Computer & Robotics

A Comprehensive Model Driven 'Secure Mobile Application for KFU Email System' (SMAKE)

Ayat Bu-Suhail [a], Al-Jwharah Al-Hulaibi [a], Zainab Al-Khalaf [a], Noor A. Jebril [a], Qasem Abu Al-Haija [b,*]

[a] Computer Science Department, 2 Electrical Engineering Department, King Faisal University, Al-Hasa 31982, Saudi Arabia
[b] Tennessee State University, Computer and Information Systems Engineering Department, Nashville, TN, USA

Received 16 May 2019; Revised 17 July 2019; Accepted 25 August 2019; Available online 17 September 2019

Abstract

Nowadays, the development of innovative technology has emerged, particularly in mobile phones. People are often using smartphones daily in almost every aspect of their lives to use different applications and share various types of information quickly while moving anywhere. Mobile's email applications are classified as one of the important applications to communicate ubiquitously since the use of email is considered as the best formal way for communication inside any organization. Due to this importance of e-mail and the daily needs of using it especially for faculty members and students, we propose to develop a mobile application for KFU E-Mail system with secure data transmission. The proposed application has encryption and decryption features to ensure security. As a result, the students and faculty members can communicate via the email application in a safer and more comfortable way.

Keywords: *King Faisal University (KFU), Email System, Android, Data Security, Advanced Encryption Standard (AES).*

1. Introduction

Even though communication technology plays an essential part of every field especially in the workplace, however, the effective and secure communication processes are on-demand to meet several intended goals. Therefore, the communication process can be described to be either good or poor communication. Good communication is a primary element in the relationship between staff to increase the productivity and efficiency of the organization and attain the best outcomes. On the other hand, poor communication has catastrophic impacts on the quality of an organization. Moreover, there are various ways of communications between each other such as instant messages, emails, voice, and video calls. In King Faisal University (KFU), email messages take up a significant portion of all students and faculty members' workday as it is utilized the main formal way to interact. One important aspect of the recent email systems is the data security for communicated emails.

Recently, an enormous technological revolution in telecommunication and data sharing such has raised the demand for essential infrastructure to develop secure communication over insecure channels for different applications. Many solutions have been proposed and investigated to construct algorithms of secret data sharing/storing by employing different mathematical

* Corresponding author. Email: qabualha@my.tnstate.edu

schemes along with computer engineering techniques. The art of providing such solutions is called cryptography.

Using the email in the KFU website, any kind of information like text and any attached files can be transferred easily. However, accessing the email through mobile devices provides easier and faster. Indeed, accessing the application through mobile devices like smartphones and tablets is faster than using computers. Thus, the KFU email application will be a better choice to enable KFU members to navigate their emails continuously and be more aware of the coming emails. Finally, the developed application will be connected with the KFU database server of mail users before the final deployment for KFU users. In addition, due to the sensitivity of some of the transferred data like transferring exams between professors, the techniques for data protection are needed to provide such secure communication. For instance, cryptographic algorithms are highly efficient and popular techniques that can be employed to secure confidential against different cyber-attacks. However, wide-range of crypto-algorithms are used for data encryption/decryption [1] such as DES (Data Encryption Standard), Blowfish, and AES (Advanced Encryption Standard). In this proposed mobile email application, we employ AES Cryptographic algorithm to perform security actions (encrypt/decrypt) of messages due to its proved high security levels in many applications such as banking and military [2].

AES [originally known as Rijndeal] is a very common symmetric key scheme that was published by National Institute of Standards and Technology (NIST) in 2001 [3]. It can be efficiently implemented in both hardware and software. AES algorithm can encrypt/decrypt blocks dealing with different secret key sizes such as 128, 192, or 256 bits depending on the number of rounds that are applied to the data. For example, it uses 10 rounds for 128-bit keys, 12 rounds for 192-bit keys and 14 rounds for 256-bit key [4]. The typical AES security system consists of four different transformation stages: Byte substitution using a substitution table (Sub Bytes, shifting rows of the State array by different offsets (Shift Rows), Mixing the data within each column of the State array (Mix Columns), and Adding a Round Key to the State (Add Round Key). The complete steps of AES algorithm for encryption and decryption processes can be retrieved from [2].

In this work, we proposed Secure Mobile Application for KFU Email (SMAKE) system utilizing both the new developed mobile programming languages and operating systems along with an efficient cryptographic algorithm which is Advanced Encryption Standard (AES) to help users (faculty, students, and staff) to respond to their emails in more secure and easier way.

In KFU, two types of email domain system as the major official communication method used by faculty members (xxx@kfu.edu.sa) and students (xxx@student.kfu.edu.sa). Thus, KFU offers a web-based link to access the institute email system via login by username and password located on the KFU website. This method takes a relatively long time as the user needs to access the KFU website first and then you go through many webpages to access the email. Therefore, the main problem is there is no strong secure way to ensure the security of messages. Thus, we suggest accessing the emails by using a new secure mobile-based application that we are willing to design throughout this project. We can illustrate the problem statement for the proposed work as depicted in Fig. 1. The encrypt and decrypt processes will be offered as buttons in the mail composition area with secret keys generated randomly using the pre-established key distribution center (KDC) as a third party of the communication process. This KDC is already developed by information technology division at KFU to auto-randomly generate secret keys for every email communication process/session.

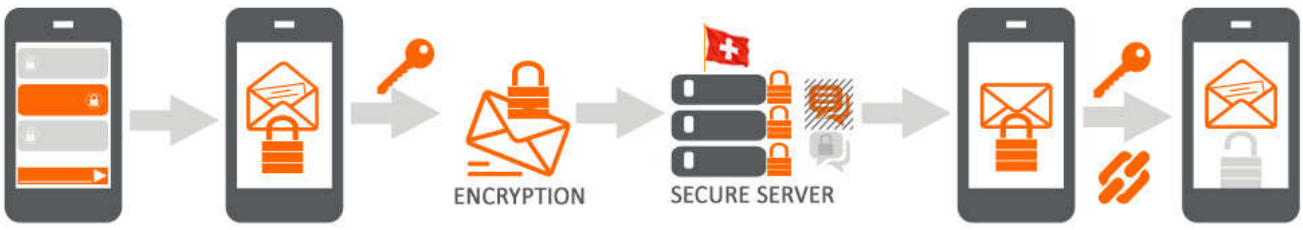

Fig. 1. Scheme of Secure Communications: the proposed solution [5].

Eventually, the idea of our tool is to use AES cryptosystem on both sides (sender/receiver) to encrypt and decrypt any outgoing or incoming email before publishing the email on the communication channel (which is assumed to be insecure channel by nature). The proposed application can be easily installed across a range of platforms that use Android systems. However, no one can use it except the KFU faculty members and their students because it is developed especially for them. Also, they can access by using the academic user id and password that are same as their banner accounts.

2. Comprehensive Analysis of Related Work

In recent years, advanced synthesis and design have been achieved in the development of new telecommunication and data sharing technologies such as mobile-based applications, cloud computing, and Internet of things (IoT) [6]. This, in turn, has raised the demand to develop secure communication over insecure channels for different applications. Many types of research have been conducted to ensure data security for many shapes of shared data. For example, the software-based Rivest–Shamir–Adleman (RSA) cryptosystem which is used to encrypt and decrypt text messages prior communicating them by sender and receiver [6]. On the other hand, there is a need for portable email version along with the one offered by KFU official website which enables the user to access the KFU email by the web-based links. These two reasons form the main motivation for us to utilize MAP (Mobile application programming) techniques to develop a new secure tool to access KFU's Email system. Besides these, there are many other reasons that have also contributed to this motivation such as the time spent on mobile phones is quite large which enable us to check our emails continuously, the preference of using application instead of browsing website as it saves time and effort. This section is organized in subsections. Each of subsections discusses some related works to this project from two perspectives: mobile-based email applications and secure cryptographic algorithms related to AES algorithm.

2.1. Overview of Mobile Platforms

Mobile applications are mainly differed depending on the kind of mobile phone (hardware) and the operating system (software). The mobile operating system is the software platform that each mobile phone supported to provide its functions like keyboards, wireless security, messaging and many others [7]. There are many types of mobile operating systems, but the most known ones are the Android system developed by Google and IOS system which developed by Apple. We planned to develop the application using Android system. So here, you will find a description of the android system architecture. The Android system consists of three basic layers as shown in (Fig. 2).

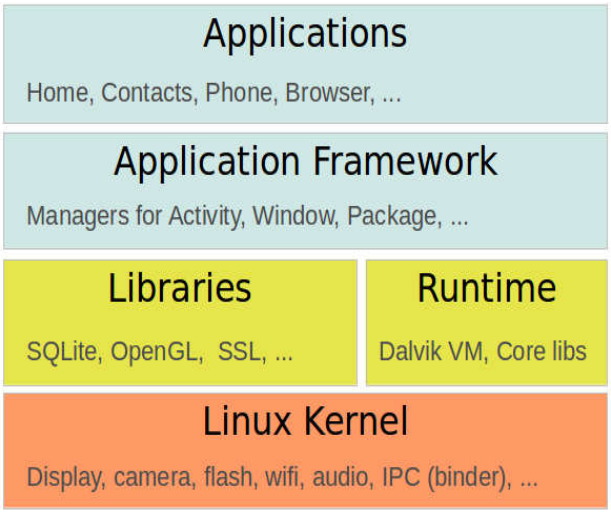

Fig. 2. Android architecture.

The first layer from the bottom is the Linux kernel. It is created using C programming language and it is responsible for providing system services like security, memory management, process management and so on. In addition, this layer works as the abstraction layer between the Android devices and other software layers. Second, the middle layer is the runtime and libraries. This layer is responsible for running Android applications using different core libraries of Java programing language and Dalvik virtual machine which executes files in (.dex) extension. Finally, the third layer in the up-level is applications. It allows the developers to build up various Android applications which are usually created by using java programing language [8].

2.2. Related Email Application for Mobile

Since email is an important technique in the social communication side, the number of email applications is getting increased. The email application is mainly used for sending and receiving messages using a specific email address. Now we will clearly identify two of the most common email applications that are highly-used these days to provide daily email activates. These are namely: Microsoft Outlook and Gmail applications.

Microsoft Outlook is one of the most important free emails that is highly used in Android and IOS system. It is published by Microsoft Company which sets that more than 400 million users have been communicated socially using outlook in 2016. [9] Frist, Outlook can be connected with other email providers to open the emails of other sources like Gmail, Yahoo, Hotmail, and Exchange. The storage capacity of outlook is 5 GB. [10] Consequently, there are many great advanced features and tools that make outlook a special application. Outlook can keep the inbox under control. For example, it has a smart feature called (Clutter) where it can separate the less important emails from the inbox. It does that by figuring out the emails that the user always responds to. By this way, the user can concentrate only on the most important emails and find them in a fast way [11]. Also, it provides two kinds of sorting and arranging messages which are automatic sort or sorting by creating subfolders. Moreover, outlook offers searching facility for emails. The user has many elements for searching like all folders in inbox or draft, from, to, contact list and date options. Furthermore, if the user deletes any email accidentally, the outlook is capable undo the deleting process. Also, there is a fundamental feature which is the calendar that helps the user to manage time. Spam checker is supported in outlook to ensure security. When there is a possibility of any spam email, it will alert the user by a red bar that appears in the top of an email [10].

On the other hand, Gmail is developed by Google Company. It is a free email application and as outlook, Gmail can be downloaded in Android and IOS mobile devices. Statistics written by TechCrunch shows that over a million users have their own Gmail accounts in 2016 [8]. In fact, Gmail supports only Gmail accounts and cannot open any other accounts. Furthermore, its storage capacity is around 15 GB divided between Google Drive, Google Photos, and Gmail [9]. Also, Gmail has many helpful features like managing calendar, forwarding messages, searching, organizing inbox, deleting emails and so on. As an outlook, the Spam filter is done to ensure security while transforming personal or work-related messages, but it is very limited compared to outlook [10]. Table 1 shows a comparison that depends on some criteria between the Gmail, Outlook, KFU website, and our proposed application.

Table 1. Comparison between Outlook, Gmail, KFU website, KFU Mobile Application

Evolution Criteria	**Security**	**Speed to access**	**Encrypt/Decrypt buttons**	**Ability to open another account fort different server provider**	**Ability to display emails while offline**
Outlook Mobile Application	High	High	No	Yes	Yes
Gmail Mobile Application	Less than outlook	High	No	No	Yes
KFU Web-based Application	High	Less than KFU Mobile APP	No	No	No
KFU Mobile Application	High	High	Yes	No	Yes

2.3. Related AES Algorithms

File Encryption, Decryption Using AES Algorithm in Android Phone paper (2015) shows that a successful implementation of file and image encryption as well as decryption [12]. They used AES algorithm to protect information in data storage while transmitting the data. This algorithm has been selected as the best algorithm among others different algorithms to overcome the several problems that are in other algorithms like Data Encryption Standard (DES), Triple Data Encryption Standard (3DES), Riveset Ciphers2 (RC2), etc.

The system is performing the encryption and decryption process of original files. The original file is passed through the AES encryption algorithm which encrypts the file by using a secret key. In decryption, the encrypted file is considered as input and then, it passed through the AES decryption algorithm which uses the same key for encryption to decrypt and get the original file. This application has been running on Android platform to encrypt the file before it transmits over the network. It was used for all types of files such as text, Docx, PDF, and image.

In a Review on Data Encryption Techniques Used for Social Media on Internet (2016), the authors displayed the techniques that used in inception in social media and phones [3]. Also, the purpose to encrypt the electronic data is shown in this paper. In social media, communication between two parties allows the people to transfer and share the information which may contain sensitive data across the globe. In order to protect the sensitive data, the AES algorithm is highly recommended. It is considered a very safe technique for both concepts' cryptography and steganography [13]. Also, in Amazon web services, users can encode and transfer the data to Amazon S3 and encrypt them using 256-bit AES encryption.

Evaluating the Performance of Symmetric Encryption Algorithms paper provides the evaluation of six of the most common encryption algorithms namely: AES (Rijndael), Data Encryption Standard (DES), Triple Data Encryption Standard (3DES), RC2 or Alternative Ron's Code (ARC2), RC6 and Blowfish [14]. A comparison has been developed for those types of encryption algorithms at different ranges such as different sizes of data blocks, different data types, battery power consumption, different key sizes and finally encryption/decryption speeds.

As a result, they found that DES has high performance compared to a 3DES algorithm. However, RC2 was the worst in performance overall algorithms where AES was the better in the performance than three common algorithms RC2, DES, and 3DES.

3. Functional/Non-Functional Requirement

The work requirements are often used as a guideline to give us information about how the application should work. Collecting the functional and non-functional requirements is an important step to measure qualification of the application. In order to accomplish the proposed application, the application aims to facilitate the following non-functional requirement:

1) Availability: The application will be available (responding on time) at any time, and even if there is no internet connection; the application can view the emails that already existed in the mailbox.

2) Usability: The application must be easy to download and use. It needs to have a clear interface.

3) Security: Security requirement in the application refers to make unauthorized user or intruder unable to read the email that is transferred between sender and receiver.

4) Reliability: The application should be reliable and perform the email services as requested.

5) Integrity: The application should be able to maintain the content of an email and ensure that its contents are not changed.

6) Performance: The performance is evaluated according to the output or behaviors of the application, the amount of time it takes to provide the services and the size of the application.

On the other hand, the functional requirements are needed to satisfy the required functionality. The use case diagrams for the required functionally are illustrated in Fig. 3. The description of each part of this figure is as follows:

a) Log in: If the user wants to login into the email for the first time, the user must activate his/her accounts because the university is already providing an account for each student and staff. After that, the user can log into the application using the KFU academic user id and the password must be the same as the password in the banner system.

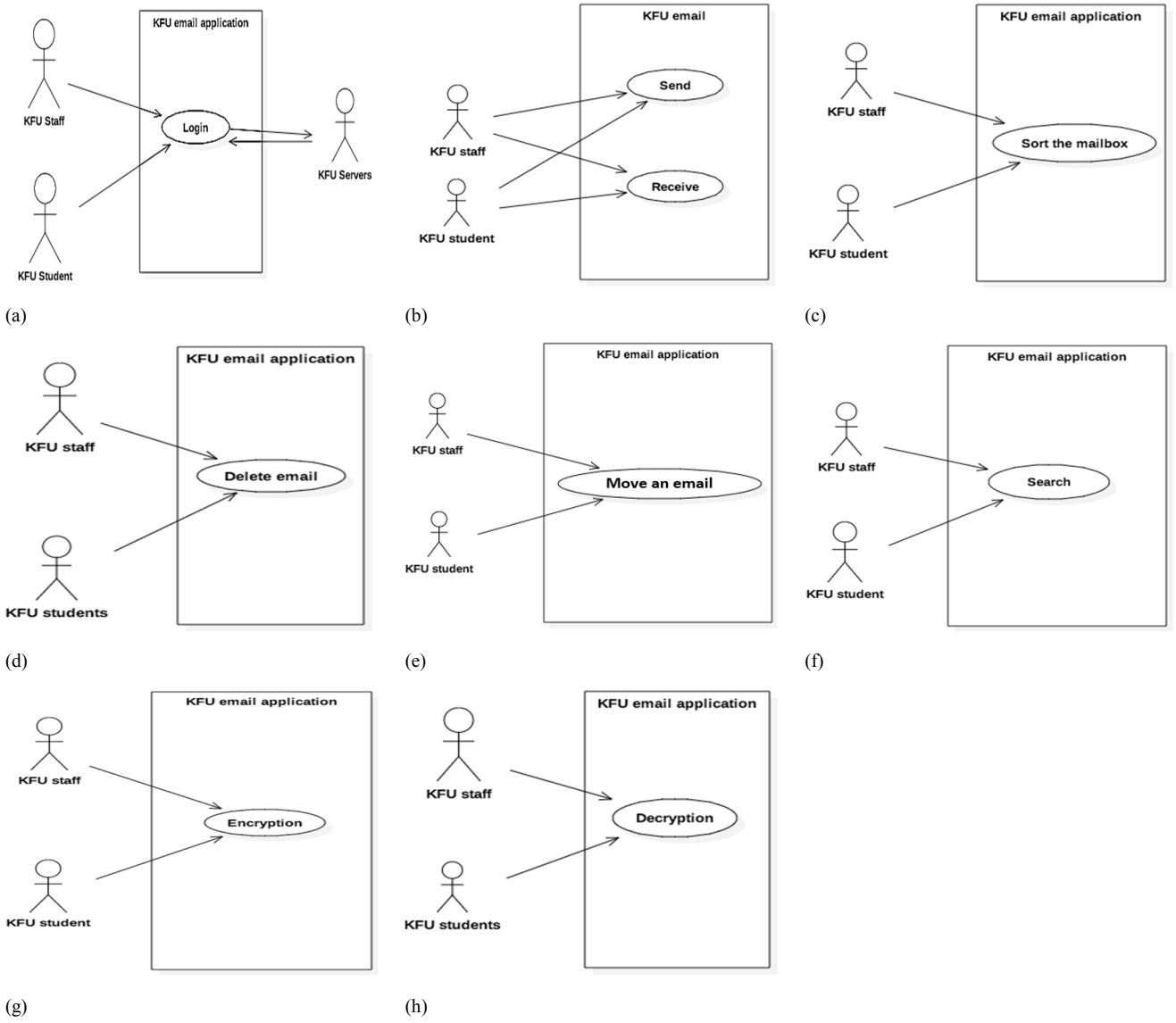

Fig. 3. The Use Case Diagrams of the functional requirements.

b) Send and receive emails: The user can send and receive an email within a local database.

c) Sorting emails in a folder: The application is giving a great feature which is that it can sort the emails automatically by showing the last received emails firstly. So, it can manage the emails and arrange them.

d) Delete an email: The user can delete unwanted email to keep only the important emails.

e) Move an email: The user will be able to arrange the emails and move them to any email box.

f) Search: If the user wants to find a specific email, he/she can apply searching by Title.

g) Encryption of the email: In the KFU email application; there will be a button that is specialized for performing encryption using Advanced Encryption Standard (AES) along with a secret key.

h) Decryption of the email: If the receiver knows the key that the sender used in encryption, he/she can decrypt the email and the plaintext will be shown.

4. Alternative Problem Solving Methods

Since emails take a significant portion of each faculty members and student's day, it is extremely important to find ways that could help us to be in constant touch with our emails. In fact, there are many ways of accessing KFU emails. One of them is accessing the emails through a website. This way is considered as the primary way. Unfortunately, this way has many drawbacks. The main problem is that the website has a higher possibility to be hacked than the applications. Recently, there are some statistics that show that around 30000 websites infected with some type of malware every single day, and there are around 70 million people who their information has been hacked because of less security [15]. In addition, accessing website takes a long time because we must open several pages until we reach the mailbox. The other way is accessing the KFU email through mobile applications like Outlook and Mailbox where you can open all your email accounts in one place. Opening all your accounts in one application could be annoying especially in sending process because you may pick the wrong email account for the wrong organization. Moreover, the mailbox at the mobile may stop because of the huge amount of emails that have been received from the email accounts. On the other hand, KFU faculty members are only dealing with the official email account and ignore all other personal accounts to avoid malware and spam emails. So, if I send an email to the university through my personal email account, the message will be ignored or considered as unimportant email.

Also, the discussion will mainly focus on some alternative symmetric keys algorithms that are selected by National Security Agency (NSA) to identify clearly why we chose the AES as the best one. These algorithms are Data Encryption Standard (DES), Triple Data Encryption Standard (3DES) and Rivest Ciphers 2 (RC2) [16]. However, Advanced Encryption Standard (AES) is considered as the best algorithm in many aspects as seen clearly in the comparison between the discussed algorithm and AES in table 2.

Table. 2. Comparison of encryption & decryption algorithms by NSA.

Factors	AES	3DES	DES	RC2
Key Length	128, 192 and 256 bits.	(K1, K2, K3) 168 bits, (K1 & K2 is same) 112 bits.	56 bits.	8-128 bits, in steps of 8 bits; default 64 bits.
Block Size	128, 192 and 256 bits.	64 bits.	64 bits.	64 bits.
Cryptanalysis Resistance	Strong against differential, truncated differential, linear interpolation and square attacks.	Vulnerable to differential brute force attacker could be analyzing plain text using 7differential cryptanalysis.	Vulnerable to differential and linear cryptanalysis; weak substitution tables.	Vulnerable to differential brute force attacker.
Factors	AES	3DES	DES	RC2
Security	Considered as secure.	One weak is exit in DES.	Proven inadequate.	Vulnerable
Rounds	10(128 bits), 12(192 bits), 14(156 bits).	48	16	16 of type maxing, 2 of type mashing.
Key(s)	Single.	Single (divided to 3 parts)	Single.	Public.

5. Tools and Techniques

SMAKE can provide secure email services for faculty, staff and students by including encryption and decryption methods using RIJNDEAL AES-128 CIPHER cryptosystem. In this section, we review the set of tools used during the work in project proposal phase and implementation phase (Hardware and software tools).

- Microsoft SQL Server Management Studio: Is an integrated environment for managing SQL based infrastructure. We have used it to create an initial database for our project proposal.
- Star UML: Is an open-source software modeling tool that supports UML. We have used it to draw use case diagrams for our project proposal.
- CACOO: Is a diagramming web-based application for making different design diagrams such as flowcharts, UML (Unified Modeling Language), ER (Entity-Relationship) Model, activity diagram, and others. We have used it in creating ER and activity diagrams for our project proposal.
- In Vision: A powerful design prototyping tool, we have used it to design a prototype for our SMAKE Application.

• Google Scholar: An online academic web search engine that provides full text or metadata of scholarly literature across an array of publishing formats and disciplines. We have used it to browse and download the research papers and reports needed to accomplish our project's work.

• Microsoft Word: Is a documentation word processor developed by Microsoft as a part of Microsoft Office suite to prepare different kinds of writing items such as technical reports, mails merging, research papers, and many others. We have used it to document the proposed system in all phases of millstones using the KFU template.

• PowerPoint: is powerful presentation software developed by Microsoft as a part of Microsoft office suite. It uses slides to convey rich information in multimedia. We have used it to prepare the presentations for each milestone using the KFU template.

• Personnel Computers (PCs): to install the required software to implement the proposed application.

• Android device / Emulator: to run and verify the developed codes of our application in Android Studio. Android Studio is an integrated development environment (IDE) to build and validate the proposed Android Secure mobile application for KFU email.

• Php My Admin: A free and open-source code written in PHP used to handle the administration of MySQL over the internet and the database associated with our proposed application. We have changed the database that we created in Microsoft SQL Server Management Studio because we discovered that our database must be online as we are using email situation.

• Brackets: A modern text editor used to write and test PHP code in the browser and then bind it with Android Studio.

• Xampp Server: A standard for Cross-platform (x), Apache (A), MariaDB (M), PHP (P) and Pert (P). It is a simple lightweight Apache distribution used to create a local web server for testing the database in Php My Admin.

6. Appropriate Analysis

The project can be analyzed in terms of different design components such as database diagram, Entity Relationship Diagram (ERD), Activity Diagram, and Use Case diagram. In terms of database diagram, in PHP My admin, we have created our database that contains three tables, which are Users, Emails, and folder.

Fig. 4 shows the relationship between user entities and email entity which classified as one-to-many relationship where each user has many email messages. In addition, the email entity has may-to-many relationships with folder entity, which represents that many emails can be placed in many folders. Moreover, the activity diagram is a UML diagram that represents the workflow of actions and activities that may occur in the secure mobile application for KFU email.

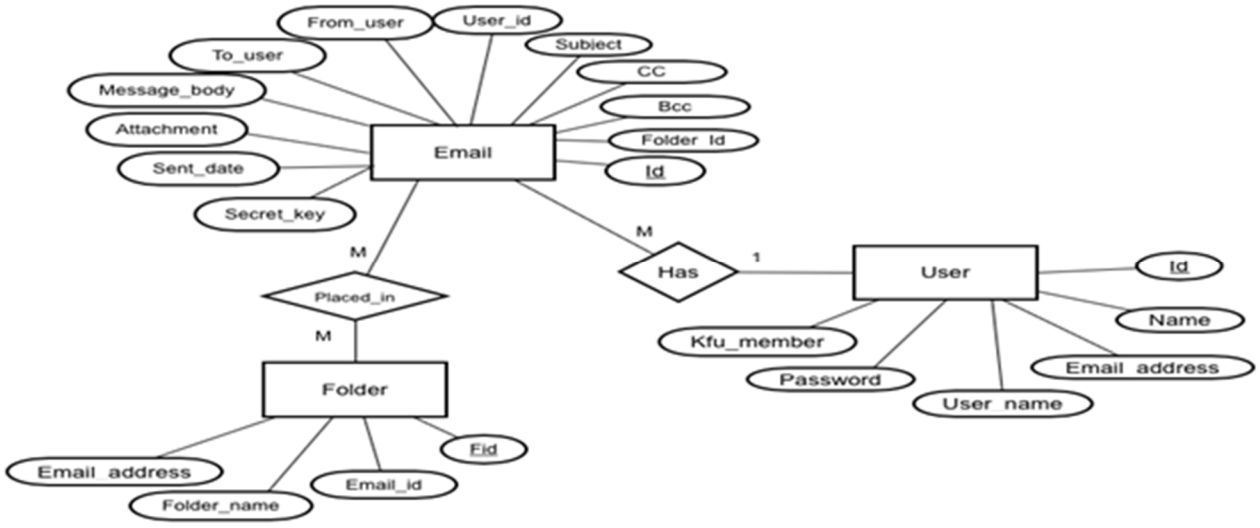

Fig. 4. Entity Relationship Diagram

The user table is holding user information which is mainly used for the authentication process. Email table contains the primary data that is necessary for any email message such as subjects, contents, date and many others. In addition, email table has a secret key column which holds the secret key if the message has been encrypted. Folder table is holding the folders names which represent different locations of email.

Also, it has a relationship with the email table in order to count the number of emails in each folder. Also, ERD is a diagram that contains entities which specify the tables in the database (DB) that we have created. Each entity has a specific attribute like the name of the column in each table of the DB and they are linked via many relationships.

Fig. 5 shows the activity diagram of the proposed system. Finally, Fig. 6 provides the use case diagram of the proposed application. It illustrates the connection between the different users and different use cases where the users are involved, i.e., the user interactions with SMAKE application.

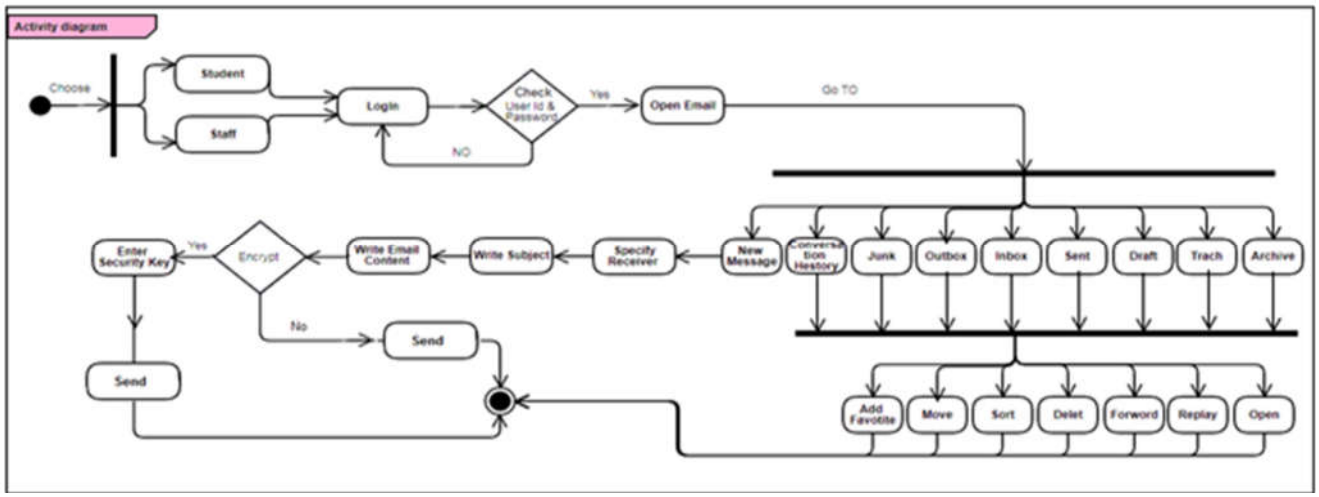

Fig. 5. Activity Diagram

Fig. 6. Use Case Diagram.

7. Proposed Design Implementation

SMAKE application is a promising solution to replace the available accessing method of KFU email since the user can access his KFU account anywhere and anytime with high level of security based on AES cryptosystem.

- Loading Phase/Role Phase/ Login Phase/ Email Navigation Phase: these three phases are activated in order. Once you select your role, you can then login using your credentials (username and password) to access email options as in Fig. 7.

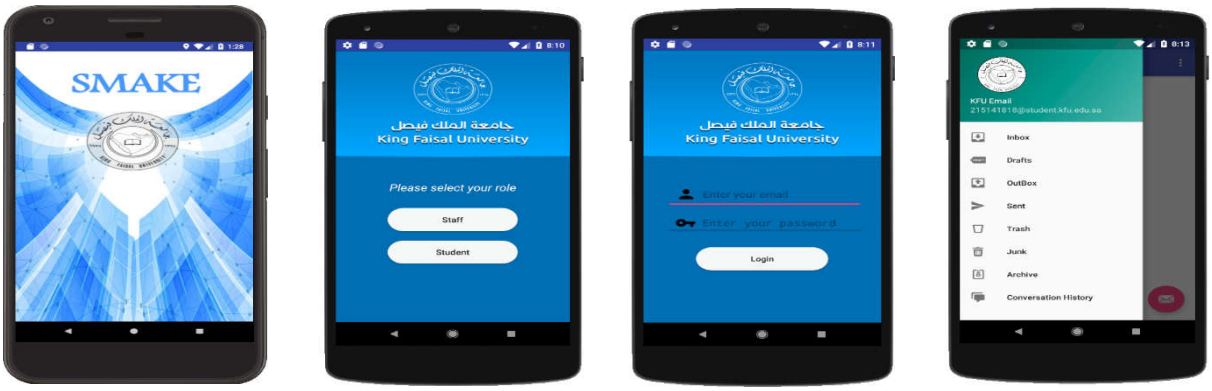

Fig. 7. (a) Loading page (b) Start page (c) Login page (d) All boxes page.

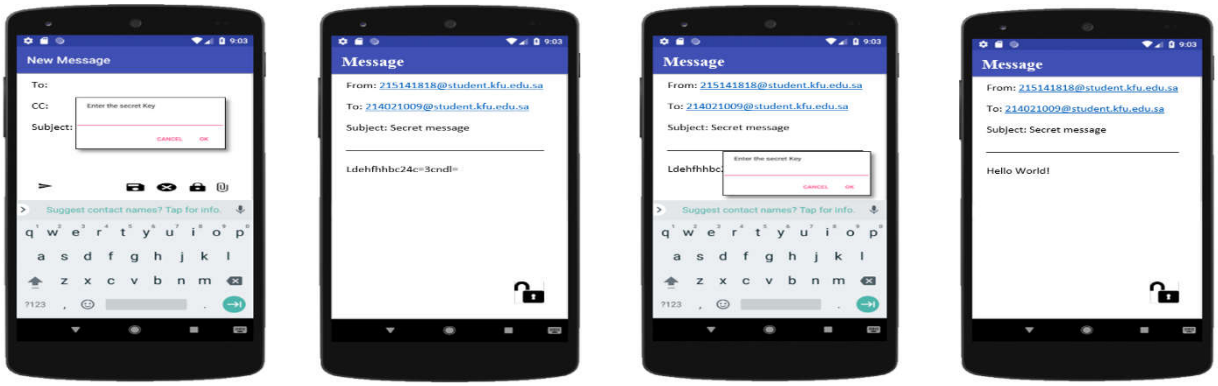

Fig. 8. Ciphering process: (a) Encryption process (b) Secret message (c) Decryption process (d) Decrypted Message.

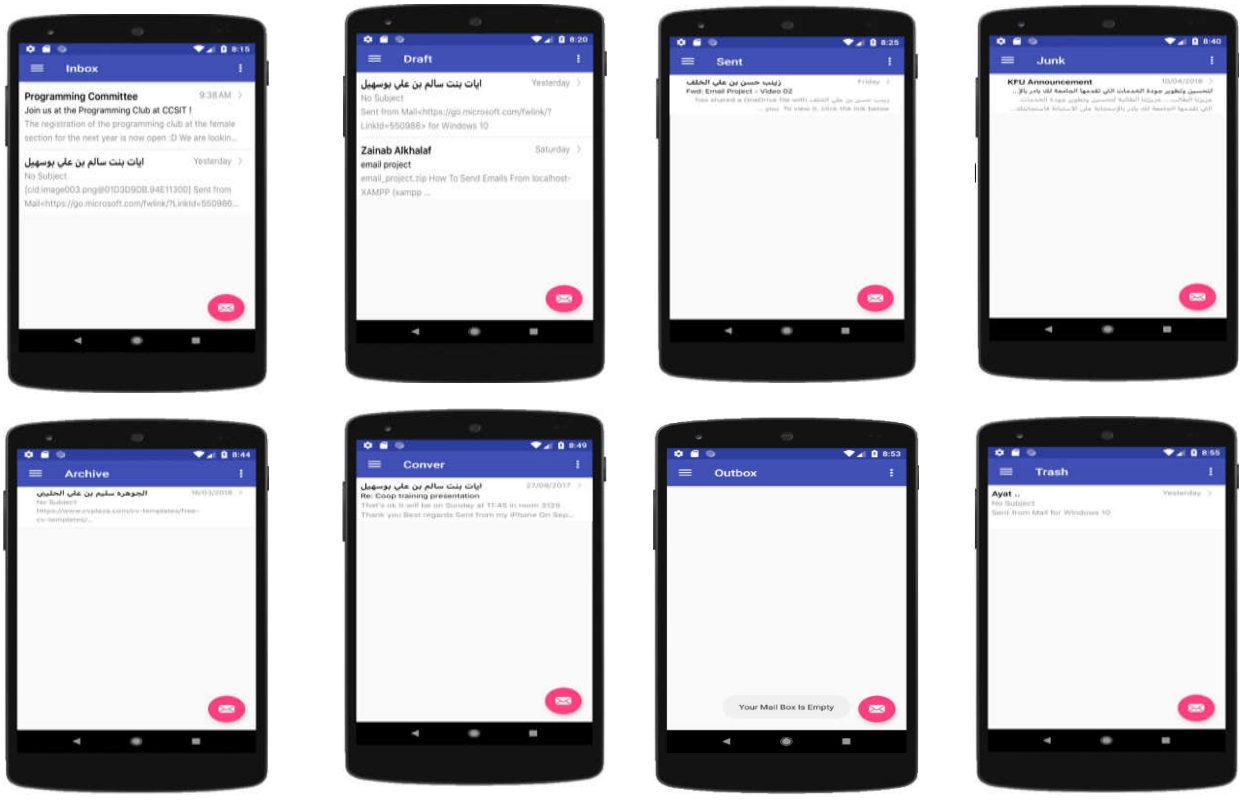

Fig. 9. (a) Inbox page (b) Drafts page (c) Sent Items (d) Junk page (e) Archive page (f) History page (g) Outbox page (h) Trash page.

- Message Encryption/Decryption Phases: The "New Message" page offers many other options such as encrypt messages that are used to encrypt the email contents with your secret key as shown in Fig 8.a.
- Oppositely, you can decrypt the encrypted message if you know the secret key that the sender uses by touching the key icon in the bottom. The steps of decryption process are clearly described in the following Fig 8. (b-c)
- Email Components which are illustrated in Fig.9.

The proposed application is composed of many activities and each activity has two major parts: the .xml file and the coding file that depends on the selected programming language such as the Java programming language (our target coding platform). Therefore, the .java file is the core part of this project since it includes all the functions of the internal activities while the .xml file is responsible for designing the appearances or (the design) of the activities.

8. Application Verification: Results Analysis

The research team of SMAKE application has verified that the system functionalities in many ways as shown in tables below which explains several test cases for each preliminary result that mentioned in SMAKE.

Table. 3. Test Case # 1- Login Test Case

Test Case ID: LOGIN-01			Test Title: Login verification test			
Test Priority (Low/Medium/High): High			Test date: 25/3/2018			
Module Name: Login			Test Executed by: ALJwharah			
Description: Verifying login with valid username and password for student and staff						
Pre-conditions: User is in login activity and has a valid username and password						
Dependencies: loading activity and role activity are passed.						
Step	Test Steps	Test Data	Expected Result	Actual Result	(Pass/Fail)	Notes
1	Loading activity is loading the picture of KFU logo.		Logo picture shall display.	Logo picture displayed successfully.	Pass	
2	Role activity is automatically displayed after role activity, and user needs to specify the role by clicking on staff or student button.	Choosing student role.	Login activity shall display.	Login activity displayed successfully.	Pass	
3	Providing valid username and password in login activity.	Username: 214021009 Password: gogo	Username & password should match the database.	Matching username and password is successfully done.	Pass	
4	Clicking on Login button		User shall be able to login	User login successfully.	Pass	
Post-conditions: User is validated with the database and successfully login to account + User is navigated to the mailbox of his account.						

Table .4. Test Case # 2-Send and Receive

Test Case ID: Send and Receive -02			Test Title: Sending and receiving test			
Test Priority (Low/Medium/High): High			Test Designed date: 27/12			
Module Name: Send and Receive			Test Executed by Ayat			
Description: Verifying sending the information of a new email to the local database and receiving the email from that sender.						
Pre-conditions: The sender opened the new message window and has the information of the new email like receiver email address, subject, and message content.						
Dependencies: login activity.						
Step	Test Steps	Test Data	Expected Result	Actual Result	(Pass/Fail)	Notes
1	The sender types the information of the new email like receiver email address, subject, and message content.	zainb@kfu.edu.sa Subject: Exam Message: Dr. Zainb, When will be our exam?	User shall be able to write the information of the email.	User wrote the information of the email.	Pass	
2	Pressing sending button.		Information shall be sent to the local database and the email appear in sent box.	Information sent to the local database and the email appeared in the sent box.	Pass	
3	The receiver opened the inbox of her account.		The email should be received and displayed in the inbox.	The email received and displayed in the inbox.		
Post-conditions: The application is validated with database and successfully sent the email + The email details are successfully added to a new record in the database.						

Table .5. Test Case # 3- Move test case

Test Case ID: Move-03			Test Title: Moving test			
Test Priority (Low/Medium/High): Med			Test date: 20/4			
Module Name: Move			Test Executed by: ALJwharah			
Description: Verifying moving a specific email from an email box to another email box.						
Pre-conditions: The user must select the message that he/she wants to move.						
Dependencies: login activity.						
Step	Test Steps	Test Data	Expected Result	Actual Result	(Pass/Fail)	Notes
1	The user selects the specific email to move.		Email shall be selected.	Email selected successfully.	Pass	
2	The user presses move button.		Dropdown list shall appear to specify the new location and then move the email to new location.	Dropdown list appeared to specify the new location and then the email moved to new location successfully.	Pass	
Post-conditions: Program moved the selected email to the required box.						

Table .6. Test Case # 4- Search test case

Test Case ID: Search-04			Test Title: Searching test			
Test Priority (Low/Medium/High): Med			Test date: 22/4			
Module Name: Search			Test Executed by: Ayat			
Description: Verifying searching for a specific email in all email boxes by specifying the email subject.						
Pre-conditions: The user holds the subject of the email in order to search.						
Dependencies: login activity.						
Step	Test Steps	Test Data	Expected Result	Actual Result	(Pass/Fail)	Notes
1	The user selects the search choice from the dropdown list.		Text filed shall appear to type the subject.	Text filed appeared successfully to type the subject.	Pass	
2	The user types the subject and presses enter.		The email shall appear depending on entries.	The email appeared successfully.	Pass	
Post-conditions: The application displayed the email.						

Table. 7. Test Case # 5- Sort test case

Test Case ID: Sort-05			Test Title: Sorting test		
Test Priority (Low/Medium/High): Med			Test date: 19/4		
Module Name: Sort			Test Executed by: Zainb		
Description: Verifying sorting the emails of mailbox.			Dependencies: login activity.		
Pre-conditions: User can sort the emails by date.					
Step	Test Steps		Expected Result	Actual Result	(Pass/Fail)
1	The user opens the dropdown list to select sort choice.		Dropdown list shall be opened.	Dropdown list opened	Pass
2	The user selects the sort choice.		Emails shall sort automatically by date in descending order.	Emails sorted automatically by date in descending order.	Pass
Post-conditions: The emails ordered by date in descending order.					

Table .8. Test Case # 6- Delete test case

Test Case ID: Delete-06			Test Title: Deleting test		
Test Priority (Low/Medium/High): Med			Test date: 20/4		
Module Name: Delete			Test Executed by: Zainb		
Description: Verifying deleting a specific email.			Dependencies: login activity.		
Pre-conditions: The user must select the message that he/she wants to delete.			Dependencies: login activity.		
Step	Test Steps		Expected Result	Actual Result	(Pass/Fail)
1	The user selects the specific email to delete.		Email shall be selected.	Email selected successfully.	Pass
2	The user presses delete button.		The email shall move to the trash box.	The email moved to the trash box successfully.	Pass
3	The user selects the message from trash box if he/she wants to delete the message forever.		Pop up message window shall appear to ensure that the user wants to delete.	Pop up message window appeared successfully.	Pass
4	The user presses ok in pop up message window.		The email shall be deleted from the database.	The email deleted from the database successfully.	Pass
Post-conditions: The application moved the selected email to the trash box + The application is validated with database and successfully deleted the email.					

Table. 9. Test Case # 7-Encryption test case

Test Case ID: Encryption-07			Test Title: encrypting test		
Test Priority (Low/Medium/High): High			Test date: 22/12		
Module Name: Encryption			Test Executed by: Zainab		
Description: Verifying encrypting process on a new message.			Dependencies: login activity.		
Pre-conditions: The sender opened the new message window and has the information of the new email like receiver email address, subject, message content and secret key.					
Step	Test Steps	Test Data	Expected Result	Actual Result	(Pass/Fail)
1	The sender types the information of the new email like receiver email address, subject, and message content.	215141818@kfu.edu.sa Subject: Goodness Message: Be good and destroy exams.	User shall be able to write the information of the email.	User wrote the information of the email.	Pass
2	Pressing on the key button and typing the secret key.	Secret key: SMAKE.	Pop up window shall appear to type the secret key.	Pop up window appeared and typing done successfully.	
3	Pressing encrypt button.		Email message shall encrypt, and result shown in a text view.	Email has been encrypted, and result shown successfully.	Pass
4	Pressing sending button.		Information of the email and encryption shall be sent to the local database and the email appear in sent box.	Information of the email and encryption sent to the local database and the email appeared in the sent box.	Pass
5	The receiver opened the inbox of her account.		The encrypted email should be received and displayed in the inbox.	The encrypted email received and displayed in the inbox.	
Post-conditions: The application encrypted the message using AES algorithm + The application is validated with database and successfully sent the encrypted email + The application stored the data of encryption in the database + The email details are successfully added to a new record in the database.					

Table. 10. Test Case # 8-Decryption test case

Test Case ID: Decryption-08			Test Title: Decryption test		
Test Priority (Low/Medium/High): High			Test date: 22/4		
Module Name: Decryption			Test Execution date: 22/4		
Description: Decrypting a message of an email within a secret key.			Dependencies: login activity.		
Pre-conditions: The user must have the secret key in order to decrypt the encrypted email.					
Step	Test Steps	Test Data	Expected Result	Actual Result	(Pass/Fail)
1	The user opens the encrypted message by touching on the email.		Email shall be opened.	Email opened successfully.	Pass
2	The user presses decrypt button to enter the secret key and perform encryption process.	Secret key: SMAKE.	Pop up window shall appear to type the secret key and the message shall be decrypted, and plaintext shown in a text view.	Pop up window appeared and typing done then the message decrypted successfully, and plaintext shown in a text.	Pass
Post-conditions: The application decrypted the encrypted message.					

Eventually, the actual result of Secure Mobile Application for KFU Email (SMAKE) that we achieved until know enabling the faculty, staff and students (i.e. the user) to login to KFU email via an android mobile application by using his/her KFU academic user id along with the password that is similar to the one in our database. Also, the user can easily open the mailbox page that contains the navigation drawer activity to navigate through the mailboxes (sent, draft, archive, delete, conversation history, junk, Favorite and outbox). In addition, the user can also press the floating button in the mailbox to open a new message page. Furthermore, the user can write and send the messages and all information of the message will be saved in the database. In additions, the user also can encrypt the email message with a secret key and then send the cipher text to the receiver. On the other hand, the receiver can decrypt the email message if he/she has the same secret key that is used in the encrypting process. Moreover, the user can sort the email messages by date, search by email subject, move specific emails to any email box, and delete a specific email and logout from the account.

9. Conclusions

According to the huge usage of mobile phones, we consider building a mobile application that helps KFU members and students to access their email accounts easily and providing a secure channel for their communication. This application will concentrate on providing the common email services like sending and receiving email and searching for emails and so on. As a new feature, this mobile application will be capable of encrypting and decrypting messages to protect the conditional information from hackers. It will use a great and helpful algorithm which is Advanced Encryption Standard (AES) to fulfill high secure data. SMAKE application will be used by the faculty members and students of KFU. Thus, we have implemented the usable functions as we planned successfully which can improve the secure mobile application for KFU email to be really used by KFU faculty members and students and help them to deal with secure emails at anytime and anywhere. In the future, this work can be enhanced by implementing a key establishment phase to securely distribute the security keys between the communication parties. This phase will enable the users to generate their secret keys without the use of the KDC system.

References

[1] Singh, G, "A study of encryption algorithms (RSA, DES, 3DES and AES) for information security." International Journal of Computer Applications, vol. 67, no. 19, pp. 33-38 (2013).

[2] Jain, R., et.al, "AES Algorithm Using 512 Bit Key Implementation for Secure Communication." International Journal of Advanced Research in Computer Science, vol. 1, no. 3 (2014).

[3] Sharma, N.; Yadav, S.; Bohra, B., "A Review on Data Encryption Techniques Used for Social Media on Internet." Advanced Computational Engineering and Networking, vol. 4, no. 9, pp. 64-68 (2016).

[4] A. Mishra, S. Sharma, "Design and Implementation of High-Speed AES Algorithm for Data Security." International Journal of Engineering Sciences & Research Technology. doi:10.5281/zenodo.5964. vol. 5, no. 8, pp. 325-337 (2016).

[5] Abu Al-Haija, Q.; et. al, "A tiny RSA cryptosystem based on Arduino microcontroller useful for small scale networks." Procedia Computer Science, Elsevier, doi.org/10.1016/j.procs.2014.07.091. vol. 34, pp. 639-646 (2014).

[6] Al-Qadeeb, H.; Abu Al-Haija, Q.; Jebril, N. A., "Software Simulation of Variable Size Message Encryption Based RSA Crypto-Algorithm Using Ms. C#. NET". International Journal of Cyber-Security and Digital Forensics (IJCSDF), DOI: http://dx.doi.org/10.17781/P002241. Vol. 6, no. 1, (2017).

[7] Sheikh, A.; et. al, "Smartphone: Android vs. IOS." The SIJ Transactions on Computer Science Engineering & its Applications (CSEA), vol. 1, no. 1, (2013).

[8] Narkhede, S., "Kisan Monitoring System Focused on Android based Application." International Research Journal of Engineering and Technology (IRJET), vol. 3, no. 2, pp. 965-968 (2016).

[9] Spencer, L., (2017, February 8). The 10 Best (Free) Email Service Providers for Your Business. Retrieved from https://business.tutsplus.com/articles/best-free-email-service-providers--cms-28160

[10] Spencer, L., (2017, February 23). Gmail vs. Outlook: What's the Best (Free) Email Service? Retrieved from https://business.tutsplus.com/articles/gmail-vs-outlook-whats-the-best-free-email-service--cms-28195

[11] Agrawal, A., Which email application is right for you: Outlook or Gmail? Retrieved August 18, 2014, from https://blogs.office.com/en-us/2014/08/18/email-application-right-outlook-gmail/?eu=true

[12] Siledar, S., "File Encryption, Decryption Using AES Algorithm in Android Phone." International Journal of Advanced Research in Computer Science and Software Engineering, vol. 5, no. 5, pp. 550-554 (2015).

[13] Kashyap, S.; Madan, E.N., "A Review on: Network Security and Cryptographic Algorithm." International Journal of Advanced Research in Computer Science and Software Engineering. vol. 5, no. 1 (2015).

[14] Abd Elminaam, D. S.; Abdual Kader, H. M.; hadhoud, M. M., "Evaluating the Performance of Symmetric Encryption Algorithms." International Journal of Network Security, vol. 10, no. 3, pp. 213-219 (2010).

[15] Stellar Blue Technologies. (2015, August 4). Scary Hacking Statistics You Probably Didn't Know About. Retrieved November 15, 2017, from https://stellarbluetechnologies.com/2015/08/4-scary-hacking-statistics/

[16] Mathur, M.; Kesarwani, A., "Comparison between DES, 3DES, RC2, RC6, BLOWFISH and AES." Proceedings of National Conference on New Horizons IN IT – NCNHIT (2013).