IJNRD.ORG ISSN : 2456-4184
International Research Journal IJNRD Research Through Innovation
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

Android Based SMS Encryption System

Arivazhagan S[1], Potturi Naveen[2], Pradeep Kumar R[3]

1Student, Dept. of Computer Science Engineering, Dr.M.G.R Educational and Research Institute, Chennai, Tamilnadu, India

2Student, Dept. of Computer Science Engineering, Dr.M.G.R Educational and Research Institute, Chennai, Tamilnadu, India

3Student, Dept. of Computer Science Engineering, Dr.M.G.R Educational and Research Institute, Chennai, Tamilnadu, India

Abstract- This is an advanced Encryption and decryption System targeting SMS for Android Users both go and fro. The User will send an message which is encrypted while the other can decrypt the message sent. The System makes use of the SMS that you see in the inbox, but this system filters out the ones which are encrypted and show it in their Personal Inbox in the Application. So when someone want to send an message one should know the other persons address and send the messages so that when one person login to account every msg is visible in encrypted statge. The Id is Auto-generated and cannot be changed but for the user's ease, the system allows the user to save the recipient’s id in a separate column as Favorites saving his Id, Name and Mobile No. Login is a mandatory function as one can as many accounts he need to differentiate them it is used. This System makes use of the AES Encryption Algorithm to encrypt and decrypt the messages. This App uses Android Studio as its front end and SQLite as its back end functions.

Keywords-AES, Android,Decryption,Encryption

I. Introduction

Securing encrypted and decrypted information using Cryptography and Steganography techniques. Due to recent developments in steganography analysis, providing security to personal contents, messages, or digital images using steganography has become difficult. By using steganography analysis, one can easily reveal the existence of hidden information in carrier files. This project introduces a novel steganography approach for communication between two private parties. The approach introduced in this project makes use of both steganography as well as cryptographic techniques. In Cryptography we are using RSA. In Steganography we use Image Steganography for hiding the data. And we also use the Mutual Authentication process to satisfy all services in Cryptography i.e., Access Control, Confidentiality, Integrity, and Authentication. In this way, we can maintain the data more securely. Since we use the RSA algorithm for securing the data and again on we perform Steganography to hide the data in an image. Such that any other person in the network cannot access the data present in the network. Only the sender and receiver can retrieve the message from the data.

II. PROBLEM STATEMENT

For data security an individual is more responsible . How the user handles his credential is important in data security. If the user is aware and keeps his credential and device safe from any attacker then the data in the device is safe. But if the device is stolen or an attacker gets the credential for the application then it creates a security risk. These days, everyone is using encryption and decryption. But it has some features missing like controlling the encryption and decryption. In order to facilitate these functions, we are developing an app that gives users control over encryption and decryption, and they can decide when to encrypt and when to decrypt at their own pace.

III. EXISTING SYSTEM

The problem with the existing System is that mailing or messaging is done through the browser by using services like Hotmail, Yahoo, Google, etc. These systems use HTTP port 80 to access the emails, and the overall procedure here is not safe to send confidential messages. This existing system can be easily hacked by hackers, some data may be modified or even lost..

Disadvantages:

- The user has to log in from his phone to decrypt the messages.
- If the user deletes the message from his phone’s default app or inbox, it will be reflected on the current system also**.**

IV. PROPOSED SYSTEM

In this project, message entered is encrypted by the application and its is decrypted by clicking on decrypt option to see the original text. Users communicate overall on social media, but messages aren't secured when it passes through the network. Intruders can access the user's message easily. We want to secure users' communication overall social media. So here we proposed a system where the user will enter the plain text and choose the algorithm type from AES and supply the key, a chipper text is going to be formed which will be sent via any communication application and the user can decrypt the text by selecting an equivalent algorithm type and must enter an equivalent sender secret key. Users can use our application and may enter the plain text and must select the algorithm type and must enter the key to encrypt the message, receiver can decrypt the message by specifying an equivalent algorithm used for encryption and must use an equivalent secret key employed by the sender. An intruder will find it difficult to decrypt the message. By using this method you'll double make sure that your secret message is shipped securely without outside interference from hackers or crackers.

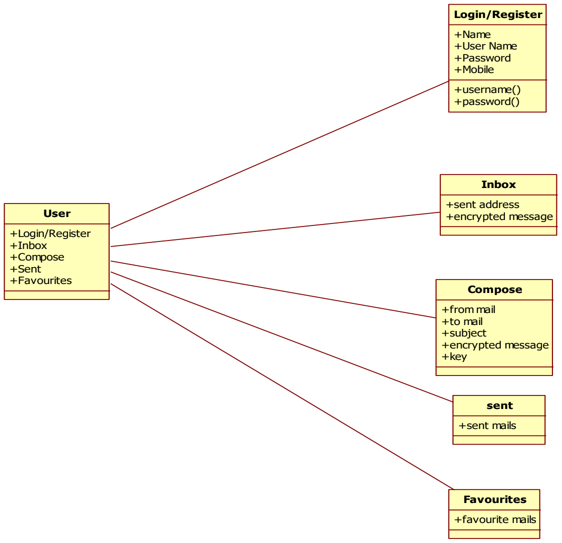
Advantages:

- The user has to log in to keep the data secure.
- The Messages are already decrypted for you.
- The system also allows you to save recipient details which can be accessed only by the user.
- The app makes a difference for encrypted ones and non encrypted .
- Fast and Easy to use.
- No Internet Needed.
- It is highly reliable and secure.
- As only encrypted messages are seen so the previous will are also takes less time while loading .

V. SYSTEM ANALYSIS

MODULES:

- Registration: The user has to register himself into the system to generate the unique id.
- Login: The user has to login into the system providing his username and password keeping all the data secure.
- Inbox: The user gets to see a list of messages which were encrypted and only sent to him i.e. To his account. The inbox will only have the senders name and date/time.
- Message: The user is allowed to view the complete message which is already decrypted as he selects the messages from the inbox.
- Favorites: As the recipient's id is difficult to keep in mind the system allows the user to save the recipients id, name and mobile number for future messages.
- Send message: The user can send messages which will be encrypted once he sends it, here the user should add mobile number and the receipts id or he can make use of the data saved in favorites.
- Sent: The user can view the messages that he has sent i.e. Only the encrypted ones in the sent folder..



APPENDIX

Appendixes, if needed, appear before the acknowledgment.

CONCLUSION

In this project, we deal with the concepts of security of digital data communication across the network. This project is designed for combining steganography and cryptography features for better performance. We performed a new steganography method and combined it with AES Algorithm. The data is hidden in the text format so there will be no chance for the attacker to know that data is being hidden in the text. We performed our method on a text by implementing a program written in Java language. The method proposed has proved successful in hiding various types of text messages. We concluded that in our method the AES and DES are better. Because of their high capacity. This work presents a scheme that can transmit large quantities of secret information and provides secure communication between two private parties.

REFERENCES

[1] Fang Yuan, Guang-Yi Wang, Bo-Zhen Cai. Android SMS Encryption System Based on Chaos. IEEE 2015.

[2] N. K. Pareek, V. Patidar, and K. K. Sud. Image encryption using chaotic logistic maps. Image Vision Comput. 2006, 24, 926-934.

[3] H. S. Kwok, K. Wallace, and S. Tang. A fast image encryption system based on chaotic maps with finite precision representation. Chaos, Solitons and Fractals, 2007, 32, 1518-1529.

[4] Yicong Zhou, Long Bao, C. L. Philip Chen. A new 10 chaotic system for image encryption[J]. Signal Processing, 2014 (97), 172-182.

[5] Zhang Ying-Qian, Wang Xing-Yuan. A symmetric image encryption algorithm based on mixed linear-nonlinear coupled map lattice [.I]. Information Sciences, 2014: 1-23.

[6] Pan Bo, Feng Jinfu Tao Qian, et al. Image Encryption Communication Scheme Based on Clifford Map and Additive Modular Arithmetic[J]. Computer Science, 2009,36(8):273-27.