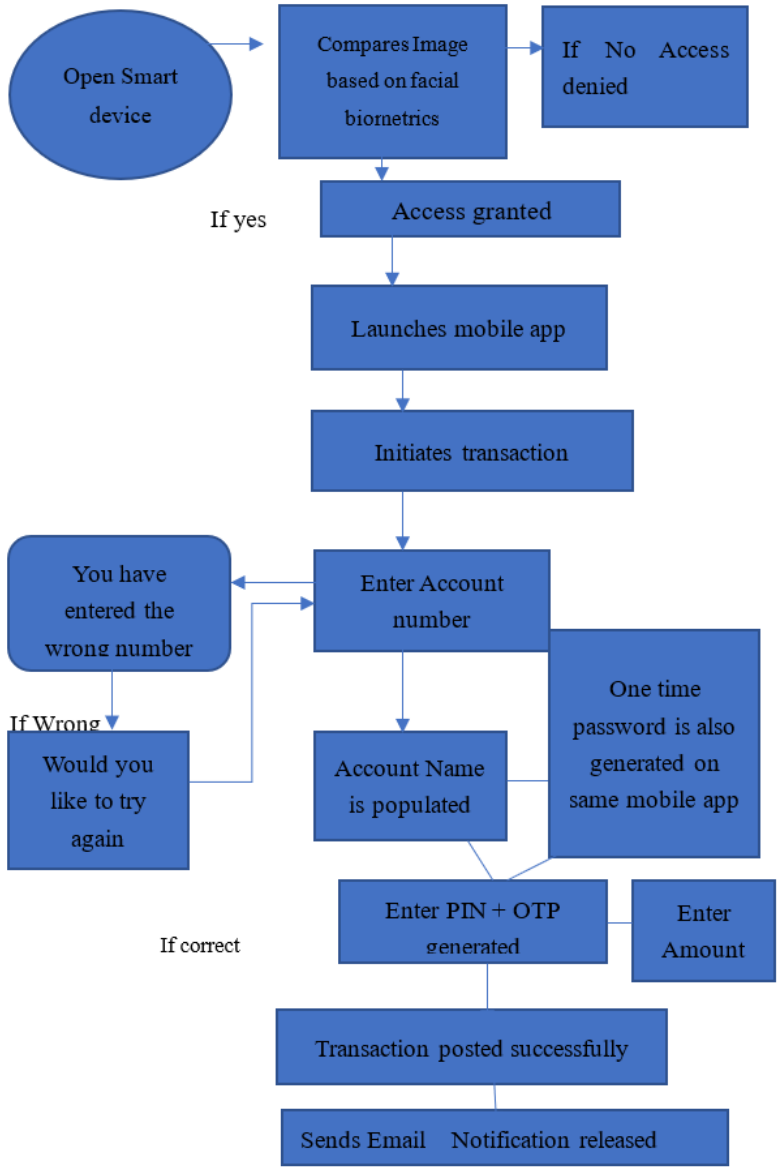


Figure 3: Mobile App Development Design - shows the various development stages of the mobile application design.it explains the steps taken to consummate the transaction on the mobile app based on facial biometric identification and a resident token generator for approval.

As mentioned by (Estrela, Albuquerque, Amaral, Giozza, & de Sousa Júnior, 2021) biometrics help tackle identity fraud issues based on machine learning and the use of features provided on touchscreen sensors having

considered other sensors like accelerometer, gyroscope, and magnetometer. Mobile language, tools, and IDE which is a standard integrated development environment (IDEs) will be used. Token generator involves the application of AI by learning the customer's data history to provide a uniquely generated set of numbers for authorization of transactions. DART is a multi-platform language with onboarding installation IDE and SDK for coding. This will be used because it allows for a bigger-sized application and it is efficient. It provides the User interface (UI), functional level tests, and changes that can be made on DART code as well as enables efficient documentation. Furthermore, a Cloud platform will be used for storage, (GPU) graphical processing for graphical computation, and conversion to reduce the work of the CPU.

3.1.1 Build an interactive Resident Token Generator using Flutter/Dart Programming

Figure 4:Token input animations part, shows a third-party library called animated widgets and do a 'flutter packages get' a basic stateful widget that has a TextEditingController for a TextField for the customer to type the code, a FocusNode that can be attached to the TextField, a 'code' string which will hold the value of the code, a 'loaded', 'shake' and 'valid' boolean variables for toggling the state based on whether the backend returned after validating the code, the text fields must shake(animate with a red) for invalid code and if the code is valid or not respectively. Now, for the onChange() callback of the TextField, let's define a method that takes the current value of the code and sets the state of the code variable to that value.

For the onClick() callback of the Verify button, and to define a function where the backend call, validate2FaCode(code) which is asynchronous.

The logic for this method is,

- Set loaded to false, so that one can use this variable to display a spinner/activity indicator while the backend call is processing
- Make the backend call asynchronously
- Now set loaded back to true and set valid to the result of the call
- If it's valid, move on to the next screen or sign in according to the flow
- If it's not valid, set shake to true which will trigger the text field to shake and change color to red for 300 milliseconds, and then set shake back to false so that it stops.

The design has two problems to solve:

- Render a text field that looks like 6 dashed lines for the 6 characters of the code.
- The dashed lines behave like a TextField widget so that we can leverage the onChange() property and also attach a TextEditingController and FocusNode.

The suggested mobile app is a developed facial recognition using the front camera, where the facial features and pictures of an individual customer are stored in the javascript file in the device memory.

3.1.2 Face Recognition Authentication using Flutter/Dart Programming and TensorFlow Lite

Process summary

Sign up

1. The customer takes a photo.
2. The ML models process it and create an output (array of numbers) to be stored in a database.
3. A name and a password are requested

Sign in

1. The customer takes a photo.
2. The Machine Learning models process it and create an output.
3. The output will be compared against the outputs already stored in the database (it compares by proximity the closest one it finds). As a condition, the proximity has to be under the threshold (minimum distance), if overcomes it, it will process it as a non-existent customer.
4. If the customer exists (face already processed) it requests the password for that customer, validates, and

authenticates it.

Clear DB: This functionality is just for debugging, It deletes all the data saved in memory.

Note: The purpose of this application is simply to show the main functionality (which is facial recognition). That's why the records are not stored in a database on a server, but saved in a js on file in the device memory.

3.1.3 How it works

It works with two computer vision models working together, the Firebase ML vision model to perform the face detection and preprocessing in the image, and the MobileFaceNet model to process, classify and transform into a data structure 'savable' by a database (an array of numbers).

i. Tensorflow Lite:

To integrate the MobileFaceNet it's necessary to transform the TensorFlow model (*.pb* extension) into a file with .tflite extension.

ii. About MobileFaceNet models:

MobileFaceNets are a set of CNN models, which use less than 1 million parameters and are specifically tailored for high-accuracy real-time face verification on mobile and embedded devices, for facial identification task.

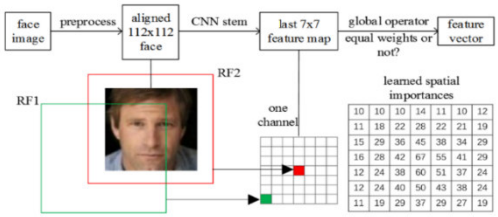


Figure 5. Face verification through image preprocessing using CNN to evaluate visual imagery.

It receives a matrix of 112x112 inputs and returns as output a matrix of 7x7 with values adjusted according to the importance

iii. Firebase ML vision:

With ML Kit's Face Detection API, you can detect faces in an image, identify key facial features, and obtain the contours of detected faces. It works very well preprocessing the image to detect the zone to be cropped and then processed by the MobileFaceNet model.

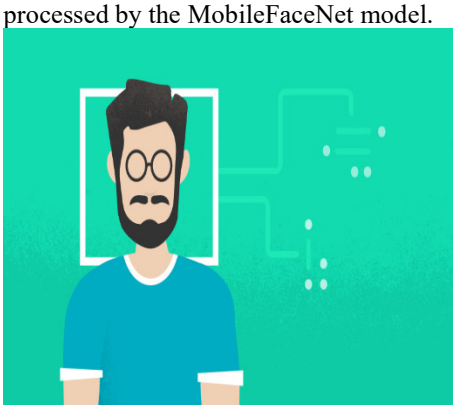


Figure 6: Face detection based on facial key attributes before MobileFaceNet processes and crops the image.

3.2 Flutter implementation/Dart Programming

3.2.1 Description

As soon as the customer enters the signup or sign-in option, the ML vision model detects existing human faces in the frames that the camera preview, the class Face contains the coordinates of the points that make up the frame around the face.

If the sign-in or sign-up button is pressed (as the case may be). The detected face of the last frame is captured, cropped, and then pre-processed to be processed by the MobileFaceNet model.

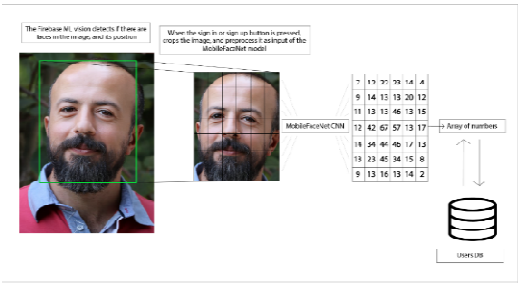


Figure 7: Facial sign up: identifies the presence of an image and its position, crops image then preprocesses as input using mobilefacenet CNN.

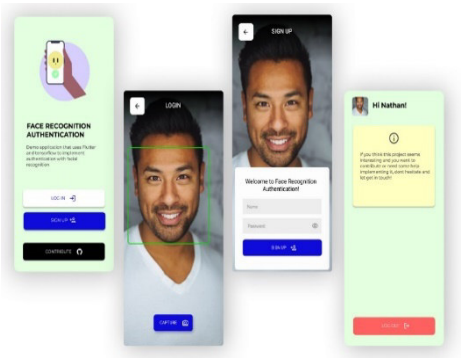
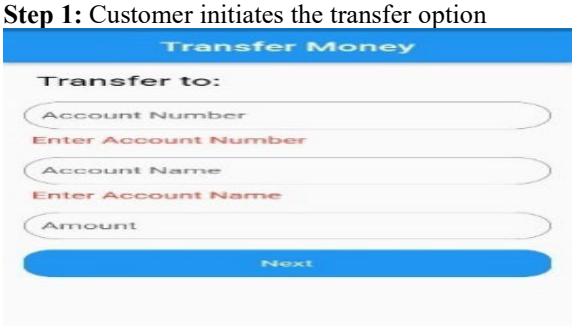


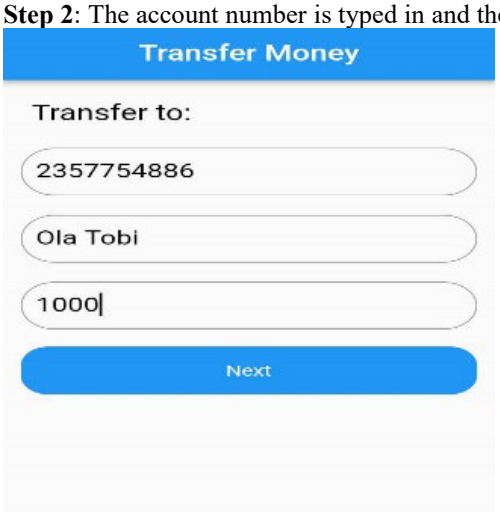
Figure 8: Facial recognition and Authentication of signed-up images.

3.2.2 Process of Mobile banking transfer steps:

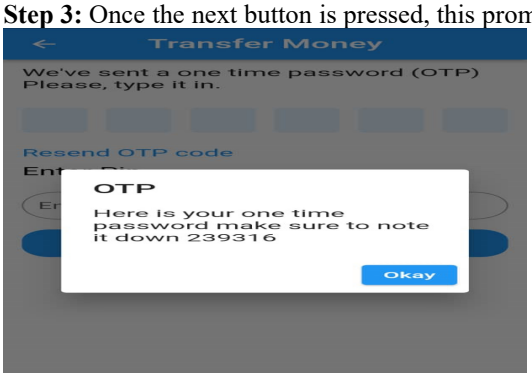
Step 1: Customer initiates the transfer option



Step 2: The account number is typed in and the account name is verified from the database



Step 3: Once the next button is pressed, this prompts the generation of the 6- digits otp



Step 4: The known Pin of the user is keyed in along with the token digits generated

Step 5: If the Pin keyed in is valid then a successful message is passed and an email notification is sent.

4 Result of findings

The study showed that having a resident token generator on the mobile app using facial recognition as a means of signing into the app is of high gain and relevance. This provides two-factor authentication as well as ease where there is no need to move in-between apps to generate tokens in the case of software tokens since it's embedded in the app itself. This overcomes the attacks associated with SMS token alerts. It has also defeated the need to carry hardware tokens around but rather software token is adopted having it resident on the same app instead of both on a separate application. Also, for logging in, the attacks of impersonation are defeated since, during the process of logging into the mobile app, the features and facial details are compared with that which is stored in the database. If there is a True Positive then it is matched and access is granted however if we have a true negative where the mobile app correctly identifies a wrong user then access is denied. This mobile resident token-based generator is developed using Dart programming language powered by google Flutter frame and the application use data analytics which will provide data collection while the Android developer platform is used for the mobile app design. This provided a seamless and safe personal experience comprising of payment gateway.

5 Recommendation and Conclusion

The priority of many banks is to provide financial services to clients in other to gain their trust and confidence through the evolving technology. Fintechs and banks have tried to make use of mobile applications to provide

extended services to clients, however, several limitations have been identified as a result of inadequate authentication and authorization methods which can lead to identity fraud, financial loss, burden, and increased service cost. It is then highly necessary for fintech, financial institutions, and banks to provide safer and seamless banking transactions through enhanced and secure mobile applications and this cannot be over-emphasized having been embraced by over a billion people all over the world. It is essential to mitigate the risks inherent with the use of a mobile app by adopting the use of biometrics for signing and the use of a resident token generator on the mobile app with a user pin known to the customer alone. This has introduced a second layer of security, and safety, also at the same time providing transaction ease, and seamlessness and minimizing the cost of purchasing hardware tokens or migrating between apps for software tokens. For future work, a mobile application that can use biometrics for financial authorization without the need for tokens will be an interesting aspect to explore.

References

Ali, G., Dida, M. A., & Sam, A. E. (2020). Two-factor authentication scheme for mobile money: A review of threat models and countermeasures. Future Internet, Vol. 12. https://doi.org/10.3390/fi12100160

Ashibani, Y., & Mahmoud, Q. H. (2020). A Multi-Feature User Authentication Model Based on Mobile App Interactions. IEEE Access, 8. https://doi.org/10.1109/ACCESS.2020.2996233

Awotunde, J. B., Ogundokun, R. O., Misra, S., Adeniyi, E. A., & Sharma, M. M. (2021). Blockchain-Based Framework for Secure Transaction in Mobile Banking Platform. Advances in Intelligent Systems and Computing, 1375 AIST. https://doi.org/10.1007/978-3-030-73050-5_53

Basar, O. E., Alptekin, G., Volaka, H. C., Isbilen, M., & Incel, O. D. (2019). Resource usage analysis of a mobile banking application using sensor-and-touchscreen-based continuous authentication. Procedia Computer Science, 155. https://doi.org/10.1016/j.procs.2019.08.028

Borowski-Beszta, M., & Kiermas, A. (2019). THE USAGE OF MOBILE BANKING APPLICATIONS IN POLAND: EMPIRICAL RESULTS. Copernican Journal of Finance & Accounting, 8(1). https://doi.org/10.12775/cjfa.2019.001

Clark, R. A. (2021). Consumers perspectives on using biometric technology with mobile banking. Dissertation Abstracts International: Section B: The Sciences and Engineering, 82(9b).

Estrela, P. M. A. B., Albuquerque, R. de O., Amaral, D. M., Giozza, W. F., & de Sousa Júnior, R. T. (2021). A framework for continuous authentication based on touch dynamics biometrics for mobile banking applications. Sensors, 21(12). https://doi.org/10.3390/s21124212

Gerami, M., & Ghiasvand, S. (2016). One-Time Passwords via SMS. Bulletin de La Société Royale Des Sciences de Liège. https://doi.org/10.25518/0037-9565.5208

Habibur Rahman, M., Al-Amin, M., & Sharmin Lipy, N. (2020). An Investigation on The Intention to Adopt Mobile Banking on Security Perspective in Bangladesh. Risk and Financial Management, 2(2). https://doi.org/10.30560/rfm.v2n2p47

Hammood, W. A., Abdullah, R., Hammood, O. A., Mohamad Asmara, S., Al-Sharafi, M. A., & Muttaleb

Hasan, A. (2020). A Review of User Authentication Model for Online Banking System based on Mobile IMEI Number. IOP Conference Series: Materials Science and Engineering, 769(1). https://doi.org/10.1088/1757-899X/769/1/012061

Haupert, V., & Müller, T. (2018). On App-based Matrix Code Authentication in Online Banking. ICISSP 2018 - Proceedings of the 4th International Conference on Information Systems Security and Privacy, 2018-January. https://doi.org/10.5220/0006650501490160

Hayikader, S., Hadi, F. N. H. A., & Ibrahim, J. (2016). Issues and security measures of mobile banking apps. International Journal of Scientific and Research Publications, 6(1).

Husayn, H. (2020). Biometrics in Android | ProAndroidDev. Retrieved May 2, 2022, from https://proandroiddev.com/biometrics-in-android-50424de8d0e

Incel, O. D., Gunay, S., Akan, Y., Barlas, Y., Basar, O. E., Alptekin, G. I., & Isbilen, M. (2021). DAKOTA: Sensor and Touch Screen-Based Continuous Authentication on a Mobile Banking Application. IEEE Access, 9, 38943–38960. https://doi.org/10.1109/ACCESS.2021.3063424

Maček, N., Adamović, S., Milosavljević, M., Jovanović, M., Gnjatović, M., & Trenkić, B. (2019). Mobile banking authentication based on cryptographically secured iris biometrics. Acta Polytechnica Hungarica, 16(1). https://doi.org/10.12700/APH.16.1.2019.1.3

Norrestad, F. (2022). • Online banking users worldwide by region 2020 | Statista. Retrieved May 2, 2022, from https://www.statista.com/statistics/1228757/online-banking-users-worldwide/

Oludele, A., & Oluwabukola, O. (2016). A survey of mobile cloud computing applications: Perspectives and challenges. 7th International Multi-Conference on Complexity, Informatics and Cybernetics, IMCIC 2016 and 7th International Conference on Society and Information Technologies, ICSIT 2016 - Proceedings, 1, 238–243. International Institute of Informatics and Systemics, IIIS.

Omotosho, B. S. (2021). Analysing User Experience of Mobile Banking Applications in Nigeria: A Text Mining Approach. Central Bank of Nigeria Journal of Applied Statistics, 12(No. 1). https://doi.org/10.33429/cjas.12121.4/6

Patrick Ajibade, A., Mutula, S. M., & Ajibade, P. (2020). Big data, 4IR and electronic banking and banking systems applications in South Africa and Nigeria. Banks and Bank Systems. 15(2), 2020. https://doi.org/10.21511/bbs.15(2).2020.17

Phan, D. T. (2020). I have seen the future, and it rings - What we know about mobile banking research. Theory, Methodology, Practice, 16(2). https://doi.org/10.18096/tmp.2020.02.07

Shankar, A., & Rishi, B. (2020). Convenience matter in mobile banking adoption intention? Australasian Marketing Journal, 28(4). https://doi.org/10.1016/j.ausmj.2020.06.008

Sharma, L., & Mathuria, M. (2018). Mobile banking transaction using fingerprint authentication. Proceedings of the 2nd International Conference on Inventive Systems and Control, ICISC 2018. https://doi.org/10.1109/ICISC.2018.8399016

Singh, S., & Srivastava, R. K. (2018). Predicting the intention to use mobile banking in India. *International Journal of Bank Marketing*, *36*(2). https://doi.org/10.1108/IJBM-12-2016-0186

Thakur, T. N., & Yoshiura, N. (2021). AntiPhiMBS-Auth: A New Anti-phishing Model to Mitigate Phishing Attacks in Mobile Banking System at Authentication Level. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *12680 LNCS*, 365–380. Springer Science and Business Media Deutschland GmbH. https://doi.org/10.1007/978-3-030-73216-5_25

Wang, C., Wang, Y., Chen, Y., Liu, H., & Liu, J. (2020). User authentication on mobile devices: Approaches, threats and trends. *Computer Networks*, *170*. https://doi.org/10.1016/j.comnet.2020.107118