DOI: 10.53704/fujnas.v8i2.283

A publication of College of Natural and Applied Sciences, Fountain University, Osogbo, Nigeria.
Journal homepage: www.fountainjournals.com
ISSN: 2354-337X(Online),2350-1863(Print)

An Enhanced Bilateral Authentication System for Android Devices

***Ogunrinde, M. A., Adebare, W. A., Azeez, R. A. and Osuolale, I. A.**

Department of Mathematical and Computer Sciences, Fountain University, Osogbo, Nigeria

Abstract

Authentication is a method that verifies that users or systems are who they claim to be, based on identity of any form. Smart devices are often lost or stolen; password could be easily detected or hacked. Most of the new model smart devices have inbuilt security for authentication which most times do not work perfectly. For that purpose, high level of authentication for smart devices is needed. The need to ensure security of information on these devices is highly necessary and at the same time difficult. This work developed an enhanced authentication system for android based mobile devices to increase the security level and confidentiality of its information which enables user-friendliness environment. It combines face recognition methods with pin or pattern which makes it more robust and reliable in securing our mobile devices. The implementation was done using Schulz Android Studio SDK and developed with the following programming languages: JavaScript, XML (Extensible Markup Language), OpenCV, and Java. The developed application can be installed and work on any mobile device with the latest android operating system and its backward compatible. The system was tested on different smart devices from different vendors and its efficiency is above 90%. Evaluating the application with some existing systems was done in order to ascertain the reliability of the solution and strengthen it. The system tagged MULTILOCK enables users to register more than one user, and gain access to the device with either pin or pattern together with a registered faces.

Keywords: Face detection, Security, Mobile devices, Confidentiality, Pin, Pattern.

Introduction

The usage of smart devices has been significantly increased in the recent years, as it provides users with several services ranging from phone calls, internet services, sharing data, keeping data, online / off-line games, and some entertaining online/ off-line applications to mention a few. On a more advanced use, smart devices have become a commercial device for those who choose it for such. Many users have converted it to a marketplace where they buy and sell and at the same time track their deliverables without leaving the four walls of their bedroom. For some users, it's their wallet used to transact billions worth of Naira or dollars as the case may be (Qin *et al.*, 2017).

One of the underlining features of the smart devices is mobile Operating system (OS). This feature eases the smooth functionality of other features of the smart devices. There are many mobile Device operating systems available, such as

*Corresponding author: +2348054280030
Email address: bogunrinde@gmail.com

Android, iOS, Microsoft Window mobile, Symbian and BlackBerry (Yildrim *et al.,* 2014). Android is the widely used mobile device operating system with better performances as compared to other mobile device operating systems (Yildrim *et al.,* 2014). Android OS is based on Linux operating system architecture. The desktop OS and the mobile device versions of such operating systems are very different, especially in user interfaces and architecture design. With smart devices, one can connect to the internet and instantly communicate with friends, partners and browse data and information from the World Wide Web (Schulz & Plohmann, 2012).

Morgan, the editor-in-chief of Cybersecurity Ventures said in his 2019 Cybersecurity report that "Cybercriminal activity is one of the biggest challenges that humanity will face in the next two decades". According to the editor-in-chief, most of these crimes are done using smart devices. Morgan forecasts that more than half a billion wearable devices will be sold worldwide in 2021, up from roughly 310 million in 2017. Wearables include smart watches, head-mounted displays, body-worn cameras, Bluetooth headsets, and fitness monitors, etc (Morgan, 2019).

The need to maintain the security of information in smart / mobile devices is becoming both increasingly important and very difficult. Most of the current phones have security for authentication. Authentication verifies that users or systems are who they claim to be, based on identity (e.g., username) and credentials (e.g., password). Mobile devices are easily lost or stolen; moreover, password could be easily hacked or detected. For that purpose, high level of authentication for mobile devices is needed (Joseph, 2015).

The security and privacy challenges on mobile devices can be overcome through the use of authentication system like pin, pattern, fingerprint and face authentication (Patel *et al*., 2016). But these authentication methods are not secured at high ratio because with brute forcing, such measures could be penetrated. Combination of all security technology is better; one can use the fingerprint **(password)**, pin and combined with the face lock so as to have a strong security. There are problems associated with fingerprint, like having a wounded finger, which is not associated with the face.

Username and password are the most commonly used mechanism for authentication because of simplicity and convenience. However, it suffers from few drawbacks like selection of weak passwords by the users, users disclosing their passwords etc. This weakens the security posture of the mobile devices. Similarly, as mobile device provides vast operations which are performed on Internet, thus are saddled with some challenges like security, safety and privacy of data and information as well. Critically, a lot of Malware, Viruses and Trojans have been developed which are based on mobile devices APIs (application program interface) and most of them look like safe software; some like reliable applications (Gmail, Facebook, etc.) collect user's information such as geolocation without user's knowledge with GPS service in mobile device (Agrawal & Patider, 2014). Hence, the need for the development of an enhanced android based bilateral authentication system for devices.

Review of Related works

In the year 2013, Khan *et al*. performed a thorough survey on mobile devices, by considering them not as communication devices but as personal sensing platforms. Their research focused on two main categories, participatory and opportunistic mobile phone sensing systems. Having that in mind, they presented the existing work in the area of security of mobile phone sensing. They concluded that security and privacy issues need more attention while developing mobile phone sensing systems and applications, since as mobile phones are used for social interactions; users' private data are vulnerable. The authors didn't present any systems for user authentication for mobile devices (Khan, *et al*., 2013).

Harris *et al*. (2014) in their survey tried to identify all emerging security risks that mobile devices impose on Small and Medium Enterprises (SMEs) and provided a set of minimum security recommendations that can be applied. Adapting mobile devices by the SMEs is on a fundamental

dilemma, whether to move to the mobile era, which results in facing high risks. Focusing on Android platforms, Harris *et al.* (2014) and Faruki *et al.* (2015) surveyed several security aspects, such as code transformation methods, strength, and limitations of notable malware analysis and detection methodologies. By analyzing several malware and different methods used to tackle the wide variety of new malware, they concluded that a comprehensive evaluation framework incorporating robust static and dynamic methods may be the solution for this emerging problem.

As pointed out by Meng *et al*. (2015) password and PINs means of authentication are still with many problems, the authors carried out a thorough research on biometric-based methods for authentication on mobile phones. The research included a survey article using both physiological and behavioral approaches, the deployment feasibilities on touch-enabled mobile phones analyzes, identification of points of attack and the appropriate countermeasures. Their conclusions were that a hybrid authentication including both multimodal biometric authentication along with traditional PINs or password can improve both security and usability of the system. In order to further increase security and privacy of mobile devices, active authentication techniques, which constantly monitor the behavior of the user are employed by Patel *et al*. (2016) where a thorough analysis of their pros and cons were presented along with open areas for further exploration. Using physiological and behavioral biometrics-based techniques similar to the ones surveyed in Meng, *et al*. (2015) along with a multimodal biometrics-based fusion methods have also been found to be the most efficient in terms of security and usability. One main issue that arises from the use of biometric characteristics is the possible theft, which can be prevented with the use of template protection schemes.

Similarly, Touch dynamics was published by Teh *et al.* (2016). It is a behavioral biometrics, which captures the way a person relates with a touch screen device both for static and dynamic authentication of users. Details of implementations, experimental settings covering data acquisition, feature extraction, and decision-making techniques were explored in the research.

Alizadeh *et al*. (2016) examined authentication issues in Mobile Cloud Computing (MCC) and compared it with that of cloud computing. They introduced both Cloud-side and client validation techniques and spotted significant parameters that are critical for structuring present day confirmation frameworks for MCC as far as security, strength, protection, ease of use, productivity, and versatility.

Aslam *et al*. (2017) studied authentication protocols to access the Telecare Medical Information Systems and examined their qualities and shortcomings as far as guaranteed security and protection properties, and calculation cost. The plans were partitioned into three broad categories of one-factor, two-factor, and three-factor authentication schemes.

Velasquez *et al*. (2018) introduced existing validation strategies and techniques so as to observe the best ones for various settings. In the same year, Kilinc & Yanik (2018) looked into and assessed a few SIP verification and key understanding conventions as per their presentation and security highlights. In another overview article that was distributed in 2018, Spreitzer et al. concentrated on side-channel assaults against cell phones and quickly examined different assaults that have been applied in the brilliant card or work area/cloud setting, since the interconnectivity of these frameworks makes advanced mobile phones defenseless against them too. The creators inferred that the vast majority of the assaults target Android gadgets, because of the huge piece of the overall industry of Android stages. They additionally suggested that future research should concentrate on wearables, for example keen watches; that may experience the ill effects of similar assaults soon, and brought up that side-channel assaults can be joined with different assaults that misuse programming vulnerabilities so as to be progressively proficient (Spreitzer *et al*., 2018).

From the above reviewed articles, just few of them deal with authentication schemes for mobile devices while none comprehensively covers the

authentication angles as associated with smart devices. To the best of our knowledge, this work introduced an upgraded confirmation framework for android based brilliant gadgets by joining the facial information with either a PIN or secret key.

Review of available Mobile Authentication System and their Features

Some of the existing applications were downloaded, installed and their usability was tested considering the form of authorization employed and how effectives they were such as recognizes unregistered face and how long they worked before stopping. Table 1 shows analyses in detail of how they were developed, forms of authorization used, the operating system supported together with their weaknesses.

Problem of the Existing System

Many face recognition software have been implemented in the past decade. Each of the software uses different methods and different algorithm than other software. Some extracts the facial features from inputted image to identify the face while other algorithms normalize a set of face images and then compress the face data; save it as one image that can be used later for facial recognition by comparing with the input.

System Analysis and Design

In the development of this application, a client server architectural approach was adopted. The steps involved in the development of the application are summarized in the Figure 1.

The Context Diagram

Context diagram defines the system boundaries, or part of a system, and its environment, showing the entities that interact with it. This diagram is a high-level view of a system. It is similar to a block diagram. Figure 2 shows the context diagram of the proposed enhanced system for securing android smart device.

Table 1: Review of some existing Application

S/N	NAME OF APP	TOOLS USED	FORMS OF AUTHORIZATION	OPERATING SYSTEM	WEAKNESS
1	Applock face	Microsoft Azure, OpenCV	Face and Pin	Android	It recognizes unregistered face
2	OasisFace	JavaScript API, node JS	Face	iOS and Android	It works for a while then stop
3	Nametag	OpenCV, XML	Pin and Face	Android and iOS	The face interface is not functioning even after registration
4	FaceLock Screen	Node JS, OpenCV, XML	Face	Android	It recognizes unregistered face
5	FaceVault	XML, FR DB, OpenCV	Face and Pattern	iPhone, ipads, and iPod	It works for a while and starts malfunctioning

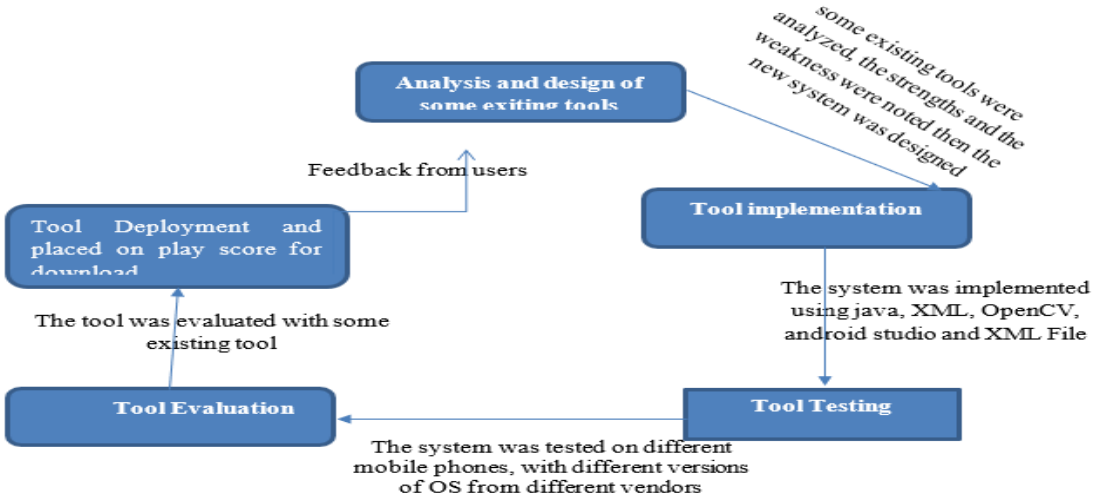

Figure 1: Framework for the developed tool

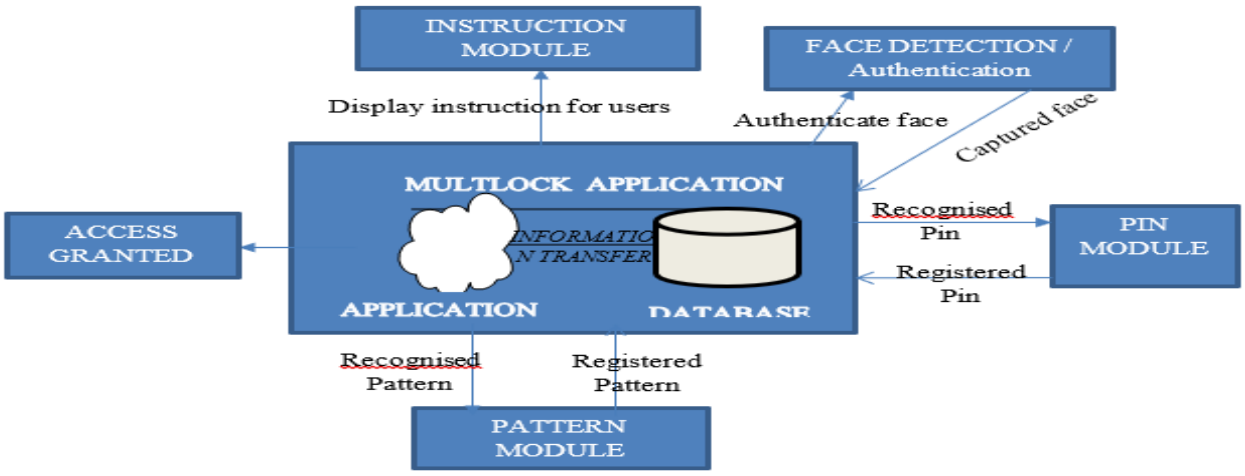

Figure 2: The System Context Diagram

Instruction Module: This module explains to the user how the system should be operated.

Face Detection / Authentication Module: The module presented the camera for capturing face at the registration page. It also authenticated captured faces while unlocking the smart devices.

Pattern Module: The interface represents the pattern lock page, which is shown when after the user enters parameter in the Input name box. It serves as an alternative to pin for the authorized user when unlocking the device with the user's face.

Pin / Password Lock Screen: The password lock screen, shown when the Pin Code button is being clicked. It serves as an alternative to pattern for the authorized user when unlocking the device with the user's face.

Access Granted Module: This module grant access to users after verifying all the inputted parameters.

The Application Workflow

The flow chart of the system is the physical graphical representation of the general process routine that the program follows starting from download, installation, running and executing its processes or tasks. It shows flow of how users are registered on the program, the acceptance of input to when the output is displayed. Figure 3a and 3b shows the designed system flow.

Development Tools

Application Implementation was actualized using a list of mobile development tools which includes Android Studio, OpenCV SDK, Java and XML.

Android Studio is an Integrated Development Environment (IDE) specifically built for developing applications that run on Android Operation systems. The IDE is Java based and uses a Gradle-based build system, emulator code templates, and GitHub integration. Every project in Android Studio has one or more modalities with source code and resource files which includes the App itself, Libraries, and Google App Engine, etc. it is the duty of Android Studio to afford the developers the interface to create their apps and manages some of the underlined issues behind the scenes. An OpenCV SDK will be used to develop the face recognition module. Java programming language will be used to code the application login of the system while Extensible Markup Language (XML) was used for designing the user interface of the mobile application because it has a flexible way of formatting information and electronically share structured data via the public Internet, as well as via corporate networks.

The MULTILOCK App

The developed mobile application was a real-time face recognition system that reads a scanning from a camera and detects any face present in front camera and then checks if this face is present in the set of face images in the database Schulz

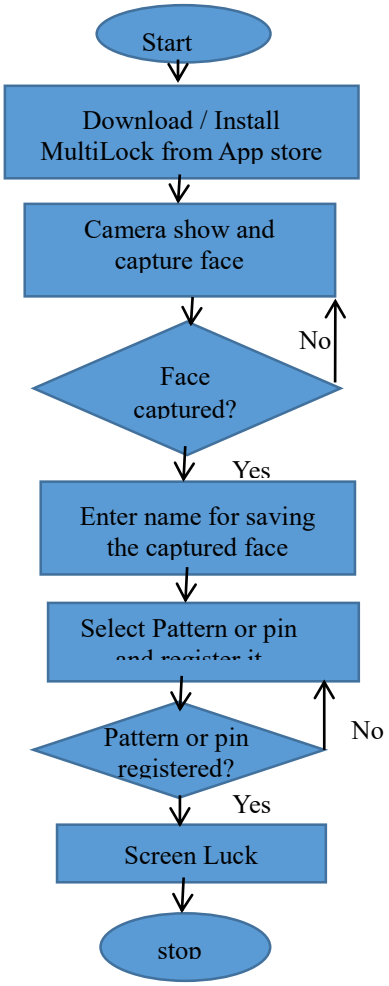

Figure 3a: The App Registration Flow

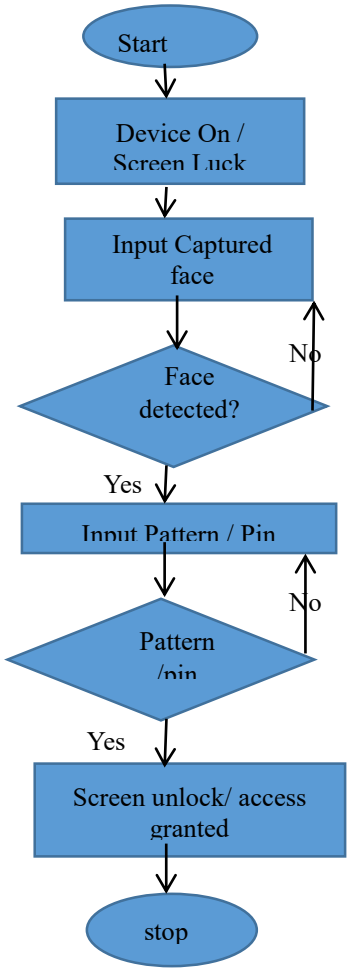

Figure 3b: The App Work Flow

face recognition technique. Once it is downloaded from the device application store and installed, it prompts the users to set it up for use to enable the lock process seen on app startup. Figure 4 shows more detail.

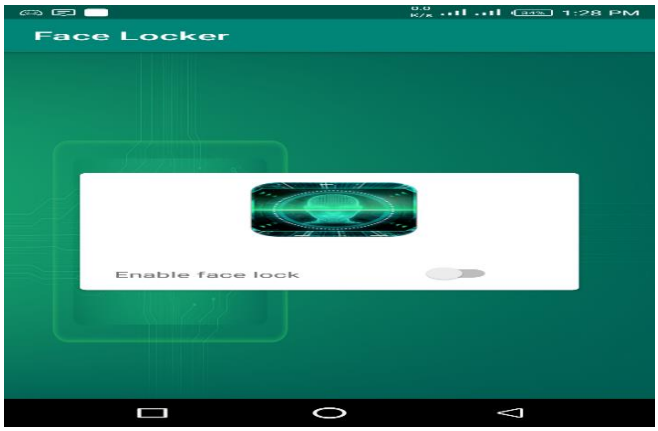

Figure 4: Splash Screen for App Enable

During the setup process, once the application is enabled, it prompts users to enter the name for which the face to be registered will be saved. At this interface, the registered faces can be added and deleted too. Figure 5 shows more details.

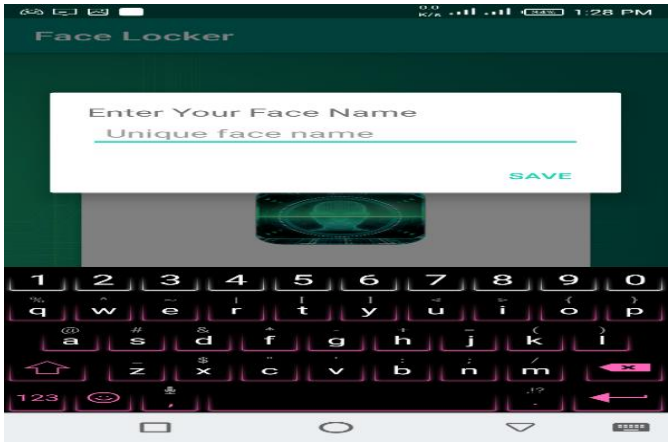

Figure 5: User registration

Pattern Input Page

After the name has been save, pattern input face (Figure 6) come up where the user selects whether to use patter or PIN with the face to. This interface represents the pattern lock page which will be used in addition with the captured face to unlock the device.

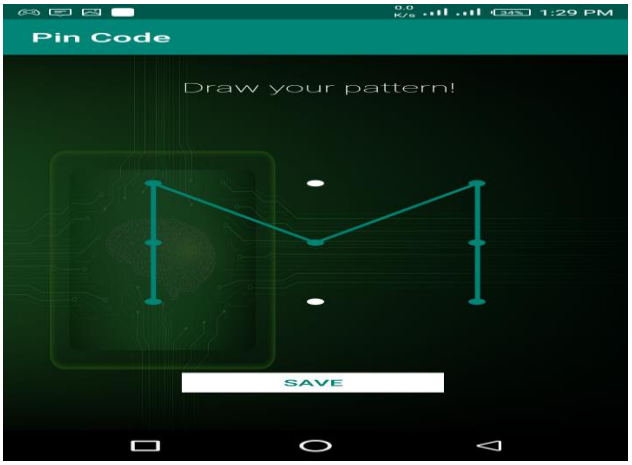

Figure 6: Pattern input interface

Pin Input Page

The interface represents the Personal Identification Number lock page, which is shown when the user enters the pattern input page. It is used in addition with the captured face when pattern are not used to unlock the device for the authorized user. Figure 7 shows how password are accepted

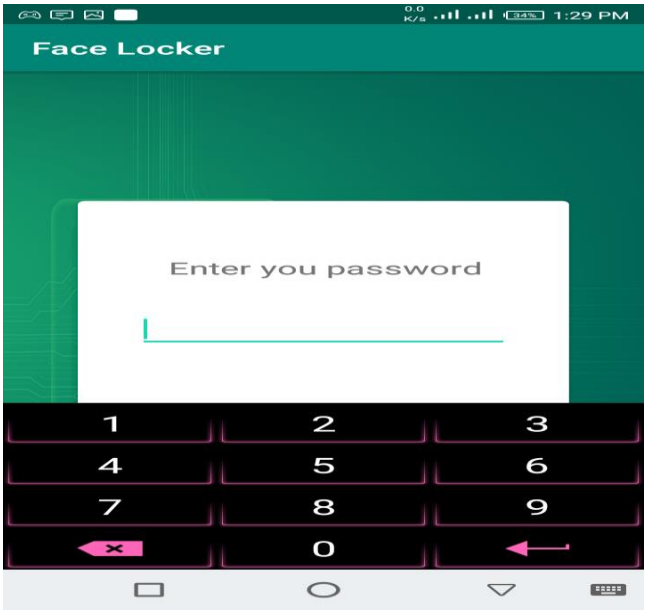

Figure 7: PIN input interface

Face Registration Page

The interface presents how face was captured which can is done through the front camera of the device. It captures and registers the face in

database for later authentication. Figure 8 shows how it works.

Figure 8: Face Registration Page

Lock Screen

The lock screen shows immediately after the registration has been completed, the device is then locked. It contains two buttons "Pin code" and "Camera" which when clicked redirects to other unlock methods available. This shown in Figure 9.

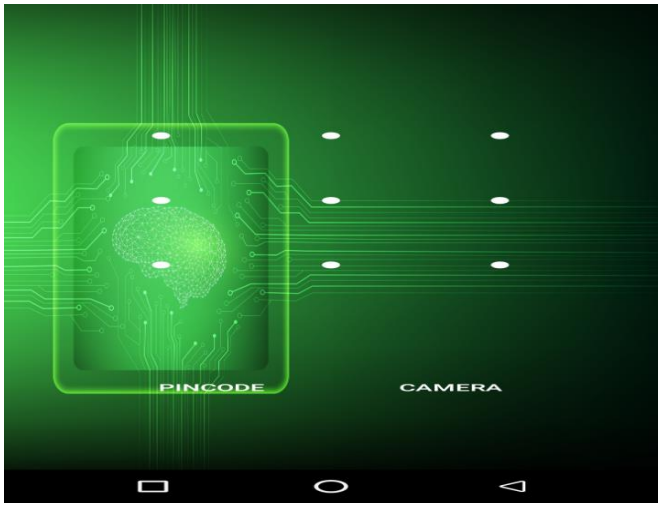

Figure 9: Pattern Lock Screen

Homepage Resources

This page shows all the names of registered faces. Already registered user's faces can be deleted here by clicking the red button while new faces can be added by clicking the plus button as shown in Figure 10. This feature allows more than one face to be registered as this will help in cases of emergences.

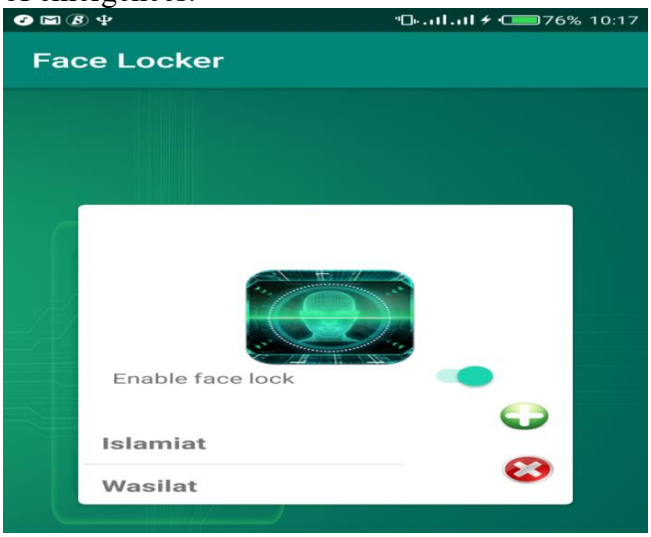

Figure 10: Homepage Resource

System Testing

The main aim of system testing is mainly to locate and correct errors, which is meant to ensure that the system works accurately and efficiently before deployment.

STEPS in testing:

1. The program is written using Schulz android studio, OpenCV, XML technology; hence modules were run separately before running the whole program
2. Errors and debugging process were highlighted and carried out
3. Program was debugged
4. User acceptance tests were run and reports were taken
5. The system was tested on different mobile devices from different vendors with different mobile operating systems. The results were reported in Table 2.

System Evaluation:

After testing, the developed application was evaluated and some of the existing applications, Table 3 shows the result.

Table 2: Testing the Tool with Different Mobile Devices

S/n	Device name	Device model	Operating system	Operating system Version	Device ram	Performance of the system on the device
1	Samsung	SM-J106H	Android	6.0.1	2.00GB	It works on the device, the application lock and unlocks the device.
2	Itel	533	Android	8.1.0	4.00GB	It works on the device, the application lock and unlocks the device.
3	TECNO	K7	Android	7.0	1.00GB	It works on the device, the application lock and unlocks the device.
4	INFINIX	X606C	Android	8.1.0	2.00GB	It works on the device, the application lock and unlocks the device.
5	TECNO	Camon CX	Android	7.0	2.00GB	It works on the device, the application lock and unlocks the device.
6	TECNO	KA7	Android	8.1.0	1GB	It works on the device, the application lock and unlocks the device.
7	Blackview	A7	Android	7.0	4GB	It works on the device, the application lock and unlocks the device.

Table 3: Evaluation with Existing System

S/n	**Existing system**	**Forms of authorization**	**Weakness**	**Developed MULTILOCK**
1	Applock Face	Face and Pin	It recognizes unregistered face	It recognizes only faces that are registered
2	OasisFace	Face	It works for a while then stop	It does not stop working unless user decline, or disabled it the access granted
3	Nametag	Pin and Face	The face interface is not functioning even after registration	The face interface functioning immediately after registration
4	FaceLockScreen	Face	It recognize unregistered face	It recognizes only faces that are registered
5	FaceVault	Face and Pattern	It works for a while and starts malfunctioning	It does not malfunction

Conclusion

This work took a profound look into different approaches to secure Android smart devices. It was seen that currently, there were many methods and approaches for securing our mobile devices; e.g Pattern, Pin, Thumbprint, facial lock etc. Here, the focus was on pin, pattern and face recognition methods which are very much reliable in securing our mobile devices.

In this work, a combination of multiple methods of security mechanisms for the purpose of optimizing and improving the security level of our mobile devices was the focus. The results showed our approach had significant advantage over existing applications for some cases, and the combination of the method provides a strong security. The extension of the work to cover other operating systems might be of future interest.

References

Agrawal, A. & Patidar, A. (2014). Smart Authentication for smart phones. *International Journal of Computer Science and Information Technologies* 5 (4), 4839-4843.

Alizadeh, M., Abolfazli, S., Zamani, M., Baharun, S. & Sakurai, K. (2016). Authentication in mobile cloud computing: A survey. *Journal of Network and Computer Applications,* 61:59–80, DOI 10.1016/j.jnca. 2015.10.005.

Aslam, M. U., Derhab, A., Saleem, K., Abbas, H., Orgun, M., Iqbal, W. & Aslam, B. (2017). A Survey of Authentication Schemes in Telecare Medicine Information Systems. *Journal of Medical Syst*ems 41(1), 14, DOI 10.1007/s10916-016-0658-3.

Faruki, P., Bharmal, A., Laxmi, V., Ganmoor, V., Gaur, M. S., Conti, M. & Rajarajan, M. (2015). Android Security: A Survey of Issues, Malware Penetration, and Defenses. *IEEE Communications Surveys and Tutorials* 17(2), 998–1022, DOI 10.1109/COMST.2014.2386139.

Gandotra, P., Kumar, Jha R. & Jain, S. (2017). A survey on device-to-device (D2D) communication: Architecture and security issues. ACM *Journal of Network and Computer Applications* 78, 9–29, DOI 10.1016/j.jnca.2016.11.002.

Harris, M. A. & Patten, K. P. (2014). Mobile device security considerations for small- and medium-sized enterprise business mobility. *Information Management and Computer Security,* 22(1), 97–114, DOI 10.1108/IMCS-03-2013-0019.

Khan, W. Z., Xiang, Y., Aalsalem. M. Y. & Arshad, Q. (2013). Mobile Phone Sensing Systems: A Survey. *IEEE Communications Surveys & Tutorials* 15(1), 402–427.

Meng, W., Wong, D. S., Furnell, S. & Zhou, J. (2015). Surveying the Development of Biometric User Authentication on Mobile Phones. *IEEE Communications Surveys & Tutorials* 17(3):1268–1293,DOI 10.1109/COMST.2014.2386915.

Patel, V. M., Chellappa, R., Chandra, D. & Barbello, B. (2016). Continuous User Authentication on Mobile Devices: Recent progress and remaining challenges. *IEEE Signal Processing Magazine*, 33(4), 49–61.

Qin, Z., Sun, J., Wahaballa, A., Zheng, W., Xiong, H. & Qin Z. (2017). A secure and privacy preserving mobile wallet with outsourced verification in cloud computing. *ACM Journal of Computer Standards & Interfaces,* 54, 55–60, DOI 10.1016/j.csi.2016.11.012.

Spreitzer, R., Moonsamy, V., Korak, T. & Mangard, S. (2018). Systematic Classification of Side-Channel Attacks: A Case Study for Mobile Devices. *IEEE Communications Surveys and Tutorials*, *20(1),* 465 - 488, DOI 10.1109/COMST.2017.2779824

Teh, P. S., Zhang, N., Teoh, A. B. J. & Chen K (2016). A survey on touch dynamics authentication in mobile devices. *Elsevier Journal of Computers and Security,* 59, 210–235, DOI 10.1016/j.cose.2016.03.003

Velásquez, I., Caro, A. & Rodríguez, A. (2018). Authentication schemes and methods: A systematic literature review. Elsevier Journal of *Information and Software Technology,* 94:30–37, DOI 10.1016/j.infsof.2017.09.012.