The Emerging Framework To Improve Mobile Phone Security System

BY

MD.ABDUL AZIZ
ID: 153-15-6526

AND

PABEL MIAH
ID: 153-15-6512

This Report Presented in Partial Fulfillment of the Requirements for the Degree of Bachelor of Science in Computer Science and Engineering.

Supervised By

Dr. Karim Mohammed Rezaul
Visiting Professor
Faculty of Arts, Science and Technology
Wrexham Glyndŵr University, UK

DAFFODIL INTERNATIONAL UNIVERSITY

DHAKA, BANGLADESH

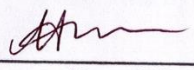
SEPTEMBER 2019

APPROVAL

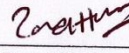
This Project titled **"The emerging framework to improve mobile phone security system"**, submitted by MD. ABDUL AZIZ and PABEL MIAH, ID No: 153-15-6526, 153-15-6512 to the Department of Computer Science and Engineering, Daffodil International University has been accepted as satisfactory for the partial fulfillment of the requirements for the degree of B.Sc. in Computer Science and Engineering and approved as to its style and contents. The presentation has been held on 14th September 2019.

BOARD OF EXAMINERS

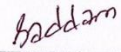
Dr. Syed Akhter Hossain — **Chairman**
Professor and Head
Department of Computer Science and Engineering
Faculty of Science & Information Technology
Daffodil International University



Nazmun Nessa Moon — **Internal Examiner**
Assistant Professor
Department of Computer Science and Engineering
Faculty of Science & Information Technology
Daffodil International University



Md. Zahid Hasan — **Internal Examiner**
Assistant Professor
Department of Computer Science and Engineering
Faculty of Science & Information Technology
Daffodil International University



Dr. Md. Saddam Hossain — **External Examiner**
Assistant Professor
Department of Computer Science and Engineering
United International University

DECLARATION

We hereby declare that, this project has been done by us under the supervision of **Dr. Karim Mohammed Rezaul, Visiting Professor,** Wrexham Glyndŵr University, United Kingdom. We also declare that neither this project nor any part of this project has been submitted elsewhere for award of any degree or diploma.

Supervised by:

Dr. Karim Mohammed Rezaul
Visiting Professor
Faculty of Arts, Science and Technology
Wrexham Glyndŵr University
Mold Road, Wrexham, LL11 2AW
United Kingdom

Submitted by:

Md. Abdul Aziz

Md. Abdul Aziz
ID: 153 -15-6526
Department of CSE
Daffodil International University

Pabel Miah

Pabel Miah
ID: 153-15-6512
Department of CSE
Daffodil International University

ACKNOWLEDGEMENT

First we convey our heartfelt thanks and gratitude to Almighty Allah for His divine blessing which enables the successful completion of the final year research based project.

We really grateful and wish our profound our indebtedness to **Dr. Karim Mohammed Rezaul, Visiting Professor,** Wrexham Glyndŵr University, United Kingdom. Deep Knowledge & keen interest of our supervisor in the field of Data *Science* to carry out this project. His endless patience, scholarly guidance, continual encouragement, constant and energetic supervision, constructive criticism, valuable advice, reading many inferior draft and correcting them at all stage have made it possible to complete this project.

We would like to thank all of our course mate at Daffodil International University who participated in this discussion while finishing the course work.

Lastly, we must recognize our parents continuous assistance and patients with due regard.

ABSTRACT

It is obvious that the Mobile phone technology was one of the greatest innovations in the 20th century. Mobile's safety (MS) issue is currently a great concern as it is used in various industries and business organizations. Mobile phones are the perfect way to remain connected and provide a feeling of safety and security for the user. MS implies anti-theft security system activated within the mobile system as well as the phone functioning. Mobile security relates attempting to secure data on mobile devices such as Smartphones and Tablets. Data security means how our information can be protected against unauthorized access. Many techniques are nowadays being used to safeguard the mobile phone. However, with these techniques, mobile devices and information are not completely secure. There are some security concerns of mobile phone, data and mobile network use. This research reviews concurrent literature on mobile phone security system and proposes a framework named "Emerging Mobile Phone Security System" (EMPSS) that secure mobile authentication, mobile data both (online and offline), mobile Internet, mobile network, sharing data (both online and offline) and mobile anti-theft security at a time. For verification purpose, the framework has been partially implemented for the mobile authentication part by developing a mobile application (Mobile App). The implemented application has been installed in the several mobile devices and it works pretty well as per the authentication part of the framework. It is believed that this app fulfills the requirements concerning user authentication of a mobile device and can easily verify the unauthorized user who tries accessing the mobile device.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

CHAPTER 1
INTRODUCTION

1.1 INTRODUCTION

A mobile phone is a handheld wireless device that enables users, among other characteristics, to make and collect calls and send text messages. Only calls could be made and received by the earliest mobile phone generation. However, today's mobile phones are packed with many additional features, including web browsers, games, cameras, video players, and even navigation systems. A mobile phone may also be referred to as a mobile phone or just a cell phone. Martin Cooper of Motorola's first cell phone called using the Motorola Mobile Product in the mid-20th century and this mobile's specification involves weight of 2.5 pounds and battery life is 20 minutes. The first commercialized cell phone was openly announced later in 1983 at a cost of $3,995 as Motorola DynaTac. Motorola built the first "Flip" phone in 1989 using Microtac technology and its cost was $3,000. In 1993, BellSouth of IBM Simon, the private communication device with the fundamental touch screen, introduced the first "smart-phone" [1].

The mobile phone's privacy and security are always far behind the danger. Today we use the mobile phone in different sectors like Financial Industry, E-commerce, Education, Health, etc. And the user of people in that sector is not enough concerned about their privacy and security of data. That's why the third party takes advantage of us and uses our private data through unauthorized access, and then with mentally or financially or both of them we suffer a lot. The different mobile Companies utilizes different kinds of mobile phone security system Framework. However, these frameworks cannot secure Mobile Antitheft (Both, On State or Off State), Mobile Data (Both, Online or Offline), Share Data (Storage or Cloud Data), Mobile with Secured Network, etc. In this paper, we propose a framework that helps secure Mobile Antitheft (Both, On State or Off State), Mobile Data (Both, Online or Offline), Share Data (Storage or Cloud Data), Mobile with Secured Network, and Internet Browsing simultaneously. Currently, Rapid development and implementation have been seen in safety systems for mobile devices. In order to secure the

mobile phone, users require high safety and excellent service quality. Our suggested framework helps increase mobile security which leads to providing excellent service quality. In earlier researches, there are many frameworks for authentication systems provided which are different from our approach. Recent study has shown the options to obtain certain cognitive characteristics such as touch dynamics, keystroke dynamics and gait detection using smartphone sensors and accessories. These characteristics are known as cognitive biometrics and can be used for implicitly and continually verifying or identifying people on smartphones [2]. The touchscreen biometrics enables the user to passively authenticate without the need for additional sensors in the device. Data is acquired from the user's ordinary touchscreen interaction, without having to perform any particular tasks. Here three distinct schemes have been studied, one using SVM, another using UBM adjusted GMM statistics and the third one using their fusion [3]. The concept of keystroke is based on biometric authentication. And it presents a comprehensive study of the latest research on keystroke dynamic authentication, the techniques, and algorithms used, the rate of precision and the deficiencies of those research. It also defines some problems that need to be resolved in the design of keystroke dynamic biometric systems, suggests improvements in the precision rate of KB (keystroke based) systems, and suggests possible future directions for studies [4]. The proposed DeepService, the latest method which enables user identification based on the user keystroke data recorded by a specific web browser or keyboard [5]. Biometric gait based on accelerometer is an inconspicuous way for people to authenticate their smartphones [6]. Gait recognition is a method used to identify or verify people based on their patterns of walking. Smartwatches containing an accelerometer and a gyroscope have been used to implement biometrics-based on gait [7]. The suggested article introduces a multi-biometric scheme for personal authentication based on the observation that the instinctive gesture of reacting to a phone call can be used to capture two distinct biometrics, namely ear and arm gestures, matched by their physical and cognitive character, respectively [8]. Another multi-biometric authentication system that developed convolutional neural networks (CNN). CNN architectures that fuse multiple information sources in order to improve performance in ocular biometrics. Different CNNs are intended to fuse left and right units and perform profound depiction of soft biometric

data (such as sex and age) together with main biometrics at the feature stage and intermediate level of CNN architecture [9]. A further scheme is an authentication with two factors. It suggested a Translucent Two-Factor Authentication (T2FA) based on Physical Unclonable Function and voiceprint. T2FA prevents tedious communication and offers the same high level of satisfaction with user experience as single-factor authentication and at the same time shows elevated security [10]. Bio-signal based scheme also provides authentication security, where Electroencephalography (EEG) recorded signals during this unlocking period provide the user with a distinctive biometric property and process the EEG signals collected while customers conduct unlocking and authentication analyses [11]. Another suggested scheme is Secure Pick Up (SPU), a convenient, lightweight, indevice, non-intrusive and automatic-learning system for smartphone user authentication. Operating in the background, the system implicitly observes users' phone pick-up movements, the way they bend their arms when they pick up a smartphone to interact with the device, to authenticate the users [12]. This research proposed an EMPSS framework that provides all types of mobile phone security system. The implementation of authentication part in this framework ensures the security of the mobile devices authentication System.

1.2 Motivation

Nowadays mobile phone security is the biggest concern since mobile phone usage in various sectors. There are lots of mobile application uses for mobile security but those are not able to secure all types of mobile security in one frame. Some security features given by Mobile Industries and some we are taken from different types of external applications and Security services like as finding location of a device. So we think how it will be if we proposed a framework which is able to secure mobile device fully at a same window that will tackle all types of mobile security problems such as anti-theft, mobile data security, mobile network security, and internet browsing security.

1.3 Rational of the Study

Nowadays mobile phone is facing so many securities problems. So user always take some responsibility from different source to be secured them self. Users always wants the best security but technology hampered user's security. Peoples always wants all types of security in a window but there is no this types of system at all in present. So Peoples always not to feel enough secure when they using mobile device. Therefore we proposed a mobile security framework that's help users all types of security in a one window. After using this user don't need others external security features. Our proposed framework is able to secure user authentication, mobile data security, internet security, mobile anti-theft and mobile with secured network. But for each security purpose at present we are using different types of external sources or features. But our proposed framework reduces external sources for different security features and improve the mobile phone security most which user emergency need at presents. We hope after using our propped framework the future risk for mobile device will be reduced.

1.4 Research Questions

We can find out the answers to these issues from this research:

- Is mobile phone security sufficient?
- Is there any complexity in the current safety scheme for mobile phones?
- Should the security system for mobile phones be updated?
- What would be the consequence of mobile phone remain in one frame?
- What is the future risk for mobile phone Security and how to handle it?

1.5 Expected Outcome

Some of the main expected outcomes are given below:

- Ensure User mobile phone security satisfaction of data or information.
- Ensure to minimize the attacks of mobile device for future generations.
- Ensure mobile anti-theft both ON state and OFF State of the mobile device.
- Ensure mobile phone data share security.
- Ensure mobile Device with a Secured Networks.

- Ensure all types of Security issues will remain in a one frame so that the system will be user friendly.

1.6 Report Layout

This paper is organized as follows: In chapter 1, we discuss the introduction part of our whole work. Background of our research project has been depicted in the chapter 2. In chapter 3, Research Methodology has been illustrated properly. In chapter 4, System Implementation has been described. Experiment results and discussion have also been outlined in chapter 5. Finally, summary, conclusion, recommendation and implication for future research has been described in the chapter 6.

CHAPTER 2
BACKGROUND

2.1 Introduction

Users are not sufficiently worried about their privacy and data security. That's why the third party takes benefit of us and utilizes our private data through unlawful access, and then we suffer a lot with both mentally or financially. Mobile phones have become an incredibly powerful technology, without which we cannot think of our lives. Currently, the total mobile phone consumer is nearly 3 billion [13]. The consumer of mobile phones is growing day by day so that the safety problem is rising depending on the number of users. That's why people are concerned about mobile phone security issues. The Android is mostly used operating system in the mobile device.

2.2 Related Works

Firstly, authentication checks simply for the physical devices own security. Authentication is concerned when participants were asked a number of questions about their use of PIN-based authentication. While alternative methods of authentication are starting to appear, such as the Google Androids pattern or more recently through face recognition, at the moment of conducting this research, these methods still stay in the minority [14]. People also worry about data security. A suggested method [15] aimed at preventing untrusted parties from achieving information stored on the cloud side and proposing a strategy called the Proactive Dynamic Secure Data Scheme (P2DS). This system is intended in a dynamic operational context to safeguard delicate financial data. If we're talking about mobile phishing, that is a growing risk of mobile customers concentrating on money-related organizations, internet customers, and social networking. Despite the reality that this amount accounts for less than 1% of all phishing URLs collected, it emphasizes that mobile phases have turned out to be fresh focuses of phishing attacks customers could also be caricatured by normal phishing website pages when browsing their phones [16]. Our data must be protected from various types of malware attacks. The research [17] proposed an approach providing with two phases. In the first stage, conduct the static analysis to define

the possible critical route of attack based on the Android API and the current patterns of attack and conduct the dynamic analysis following the route to execute the program in a restricted and concentrated range, and detect the possibility of attack by checking the conformity of the detected route to the existing patterns of attack. In the second phase of dynamic analysis of runtime, dynamic inspection will report the sort of private information leakage situations, such as internet browser cookies, without accessing any true critical and protected mobile information sources. Another method is to enhance cyber-resilience by implementing the heuristic strategy that focuses on user conduct on mobile devices and this method solution allows to identify and generate warnings automatically when such systems are attacked by malware [18]. The 2-hybrid scheme can also be used to detect malware. In terms of time, resource consumption and efficiency, it is suggested to develop a balanced and efficient analysis for evaluation and detection. The concept 2-hybrid is used to define a strategy that integrates both analysis and detection of hybrid malware as well as hybrid implementation. The scheme is made up of a cloud service and a mobile device group. The mobile devices are continually running a local, effective, not particular algorithm for malware detection to detect recognized families of malicious conduct. Upon detection, an alarm will be raised on the device and sent to the cloud service to select a set of high-precision detection algorithms to be performed [19]. When we share our data from one device to another or one cloud to another cloud, we should also be conscious. For mobile phone storage, Public main cryptography is regarded as an efficient means of offering mobile communication with safety characteristics. To attain secure data encryption and information decryption in public key management, it is important to present a design of an analytical model based on Galois-Field Cryptography. A greater improvement in confidentiality, authentication, integrity, and non-repudiation in mobile interaction can be accomplished through the analytical model [20]. In the case of cloud information, the suggested new data communication security framework used the notion of the key generation and management public-key encryption system that enables information to be secured a lot. It followed some measures, such as providing key services for safe data sharing. Keys are produced in the database and stored. Using proxy servers, the cloud data service (CDS) encrypts the keys [21]. Another proposed scheme [22] that

utilizes the technique of secret sharing to keep outsourced information confidential. Here customer-aware partitioning strategy subdivides the shared domain so that customers can search within distributed shares effectively and it also protects untrusted information servers from inferring values from distributed shares in the initial attribute. Mobile network security is another significant word for mobile safety in which 5G network infrastructure uses autonomous radio access technologies to support more network interfaces [23]. In this case, SDMN integrates SDN and NFV, and works to improve network features, performance, flexibility and scalability, the study of SDMN and its associated safety issues is a significant element of the next-generation telecommunications networks [24].

Mobile anti-theft is the most important part of the security system for mobile phones. This security system is needed for both cases when the device is on and the device is off. For on state, Hayashi et al. [25] presented Context-Aware Scalable Authentication (CASA) that uses a Naive Bays classifier to determine how to expressly authenticate the user based on the mixture of various passive and active variables. In a probabilistic structure, the scheme utilizes the active authentication technique based on the location of a user. For off state, the suggested [26] mobile phone security system is a fundamental input/output scheme (BIOS). This security system for mobile phones enables to determine the mobile device position. This security system is based on the method of hardware application in which mobile is intended so that a mobile can be traced even if the battery and subscriber identity module (SIM) is plug-out. In short, the main problem of mobile device users is to protect unauthorized access, data security, malware detection, data sharing safety, and mobile anti-theft. The strategy suggested by this article allows users to deal with the safety problems of mobile devices that users still want.

2.3 Research Summary

Our research is about how to improve mobile phone security system. Our Mobile Authentication system works based on randomly password change. Mobile anti-theft works based on mobile ON state and OFF state. Mobile data share works based on encryption and decryption technology. Our proposed framework secured with mobile with

secured network and improved mobile Internet security. Our proposed framework is updated from existing framework.

2.4 Scope of the problem

There is lots of problem in the security of mobile device but we cannot make fully error free. Hope the proposed framework will improve the past mobile phone security problem from our point of view.

- In the general we use password to access the mobile device but it has lots of problem if anyone knows my password they can easily access our device. And this makes the security violation of authentication. The mobile device user always afraid of leakage of mobile information. So our propped framework create random password for user and we think this security of authentication features improve the violation of authentication and the user of mobile device remain doubt free.
- In our daily mobile security features if anyone access the mobile device they can easily access the Online and Offline storage. So we added fingerprint to access the Online and Offline storage and hope this features will improve the mobile data security.
- When we share any data we are facing so many problem at present. Sometimes we want to share data to our preferred peoples but in mistake we send to others. And that's why we thought how we improve the data share security. In our proposed framework when data is shared to others there will be generate a decryption key for receiver and the receiver cannot decrypt the receive data without decryption key.
- Nowadays mobile theft is increasing day by day. At present only mobile anti-theft works when device is ON state. But there is no system exist at present when the device is OFF state. So in our proposed system we talk how we track our mobile device when switch of the device or sim card is plug out. We think this mobile anti-theft technique increase the mobile security Both ON state and OFF state and reduce mobile theft in future.

2.5 Challenges

Developing the mobile phone security framework presents many difficulties

- We have to notice mobile real time during mobile authentication and password will be change randomly.
- We have to develop a middleware to protect mobile internet security so that virus and malware cannot attack the mobile device.
- When data is share to others user must have to share decryption key for receiver otherwise receiver don’t able to saw those things.
- Our anti-theft works ON state and OFF state both. For OFF state we need a hardware must be added to the mobile phone (Incorporate BIOS Cell to the hardware installed).
- The mobile with secured network is one of the most challenging issues for our proposed framework.

CHAPTER 3
RESEARCH METHODOLOGY

3.1 Introduction

Actually there are lots of security issues nowadays for mobile device. There are many researcher who tries their best to increase the mobile device security. Our work is about how we increase the mobile phone security with an easy way for user needs. We complete our work by maintain some procedure. First of all we think about how to increse the mobile phone security and we learn about the field of data science for mobile usage. Data science is using for mobile in our daily life whenever we usage the mobile. So we have to know very well about the mobile data science for improve the Security issues of mobile device. Then we have collects our secondary data from reliable website and different types of journal and conference paper. Then create a research gap whenever we study the secondary data and finding the research questions. After investigate the answer of the research questions we get a research finding as a proposed framework. We think the proposed framework will reduce the security concern of mobile device user. The framework has been partially implemented to validate this research and it is authentication part.

3.2 Research Procedure Flowchart

Figure 3.2 illustrates the research procedure of our entire work.

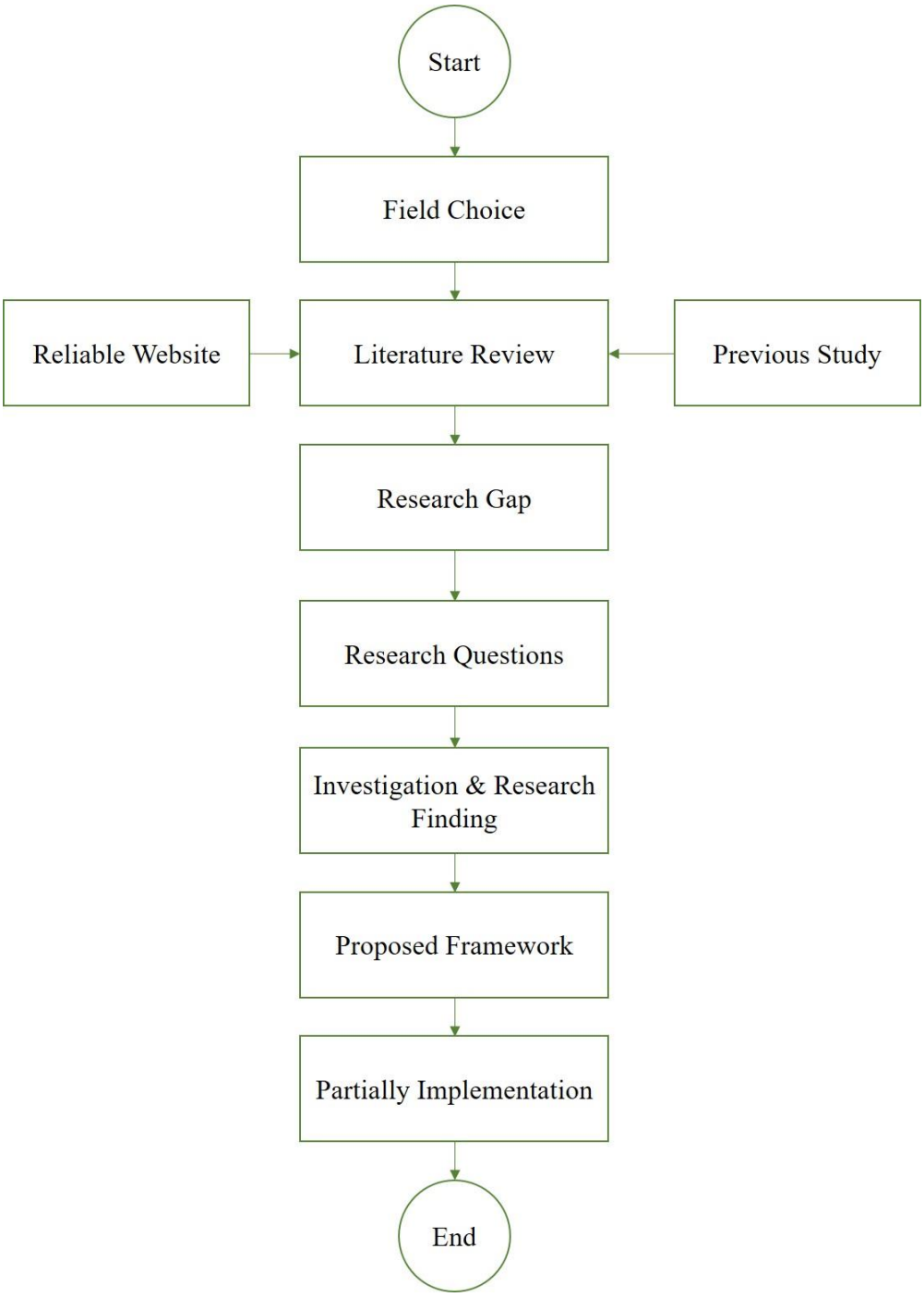


Figure 3.2: The Research Procedure

3.3 Research Subject and Instrumentation

3.3.1 Research Subject:

We are working about how to rise the security issues of mobile device. The mobile data science is one of the major field of Data science. Mobile safety is protecting smartphones, tablets and other mobile computing devices and linked networks from wireless computing-related hazards and security flaws. Also known as wireless security is mobile security. In the latest years, securing mobile devices has become progressively crucial as the number of phones in service and the uses to which they are placed has dramatically increased. Everything is use in the mobile device is data science. We store data in our mobile device when we use the mobile. So our data security purpose we have to deep knowledge about mobile data science and how to improve the security issues of mobile data science.

3.3.2 Research Instrumentation

As we are working how to improve the mobile device security first of all we have to know previous security framework and technologies for mobile device. Peoples always want best security but technology always create hampered user security concern. We investigate various types of features of mobile device security and those advantage and disadvantage from reliable website and different journal and conference papers. And then we evaluate those security framework and represent our proposed framework for mobile device security. Our proposed framework is able to secure authentication, mobile data, share data, mobile anti-theft (ON state and OFF state) and our proposed framework also able to secure mobile network also.

3.4 Data Collection Procedure

As it is a research on mobile device security purpose we have to need data. Data may be primary or secondary and our data is mainly secondary data. This research examines the impacts of how to improve the mobile device security for mobile device user. There are lots of organization who uses mobile devices for their organizations.

3.5 Proposed Framework

In our suggested scheme, our mobile device can be protected from unauthorized access, mobile anti-theft, virus attack security, sharing information, and providing Mobile with secured network. First of all, we need to give a password when our mobile device is locked to access the mobile. And the interesting thing is that with the assistance of using mobile real time, our suggested scheme will produce password randomly and includes 4-digit number password. Imagine the real time of the phone now is 11:12 pm, so we have to put the password according to the amount of the hour first and then the amount of the minutes to access the device. So, this time, the password for accessing the phone will be 1112. But now assume our real-time clock is 11:18 pm then we can't use the previous password to access our mobile phone at this moment. We have to insert 1118 as a password to access the phone.

If anyone comes to know how to access the phone (using the digits from 'hour: minute') as explained earlier, there is another choice for mobile device users to alter their password by setting preferred characters in such a way that the user will select 2 numbers (1number for hour and 1 number for minute) between 1 and 9 (1-9) which will be added with real-time mobile hours and minutes. Suppose, the actual portable time is 11:51 pm this time, and the user likes to add 5 with real-time mobile hour and 6 with real-time mobile minutes; so the required password for accessing the phone would be 1657. If someone enters the incorrect password for 5 times, the front mobile camera will turn on (but not be seen by others) and be capturing the user's picture and saving it to mobile storage as well as cloud storage. So, after adding these safety characteristics to our phone, we can quickly find out who is trying to access the phone and that's why unauthorized access will be so hard.

Obviously, after entering the valid password, only user can access the mobile device otherwise not. But when someone enters valid password and accesses the mobile device, and then intends to use information from mobile storage and cloud information, the user needs to apply fingerprint sensor to access. If fingerprint does not match for 5 times, the front mobile camera will be turned on but not seen by us, capturing the user's picture and

saving it to mobile storage and mobile cloud storage as before; however, it will be saving the captured file to another name folder. Thus, after adding these safety characteristics to our mobile storage information and mobile cloud information, no third party or unauthorized access is feasible at all.

The supported framework also includes mobile devices with secured network. Nobody can keep track of users' call, SMS, etc. The proposed framework also allows our mobile device to combat viruses and malware. There will be a middleware embedded between the mobile device and the access point for hybrid malware detection. Mobile internet access will be safe for us as the suggested framework will remove all viruses and malware or harmful things. As a result, it will be quite difficult to attack mobile devices using viruses and malware. The proposed framework, named Emerging Mobile Phone Security System (EMPSS), has been illustrated in Figure 3.5.

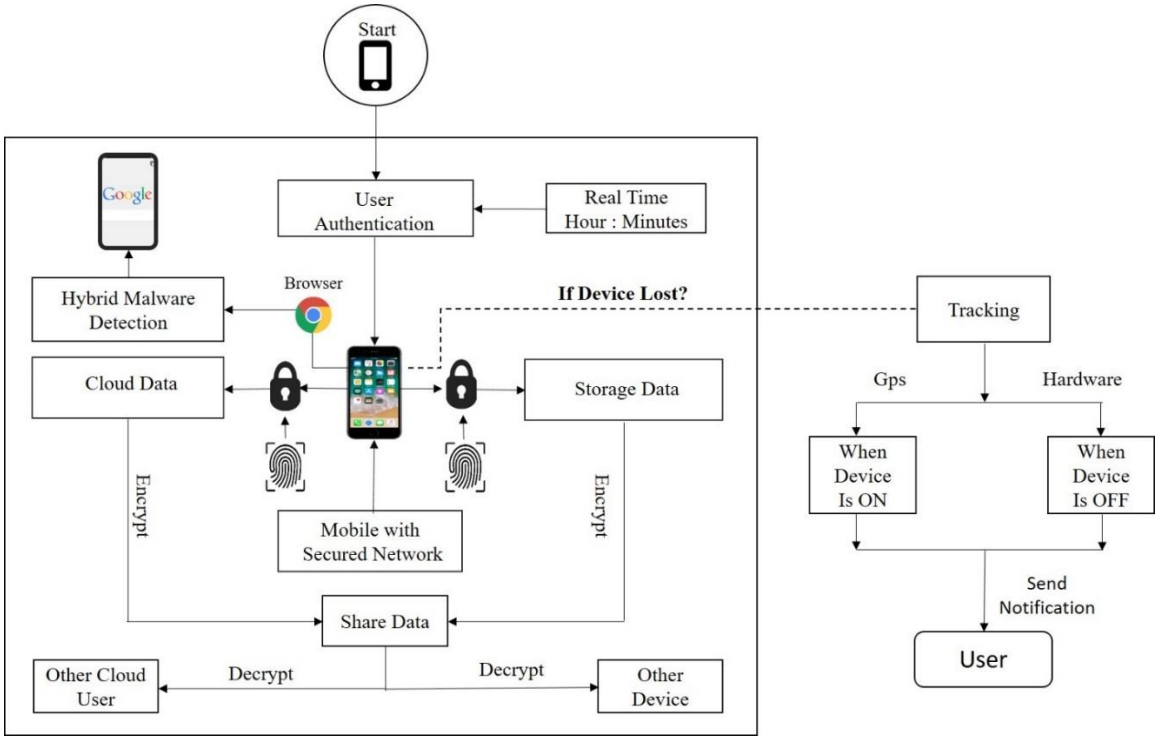


Figure 3.5: Proposed (EMPSS) Mobile Security Framework

In the suggested framework, there is a protection for sharing any information from one mobile device to another and from one mobile cloud user to another mobile cloud user. When we want to share any data, the sharing data will first be encrypted and a key to decrypt for the receiver will be generated. Now the receiver receives only that information, but cannot see those data until the decryption key has been placed by the receiver. Thus, it is impossible for third parties to obtain our information after adding this function, and this function most increases the safety of our sharing information.

The suggested framework also outlines how we are currently reducing portable anti-theft. While the device is on (after lost or stolen), it could discover the mobile device by monitoring with another phone using GPS which will send the notification to the user. But if the phone is off state (which implies that the battery and sim card are unplugged), the suggested framework can also monitor the mobile device. To do this, a hardware system must be added to the mobile phone, i.e. Incorporate BIOS Cell to the hardware needs to be installed. On the Mobile GPS, the hardware system will assist and maintain tracking whenever the battery is run out and sim card has been removed.

3.6 Implementation Requirements

To implement the proposed framework, we require both hardware and software tools.

Hardware requirement

To develop our proposed framework, we need the following hardware tools:

- Computer
- Smart Mobile device
- Camera & finger print support
- GPS sensor
- Need a hardware for offline tracking

Software requirement

To build our proposed System we need different types of software. Some of them are given below:

- Android Studio
- Java Language
- Java Development Kit
- Software development Kit
- Photoshop
- JavaMail API
- Shared Preference

CHAPTER 4
SYSTEM IMPLEMENTATION

4.1 Introduction

We have partially implanted the EMPSS framework for valid authentication. The apps name is EMPSS also given by us. We already told about our proposed framework and its all features before. It is quite difficult to implement full system so we work for the user authentication part. Our build application is able to protect unauthorized access with some emerging features and technologies.

4.2 Overview

We have built our authentication application using java language. To develop our application we uses Android Studio (version 3.4). For UI/UX design we uses XML. For mail service we using JavaMail API. We uses shared preference database to save the capture image into the device. Our system have four parts

1. Front End (UI).
2. Back End (Java Code).
3. Save Picture into device (Shared Preference).
4. Save picture into Mail (JavaMail API).

4.3 Front End

Front End use for user interaction. The good UI makes eager user to using the system. Our build application contains those parts given below:

- EMPSS security Service Switch.
- Select Number for Hour (default or 1-9).
- Select Number for Minute (default or 1-9).
- Image Mail Service Switch.
- Sender and Receiver Mail.
- And menu bar contains Setting, About us, F A Q, Privacy policy.

4.3.1 User Interface: User needs to follow System's Application procedure

To use application, some steps to complete the authentication process and once the user is authenticated by the application it allows to access the mobile device.

Step 1:

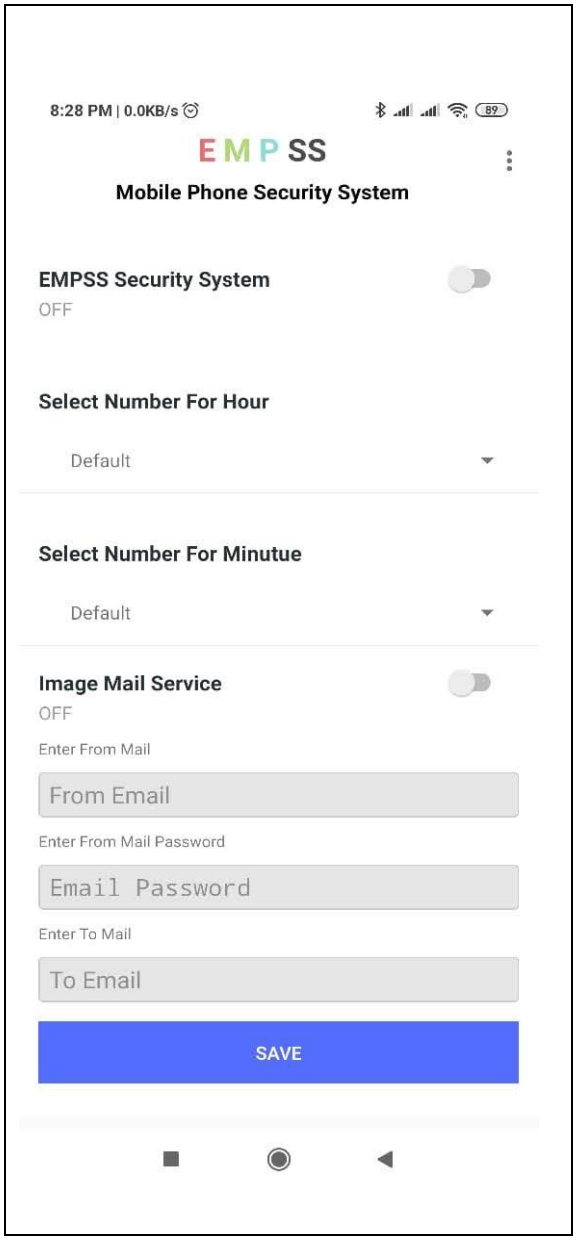


Figure 4.3.1(a): Home Interface

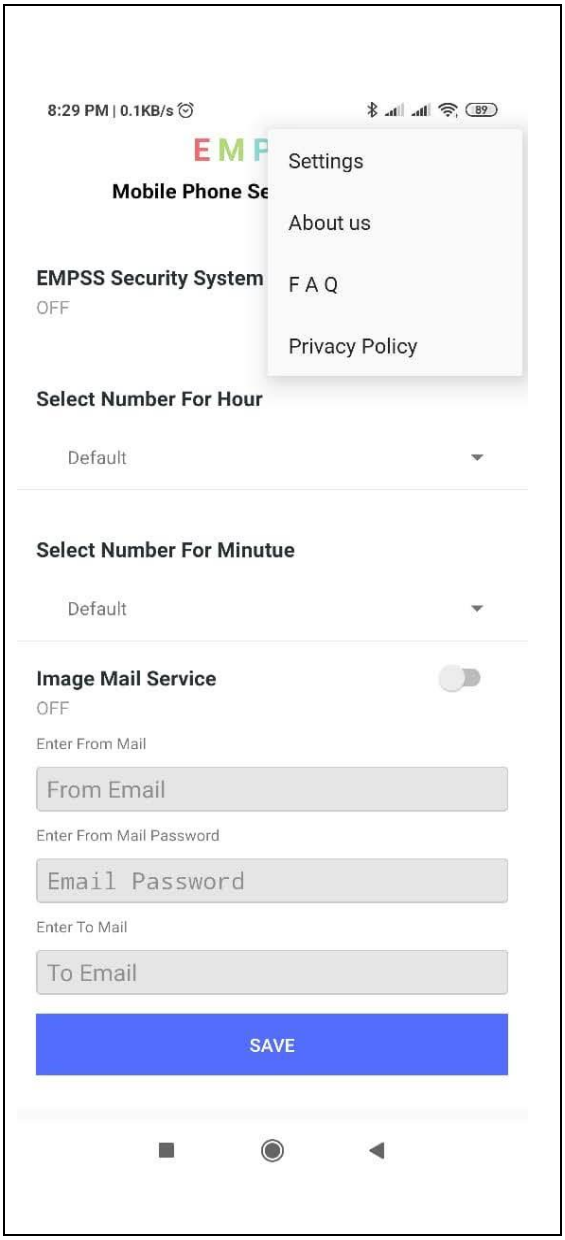


Figure 4.3.1(b): Home interface with menu list

While a user installs this application, the Home Interface will be appeared which is shown in Figure 4.3.1(a). If anyone wants to use this application, at first they have to select ON option to the EMPSS Security System otherwise the application will not enable the authentication security. However, when the user selects only ON option, the system (EMPSS) will only ensure the authentication part but not determine the unauthorized user as the option for "Image Mail Service" has not been selected yet. Note that the mobile 'Clock time' will be default pin for entry lock while the user selects ON option for the EMPSS Security System. Figure 4.3.1(b) also represents the user interface that focuses mainly on the menu list. There are four items on the menu list. These are 'Setting', 'About us', 'FAQ' and 'Policy Privacy'. 'Setting' explains the application setting features. 'About us' gives information about the application version and email for user suggestion. 'FAQ' contains some questions with their answers which is very useful for the user to use the application. 'Privacy policy' contains the security and privacy with policy.

Step 2:

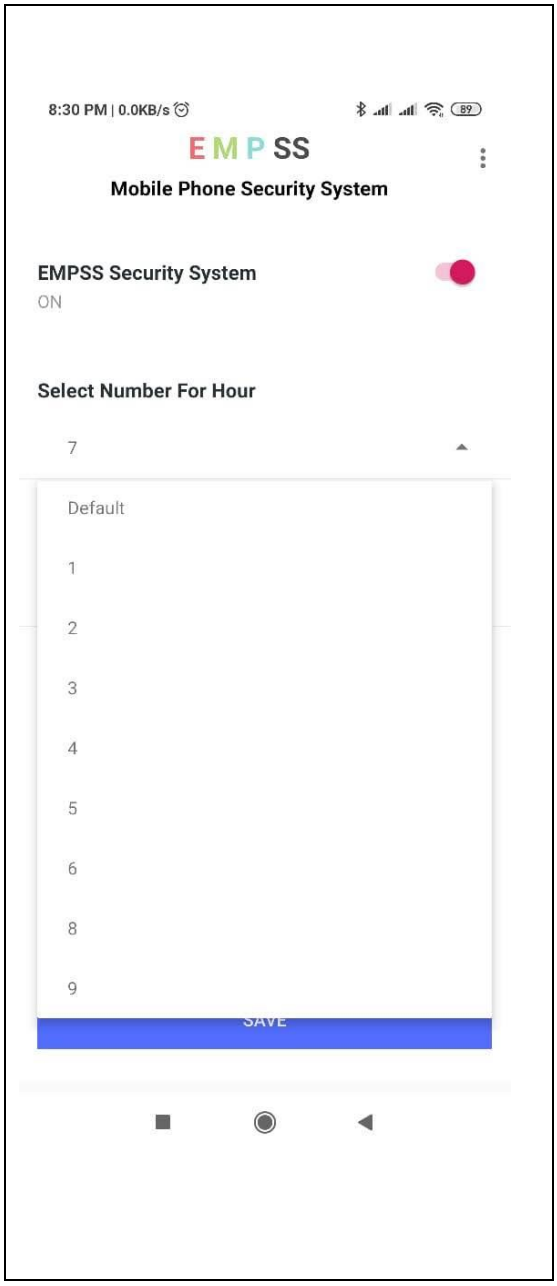


Figure 4.3.1(c): Home Interface with adding Number with hour and Minutes

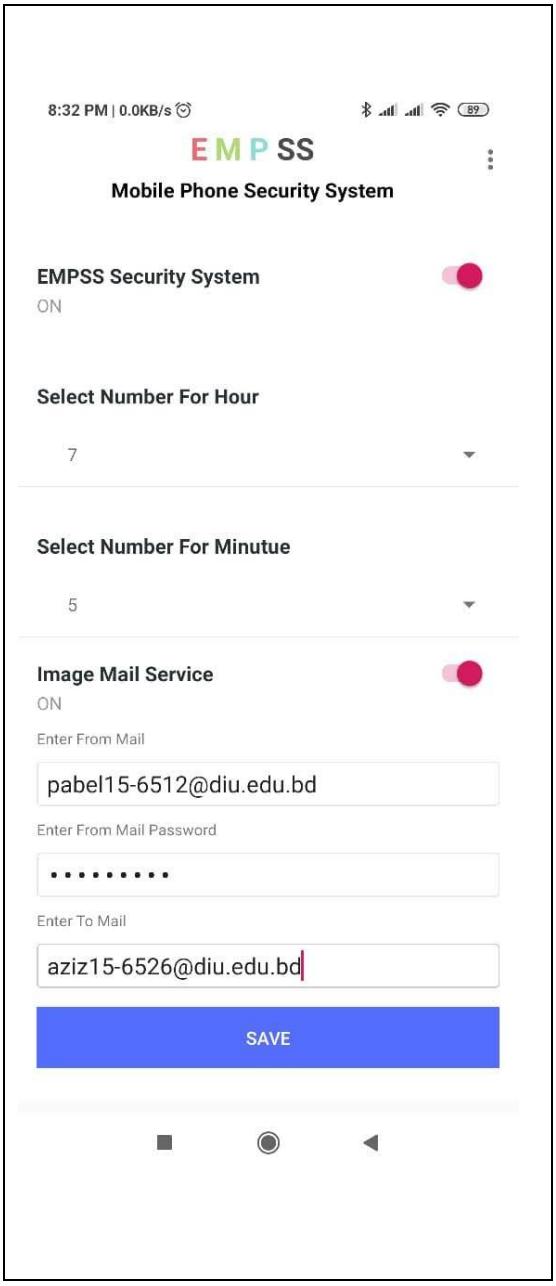


Figure 4.3.1(d): Home Interface with Image service

Figure 4.3.1(c) implies home Interface along with adding number with the hour and minute. By default, we can use phone lock pin as clock time in hour and minute. For more security, we can add value between 1 and 9 (1 to 9) with the real-time hour and minute. 'Image Mail'

service is shown in Figure 4.3.1(d). If the user enters the incorrect pin for 5 times, his/her image will be captured and forwarded to email. The captured image will also be stored in the mobile device.

Step 3:

Figure 4.3.1(e): Lock Screen view

Figure 4.3.1(f): Lock screen with suspending

The outlook of the locks screen is shown in Figure 4.3.1(e). After activating the EMPSS application, when the phone is locked, this screen will appear in the phone window. To access the phone, the user needs to enter real-time 4-digit (hour: min) as authentication pin.

Figure 4.3.1(f) represents the lock screen with suspending time. If someone places the incorrect password for 5 times he/she will be treated as an unauthorized user who will be suspended for 15 seconds and a photograph of that user would be captured. The taken picture will be saved into the device storage and it will also be sent to the email should the device is connected to the Internet.

Step 4:

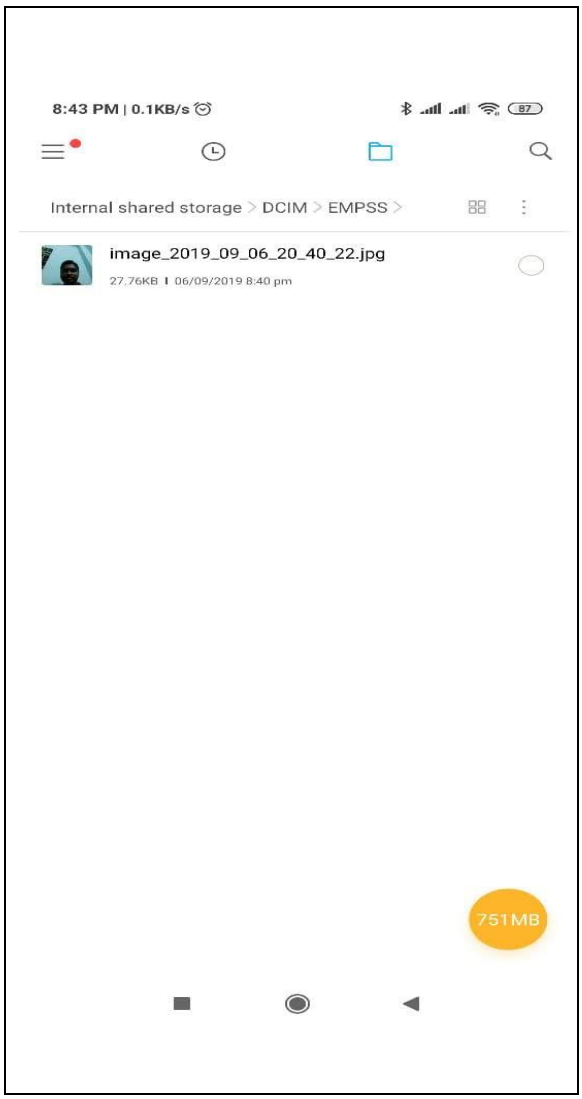


Figure 4.3.1(g): Picture directory in Mobile

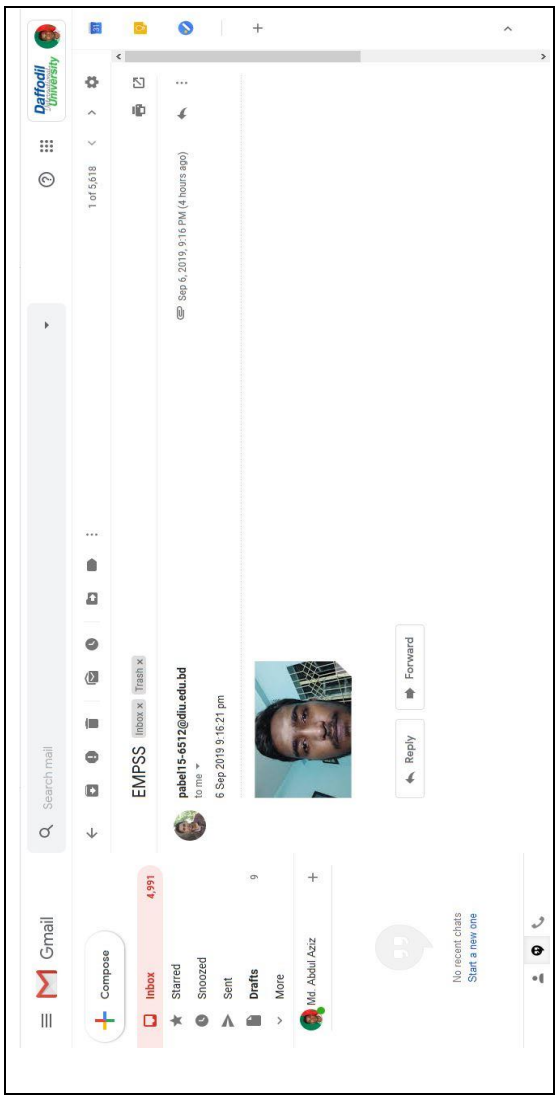


Figure 4.3.1(h): Picture stored in Mail

Figure 4.3.1(g) reflects a Mobile image directory. When someone puts the incorrect pin 5 times, it takes the unauthorized user's photos and then stored in mobile storage. Image in Mobile device will be saved on DCIM folder and when we open DCIM folder we get a folder named EMPSS. All pictures will be saved into this folder. Figure 4.3.1(h) demonstrates how EMPSS sends the unauthorized user's picture to the user email.

E. Step 5:

Figure 4.3.1(i): Forgot Password

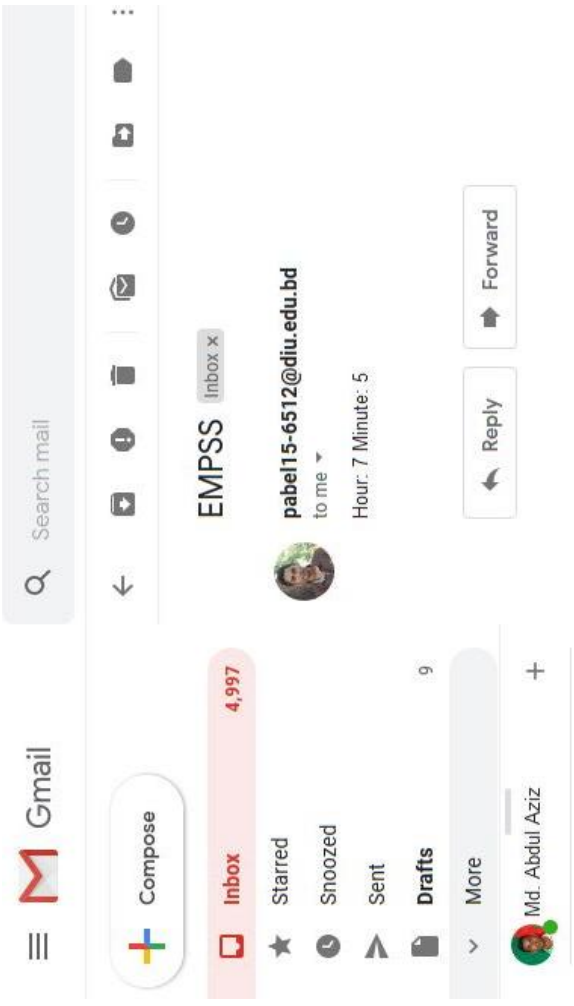


Figure 4.3.1(j): Password Recovery Mail

Figure 4.3.1(i) displays us ‘Forgot Password’ button to recover the password while the user forgot the password. To recover password, the user needs to press ‘Forgot Password’ button and then an email will be sent to the user mail that contains which numbers to be added hour and minute to access the phone. So, the valid user easily recovers the password but the unauthorized user cannot access using ‘Forgot Password’ button as the mail will always be sent to the valid user mail. Figure 4.3.1(j) displays how valid user receives mail to recover password. We believe this feature keeps the valid user more secure and reliable to use the application for authentication.

4.4 Back End

Here is the back End part of our system. For back End we are using Java language And XML for Design the UI of our application. We are using the java development kit and Software development kit. When the capture image is saved to the device storage we need to use shared preference. And if we want to send the capture pic to the email of the user the device should have to connect with the internet connection. When the device is connected to the internet the image will be sent to the user Gmail using JavaMail API.

4.5 Connection Process

Our EMPSS application is develop in using Android Studio IDE. Where using Java language in back end and for UI designing using XML. This application is providing user authentication. If user provide wrong password then it take image and send in Gmail if internet connection is available otherwise it store in mobile storage. For picture sending in Gmail we have used JavaMail API and for mobile storage we used Shared Preference.

4.6 Steps to Reproduce

The business process model exhibits the working principle of a system. The Figure 4.6 depicts the business process model and how we use the authentication application. The following figure reflects if anyone needs to access the device the user should have put a valid password. There is no option to access the device without putting the valid password. If someone puts wrong password five times the business process model shows how it takes

the unauthorized user's picture and saves it to not only in the device storage but also send to the user's Gmail if the device is connected to the Internet.

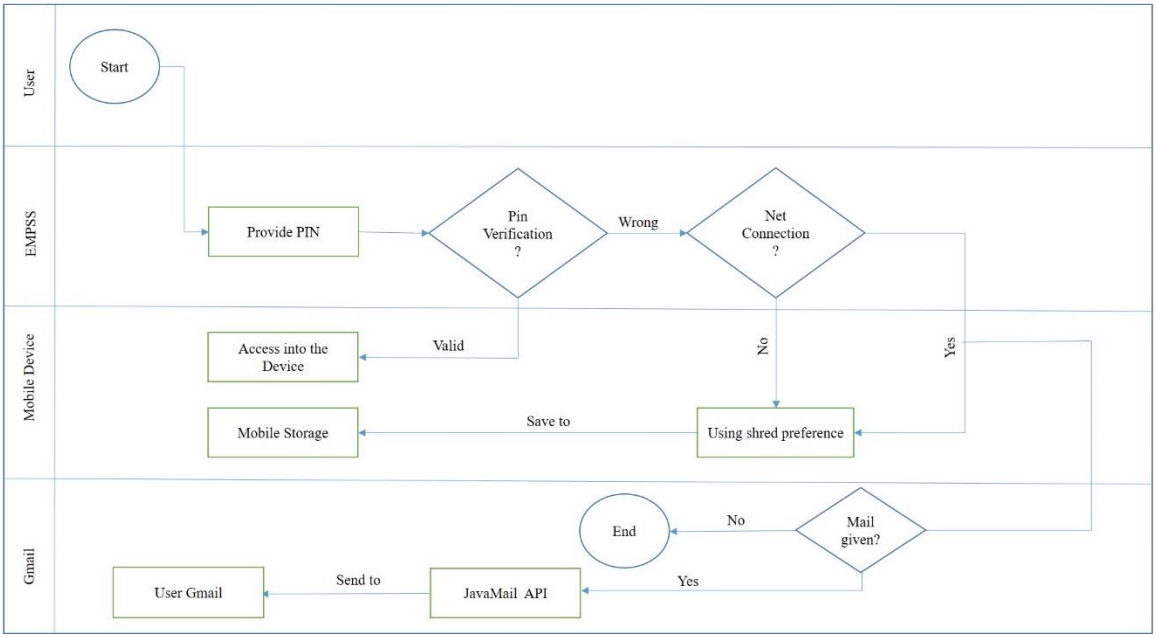


Figure 4.6: Business Process Model

CHAPTER 5
EXPERIMENTAL RESULTS AND DISCUSSION

5.1 Introduction

Our developed system have tasted in different types of Mobile device. When we tasted in various devices then maximum time it works perfectly. Sometimes its few feature may fault for some devices but it happened rare.

5.2 Experimental Results

The experiment result shows that how application are works on different mobile device.

Table 5.2: Test case for different types of mobile device.

Device Name	Installation	User authentication	Capture Image	Storage in Device	Send to user Gmail	Overall Preference
SAMSUNG	✓	✓	✓	✓	✓	Outstanding
HUAWEI	✓	✓	✓	✓	✓	Outstanding
NOKIA	✓	✓	✓	X	X	Satisfactory
XIAOMI	✓	✓	✓	✓	X	Good
WALTON	✓	✓	✓	X	✓	Good
SYMPHONY	✓	✓	✓	✓	✓	Excellent

5.3 Descriptive Analysis

5.3.1 Changing Generation of Mobile Technology

Martin Cooper, an engineer at Motorola in the 1970s working on a handheld device capable of two-way wireless communication, created the first-generation mobile phone. The first prototype was tested for use in a car in 1974, it was initially developed. This invention was

seen as a turning point in wireless communication that had resulted in many future developments in methods and standards. For a mobile device, there are mainly five generations of mobile technology, such as 1G through 5G (1G-5G). Table 5.3.1 shows various generations and characteristics of mobile technologies.

Table 5.3.1: Generation of Mobile Technology

Generation	Year	Speed	Accesses Technology	Primary Service	Key differentiator	Weakness	Switchig	Ref
1G	1970-1980	2Kbps	AMPS, FDMA	Voice Only	Mobility	Poor spectral efficiency, major security issue	Only Circuit	[27,28, 29,30]
2G	1990-2004	10Kbps -200Kbps	GSM, TDMA, CDMA, GPRS, EDGE etc.	Voice and Data (Both)	Secure, Mass adoption	Limited data rates, difficult to support demand for internet and email	Circuit, Packet	[27,28, 29,31]
3G	2004-2010	384Kbps - 200Mbps	CDMA 2000, UMTS, EDGE, EVDO etc.	Voice + Data + Video Calling	Better Internet experience	Real performanc e fail to match type, failure of WAP for internet access	Circuit, Packet	[27,28, 32,30]
4G	2010-Now	1Gbps	Wi-Max, Wi-Fi, LTE, SOFDMA	3G + Online Gaming + stream a TV show in HD	Faster Broadband Internet, Lower Latency, enable ubiquitous access to diverse multimedia streaming Service, crystal clear voice calls	Battery use is more, Required complicate d And expensive hardware	All Packet	[33,27, 23,28, 34]
5G	Soon (proba bly by 2020)	More than `1Gbps	BDMA, FBMC, UDCSNet , SoftNet, ANYaaS	4G + Ultra High Definiti on Video + VR Applicat ions	Better coverage and no dropped calls, much lower latency, Better performance	Costly because full infrastructu re should to be change	All Packet	[35,28, 36,23, 37,38, 39,27, 30]

5.3.1.1 First Generation

At first, something was never called as 1G. It was basically a network with only capabilities for voice calling and only got the name 1G. In 1G or First-generation wireless telecommunications technology, the network includes many cells, so that the same frequency can be reused many times, resulting in big spectrum utilization and thus enhancing system ability that could readily accommodate a big number of customers.

5.3.1.2 Second Generation

After 1G the next Generation of Mobile Technology is called 2G. It was praised for several reasons when 2G was brought to cellphones. Its digital signal used less energy than analog signals, so it lasted longer for portable batteries. In addition to MMS and picture messages, environmentally friendly 2G technology made it possible to introduce SMS. Digital encryption of 2G added information and voice calls privacy.

5.3.1.3 Third Generation

The next mobile technology is 3G. 3G technology enables customers to access the Internet while they're on the go. But the service differs because it uses a cellular-based technology. Users close to the tower have a better signal, so the further from the tower, the weaker the signal. But that's not so much an issue now because telecommunications businesses have set up telephone towers in different locations, even in the most remote regions, in the previous few years.

5.3.1.4 Fourth Generation

The term 4 G stands for ' fourth generation ' and relates to a mobile network technology that allows 4G-compatible devices to connect more quickly than ever before to the Internet.4G is a big step up of 3G and 10 times quicker than 3G. Starting in 2009, Sprint was the first carrier in the United States to offer 4G speeds. Now all carriers in most parts of the country offer 4G service, although some rural areas still have only slower 3G coverage.

5.3.1.5 Fifth Generation

The 5G mobile cellular communications system delivers a much greater efficiency level than past mobile communications systems generations. The new 5G technology is not only the next mobile communications version, evolving from 1G to 2G, 3G, 4G and now 5G. 5G was motivated by the need to provide omnipresent connectivity for apps as varied as automotive communications, haptic-style remote control feedback, vast video downloads, as well as very low data rate apps such as remote sensors and so-called IoT, the Internet of Things.

5.3.2: Anti-theft Mobile device safety technique

Anti-theft is used to safeguard mobile device's information against unlawful access and to identify the device when it is lost or robbed. Mobile phone is used in different industries in contemporary days. Many portable operating systems are protected by so many Anti-theft techniques. The Anti-theft techniques could be hardware or software based. The well-known company, such as Apple, Google, and Microsoft, uses Anti-theft security technique through the use of unique software ID, location tracking, sending messages, etc. for software-based Anti-theft technique during ON state. And the hardware-based Anti-theft security technique is using Incorporate BIOS Cell for hardware installation, so the security techniques work during OFF state. Table 5.3.2 describes different kinds of safety techniques for anti-theft mobile security.

Table 5.3.2: Various types of anti-theft mobile device safety technique

Technique	Type	Additional Factor	Determine	State	User	Ref
Apple's Security System (ASS)	Software	Apple ID with find my iPhone Application	Locate Position, Erase data, Display Message, Loud Ring	During Switch ON Device	Apple user	[40,41, 42]
Android Device Manager (ADM)	Software	Sign Google account and WIFI or Data is ON	Locate Position, Erase data, Display Message, Loud Ring	During Switch ON Device	Android user	[43,44, 45,46]
Anti-theft mobile phone security System	Hardware	Incorporate BIOS Cell to the installed in the hardware	Position of a Device	During switch off Device or Sim card plug out	Everyone	[26]
Tracking theft mobile application (TTM)	Software	Sign Google account and WIFI or Data is ON	Capture an Image, view text message, Detect Position,	During Switch ON Device	Android user	[47,48, 46]
Find my Phone (FMP)	Software	Microsoft account with Internet connection	Lock Device, Erase Data, Determine Location, Ring the phone	During Switch ON Device	Microsoft User	[26,49, 50]

5.3.3 Mobile data security techniques in different sectors

Data security is a collection of norms and techniques that safeguard information from destruction, alteration or disclosure intentionally or accidentally. The main purpose of data security is to safeguard the information collected, stored, created, received or transmitted by an organization. Infringements of data can lead to litigation instances and enormous penalties, not to mention harm to the reputation of an organization. Today, the significance of protecting information from threats to safety is more crucial than ever. Table 5.3.3 demonstrates mobile data security techniques along with characteristics used in various fields.

Table 5.3.3: Mobile data security techniques in different sectors

Technique	Type	Supporting factor	Field	User	Ref
P2DS	Dynamic	SDAA, CDAA, A-SAC, PDA	Financial Industry	Financial user	[15]
Naive Bayes	Dynamic	Permission gathering, Permission Analyzer, key logger detector	E-commerce	General user	[16]
Adapting the heuristic approach	Undefined	Sliding Window, Lemmatization, Feature Selection, Term Weighting, Incremental machine learning mechanisms, SVM, LR	General	End user	[18]
2-hybrid malware Detection	Static and Dynamic (Both)	Taintdroid, Andromaly, Crowdroid, Paranoid	Overall	Everyone	[19]
Context-Aware Authentication System	Undefined	Password, SecureID token, Location, Timezone, GPS, OS details	General, mostly (Financial transaction)	End User	[51]
Hybrid Data path Trace method	Static and Dynamic (Both)	Lexical Analysis, Safety rules analysis, Type inferring, Data Flow, Constraint Analysis	Overall	Only Android User	[17]
Behavioral Biometric Modalities	Undefined	Fingerprint, Iris, Keystroke Dynamics, Signature, Voice, Cell logs, Bluetooth Device, WIFI Networks, Location, Browser history	Universal	General person	[52]

We currently use our mobile phone in so many industries in order to store sensitive information. So, by using unauthorized access, the attacker attempts to use valuable and sensitive information or leak information. Mobile data security is nowadays the user's greatest problem. Techniques for mobile data security can be static or dynamic. These

techniques require some additional support factor to protect different user types such as the financial industry, e-commerce, and the general user.

5.3.4 Risk factor in mobile cloud

Mobile cloud storage is a type of cloud storage that uses speed and flexibility and growth instruments to store mobile device information in the cloud and provide the person with access to information from anywhere. One of the earliest phases of a malicious intruder's safety assaults, such as a hacker, cracker, or nefarious application, is a safety violation. Infringements of safety occur when infringement of security policy, processes and/or system. A safety violation can be anything from low danger to extremely critical, depending on the nature of the event [53,54,55,56].There are some Services Required by Mobile Client to use mobile cloud such as Sync, push, Offline App, Network, Database and some of the Services Required by Mobile Server such as Sync, push, Secure Socket-Based Data Services, Security [57]. Figure 5.3.4 illustrates various types of risk factors associated with mobile cloud.

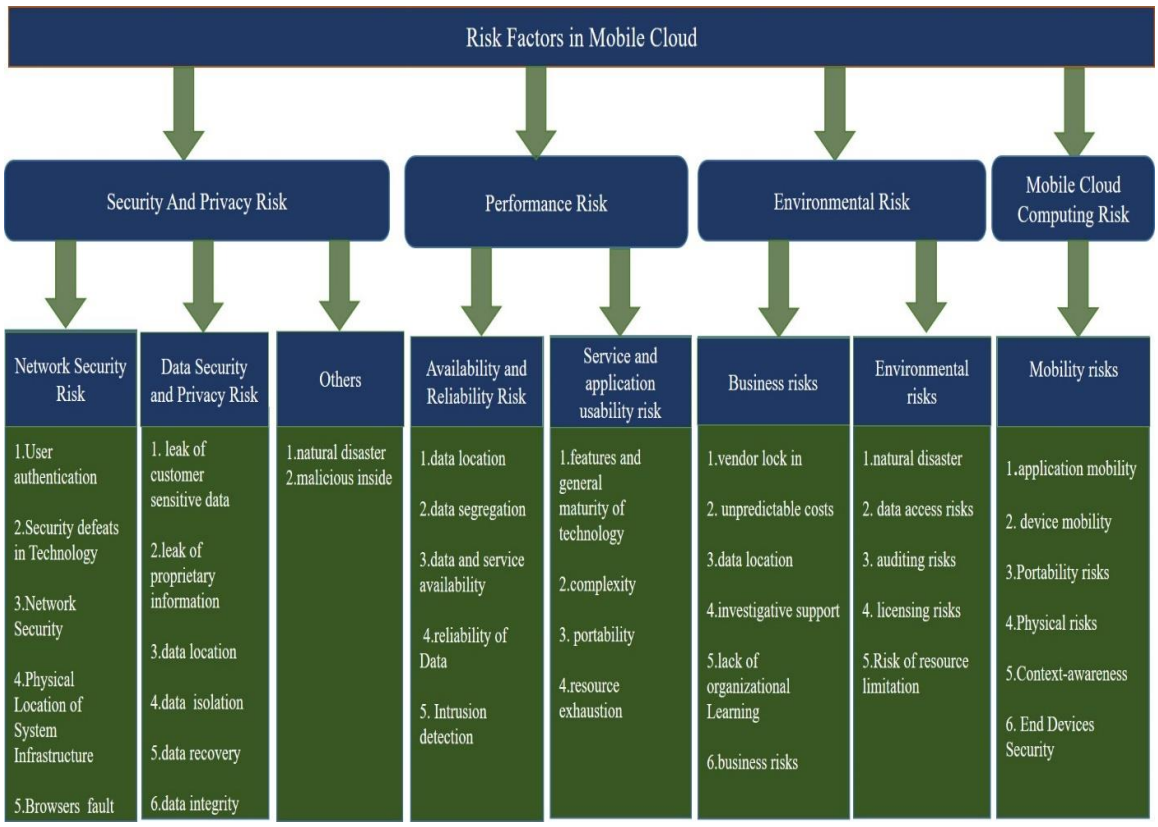


Figure 5.3.4: Various types of Risk factor in mobile cloud

In general, the mobile cloud computing risk means mobility risk [58, 59, 60, 61, 62]. Moreover, Security and Privacy Issues are the biggest concern; as we use it from anywhere so there are security and privacy risk, performance risk, environmental risk, and mobile cloud computing risk. Security and privacy Risk is a combination of network security risk, data security, and privacy risk, etc. And the performance risk is the summation of availability and reliability risk, Service and application usability risk. There is also an environmental risk for mobile cloud and the risk includes business risk and environmental risk.

5.3.5 Various Types of Mobile Application using in Various Sectors

5.3.5.1 Education

In contemporary times, learners tend more to use a mobile telephone for all purposes. Due to the use of mobile phones and the multiple application features, learners can learn different features and time to understand stuff in their own speed, as it is all just a click away. This is why the method of teaching has been changed to eLearning entirely. Otherwise, mobile apps are constantly updated as compared to textbooks. In the data provided by them, it can often be obsolete or restricted in the document prescribed by government or education boards. The Internet is available for mobile apps and the data is extensive, inclusive and up to date. There are different eLearn applications like Google Classroom, Kahoot, Remind, etc. we can learn and interact with each other free of charge. In the same context, learners, teachers, parents, Professors may take a questionnaire, task, participation, etc. and learners may take part, though they both have to sign up for it first. In addition, different app characteristics like interactive characteristics and concept-based games can facilitate understanding of a concept. Various types of Mobile apps are used in the education sector which is highlighted in Table 5.3.5.1.

Table 5.3.5.1: Mobile application using in Education sector

Ref	Apps Names	Description	Available	Sector
[63]	1. Kahoot	Kahoot is a learning platform for academic organizations that are based on games. It could make fun of a dull class.	Android, iOS	Education
[64]	2. Google Classroom	Google Classroom is free of charge for schools and includes G Suite for Education registration. With this Classroom, teachers and students can sign in for class assignments, course materials, and feedback from any computer or mobile device.		
[65]	3. NASA	NASA's app features an enormous collection of the recent NASA content including pictures, on-demand videos, mission data, news & feature stories, recent tweets and much more. NASA's app is accessible for free.		
[66]	4. Slack	Slack is a tool for communication and task management. It is designed specifically for job and cooperation. Functions such as video chatting and sharing the screen make it perfect for working together.		
[67]	5. Remind	Remind is a secure, classroom-friendly communication instrument to assist educators in sending emails to learners and parents. This app can be used for group chats, class announcements and private contact.		
[68]	6.Socrative Student	Socrative is an app for fun and efficient involvement in the classroom. Get immediate insight into teaching for students with easy-to-create quizzes, surveys, tickets for exit and more.		

5.3.5.2 Financial

In the multiple financial sectors, there are currently many mobile applications used as the transactions by mobile application is quicker. Some applications such as banking, shopping, retail and finance operate online and offline. A portable financial app gives users the option of checking their balance during travel times or in motion. Many economic operations can be undertaken with just a few clicks, including opening a fresh account, scheduling payments and payment transfers. The time needed to go to the bank is greatly

reduced. In order to use them, the customer does not need to pay any additional cash because downloads can be made free of charge. In addition, if they had to visit the business itself, clients also could save their cash. Financial institutions now offer safety codes and make secure transactions easier. Customers are notified about the transaction using the finance app by providing textual data. Customers are provided with information concerning multiple account operations, such as cash withdrawal and deposit via SMS messages. Clients can handle transactions as quickly as possible and save time. The financial transactions can be carried out at high velocity due to available mobile devices in all locations. Table 5.3.5.2 depicts the features of different mobile applications used in the financial sector.

Table 5.3.5.2: Mobile application using in financial sector

Ref	App Name	Description	Available	Sector
[69]	1. Concur	Concur is a software app and suite that helps companies automate their economic documentation to free up time and resources. Concur provides Concur Expense to handle spending for small and medium-sized businesses, Concur Invoice to automate payable accounts, and Concur Travel to book travel in accordance with business policies.	Android, iOS	Financial
[70]	2. Acorn	We will be able to connect all of our credit and debit cards to the application when using the Acorn application. The application will then automatically boost all of our expenditure to the next dollar and the balance will be put in an investment fund of our decision.		
[71]	3. Capital one mobile	It provides checking out the bank balance, reviewing payments by credit card, transferring cash, and being able to do just about anything with our bank accounts on the go.		
[72]	4. Wally	Wally is an application for personal finance. It enables us to compare our revenue with our expenditures, to know where our cash goes, to set objectives and to attain them.		
[73]	5.Moneystream	Moneystream is an application for funding that is the ideal instrument for traders. As its name suggests, Moneystream is designed to help customers streamline their company chances without constant interface confusion.		
[74]	6. Bank of America	Private Bank of America runs through Bank of America. It offers services of trust and fiduciary. It also offers products such as banking, credit card, car loans, mortgages, and home equity.		

5.3.5.3 Health

Mobile technology provides the ability to access anything anywhere at any moment to shape our future and our health objectives. Whether sleeping patterns or the diagnosis of any physical problems are being tested, health-based applications have now become standard for providing better care and healthcare at the end of the day. Mobile health was continually used as a way of improving self-management in patients with chronic diseases in behavioral studies. While the fields of medical care deal with both complicated and delicate information, the sector obviously learned to address these problems and to use mobile communication authority to make the strategy to healthcare to benefit physicians and patients more flexible and personalized. These kinds of mobile application provide quicker and easier communication and exchange of data between doctors and patients. A physician and a patient interact with one another via SMS, speech or video and the physician can view a patient's report on the platform. Health sector also uses various types of mobile apps as shown in Table 5.3.5.3.

Table 5.3.5.3: Mobile application using in Health sector

Ref	Apps Names	Description	Available	Sector
[75]	1. WebMD	The mobile application of WebMD offers easy-to-use management of health information. The app enables users to get the data they need rapidly and precisely, from symptom checking (complete with a "contact where it hurts" model) to drug side effects, to pill identification and essential first aid.	Android, iOS	Health
[76]	2. Medici	Medici is a simple mobile app that enables patients and doctors to communicate privately from our phone with each other via text, voice or video. This easy app enables patients to avoid waiting for easy healthcare requirements and other requirements.		
[77]	3. Digital Pharmacist	These apps operate to enable pharmacists to interact on distinct medicines readily with their clients. Digital Pharmacist makes it easy for pharmacists to interact with their clients while making it easy for everyone to complete the prescription process.		
[78]	4. iBlueButton	It stores critical health information in one location at all times for us and our loved ones. We gain private perspectives into our medicines and circumstances and review, investigate and label our documents with private annotations.		
[79]	5. EverlyWell	From there, customers follow the simple directions for completing that specific test and then mail it back to EverlyWell. Through a safe internet portal, the team will evaluate the test and deliver outcomes. These easy-to-read findings directly offer all they need to understand to the client, all without having to create a doctor journey.		
[80]	6.Fooducate	Fooducate is the best app for nutrition that teaches us to eat for health. Their philosophy is: eat better, lose weight, get healthy.		

5.3.5.4 Others

In the agricultural sector, we use a lot of mobile applications such as Spray Guide, AgMobile, Farmer's Partner, Crop Insurance, MachineryGuide, etc. And such applications help to boost productivity for our farmers. In social media and entertainment applications such as Facebook, Instagram, Twitter, WhatsApp, Netflix, Candy Crash Saga, Hotstar, etc. These types of Mobile applications are used because of fun and refreshment.

5.4 Summary

Our EMPSS application works perfectly in different types of devices. When tasted our app in various devices such as Samsung, Huawei, Xiaomi, Nokia, Walton, Symphony then it provide excellent result. Though it’s some of features fault in few devices but those are not for concern. It is our idea to protect the unauthorized access. There would be some chance of remaining bug in our application. To enhance the application outcome precision, runtime will require much more work to be accomplished.

CHAPTER 6
SUMMARY, CONCLUSION, RECOMMENDATION AND IMPLICATION FOR FUTURE RESEARCH

6.1 Summary of the Study

This research reflects the current limitation of mobile security system. We are uses various types of application to protect our mobile device such as antivirus, app locker, location finder, anti-theft tools etc. But there is no security system for mobile device which contains all of security features combine yet. So we think in our research if a system propose which is enable to give all types of security features combine in a one window then it will be great achievement for modern mobile phone security system . Our proposed system framework name is Emerging Mobile Phone Security System. It can protect unauthorized access with the help of randomly password change by using mobile clock time, it can not only protect storage data but also protect cloud data with the help of finger print locking system, it also ensure mobile with secured network, it also can detect virus or malware attacks by using 2-Hybrid Malware Detection middleware. Our proposed system also provide data share security for storage and cloud data with the help of encryption and decryption technique. In modern mobile anti-theft technology works when our device is switch on but when the device is switch off it is difficult to find the location of the device. So In our proposed framework we evaluate how mobile anti-theft will work both in ON state and OFF state of the mobile device. Hopefully after adding all types of security features of the mobile device in a one frame where not only remove the security challenges of mobile device but also provide the users security satisfactions.

6.2 Conclusion and Future Work

In this research, a resourceful and a constructive literature review on mobile phone security has been done based on concurrent literatures. We also propose an evolving framework (EMPSS) to improve the mobile phone security system. The framework is able to tackle all types of mobile security problems such as anti-theft, mobile data security, mobile network security, and Internet browsing security. Mobile data security also encompasses

both stages (offline and online). Mobile phone anti-theft technique is also effective while device is either on or off condition. We conducted comprehensive analyses of safety issues on mobile device and presented this methodology as a blueprint for the future execution. We developed an android application to give the authentication security for users according to our proposed EMPSS framework. Our implanted EMPSS Mobile Phone Security System application is able to not only secure unauthorized access but also helps user to find out the unauthorized user. It provides random password change according to the mobile real time. It also provides another feature to recover password for valid users when they forgot their password to access their mobile device without any difficulties. Our implemented application gives users best authentication security than the existing. If we develop our Proposed EMPSS framework fully then the mobile phone security will reach a top position and it fulfills all types of security which the consumers want at any cost at present. We believe that the research offers new researchers with a road map and sets some future instructions for security challenges of mobile devices.

6.3 Recommendations

Users must use a smartphone to use our suggested system framework. Without a smartphone, our system is totally impossible to use. Before users access the phone, they need to watch the mobile real-time. When someone places 5 times the incorrect password during authentication, it is impossible to take the image of the unauthorized user after pointing the finger at the front camera. During night when someone try to unauthorized access to the mobile device it is quite difficult to take picture of the untheorized user. The mobile device should have night vision front camera to capture image in night .When the device is not linked to the internet, capture picture that is stored only in the mobile storage but not in the cloud. To secure mobile storage information or cloud information, the device must be endorsed with fingerprints otherwise our suggested scheme is unable to secure mobile storage or cloud data. Mobile with secured network implementation is not completely described in our proposed structure. We need extra hardware to add during off-state with mobile devices for mobile anti-theft.

6.4 Implication for Further Study

This is the initial state of mobile phone security system, which provide all types of security features in one window. Nothing can be 100% perfect. So there have some limitation or difficulties to develop our proposed system framework fully. We will investigate those limitation and difficulties by further study. We are still working on our proposed framework for a better and more accurate system.

CONTRIBUTION FROM THIS R&D PROJECT

1. A framework named Emerging Mobile Phone Security System (EMPSS) has been proposed.

2. An App based on EMPSS has been developed.

3. International Publication-1: Scopus & DBLP indexed

Md. Abdul Aziz, Pabel Miah, Karim Mohammed Rezaul, " Enhancing Mobile Phone Security System by the EMPSS Framework ", Submitted to *Computer Law & Security Review: The International Journal of Technology Law and Practic*e , September 2019

4. International Publication-2: Scopus & DBLP indexed

Pabel Miah, Md. Abdul Aziz, Karim Mohammed Rezaul, "EMPSS: A Secure Mobile Authentication System", Submitted to *Journal of Information Security and Applications*, September 2019

References

[1] M. Foster, “History and Growth of Mobile Telephone Technology (Infographic),” *TCC Technology, Manage Technology Solutions*, 07-Apr-2015. [Online]. Available: http://www.tccohio.com/blog/telephone-technology. [Accessed: 15-Jul-2019].

[2] A. Mahfouz, T. M. Mahmoud, and A. S. Eldin, “A survey on behavioral biometric authentication on smartphones,” *Journal of Information Security and Applications*, vol. 37, pp. 28–37, Dec. 2017.

[3] J. Fierrez, A. Pozo, M. Martinez-Diaz, J. Galbally and A. Morales, "Benchmarking Touchscreen Biometrics for Mobile Authentication," in *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 11, pp. 2720-2733, Nov. 2018.
doi: 10.1109/TIFS.2018.2833042

[4] M. L. Ali, J. V. Monaco, C. C. Tappert, and M. Qiu, “Keystroke Biometric Systems for User Authentication,” *Journal of Signal Processing Systems*, vol. 86, no. 2-3, pp. 175–190, Mar. 2016.

[5] L. Sun, Y. Wang, B. Cao, P. S. Yu, W. Srisa-An, and A. D. Leow, “Sequential Keystroke Behavioral Biometrics for Mobile User Identification via Multi-view Deep Learning,” *Machine Learning and Knowledge Discovery in Databases Lecture Notes in Computer Science*, pp. 228–240, Dec. 2017.

[6] M. Muaaz and R. Mayrhofer, "Smartphone-Based Gait Recognition: From Authentication to Imitation," in *IEEE Transactions on Mobile Computing*, vol. 16, no. 11, pp. 3209-3221, 1 Nov. 2017. doi: 10.1109/TMC.2017.2686855

[7] N. Al-Naffakh, N. Clarke, F. Li and P. Haskell-Dowland, "Unobtrusive Gait Recognition Using Smartwatches," *2017 International Conference of the Biometrics Special Interest Group (BIOSIG)*, Darmstadt, 2017, pp. 1-5. doi: 10.23919/BIOSIG.2017.8053523

[8] A. F. Abate, M. Nappi and S. Ricciardi, "I-Am: Implicitly Authenticate Me—Person Authentication on Mobile Devices Through Ear Shape and Arm Gesture," in *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 49, no. 3, pp. 469-481, March 2019.doi: 10.1109/TSMC.2017.2698258

[9] A. Rattani, N. Reddy and R. Derakhshani, "Multi-biometric Convolutional Neural Networks for Mobile User Authentication," *2018 IEEE International Symposium on Technologies for Homeland Security (HST)*, Woburn, MA, 2018, pp. 1-6.
doi: 10.1109/THS.2018.8574173

[10] J. Zhang, X. Tan, X. Wang, A. Yan and Z. Qin, "T2FA: Transparent Two-Factor Authentication," in *IEEE Access*, vol. 6, pp. 32677-32686, 2018.
doi: 10.1109/ACCESS.2018.2844548

[11] P. Kumar, R. Saini, P. P. Roy, and D. P. Dogra, “A bio-signal based framework to secure mobile devices,” *Journal of Network and Computer Applications*, vol. 89, pp. 62–71, Jul. 2017.

[12] W.-H. Lee, X. Liu, Y. Shen, H. Jin, and R. B. Lee, “Secure Pick Up: Implicit Authentication When You Start Using the Smartphone,” *In Proceedings of SACMAT’17, Indianapolis, IN, USA*, pp. 67–78, Jun. 2017.

[13] “Top Countries/Markets by Smartphone Penetration & Users,” *Newzoo*. [Online]. Available: https://newzoo.com/insights/rankings/top-50-countries-by-smartphone-penetration-and-users/. [Accessed: 15-Jul-2019].

[14] N. Clarke, J. Symes, H. Saevanee, and S. Furnell, “Awareness of Mobile Device Security A Survey of User’s Attitudes,” *International Journal of Mobile Computing and Multimedia Communications*, vol. 7, no. 1, pp. 15–31, Jan. 2016.

[15] M. Qiu, K. Gai, B. Thuraisingham, L. Tao, and H. Zhao, “Proactive user-centric secure data scheme using attribute-based semantic access controls for mobile clouds in financial industry,” *Future Generation Computer Systems*, vol. 80, pp. 421–429, Mar. 2018.

[16] Narander Kumar and Priyanka Chaudhary, Mobile Phishing Detection using Naive Bayesian Algorithm, *International Journal of Computer Science and Network Security*, VOL. 17, pp. 142-147, July 2017.

[17] Y. Shi, W. You, K. Qian, P. Bhattacharya and Y. Qian, "A hybrid analysis for mobile security threat detection," *2016 IEEE 7th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON)*, New York, NY, 2016, pp. 1-7.

[18] G. Nguyen, B. M. Nguyen, D. Tran, and L. Hluchy, “A heuristics approach to mine behavioural data logs in mobile malware detection system,” *Data & Knowledge Engineering*, vol. 115, pp. 129–151, May 2018.

[19] A. Rodríguez-Mota, P. J. Escamilla-Ambrosio, S. Morales-Ortega, M. Salinas-Rosales and E. Aguirre-Anaya, "Towards a 2-hybrid Android malware detection test framework," 2016 International Conference on Electronics, Communications and Computers (CONIELECOMP), Cholula, 2016, pp. 54-61.

[20] Tejashwini N, D. R. Shashikumar and Satyanarayan Reddy K, "Mobile communication security using Galios Field in elliptic curve Cryptography," *2015 International Conference on Emerging Research in Electronics, Computer Science and Technology (ICERECT)*, Mandya, 2015, pp. 251-256.

[21] S. M. Daisy, R. S. Shaji and J. P. Jayan, "Asymetric key based data communication under mobile cloud system," *2015 Global Conference on Communication Technologies (GCCT)*, Thuckalay, 2015, pp. 559-564.

[22] M. A. Hadavi, R. Jalili, E. Damiani, and S. Cimato, “Security and searchability in secret sharing-based data outsourcing,” *International Journal of Information Security*, vol. 14, no. 6, pp. 513–529, Feb. 2015.

[23] Q. Han, S. Liang and H. Zhang, "Mobile cloud sensing, big data, and 5G networks make an intelligent and smart world," in *IEEE Network*, vol. 29, no. 2, pp. 40-45, March-April 2015.

[24] M. Chen, Y. Qian, S. Mao, W. Tang, and X. Yang, “Software-Defined Mobile Networks Security,” *Mobile Networks and Applications*, vol. 21, no. 5, pp. 729–743, Jan. 2016.

[25] E. Hayashi, S, Das, et al. Casa: context-aware scalable authentication, Proc. the Ninth Symposium on Usable Privacy and Security, ACM, July 2013.

[26] A. Waheed, M. Riaz and M. Y. Wani, "Anti-theft mobile phone security system with the help of BIOS," *2017 International Symposium on Wireless Systems and Networks (ISWSN)*, Lahore, 2017, pp. 1-6.

[27] Ms. Lopa J. Vora, “Advanced Wireless Networks: Vision And Future Of 5G Wireless Mobile Technology,” *International Journal of Recent Trends in Engineering and Research*, vol. 4, no. 3, pp. 141–149, 2018.

[28] A. Gupta and R. K. Jha, "A Survey of 5G Network: Architecture and Emerging Technologies," in *IEEE Access*, vol. 3, pp. 1206-1232, 2015. doi: 10.1109/ACCESS.2015.2461602

[29] A. Fendelman, “An Introduction to 1G, 2G, 3G, 4G & 5G Wireless,” *Lifewire*, 12-May-2019. [Online]. Available: https://www.lifewire.com/1g-vs-2g-vs-2-5g-vs-3g-vs-4g-578681. [Accessed: 15-Jul-2019].

[30] “1G Vs. 2G Vs. 3G Vs. 4G Vs. 5G,” *What are the differences between 1G, 2G, 3G, 4G and 5G?* [Online]. Available: http://net-informations.com/q/diff/generations.html. [Accessed: 15-Jul-2019].

[31] “Network coverage,” *Network coverage - 2G/3G/4G mobile networks*. [Online]. Available: https://www.gsmarena.com/network-bands.php3. [Accessed: 15-Jul-2019].

[32] EngineersGarage, “3G Technology,” *What is 3G Technology: 3G Technology Specifications*. [Online]. Available: https://www.engineersgarage.com/articles/what-is-3g-technology-specifications. [Accessed: 15-Jul-2019].

[33] C. Xu, S. Jia, L. Zhong and G. Muntean, "Socially aware mobile peer-to-peer communications for community multimedia streaming services," in *IEEE Communications Magazine*, vol. 53, no. 10, pp. 150-156, October 2015.

[34] “What is 4G?,” *4G*. [Online]. Available: https://www.4g.co.uk/what-is-4g/. [Accessed: 15-Jul-2019].

[35] H. Zhang, Y. Dong, J. Cheng, M. J. Hossain and V. C. M. Leung, "Fronthauling for 5G LTE-U Ultra Dense Cloud Small Cell Networks," in *IEEE Wireless Communications*, vol. 23, no. 6, pp. 48-53, December 2016.

[36] M. Aydemir and K. Cengiz, "Emerging infrastructure and technology challenges in 5G wireless networks," *2017 2nd International Multidisciplinary Conference on Computer and Energy Science (SpliTech)*, Split, 2017, pp. 1-5.

[37] R. Siddavaatam, I. Woungang, G. Carvalho and A. Anpalagan, "An efficient method for mobile big data transfer over HetNet in emerging 5G systems," *2016 IEEE 21st International Workshop on Computer Aided Modelling and Design of Communication Links and Networks (CAMAD)*, Toronto, ON, 2016, pp. 59-64.

[38] H. Wang, S. Chen, H. Xu, M. Ai and Y. Shi, "SoftNet: A software defined decentralized mobile network architecture toward 5G," in *IEEE Network*, vol. 29, no. 2, pp. 16-22, March-April 2015.

[39] T. Taleb, A. Ksentini and R. Jantti, ""Anything as a Service" for 5G Mobile Systems," in *IEEE Network*, vol. 30, no. 6, pp. 84-91, November-December 2016.

[40] S. Ganjoo, “Hackers are using iPhone prototypes for cracking open Apple's security system,” *India Today*, 09-Mar-2019. [Online]. Available: https://www.indiatoday.in/technology/news/story/hackers-are-using-iphone-prototypes-for-cracking-open-apple-s-security-system-1473159-2019-03-08. [Accessed: 15-Jul-2019].

[41] “If your iPhone, iPad, or iPod touch is lost or stolen,” *Apple Support*, 05-Dec-2018. [Online]. Available: https://support.apple.com/en-us/HT201472. [Accessed: 15-Jul-2019].

[42] J. Clover, “What to Do If Your iPhone is Lost or Stolen,” *Apple, Mac, iPhone, iPad News and Rumors*. [Online]. Available: https://www.macrumors.com/guide/what-to-do-if-your-iphone-is-lost-or-stolen/. [Accessed: 15-Jul-2019].

[43] H. Jonnalagadda, “The ultimate guide to finding your lost Android phone,” *Android Central*, 15-Jul-2018. [Online]. Available: https://www.androidcentral.com/find-my-device. [Accessed: 15-Jul-2019].

[44] “Find, lock, or erase a lost Android device,” *Google Account Help*. [Online]. Available: https://support.google.com/accounts/answer/6160491?hl=en. [Accessed: 15-Jul-2019].

[45] “How to track a lost Android phone with Android Device Manager,” *Android Tips and Hacks*, 10-Oct-2014. [Online]. Available: https://www.androidtipsandhacks.com/android/how-to-track-lost-android-phone-with-android-device-manager/. [Accessed: 15-Jul-2019].

[46] “7 Best Apps to Locate, Lock and Wipe your Lost Android Device,” *Mashtips*, 21-Mar-2018. [Online]. Available: https://mashtips.com/apps-to-track-lost-android/. [Accessed: 15-Jul-2019].

[47] R. Danu, “Tracking Theft Mobile Application,” *Indian Journal of Science and Technology*, vol. 9, no. 11, pp. 1–4, 2016.

[48] M. Knoll, “How to find a lost phone: Track and locate your Android device,” *trendblog.net*, 15-Aug-2018. [Online]. Available: https://trendblog.net/how-to-track-your-lost-android-phone-without-tracking-app/. [Accessed: 16-Jul-2019].

[49] “Find and lock a lost Windows device,” *support.microsoft.com*. [Online]. Available: https://support.microsoft.com/en-us/help/11579/microsoft-account-find-and-lock-lost-windows-device. [Accessed: 16-Jul-2019].

[50] “Find a lost phone,” *support.microsoft.com*. [Online]. Available: https://support.microsoft.com/en-us/help/17240/windows-10-mobile-find-phone. [Accessed: 16-Jul-2019].

[51] K. Benzekki, A. E. Fergougui, and A. E. Elalaoui, “A Context-Aware Authentication System for Mobile Cloud Computing,” *Procedia Computer Science*, vol. 127, pp. 379–387, 2018.

[52] T. J. Neal and D. L. Woodard, "Spoofing analysis of mobile device data as behavioral biometric modalities," *2017 IEEE International Joint Conference on Biometrics (IJCB)*, Denver, CO, 2017, pp. 62-70.

[53] D. Thilakanathan, S. Chen, S. Nepal, R. Calvo, and L. Alem, “A platform for secure monitoring and sharing of generic health data in the Cloud,” *Future Generation Computer Systems*, vol. 35, pp. 102–113, 2014.

[54] D. Ireland and DI Management Services Pty Limited, *RSA Algorithm*. [Online]. Available: https://www.di-mgt.com.au/rsa_alg.html. [Accessed: 16-Jul-2019].

[55] “Data breach,” *Wikipedia*, 14-Jul-2019. [Online]. Available: https://en.wikipedia.org/wiki/Data_breach. [Accessed: 16-Jul-2019].

[56] “Cloud computing security,” *Wikipedia*, 10-Jul-2019. [Online]. Available: https://en.wikipedia.org/wiki/Cloud_computing_security. [Accessed: 16-Jul-2019].

[57] P. Pranav and N. Rizvi, “Security in Mobile Cloud Computing: A Review,” *International Journal of Computer Science and Information Technologies*, vol. 7, no. 1, pp. 34–39, 2016.

[58] S. Yi, C. Li, and Q. Li, “ A Survey of Fog Computing: Concepts, Applications and Issues,” *Proceedings of the 2015 Workshop on Mobile Big Data - Mobidata 15*, pp. 37–42, Jun. 2015.

[59] T. A. Geumpana, F. Rabhi, J. Lewis, P. K. Ray and L. Zhu, "Mobile cloud computing for disaster emergency operation: A systematic review," *2015 IEEE International Symposium on Technology and Society (ISTAS)*, Dublin, 2015, pp. 1-8.

[60] N. Abbas, Y. Zhang, A. Taherkordi and T. Skeie, "Mobile Edge Computing: A Survey," in *IEEE Internet of Things Journal*, vol. 5, no. 1, pp. 450-465, Feb. 2018.

[61] H. Allam, N. Nassiri, A. Rajan and J. Ahmad, "A critical overview of latest challenges and solutions of Mobile Cloud Computing," *2017 Second International Conference on Fog and Mobile Edge Computing (FMEC)*, Valencia, 2017, pp. 225-229.

[62] S. Yi, Z. Qin, and Q. Li, "Security and Privacy Issues of Fog Computing: A Survey," *Wireless Algorithms, Systems, and Applications Lecture Notes in Computer Science*, pp. 685–695, 2015.

[63] "Kahoot! for schools: New solution for teachers and school admins," *Kahoot!* [Online]. Available: https://kahoot.com/schools/. [Accessed: 15-Jul-2019].

[64] "Classroom: manage teaching and learning | Google for Education," *Google*. [Online]. Available: https://edu.google.com/products/classroom/?modal_active=none. [Accessed: 15-Jul-2019].

[65] J. Colen, "NASA App for Smartphones, Tablets and Digital Media Players," *NASA*, 09-Mar-2015. [Online]. Available: https://www.nasa.gov/nasaapp. [Accessed: 15-Jul-2019].

[66] "Slack," *Online Tools for Teaching Learning*. [Online]. Available: https://blogs.umass.edu/onlinetools/community-centered-tools/slack/. [Accessed: 15-Jul-2019].

[67] EducationalAppStore, "Remind: Safe Classroom Communication Review," *Educational App Store*. [Online]. Available: https://www.educationalappstore.com/app/remind-safe-classroom-communication. [Accessed: 15-Jul-2019].

[68] "Plans," *Socrative*. [Online]. Available: https://socrative.com/plans/. [Accessed: 15-Jul-2019].

[69] "Business Travel & Expense Management," *Expense Management, Travel, Invoice Software, Travel Expense Reporting - SAP Concur*. [Online]. Available: https://www.concur.com/. [Accessed: 15-Jul-2019].

[70] "Invest, Earn, Grow, Spend, Later," *Acorns*. [Online]. Available: https://www.acorns.com/. [Accessed: 15-Jul-2019].

[71] "Save time, stayinformed - get theCapital One®Mobile app!," *Mobile Solutions | Capital One*. [Online]. Available: https://www.capitalone.com/applications/mobile/. [Accessed: 15-Jul-2019].

[72] "Personal Finance App," *Wally*. [Online]. Available: http://wally.me/. [Accessed: 15-Jul-2019].

[73] I. MoneyStream, “The future of personal finance,” *MoneyStream*. [Online]. Available: http://www.moneystream.com/. [Accessed: 15-Jul-2019].

[74] “Mobile and Online Banking Benefits & Features from Bank of America,” *Bank of America*. [Online]. Available: https://www.bankofamerica.com/online-banking/mobile-and-online-banking-features/overview/. [Accessed: 15-Jul-2019].

[75] “Better information. Better health.,” *WebMD*. [Online]. Available: https://www.webmd.com/default.htm. [Accessed: 15-Jul-2019].

[76] “The Mobile App The Connects Doctors & Patients Seamlessly,” *Medici*. [Online]. Available: https://medici.md/get-medici/. [Accessed: 15-Jul-2019].

[77] “Home,” *Digital Pharmacist*. [Online]. Available: https://www.digitalpharmacist.com/. [Accessed: 15-Jul-2019].

[78] “iBlueButton,” *iBlueButton*. [Online]. Available: http://www.ibluebutton.com/. [Accessed: 15-Jul-2019].

[79] “Innovative at-home Health Testing,” *EverlyWell*. [Online]. Available: https://www.everlywell.com/. [Accessed: 15-Jul-2019].

[80] “About Fooducate,” *the leader in nutrition grading*. [Online]. Available: http://www.fooducate.com/about. [Accessed: 15-Jul-2019].

APPENDIX

Appendix: A

EMPSS framework reflection

Appendix is an introduction which is used for system reflection. Our EMPSS framework helps to improve the mobile phone security system. Our proposed system is able to protect unauthorized access, data security, internet security, anti-theft, mobile network security and data share security. To develop our proposed system there is lots of requirement for each features so we develop the authentication security first. To develop the authentication security part we develop the EMPSS android application. In the test of our application we evaluate our EMPSS application give more security for authentication system with an emerging way than the others.

Appendix: B

Expensive System

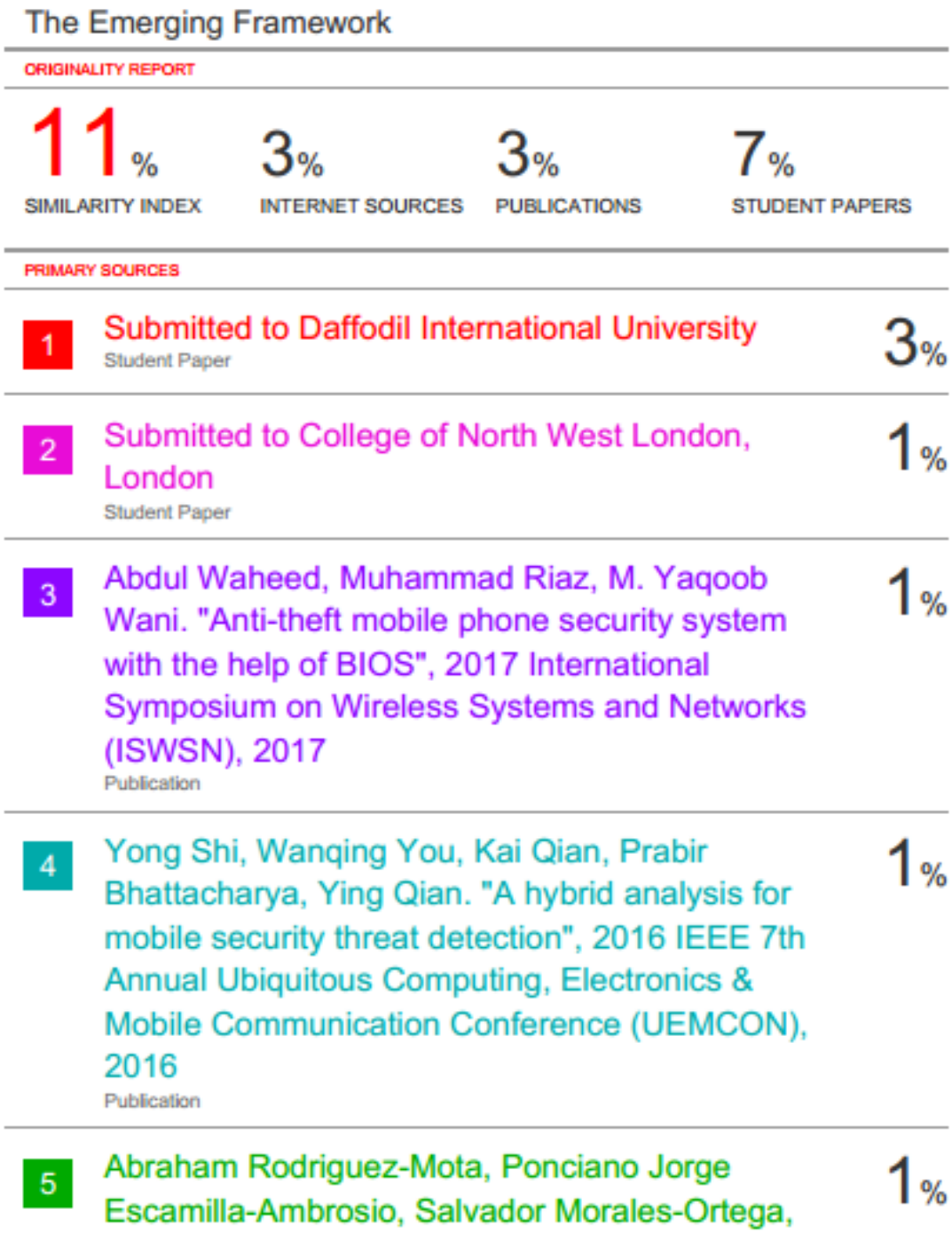
The proposed system is very difficult to use because its implementation cost is very expensive and time consuming. To develop the full framework we need the help of mobile phone operators, mobile phone Company, middleware system and the government help. So we have develop the authentication part of our proposed framework.

Appendix: C

Requirements to develop

To build our authentication part we use java language and develop the EMPSS application with the help of android studio. We also used shared preference for store the capture image into the mobile device. JavaMail API is used for send the capture image for user Gmail. Hope our application will helps user to find out unauthorized user.

Plagiarism report



The Emerging Framework

ORIGINALITY REPORT

11%	3%	3%	7%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Submitted to Daffodil International University Student Paper	3%
2	Submitted to College of North West London, London Student Paper	1%
3	Abdul Waheed, Muhammad Riaz, M. Yaqoob Wani. "Anti-theft mobile phone security system with the help of BIOS", 2017 International Symposium on Wireless Systems and Networks (ISWSN), 2017 Publication	1%
4	Yong Shi, Wanqing You, Kai Qian, Prabir Bhattacharya, Ying Qian. "A hybrid analysis for mobile security threat detection", 2016 IEEE 7th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON), 2016 Publication	1%
5	Abraham Rodriguez-Mota, Ponciano Jorge Escamilla-Ambrosio, Salvador Morales-Ortega,	1%

Figure 6.4: Plagiarism report