ISSN (Print): 2476-8316
ISSN (Online): 2635-3490
Dutse Journal of Pure and Applied Sciences (DUJOPAS), *Vol. 5 No. 1b June 2019*

Two Way Authentication for Android Mobile Phones

Magaji Yusuf[1*], Usman Abdul Gimba[1], Aliyu Uthman Bello[1], Adamu Habu Adamu[2] & Sani Salisu[1]

[1]Faculty of Computing,
Federal University Dutse,
P.M.B 7156, Jigawa State, Nigeria.
[2]Department of Mathematics and Computer Science,
Federal University of Kashere,
P.M.B 0182, Kashere, Gombe State.
Email: yhabib69@yahoo.com

Abstract
Security in mobile devices has advanced over the years, from traditional methods (PIN, android pattern etc.) to biometrics (face, fingerprint etc.). The lapses in the current security system is what brought about this research the two-way authentication. This research aims at improving the authentication mechanisms for mobile devices. The developed authentication system consists of fingerprint and facial recognition for authenticating the mobile device user. Accessing the mobile device can only be possible when the two authentications mechanisms are successful. Fingerprint is the first followed by the facial recognition for gaining access into the mobile device, if one amongst the two fails then access to the mobile device will be denied. Facial authentication requires Microsoft server's connectivity.

Keywords: Single-factor authentication (SFA), Two-factor authentication (2FA), Short Message (SMS) or Application (App)

INTRODUCTION
Information and Communication Technology (ICT) is playing a great role in everyday life. This include the use and access to everyday gadgets such as the smart phones that eases communication and provided several access and utilization of modern-day features and application.

The security provisions are usually deployed on a popular computing device, the smartphone for instance, such as those for the Apple and Samsung (Apple Support 2018) involves the Two-factor authentication (2FA) which is an extra level or layer of security such that only a person that has access to such device actually access it, even if someone else has a level of the security of such device, such as password will not be sufficient to have or allow full access, hence 2FA had provided additional security.

The 2FA is applicable on almost every day endeavours that we don't usually realize, even if the 2FA doesn't provide absolute security it does offer more security than a factor authentication as it involves two ways of identifying an individual's identity (Matt Elliott 2017).The Two-factor

*Author for Correspondence

authentication according to Matt Elliott (2017) can be categorized into three viz: what you know, what you have and then who you are: The first, things one knows, that included questions that expects specific answers, PIN and passwords. The second the device and the third involves things one has, such as voice, face, fingerprints, retina and other biometrics.

Mobile phones as stated earlier, are becoming extremely important as such technological companies like Apple and Samsung produce smart phones with sophisticated technologies for both hardware and software. The phones are used in storing and assessing private and personal data using internet capabilities. The services from the smartphones are capable of accessing and recognizing the fingerprints of the actual users of such device; in addition to an integrated built-in camera for facial recognition or iris scanning of actual users, as well as the microphone for voice recognition and a GPS providing verification of location to serve as an additional factor. With the Voice or Short Message Service (SMS), securing and protecting the data has to be given utmost priority, that further stress the needs, by utilizing one of the security mechanisms the two way authentication have to be employed in order to protect the data (Rouse, M., Loshin, P. and Cobb, M. 2018).

Despite the emphasis on the need for additional security, not much has been said on the 2FA on smartphones especially the android based as against the iOS, as much as has been on online transactions and its associated devices (Rosenblatt, S. and Cipriani, J. 2015;Elliott, M., 2017;Tellini, N. and Vargas, F. 2017; Winder, D. and McMullan, T. 2018). This is because most sites and services of famous online destinations (Elliott, M. 2017), such as Apple and Microsoft amongst others provide mostly online services for enabling 2FA.

Microsoft provides some necessary infrastructure for individual and organizations to support 2FA. The research intends to use such Microsoft Infrastructure for android smartphones in utilizing the third components of authentication of facial recognition and fingerprints against the iOS that has such, in such a way that a stand-alone biometric verification method is adopted to provide the needed 2FA security so that only an authenticated user is ascertained and granted access to the devices and resources (Rouse, M., Loshin, P. and Cobb, M. 2018)

The goal of the research is to develop a customized prototype version of an integrated android fingerprints and facial recognition technology as a two-way authentication mechanism which has the following objectives:

The goal of the research is to develop a customized prototype version of an integrated android fingerprints and facial recognition technology as a two-way authentication mechanism, while it has the following objectives:

1) To investigate the use of two-way authentication process in android devices.
2) To investigate the use of fingerprint and face recognition biometrics as security measures in mobile android devices.
3) To design and develop a two-way authentication prototype for android mobile devices.

LITERATURE REVIEW

There are several two-way authentication apps that exist, but a few popular apps include: The Google Authenticator, the Authy and the DuoMobile. The Google Authenticator, for instance, allows the user to provide their known password and username, after which if verified a set of six numbers are then expected to be entered and if verified, the user is allowed access. In all

however, there are usually some hardware tokens for the two way authentication available to support different approaches to authentication (Rouse, M., Loshin, P. and Cobb, M. 2018).

An example of a hardware token is the YubiKey, which is a popular hardware token that supports one-time passwords (OTP) and consist of a small USB device, Universal second factor protocol that was developed by the FIDO Alliance and finally the public key encryption and authentication. These tokens are sold to desiring users by Palo Alto, Calif. Inc. based, Yubico (Rouse, M., Loshin, P. and Cobb, M. 2018).

In most devices and services an option is presented to either use an SMS or application to activate a 2FA authentication system which sometimes referred to as Factor Authentication. Enabling a two-factor authentication on a system, will require providing the usual username and the password. Some sites providing these services include: Twitter, Facebook, Google's, Gmail and Windows 10 (Elliott, M. 2017; Winder, D. and McMullan, T. 2018).

However, in addition to the username and password, a request is made by the system on whether to enter text or use a verification codes from an app that allows some configurability by the user. The essence of authentication application are to replace the code from text to access any device and service (Rouse, M., Loshin, P. and Cobb, M. 2018).

The 2FA through SMS system has its weakness, as it is less secured considering its susceptibility to hackers if compared to authentication app., though it adds extra security strength to the process that is often turn out to be boring to users (Winder, D. and McMullan, T.2018; Elliott, M.2017).Though other sites exist for the same purpose, the Twitter is the most prominent in the use of SMS as a 2FA on mobile phones, as elaborated by Oberheide (as cited by Rosenblatt, S. and Cipriani, J. 2015) of the Duo Security, an identity proving apps, which makes the Twitter vulnerability as a high-value target susceptible to attack.

In the authentication app, current time, codes and a shared secret are deployed on your phone, such that if it is not utilized within the time, it expires and has to be started again, thereby serving as a hurdle to the hacker. Also an advantage of apps authentication is that it can work offline or if there is no cell service. With an authentication app, the app will have to be installed with a bit extra setup on your phone in addition to setting up a shared secret between the app and such accounts, hence making it better than the SMS based system (Elliott, M. 2017).

Some vendors that support and provide application based 2FA services on smartphones include: The Apple iOS, the Google Android, the Windows 10 and BlackBerry OS 10.The apps allows such phones to serve as a possession factor. Another vendor is the Duo Security, which allows the use of individual devices as trusted devices for the 2FA, in addition to that a user is trusted (Rouse, M., Loshin, P. and Cobb, M. 2018).

As the 2FA makes it harder for a large portion attack on your phone or device, it can be vulnerable if the 2FA authentication mechanism is disabled as result of the attack, bypass or during activation of account recovery (Elliott, M. 2017).

However, such vulnerability could be mitigated if a biometric factor is incorporated in the process, this factor include the fingerprint or facial scan, serving as three-factor authentication thereby providing stronger security (Rouse, M., Loshin, P. and Cobb, M. (2018).

METHODOLOGY

We use Android studio IDE mainly developed for android mobile platform based on IntelliJ IDEA, be it smartphones, tablets etc. (developers.android, 2019) for developing the 2-way authentication project. Android studio is so far the best mobile application development environment (Kim *et.al*, 2014). The Android virtual device which makes testing easier on the fly and all the equipment for development of the prototype is incorporated in the Android Studio.

Two different authentication processes (Fingerprint and facial recognition) where developed and integrated as one single authentication process. We provide brief description of these two projects and their integration below:

Fingerprint Authentication

This is the first authentication page that appears as soon as a mobile phone is on. The following conditions must be satisfied before the application proceed to authentication stage

1. Android version must be greater than or equal to Marshmallow
2. Mobile device must have fingerprint Scanner
3. Application must have permission to use mobile fingerprint scanner
4. Mobile phone lock screen must be secured with at least one type of lock
5. At least one fingerprint must be registered on the mobile phone

When all these conditions hold, a registered fingerprint can be used for the authentication.

At the initial stage, we created a symmetric key in the Android key Store. The symmetric key can be used only when the user's fingerprint has been authenticated. Next, we called Fingerprint Manager to start listening to the user's captured fingerprint from mobile phone fingerprint sensor with cryptographic encryption and decryption functionalities been initialized with the symmetric key created. Fingerprint Manager is an android studio class responsible for synchronizing access to the android mobile phone fingerprint hardware(dev elopers.android, 2019).Once the fingerprint is verified, fingerprint authentication page will disappear, and facial authentication page will appear.

Facial Authentication

We use Face Application Programming Interface (API), one of the Microsoft Cognitive Services to develop the second security layer. At the time of locking, the application request for a facial master image which will be stored in the phone storage. The security layer will then make the phone unstable until another facial image similar to the stored master image is clicked.

The Android operating system does not provide room for creating a custom lock on android mobile phones. Our facial-lock system is therefore simulated by creating a persistent activity which prevents a user from going out of the activity. We use a service which keeps calling the persistent activity as it tries to loss focus. The mobile screen turns off as soon as the lock start and the service terminate when a matching face is found. The termination of the service releases the activity from its persistent nature, hence unlocking the phone. When the matching face is not found, an error message is displayed.

Prototyping Model

The software prototyping referred to the development of software application prototypes that is used to emulate a model of the proposed system (Handson, 2016). The prototype model serves as a mechanism for converting requirements to a working system with a continuous review of the system. User requirement for the proposed system is achieved when there is collaboration between user and analyst of the developing system.

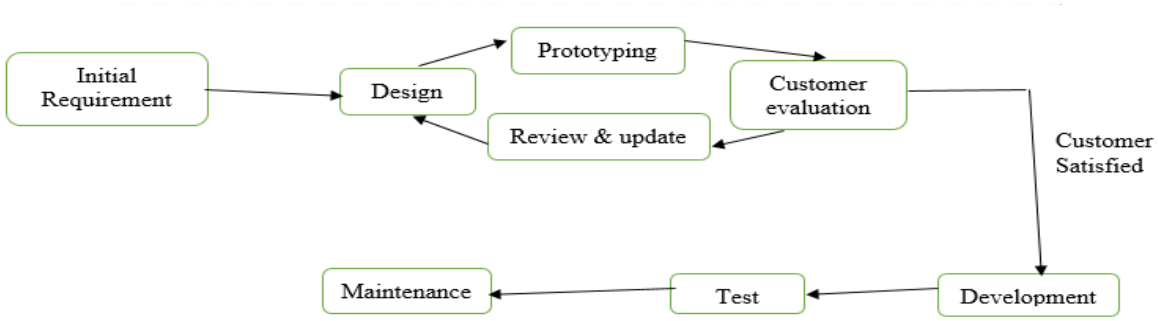

Figure 1: Software prototype model

RESULT AND DISCUSSION

The mobile phone must be connected to the internet to use the Microsoft Face API. Figure 2 is for fingerprint authentication page; it is the first biometric interface the user will encounter. The message below the fingerprint symbol shows that the mobile device satisfies all the five conditions mentioned in section 3.1. If any of the condition fails, an error message is displayed. For instance, if a mobile device does not have a fingerprint scanner, the text will read your phone has no fingerprint scanner.

Figure 2: Fingerprint Authentication page

Uploading the master image process

Figure 3: First facial recognition page

Figure 4: Master image capturing page

This is not a continues process, it is conducted only one time. Once it is uploaded and saved, the application compares any image use for authentication with the master image. Figure 3 is the second phase after the fingerprint authentication and the first page for facial recognition. The page contains a single button which when the user clicks, the page will disappear and the page in figure 4 will appear. The "select image" button of Figure 4 call a new page (figure 5) where a user will either use phone camera or upload a picture from the phone storage. While "Save and Lock" button of figure 4 is used for storing the master image on the mobile phone. The area between the two buttons display the selected image before saving as shown in figure 6. After selecting the image, theapplication will try to detect the face in the uploaded image. After detecting a red square encircled the position of the face in the image (figure 6) indicating a success detection of the face in the uploaded image.A pop-up message ask the user to save the image as master image or discard the image and tryuploading another. The saved image will be use for verification when the user want to access the phone.

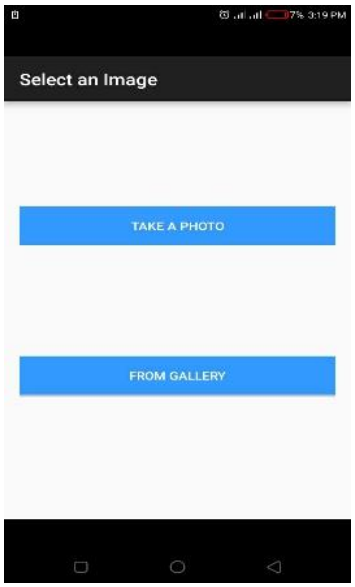

Figure *5*: Master image selection

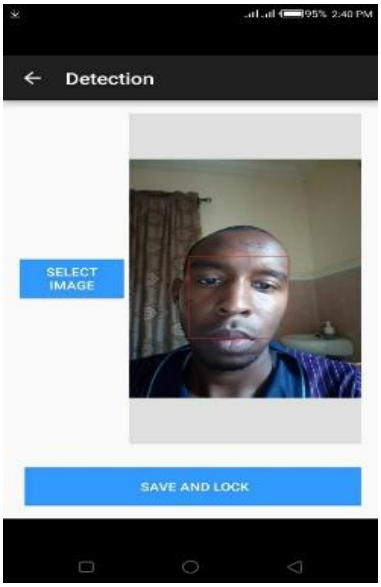

Figure *6*: Master image selected

Image verification Process

This is a continues process which must be followed whenever the user wishes to access the mobile phone. It begins with displaying the page in figure7. A user clicks on "select image" button and figure 8 will appear. As shown in figure 8, a user will click on "Take a photo" button and the camera will appear ready to snap a picture. The snapped image will appear in the area between the "select image" and "Verify" buttons, as shown in figure 9. A pop-up message tells the user to click on "verify" button in order to compare the current image and the stored master image. Once the images match, the phone will be unlocked otherwise a message will be displayed preventing access to the mobile phone as shown in figure 10.

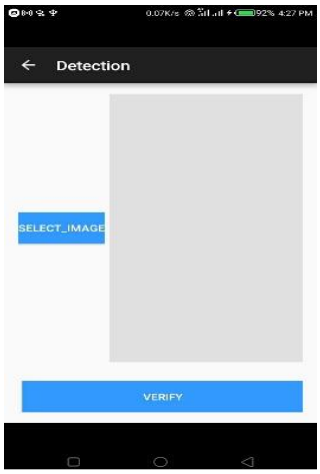

Figure 7: Verification Homepage

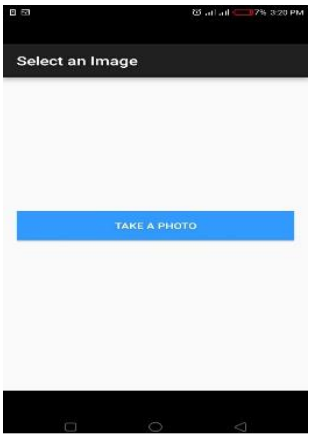

Figure 8: Take a Photo from Phone'scamera

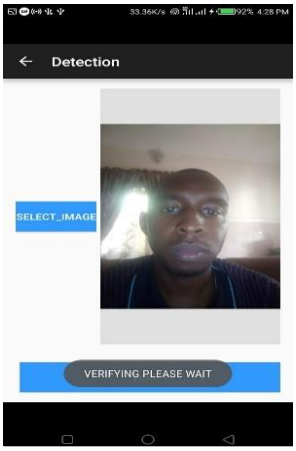

Figure 9: Verifying Image

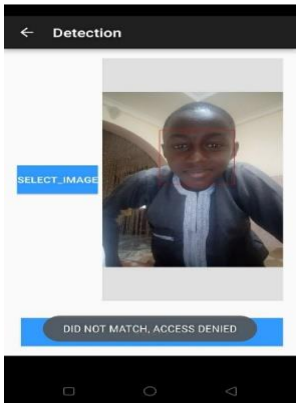

Figure 10: An image different from the master image, Access is denied.

It is important to note that the proposed 2way authentication protocols requires no special skills to use, it is easy to use and highly improves the security of the mobile device. Some of the weakness of this proposed prototype includes:

- Users with neither fingerprint nor hand cannot use the application
- Mobile network is required for facial recognition
- Mobile devices that are not equip with fingerprint sensor and inbuilt camera cannot use the application.
- Android version less than Marshmallow cannot use the Application.

CONCLUSION AND FUTURE WORK

Conclusion

The research main purpose is improving the security of android mobile device so that it can be impenetrable by unauthorised users. The two-way authentication system was designed and implemented as a prove that it's possible to use it on mobile devices. An in depth research has been conducted on areas related to fingerprint and facial recognition authentication system. are the two parameters used for user authentication. In addition to this, all the required functionality of the application has been implemented, tested and evaluated.

Future work

Some recommended future works in order to improve the two-way authentication application include.

1. The application should be able to work without communicating with the Microsoft server
2. Fingerprint and facial recognition integration should be simplified
3. People with fingerprint problem should be able to use the application

REFERENCES

Android Developers. (2019). *Meet Android Studio | Android Developers*. [online] Available at: https://developer.android.com/studio/intro/

Apple Support (2018) *Two-factor authentication for Apple ID*, Copyright © 2018 Apple Inc. All rights reserved, Nigeria.

Handson, O. (2016). Mobile – Based Multi-Factor Authentication Scheme for Mobile Banking. *university of Nairobi*.

Kim, H., Kim, J., Park, J. and Jeong, Y. (2014). Time Pattern Locking Scheme for Secure Multimedia Contents in Human-Centric Device. *The Scientific World Journal*, 2014, pp.1-9

Matt Elliott (2017) *Two-factor authentication: How and why to use it.* Image by Alexandre Normand, CC BY 2.0 CNET Mobile Leer enespañol

Rosenblatt, S. and *Cipriani,J (2015) Two-factor authentication: What you need to know (FAQ)*, CBS Interactive Inc.

Rouse, M., Loshin, P. and Cobb, M. (2018) *What is two-factor authentication (2FA)?* : - Definition, Techtarget- Search Security 2000-2018 Essential Guide

Tellini, N. and Vargas, F. (2017) *Two-Factor Authentication- Selecting and implementing a two factor authentication method for a digital assessment platform,* KTH Royal Institute of Technology, School of Information and Communication Technology (ICT),

Winder, D. and McMullan, T (2018) *alphr-Two-factor authentication explained: Why you should enable two-step security*- Dennis Publishing Limited. Under license from Felix Dennis.