



Enhancing the Information Security Constraints for Speedy Transmissions using Encryption Methods over Android Platform

Saurabh M.I. Prabhune¹, Indrajeet Sharma², Sachin Bayas³, Prof. Trupti B. Mane⁴
^{1,2,3}Pursuing B.E. Computers at Modern Education Society's College of Engineering.
⁴Assistant Professor at Modern Education Society's College of Engineering.
^{1,2,3,4}Savitribai Phule Pune University.
^{1,2,3,4}M.E.S College of Engineering Pune, Maharashtra-411001, INDIA.

Abstract: The title of our project is "ANDROID MOBILE APPLICATION FOR SECURE DATA TRANSMISSION". This project encrypts and decrypts the textual files, media files by using encrypt/decrypt cipher algorithm. Our aim was to develop the secure data transfer software, which encrypts and decrypts files by using the algorithm. Encryption and Decryption is a strong text and file in media format encryption software for personal and professional security. It protects privacy of our email messages, documents and sensitive files by encrypting them using the ciphers to provide high protection against unauthorized data access. The use of mobile phones is increasing day by day so the need of security has risen too high. Every day hundreds and thousands of people interact electronically, whether it is through emails, e-commerce, etc. through internet. Sending sensitive messages over the Internet is very dangerous. If you need to send sensitive messages over the Internet, you should send it in the encrypted form. Encryption and Decryption allows you easily encrypt and decrypt your messages. If you need to send sensitive information via email, simply paste the encrypted text into your email and all the recipients has to do is to decrypt the text. It even would focus for security of crucial data like passwords, important keys generated during banking transactions.

Keywords: Android Security, Encryption & Decryption Ciphers, SQLite Database, Virtual Server, Symmetric Key Generation, Security Applications, and Android Device Security.

I. Introduction

As observed the current encryption/decryption software's or applications over the Android platform doing the encryption and decryption task are all very complicated in their functionality. The method of encryption/decryption and key generation of current system for a new user to understand is complex in nature. The proposed system is quite simple to use. It is not complex in its functionalities. It is easy for a naïve user to use it. If you want to send sensitive information via email, simply paste the encrypted text into your email or attach the encrypted file, all the recipient has to do is to decrypt your text or file. Just select what you want to encrypt, and Encryption and Decryption software helps you keep documents, private information and files in a confidential way. The media files to be sent have to be copied in the application of device & the system would perform encryption & decryption process & forward the data to the recipient.

II. Objective & Scope

A. Objectives

The aim of our project was to develop an application or software for Android based users being an open source Operating System which would help to provide a secure transmission channel based on the Encryption & Decryption standards. The project encrypts and decrypts the textual files, media files with the help of 3 CIPHERS to maintain the security and integrity of data and information and to provide high protection against unauthorized data access. Android OS being open source system by Google is the reason of choosing this topic for implementing security system for the devices based on Android platform. The urge of implementing such a system is due to ever increasing demand of secure data transfers in all types of data formats. The reason behind implementing such software is to provide user friendly GUI wherein the client can easily share secure information through our system.

Our target is the common man who wants to interact electronically, whether it is through emails, e-commerce, net banking, e-business or trading involving transactions like transfer of money etc. through internet. Sending sensitive messages over the Internet is very dangerous. So, our project helps him to interact in a safe and secure manner in order to keep their private information confidential. This would enable the user to be satisfied that there would be no fear of loss of crucial information. The main target users of our project are the people who transmit confidential information via emails or through internet, e-commerce, e-banking, e-business facilities. The key elements of our application include the objectives, plus the following:

- The system provides the security and integrity of data or information.
- It will provide a more clear and non ambiguous description of the functions.
- It uses two different keys (a key pair) for encryption and decryption. These algorithms are called "public-key" because the encryption key can be made public. Anyone can use the public key to encrypt a message, but only the owner of the corresponding private key can decrypt it.
- The system would be easily compatible to all android based devices & user friendly.

Android applications run in a sandbox, an isolated area of the system that does not have access to the rest of the system's resources, unless access permissions are explicitly granted by the user when the application is installed. The sandboxing and permissions system lessens the impact of vulnerabilities and bugs in applications.

B. Scope

The scope of our project is presently specific. Both the sender and the receiver must have this software installed on their devices to encrypt/decrypt and compress/decompress the files transmitted between them. This includes all the users who want to interact electronically through internet in order to keep their private information confidential.

- Each step is clearly stated and user will not face any ambiguity in using the software.
- The software provides clarity in its functionality even to naive users.
- No complexity is involved.

Google has now pushed an update to Android Verify Apps feature, which will now run in background to detect malicious processes and crack them down. The "App Ops" privacy and application permissions control system, used for internal development and testing by Google, was introduced in Google's Android 4.3 release for the Nexus devices. Initially hidden, the feature was discovered publicly; it allowed users to install a management application and approve or deny permission requests individually for each of the applications. The open-source nature of Android allows security contractors to take existing devices and adapt them for highly secure uses. For example Samsung has worked with General Dynamics through their Open Kernel Labs acquisition to rebuild Jelly Bean on top of their hardened micro-visor for the "Knox" project.

III. Application Development

The software or application built would be entirely based on Android platform with the XML front-end & Java program as the back-end wherein the entire database would be maintained over SQLite-3 storage on which the processing would be done using SQL virtual server.

A. User Requirements

It is necessary that the user & client shall have an Android based device that is either a mobile phone or tablet having Jellybean or Kit-Kat versions. The user interface includes Graphic User Interface (GUI) where the user selects the data to be sent to the client in secure encrypted format. The output includes the authentication result & the device will generate the key after verification of data at the client side & would receive the original information. Also it would be compatible with the latest version of Android that is Lollipop and even Jelly-Bean, Kit-Kat that is from 4.0.0 to 5.0.0.

B. Hardware Requirements

The minimum Hardware requirements for a PC & Android Device are:

- Operating System as Windows-7 or 8 having 2 or 4- GB RAM.
- Hard Disk capacity of 500 G.B or higher.
- The minimum Hardware requirements for Android Device are:
- Android based Phone or Tablet with Jelly-Bean or Kit-Kat Versions.

C. Software Requirements

The programming for the Application & Interfacing with the System & Device will be done using the following:

- The language used to code the system is Java JDK 1.7.0 & JRE 7 or 8 & SQLite coding for database processing.
- Eclipse Kepler or Luna Versions as programming is totally Java based & would need Android AVD Manager installed.
- For system designing the Software's required would be Visual Paradigm 11.2 & Star UML 5.0.

D. Communication Requirements

The communication for our system would be based on the use of interaction between the phone & the system at client & server side respectively. The entire data transfer would take place over the Internet Connection via SQL Server which would be used for database storage. The entire admin system information will be stored over the

database securely including the user's & client's data. The Software data & encryption decryption keys would stored over Virtual SQL Server.

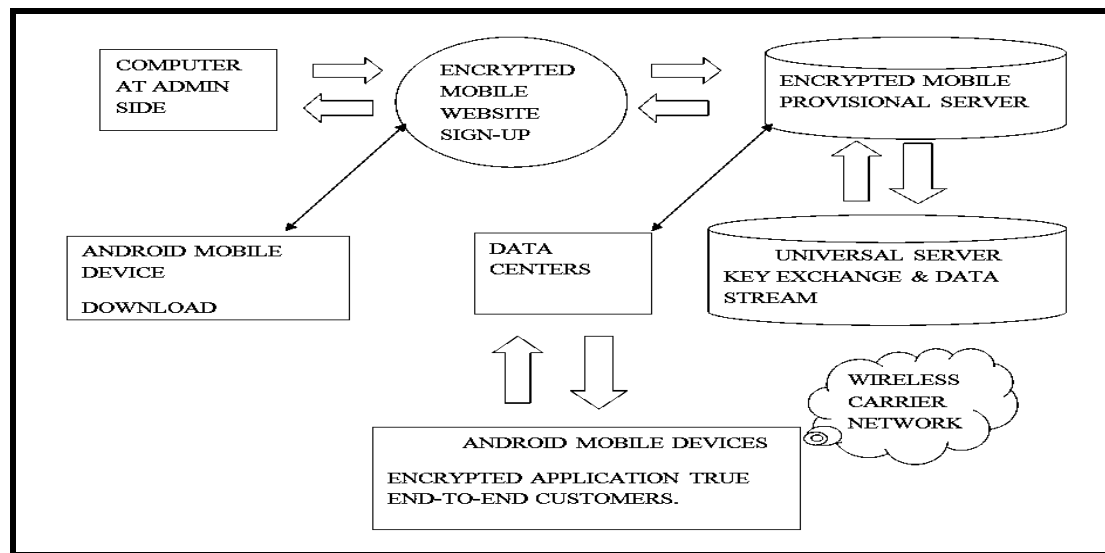
IV. Designing of the Application

The system design is prepared with the help of constructing its Architecture & by using the Android Architecture as a reference for building our Application. It also aims at presenting the conceptual aspects of our project using the UML Modeling performed by constructing basic diagrams like Use-Case, Class, Deployment, etc. diagrams with the help of tools like Star UML 5.0 & Visual Paradigm 11.2.

A. Android Application Architecture

The Fig. 1 below shows the detailed functioning of the system which includes the working of the Android mobile application for secure data transmission wherein the user & client have to register on the application after downloading it. Thereafter the admin would provide unique identification number by which on entering it he/she can easily login & send whatever data has to be sent. The diagram shows how data centers' and SQL server interacts' with the devices & admin PC.

Figure 1 Android application system architecture.



V. Encryption/Decryption Cipher Generation

The system consists of three stages for data encryption and decryption namely, Basic or Low or Unary, Intermediate or Middle, and High levels.

A. Properties of the New Encryption Technique

The cipher is only with the company rather than anyone else. The cipher is not easy to manipulate for other third party applications or companies. In case of any leak in information companies can make significant changes in cipher easily. The main intention of this paper is to make the research on encryption methods and how various types of data can be encrypted [12]. The encryption method based here is very flexible. It can be changed as per the requirement. The encryption algorithm explained below gives a brief idea of how encryption can be used to exchange data between a mobile device and a secure SQL server.

B. Low Level Cipher

This type of algorithm is used for data which would not require high level security or no protection at all. The data such as labels, personal information as name, contact details, etc. where it is not mandatory for encryption. This is the most basic type of encryption and requires less time and space complexity. This cipher is only implemented because less important objects of the document would unnecessarily be given the same level of security as that of other objects. This would further increase the time and space complexity. Using a low cipher would make it possible to increase the transmission speed and reception speed.

The cipher implemented would be easy to understand, user friendly, easily modifiable by the company or user requirements & highly efficient. The Result obtained after executing the below algorithm is that the, Input text entered into the input Tab was accepted by the Source program for verification & was converted to its equivalent Coded format by using our technique of conversion into Symbolic form by representing each character of the Input Source String into its ASCII Value. The Result is,

- Enter Input Character:: AZ

After execution,

- ASCII value for A is:: 65 90
- ENCODED-FORMAT:: #000000#00000###000000000#*##
- KEY Generated:: 165901

STEPS-

1. Initially all the data is taken in terms of ASCII value of each character for e.g.:- for alphabets ranging from a-z.
2. The ASCII values are taken in a decimal format and the value of each ASCII character is taken as an input string.
3. For e.g. If the ASCII value of a particular input is 67 then the output of the program would be #000000#0000000##.
4. The string would be then passed onto the data connection to transfer the data.
5. Although the data is very easy to detect the low cipher data would be stuffed in between the mid and high level data.
6. The data would be then transferred by the network in terms of unary digits.
7. The data would be recollected by the server side and then be decrypted in the same procedure as the encryption method. This would require less time and space complexity. Although the space requirement would be large, this would provide added security to the next ciphers.

C. Middle or Intermediate Level Cipher

This encryption algorithms aims at sub-critical information transfer such as multimedia objects, and other data items which have a less priority and have the less chances of leaking. Here in this cipher the input data type would be matched after verifying its contents that is whether it is in textual or media format. Multimedia files & sub-critical data or information would be scanned for encryption & decryption. In this cipher 8 or 16 bit Binary data is used. Mathematical functions as Permutations & Combinations are used for processing the data input into the encoded format.

STEPS-

1. The data type would be checked by the cipher.
2. It would then convert it to Symbolic Notation for the ASCII values of textual data, source code of the media file.
3. Then it would be converted to generate the encryption key & would be sent further to high level execution.
4. It would perform Encryption faster & provide the security key to the client. Thus it would be possible to perform decryption.

Advantages of having an intermediate cipher-

1. Less time and space complexity.
2. More added security & Byte-stuffing in between ciphers.

D. High Level Cipher

This encryption algorithm or cipher aims at high level security of data such as passwords and critical data which is the most important to the client and the company. It even includes information as the financial related information, its codes & passwords, etc.

STEPS-

1. The data type would be checked by the cipher.
2. It would then convert it to Symbolic Notation for the ASCII values of textual data, source code of the media file into the relevant format of our program.
3. Then it would be converted to generate the encryption key & would be sent further to high level execution.
4. It would perform Encryption faster & provide the security key to the client to receive the decrypted data.
5. Once the data is stored in the database the cipher generation takes place.
6. Then the Admin would verify & send the security key further to the client & then request for entering the address provided.
7. After matching the Key, the Admin would send confirmation & present the data at his desk on his/her device.

The Result obtained after execution of this algorithm would generate the Encryption Key & on further processing would decrypt the Data to its original format after providing the Key.

- Enter Input Character:: AZ

After execution,

- ASCII value for A is:: 65 90
- ENCODED-FORMAT:: #000000#00000###000000000#*##

- KEY Generated:: 165901

On Decryption,

- Enter the Key:: 165901
- Original Data:: AZ

Advantages of having a High Level cipher-

1. This type of cipher would be not difficult to execute. It would low time & space complexities.
2. The cipher would provide high level encryption to the crucial data preventing it from getting leaked or hacked. This type of algorithm would be easily compatible to changes if any, required to be made.

E. Data Filtration Algorithm

The Data Filtration algorithm would be used for analyzing the type of the information uploaded on the Application for further Encryption. It would be executed to check the data type in order to determine the Security Level that is Low, Intermediate or High. The data would then be encrypted using the respective 3 Ciphers with the help from [7] & [8].

The Result obtained is,

- Enter Input File- abc.txt, for example.

After processing,

- The File type is- Textual format, .txt
- Data sent to- Low level Encryption Cipher.

STEPS-

1. Accept input data.
2. Check for data variables.
3. Crosscheck the data values.
4. Place data respectively.

F. Mathematical Contents

The mapping functions are defined for the 6+2 Permutations by defining the table for 64-byte data stuffing. The functions generated are One-to-One Mapping & One-to-Many Mapping. The high level permutation include 64 bits initial and final permutation with mapping functions F3 and F4 respectively having one to one correspondence as in [4]. The 3 Ciphers when executed, firstly the type of Input Data would be verified by executing the Data Filtration Algorithm in which the data would be accepted & then checked for its type that is Textual, Coded or Media formats by performing bit-by-bit analysis as mentioned above in the steps for it ;reference from [9], [13]. The symbolic representation used for alphabets of types upper case and lower case includes ‘#’, ‘0’, ‘Special Symbol say, *’ that would be use to represent start and end symbol for ASCII values bit representation in bit stuffing. Star is used for ASCII value Zero present in letters Z, F, n, etc. The ciphers include six permutation namely as Initial, Inverse Initial, Expansion, Permutation, Permuted Choice, Final with the help of [2], [7], [8].

VI. List of Abbreviations

- OS – Operating System.
- GUI – Graphical User Interface.
- SD – Secure Digital.
- SMS – Short Messaging Service.
- PC – Personal Computer.
- UML – Unified Modeling Language.
- JRE – JAVA Runtime Environment.
- JDK – JAVA Development Kit.
- AVD – Android Virtual Device.
- APP OPS – Application Permission Control Systems.
- IP – Internet Protocol.
- CBC – Cipher Block Chaining.
- FPGA – Field Programmable Gate Array.
- DE4MHA – Data Encryption for Mobile Health Application.
- MIPS32 – 32 Million Instructions Per second.
- WBAN – Wireless Body Area Network.
- VLSI –Very Large Scale Integrated Circuit.
- IP – Initial Permutation.
- KS – Key Schedule.
- DES – Data Encryption Standard.

- AES – Advance Encryption Standard.
- DEA – Data Encryption Algorithm.
- MAC – Media Access Control.
- RSA – Ron Rivest, Adi Shamir and Leonard Adleman Algorithm.
- XMPP – Extensible Messaging and Presence Protocol.
- SQL – Structural Query Language.
- SSL – Secure Socket Layer.
- SGL – Scalable Graphics Library.
- XML – Extensible Mark-up Language.
- LIBC – C Library.
- PCI – Payment Card Industry.
- SDK – Software Development Kit.
- APK – Android Application Package.
- ASCII – American Standard Code for Information Interchange Acknowledgment.

VII. Conclusion

By using the three ciphers that we have generated & have tried to meet our goal of advancing the security standards for high speed data transmission over Android based devices. It has tried to meet the security requirements as per our implemented algorithm. The most admirable feature founded was its simplicity in terms of application to the user but its highly beneficial outputs can't be ignored. It has tried to meet the user requirements up to some extent for fast data transmission in secured channel over ANDROID devices. The aim of using less memory & achieving transmission speeds were satisfied.

- **User Friendliness:** The system is user friendly as any naïve user can use it and easily understand its functionality.
- **Security:** Security is enabled as certain features and functionalities are restricted to the registered users only and also at other levels security is implemented.
- **Future Plans:** The system is adaptable to the future changes if any are deployed in order to meet the technological advancements. To implement the same system over iOS or MAC OS Platform of Apple Phones.

References

- [1] A Data Encryption Solution for Mobile Health Apps in Cooperation Environments-Bruno Bruno M Silva¹, BSC, MSc; Joel JPC Rodrigues¹, BSC, MSc, PhD; Fábio Canelo¹, BSC, Msc Candidate; Ivo C Lopes¹, BSC, MSc; Liang Zhou², BSC, MSc, PhD. Institute de Telecommunications University of Beira Interior, Covilhã, Portugal Nanjing University of Posts and Telecommunications, Nanjing, China. Corresponding Author: Joel JPC Rodrigues, BSC, MSc, PhD; IEEE Paper Published in February 2013.
- [2] The Design and Implementation of Database Encryption-Noor Habibah Arshad, Saharbudin Naim Tahir Shah, Azlinah Mohamed, Abdul Manaf Mamat; IEEE Paper Published in May 2013.
- [3] Adaptive & Dynamic Mobile Phone Data Encryption Method-CAO Wanpeng, BI Wei-Network Technology & App; IEEE Paper Published in January 2014.
- [4] Data Security & Privacy in Wireless Body Area Networks-Ming Li & Wenjing Lou, IEEE Paper Published in February 2010.
- [5] Android: Changing the Mobile Landscape-Roy Wants; IEEE Paper Published in January - March 2011.
- [6] http://en.wikipedia.org/wiki/RSA_algorithm.
- [7] http://en.wikipedia.org/wiki/DES_algorithm.
- [8] http://en.wikipedia.org/wiki/DEA_algorithm.
- [9] "Data Communications and Networking", 4th Edition, by Behrouz A. Forouzan, Tata McGraw Hill Publication.
- [10] Roger S. Pressman, "Software Engineering a Practitioners Approach", McGraw Hill, 1992.
- [11] E Balagurusamy, "Programming with JAVA", McGraw Hill, 2003.
- [12] William Stallings, "Cryptography and Network Security".
- [13] Differential Power Analysis Attacks to Pre-charged Buses: A General-Analysis-for Symmetric Key Cryptographic Algorithms. IEEE Paper Published in July-September 2010-Massimo Alioto, Massimo Poli, Santina Rochi, IEEE Members.

Acknowledgements

We would like to express a deep sense of gratitude and appreciation to all those who helped us in the completion of this paper. A sincere thanks to our H.O.D Prof. N. F. Shaikh madam and project guide, Prof. Trupti B. Mane, whose suggestions and encouragement helped us tremendously. We would also like to acknowledge, with much appreciation, the staff of the Computer Department for their support and help whenever we needed it. Last but not the least; we would like to thank our friends and family for their valuable support.