iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 3 **Issue:** IV **Month of publication:** April 2015

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Self-Destructing Messages Using Layered Encryption for Mobile Devices

Shraddha Badade[1], Rasika Borate[2], Sayali Dhobale[3], Pooja Ghogare[4]
[1,2,3,4] *Department of Computer Engineering, Bhivarabai Sawant College of Engineering and Research, Narhe, Pune, India*

Abstract— Communication through SMS is very popular now-a-days and it is cheap, fast and simple. However, when confidential information is exchanged using SMS, it is very difficult to protect the information from SMS security threats like man-in-middle attack and eavesdropping. Most of the times, these threats are difficult to detect and therefore increasing the security of SMS communication is the only way to avoid such threats. Earlier messaging security was generally provided through single encryption mechanism but this mechanism is not sufficient to encrypt a file (i.e. audio, video, text and image). Also, there were no systems that would double encrypt a file in a single system in SMS communication. We propose self-destructing messages using layered encryption, an enhanced messaging architecture equipped with self-destructing feature and double encryption of a file in a mobile environment. Senders will be able to set location and time constraints for their messages. The constraints will determine where and when the sent messages are decrypted. The paper presents a design for Android platform application and is equipped with three modes for sending the messages, namely- Insecure, Secure and Ultra Secure.

Index Terms—File Encryption, Layered Encryption, Location Based Encryption, Time Based Encryption.

I. INTRODUCTION

This document is a research paper for the project "Self-destructing messages using layered encryption for mobile devices." It is an attempt to design and create an android mobile application for mobile devices so that they can be used by numerous different users without specific knowledge of the capabilities of this application. In today's instant messaging services the users are subjected to constant unwanted leakage of confidential information. Also, the repercussions of leaving unencrypted messages on servers may cause leakage of personal information, or even identity theft. Today's systems have features like self-destruction or location constraints for SMS transmission. To our knowledge none of these systems provide layered encryption for the data along with the time and location constraints. We present this paper to make an effort to design an enhanced and secure messaging architecture for message transmission.

II. PREVIOUS SYSTEM

A. Literature survey

1) *Self-Destructing Messaging Architecture:* The system enables the sender to send messages that will be self-destructed from server after a particular period of time [1].

2) *Location based RSA Encryption Technique:* The system makes use of location co-ordinates along with public key and private key. Use of co-ordinates ensures that data cannot be decrypted outside a particular area [2], [6], [9].

3) *Encryption and Decryption:* Existing systems use AES and RSA for encryption of data. Both the algorithms provide secure encryption and are resistant to attacks [3], [12].

B. Limitations of previous system

The existing systems do not provide encryption at administrative level. Also there are no systems that support encryption of all types of files such as audio, video, text, etc. together. Moreover, there are some systems that provide time and location based encryption, but none of these have been implemented in a single system for mobile devices.

Volume 3 Issue IV, April 2015
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

C. Problem Statement

The popularity of instant messaging has grown in an exponential way. However, most popular instant messaging services often trade speed for security. This leads to the messages being prone to threats. Thus, we are trying to create an android mobile application for securing data using layered encryption along with time and location constraints.

III. PROPOSED SYSTEM

Our paper is an attempt to create a design for overcoming the limitations stated above. The paper aims at creation of an instant messaging service that will provide encryption in three different modes- Insecure, Secure, Ultra secure and destruct the message from the server automatically after certain time elapses. The proposed system will encrypt and decrypt any type of file i.e. audio, video, text, image. Any user can state the location constraint for the message which will determine where the message will be decrypted.

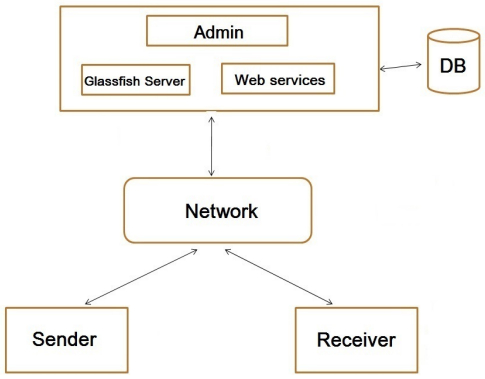


Fig 3.1. System Architecture

Fig3.1 shows the user's mobiles will have to be connected to the network. For this purpose, either virtual router or hotspots can be used. Once the users are connected in the network they can make request to the server and get access to the web services. The server that we have used is the glassfish server as it is known to be one of the most efficient servers that are available. Users will be provided with SAAS as the web service. The database will store user's information and will be created using MySQL.

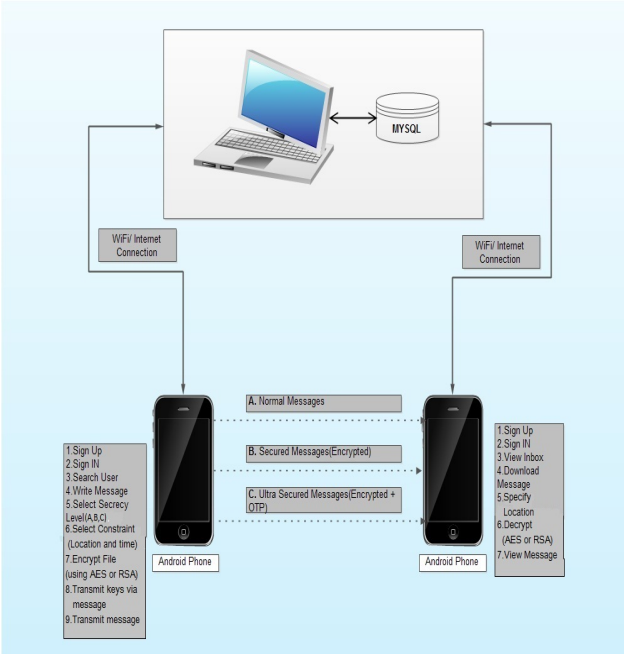


Fig3.2. Functional Block Diagram

As shown in Fig 3.2, the system will have three modes of encryption- insecure, secure and ultra-secure.

A. Insecure-No encryption will take place. Implementation will be like simple messaging system.

B. Secure- Encryption of messages will be on server using RSA algorithm. Sender will encrypt the message using the public key of the receiver. Receiver can decrypt the message using his private key. RSA generates two keys- one is public key, used for encryption and another is private key used for decryption of file. The RSA method's security rests on the fact that it is extremely difficult to factor very large numbers [8].

C. Ultra Secure- Encryption and decryption of messages will be on server as well as on the user's mobile devices using AES algorithm. AES makes use of only one key for encryption and decryption and is resistant to brute force attack [13], [14].

The main components of the process are as follows-

1) Sender
2) Receiver
3) Cloud Server

Operations performed by a sender –

1. Sign Up: The sender has to register first to use the application. The sender has to give his/her full name, address, country, e-mail id, contact number, username and password in the registration process.
2. Sign In: Once the sender has sign up, sender can sign in using the username and password that has been set in the registration process.
3. Search User: In this step, the sender will select the receiver to whom the message is to be sent. The names of only those users will appear to the sender who are registered with the server. Other names from the sender's mobile phone will not appear in the list.
4. Send Message: The sender then will select the message file that is to be sent. The file could be any file from the mobile.
5. Select the security mode: The sender will have to select the one of the three modes i.e. insecure, secure and ultra secure. If the sender is selecting the ultra secure mode, he/she first has to set a private key which will be used for encryption of the message and also for the decryption of the message by the receiver.
6. Set the constraints: Constraints determine where and when the receiver will be able to download the file and decrypt it. In this application, it is mandatory for the sender to select both the constraints i.e. time and location.
7. Encrypt File: In secure mode, file will be encrypted using RSA algorithm and in ultra secure mode, file will be encrypted using AES algorithm.
8. Sent the key: If the sender encrypts the message using the ultra secure mode, then the key with which the file is encrypted should be sent via SMS to the receiver. If the sender encrypts the message file using secure mode then keys will be generated by the server for both, the sender and receiver.
9. Transmit Message: Message will be sent to the receiver.

Operations performed by the receiver-

1. Sign Up: The sender has to register first to use the application. The sender has to give his/her full name, address, country, e-mail id, contact number, username and password in the registration process.
2. Sign In: Once the sender has sign up, sender can sign in using the username and password that has been set in the registration process.
3. Receive Message: Receiver can view the files received alongwith with the type of mode for encryption and time when they were sent.
4. Download Message: Receiver will be able to download the received file by clicking on it.
5. Give the constraints: Receiver has to specify the location at which he/she is present. If the constraints entered by the receiver match with the constraints set by the sender then and only then the message will be decrypted, otherwise not.
6. Download message: Downloaded message will be stored in the device storage of the mobile phone.
7. Decrypt message: The downloaded message will be decrypted and stored in the receiver's mobile phone.

8. View the message: Receiver can view the original message that was sent by the sender.

IV. EXPERIMENTATION

For the implementation of the application, we have used RSA algorithm for encryption in secure mode and AES algorithm for ultra secure mode.

RSA- RSA involves a public key and a private key. The public key can be known by everyone and is used for encrypting messages. Messages encrypted with the public key can only be decrypted in a reasonable amount of time using the private key. The keys for the RSA algorithm are generated the following way:

A. Choose two distinct prime numbers p and q. For security purposes, the integers p and q should be chosen at random, and should be of similar bit-length. Prime integers can be efficiently found using a primality test.

B. Compute $n = pq$. n is used as the modulus for both the public and private keys. Its length, usually expressed in bits, is the key length.

C. Compute $\varphi(n) = \varphi(p)\varphi(q) = (p - 1)(q - 1) = n - (p + q - 1)$, where φ is Euler's totient function.

D. Choose an integer e such that $1 < e < \varphi(n)$ and $\gcd(e, \varphi(n)) = 1$; i.e., e and $\varphi(n)$ are coprime. e is released as the public key exponent. e having a short bit-length and small Hamming weight results in more efficient encryption – most commonly $2^{16} + 1 = 65,537$. However, much smaller values of e (such as 3) have been shown to be less secure in some settings.

E. Determine d as $d \equiv e^{-1} \pmod{\varphi(n)}$; i.e., d is the multiplicative inverse of e (modulo $\varphi(n)$).

This is more clearly stated as: solve for d given $d \cdot e \equiv 1 \pmod{\varphi(n)}$. This is often computed using the extended Euclidean algorithm. Using the pseudocode in the *Modular integers* section, inputs a and n correspond to e and $\varphi(n)$. d is kept as the private key exponent.

AES-The algorithm begins with an Add round key stage followed by 9 rounds of four stages and a tenth round of three stages. This applies for both encryption and decryption with

the exception that each stage of a round the decryption algorithm is the inverse of it's counterpart in the encryption algorithm. The four stages are as follows:

1. Substitute bytes
2. Shift rows
3. Mix Columns
4. Add Round Key

The tenth round simply leaves out the Mix Columns stage. The first nine rounds of the decryption algorithm consist of the following:

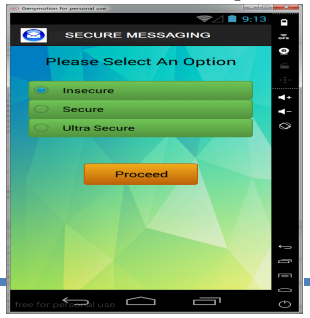
1. Inverse Shift rows
2. Inverse Substitute bytes
3. Inverse Add Round Key
4. Inverse Mix Columns

Again, the tenth round simply leaves out the Inverse Mix Columns stage.

The receiver will have to first download the file and then decrypt it to see the contents of the file. The file will be decrypted by using the key that is with the receiver. If the receiver doesn't download the file within 30 minutes after receiving it, the file will be permanently self destructed from the server and the receiver can never access it.

To demonstrate the feasibility of proposed architecture,

We have developed an application on the Android Development Toolkit. Some of the screenshots are shown in figure 4.5.



Volume 3 Issue IV, April 2015
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Fig.4.1. Screenshots of Application

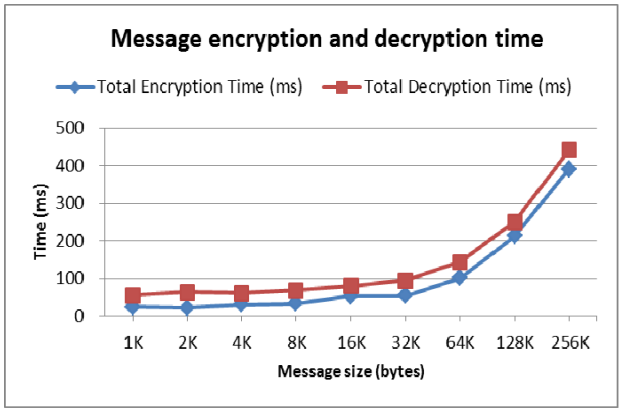
When sender is sending the message, sender can give location constraint to the file that is to be sent to the receiver. It will enable the sender of the message to decide the location at which he wants the receiver to decrypt the message. If the receiver is not present at the location specified by the sender then receiver will be unable to neither download the message nor to decrypt the message and after half an hour, the message will be destructed from the server permanently.

V. RESULTS

The figure 5.1 shows the approximate results of the time required for encryption and decryption. All types of files are getting encrypted and decrypted. The file is being self destructed from the server after certain minutes. The file is being deleted from the server even if the receiver has not downloaded it. Receiver is unable to download a file from a location that is not specified by the sender

Fig.5.1.The average time for encryption and decryption

.



VI. CONCLUSION

We are attempting to design this project with the sole objective of securing the information in SMS communication. The system will provide an enhanced security to messages that are being transmitted. The self destruction of messages ensure that nobody can have access to it after certain amount of time. Moreover, the location constraint makes it mandatory for the receiver to be present at the location specified by the sender.

VII. FUTURE SCOPE

Since the main objective of our application is to provide secure and efficient message transmission, it can be used in any organization where confidentiality of information is the top priority. As the messages have time and location constraints , they will be decrypted at a particular place. Due to this feature, the application can find it's use in government organization, military and institutions like university or college. It can be also used at personal level for secure transmission of information. In addition to that, the application can also be used to delete files from the server after a certain time to save memory.

VIII. ACKNOWLEDGMENT

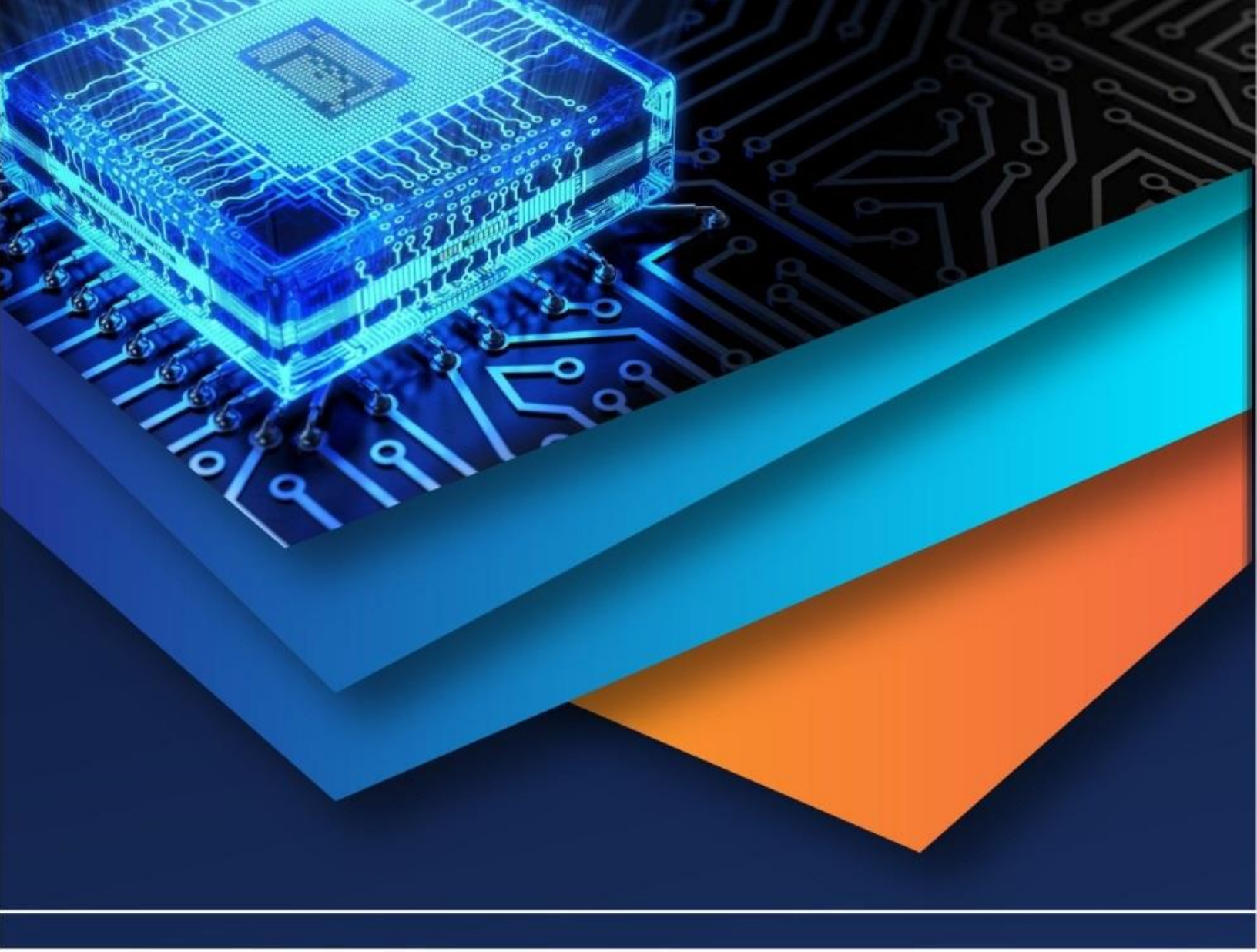
The paper has taken a considerable amount of time and resources and a number of people have helped us. We would like to acknowledge the help of all of those who have guided us. We would like to thank our project guide Dr. S.M. Chaware (HOD, Dept. of Computer Engineering, BSCOER) for his time, patience and guidance, and also for allowing the idea to be pursued originally. We would also like to thank project co-guide Prof. P.D. Chouksey and project co-ordinator Prof. Manohar Kodmelwar for their time and advice.

REFERENCES

[1] Tsai-Yeh Tung, Laurent Lin and D.T. Lee, "Pandora Messaging: An Enhanced Self –Message-Destructing Secure Instant Messaging Architecture for Mobile Devices", IEEE journal, 2012.
[2] Ayesha Khan, "geo Location Based Encryption Technique", 2013.
[3] Rajan S. Jangekar and Geeta Shantanu Joshi, "File Encryption And Decryption Using Secured RSA", 2013.
[4] Suriyani Ariffin, Ramlan Mohmad, Ratini Rehmat and Nuzul Annisa Idris, "SMS Encryption Using 3D AES Block Cipher On Android Message Application", 2013.
[5] Prof.Rashmi Ramesh Chavan and Prof. Manoj Sabnees, "Secured Mobile Messaging", 2012.
[6] Prasad Reddy, P.V.G.D., K.R.Sudha and P Sanyasi Naidu, "Modified Location Dependent Encryption for Mobile Information System", 2010.
[7] D.Lisonck and M.Drahansky, "SMS encryption for mobile communication",International conference on security technology Hainan Island ,2008.
[8] Mary Angoyi,Devrim Seral,"SMS security an asymmetric encryption approach",2010.
[9] Prsad Reddy,P.V.G.D,K.R.Sdha and S.Krishna Rao "Data Encryption technique Using Location Based Key Depandant Circular Rotation",Journal of Advance Research In Computer Engineering, 2010.
[10] A.Medai,A.Gani,O.Zakaria,A.A.Zaidan"Review of mobile short message service security issue and techniques towards solution",Scientific Research and Essay vol(6), March 2011.
[11] Geocodex,LLC,Location Based Encryption/Decryption(White Paper), June 2010.
[12] http://www.formaestudio.com/rijndaelinspector/archivos/Rijndael_Animation_v4_eng.swf
[13] Menezes, Alfred; Paul C. van Oorschot; Scott A. Vanstone (October 1996). Handbook of Applied Cryptography. CRC Press. ISBN 0-8493-8523-7.
[14] Cormen, Thomas H.; Charles E. Leiserson; Ronald L. Rivest; Clifford Stein (2001). Introduction to Algorithms (2e ed.). MIT Press and McGraw-Hill. pp. 881–887. ISBN 0-262-03293-7.

AUTHOR DETAILS

Dr. S. M. Chaware HOD of Computer Engineering Department, Bhivarabai Sawant College Of Engineering And Research, Pune.
Shraddha Badade Computer Engineering, Bhivarabai Sawant College Of Engineering And Research, Pune.
Rasika Borate Computer Engineering, Bhivarabai Sawant College Of Engineering And Research, Pune.
Sayali Dhobale Computer Engineering, Bhivarabai Sawant College Of Engineering And Research, Pune.
Pooja Ghogare Computer Engineering, Bhivarabai Sawant College Of Engineering And Research, Pune.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY