Magic Box: An Algorithmic Technique for Ensuring Security and Privacy of End User Data and Device on Social Network

Shivaprasad Jakkan[1] , Ajit Patil[2] , Suyog Mankar[3] , Shital Tarange[4]
Department of Information Technology
[1,2,3,4] All India Shri Shivaji Memorial Society's Institute of Information Technology, Pune
Savitribai Phule Pune University, Pune, Maharashtra India

Abstract- *The acceptance and widespread use of internet connects you to millions of other people and organizations located throughout the world with the help of various types of electronic gadgets. It allows individuals to stay connected with one another from almost anywhere at any time, while this has resulted in increased productivity for individual and for the groups and organizations. So the information security has become a very critical aspect of modern computing system during this end user communication. The users like business and organizations worldwide are suffering from a constant threat from hackers and attackers, who use a variety of techniques and tools in order to track computer system, steal information, modify data and cause havoc. Thus, securing information exchanged over the internet has become one of the major issues. The existing system provides security during communication of senders and receivers using encryption techniques and digital signature but privacy and confidentiality are still compromised. It proves that the data is still insecure on the end device. The proposed system ensures privacy as well as security of end devices using a 'Magic Box' algorithm. This algorithm transform the simple readable message into some another garbage message where only the authorized users can have access to the original readable message. Thus, data which was previously disclosed on end device is secured and ultimately confidentiality, privacy and security of data are ensured.*

Keywords- Social Network, Security and Privacy of Data and Device, Asymmetric key cryptography, RSA

I. INTRODUCTION

Now a day, everyone is surrounded with smart devices like laptop, smart phones, tablets computers, etc. Everything is completely digitized and online. And here internet comes in the picture. And internet has changed the complete picture in last few decades. Humans are getting replaced with machines to do work. Because of this replacement, human errors are reduced to getter extent. Every single work can be done on internet. People are sending mails electronically, doing shopping, using internet banking and many more.

Social networking or media is one of the rapidly growing subjects in today's scenario. People are so influenced with social networking applications like Facebook, what's app, twitter, hike and many more. People are exchanging uncountable information or data in every single minute. But protecting the information exchanged over internet has become one of the major issues. And undoubtedly such sensitive information can be misused by hackers in the cyber world.

Existing system provides security to the information by various encryption techniques. But this security is provided in network or network link between the sender and receiver. But the information is still unsecured on end devices used by the users. Proposed system ensures the security of the information on end devices by using magic-box algorithm. This algorithm takes the user's message as input to it and transforms it into some meaningful sentence. In this way, the original message is transformed by another text which seems to be the original message and ultimately information which was previously disclosed on the end devices is protected.

II. RELATED WORK

Talking about current affairs, it is very necessary to have a focus on security and privacy of user data and device on social network. People are exchanging huge data in every single minute. Increase in the amount of shared information will also increase the chance of exposure to information leakage risks. Hackers are always one step ahead of security specialists. They always misuse confidential information like the texts, photos, files and videos shared by the users on the online social networking site.

It is the practice of preventing unauthorized access, use, disclosure, disruption, modification, inspection, recording or destruction of information. It is a general term that can be used regardless of the form the data may take. Sometimes referred to as computer security, information technology security is information security applied to technology (most often some form of computer system). It is worthwhile to note that a computer does not necessarily mean a home desktop. A

computer is any device with a processor and some memory. A cryptographic technique ensures security of the information on computers.

Social networking becomes increasingly important due to the recent surge in online interaction. Due to popularity of using online social networks the security threats to the users of these networks also increased dramatically. However, sharing these interests online and using them without considering the security factor can lead a user to become victim of a hacker. [7]

The real growth of social networking is people can store and share their data through online. [1] By sharing the photos, chatting with friends or by sharing personal records for verification. Social networks are getting more and more popular with time. As people use these technologies, the only anxiety is about security of information exchanged on these networks.

Messaging and SMS (simple message service) has become one of the fastest and strong communication channels to transmit the information across the worldwide [2]. Sometimes, [3] we send the confidential information like password, pass code, banking details and private identity to our friends, family members and service providers using social networking sites. Securing these messages during transit is one of the most important factor. [3] The Blowfish encryption algorithm gives confidentiality to the message, the Easy SMS protocol is used to gain authentication and MD5 hashing algorithm helps to achieve integrity of the messages. Blowfish algorithm utilizes only less battery power when compared to other encryption algorithms. The protocol prevents various attacks, including SMS disclosure, replay attack, man-in-the middle attack and over the air modification. Existing system provides security in network layer and message during transit.

Existing social networking applications provides security during transmission of message but this exchanged information is still exposed on end devices [5]. Existing systems provides network layer security [1] (Easy SMS paper) Whereas Babel Crypt system [6] (babel crypt paper) addresses the problem of interface level security on chatting application. Proposed algorithm ensures privacy and security on application layer and ensures security of information on interface of application. Algorithm supports encryption of different formats of files, text and images [4]. It works on different operating systems and social networks. As algorithm never discloses the cipher anywhere in the application, intruder would never come to know that the messages were encrypted. Which makes it secure and ultimately it ensures privacy.

III. METHODOLOGY

First sender types his message into the text field of application. Then before sending this message into the network this input is given to the magic box algorithm and this message is first encrypted and then it is masked with some another text and send into the network. When message reaches to receiver, the application still displays the message in encrypted form and only decrypts if user wants to do so.

For encryption, given input to the algorithm is first copied into the array, later the contents of array are reversed and binary equivalent is calculated. Then the key which is generated by self-organizing map algorithm is again converted into binary and XORed with binary equivalent of reversed string. Then reversed content is given as input to the function. In function the actual message or data is converted into unintelligible data. And it is further converted into binary and it is XORed with output of previous XOR. Then result is again XORed with key and final Cipher Text is generated. The reverse process is done for decryption.

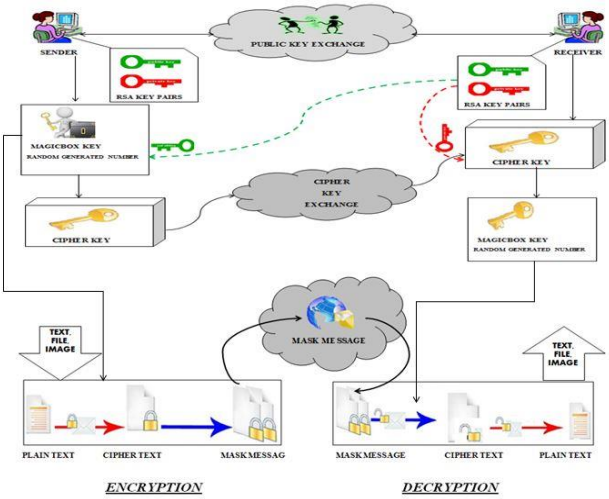

Figure System Architecture

The methodologies in the project are:

A. Key Exchange
B. Text encryption and decryption
C. File Encryption and Decryption
D. Image Encryption and decryption

A. KEY EXCHANGE

The asymmetric key cryptography involves the use of two distinct but related keys namely, the public key and the private key. Only public keys of both sender and receiver are exchanged. The public key used for authentication to ensure

that the message is coming from the intended sender. Public key cryptosystem also ensures confidentiality.

Communication of messages can be done in a secure manner since knowledge of the public key is not sufficient to decrypt the cipher text. So we follow the asymmetric key cryptography technique in our proposed system.

RSA was first described in 1977 by Ron Rivest, Adi Shamir and Leonard Adleman. Public-key cryptography, also known as asymmetric cryptography, uses two different but mathematically linked keys, one public and one private. The public key can be shared with everyone, whereas the private key must be kept secret. In RSA cryptography, both the public and the private keys can encrypt a message; the opposite key from the one used to encrypt a message is used to decrypt it. This attribute is one reason why RSA has become the most widely used asymmetric algorithm: It provides a method of assuring the confidentiality, integrity, authenticity and non-reputability of electronic communications and data storage.

If these keys are exposed then confidentiality and integrity may loss, so we are encrypting these keys again and then sending to other side. Random generated number is send to magicbox as a key for encryption of messages. Random generated number is also encrypted with RSA algorithm using receiver's public key and this encrypted key is send to receiver. At the receiver side this cipher key is decrypted with RSA algorithm using its own private key to get original random number and send to the magicbox as a key for decryption of messages.

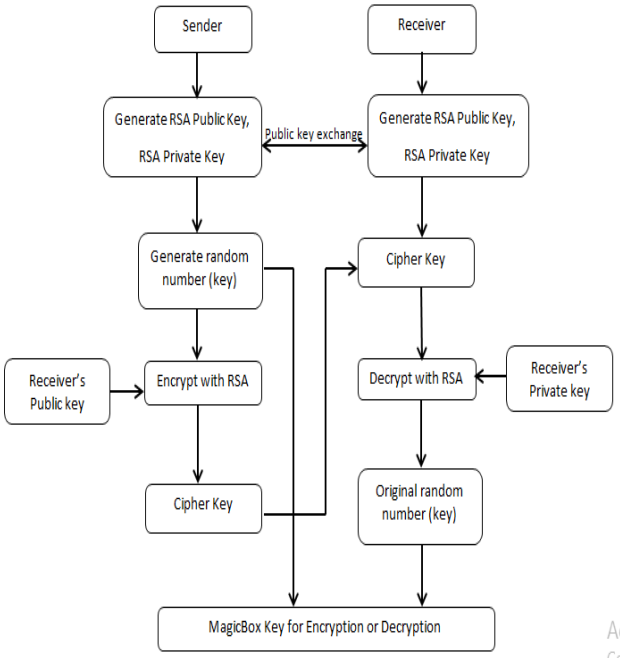

Figure Key Generation and Transmission

B. TEXT ENCRYPTION AND DECRYPTION

This module includes the encryption and decryption of text. This module will be used in chat application where user will enter message to send and that message will be encrypted with our algorithm and that encrypted message will be sent to receiver, and similarly on receiver end the massage will be decrypted and original message is shown to the receiver. This module is also used to encrypt the key which will store of file and further used for encryption and decryption of messages.

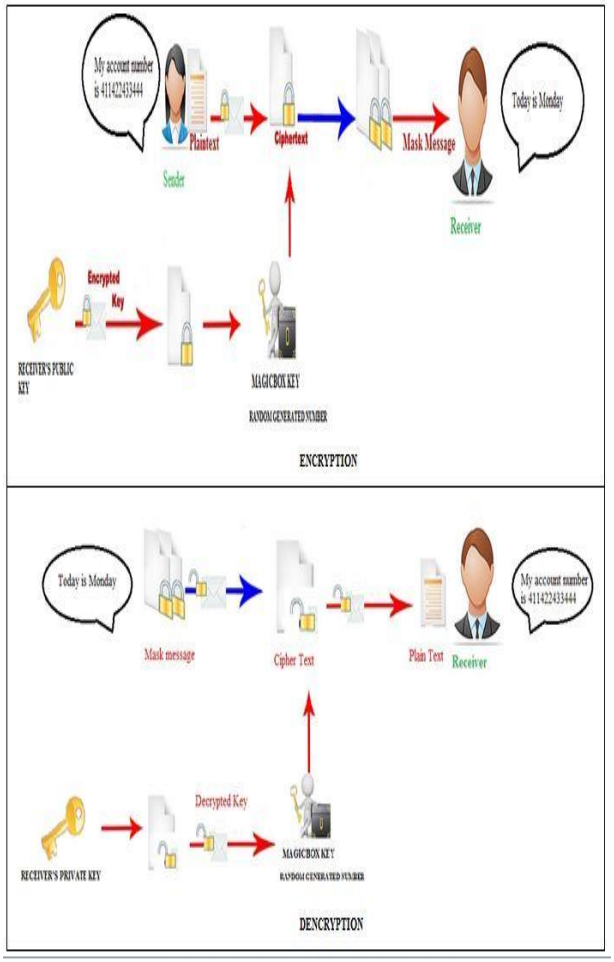

Figure Text Encryption and Decryption

C. FILE ENCRYPTION AND DECRYPTION

In this module encryption and decryption of file like text file and word file will be done. First the user will be asked to select the file which is to be encrypted, then selected file will be converted into binary and further it will be given to our algorithm and result which is obtained from algorithm is again written to the and finally file will be locked and extension will be changed. Hence unauthorized user cannot read or access the file without decrypting that file. And reverse process will be carried for decryption of file.

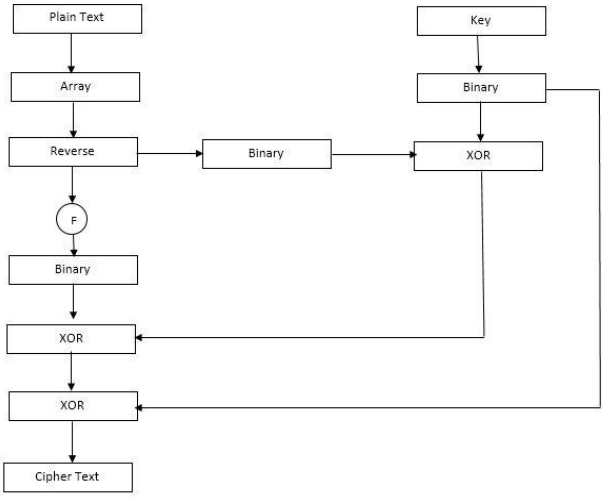

Figure Process of Encryption

D. IMAGE ENCRYPTION AND DECRYPTION

Working of this module is same as file and text encryption. First user will have asked to select image and that complete image is converted into binary and that binary value will be given as input to our algorithm. And results will be written to file and that file will be locked and extension is changed. And reverse process is done for decryption of image.

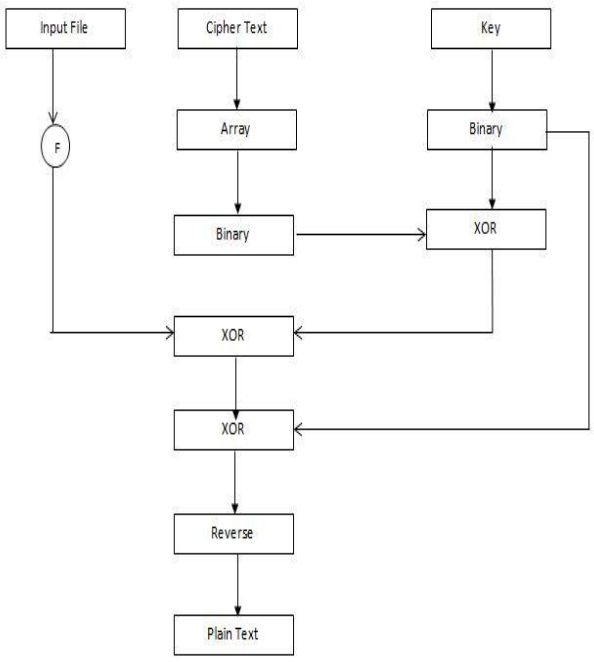

Figure Process of Decryption

IV. CONCLUSIONS

The theoretical conclusion is that the proposed system ensures privacy as well as security of end devices using a 'Magic Box' algorithm. This algorithm transform the simple readable message into some another readable message where only the authorized users can have access to the original readable message. Thus, data which may be disclose on end device is secured and ultimately confidentiality, privacy and security of data are ensured. We wish to apply Magic Box algorithm for video encryption and decryption. As well as to improve the password mechanism in proposed system by using voice recognition mechanism.

REFERENCES

[1] Neetesh Saxena,"EasySMS: A Protocol for End-to-End Secure Transmission of SMS", IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 9, NO. 7, JULY 2014

[2] Ekiti State University, Ado-Ekiti, Ekiti State Nigeria , "A Manipulated Cyclic Permutation Data Scrambling Approach for Data Security", International Journal of Science and Research (IJSR).

[3] Minta Thomas, Panchami V," An Encryption Protocol for End-to-end Secure Transmission of SMS" , 2015 International Conference on Circuit, Power and Computing Technologies [ICCPCT].

[4] Minati Mishra, Brojo Kishore Mishra," Secret Communication through Information Camouflaging in the Mimesis and the Crypsis way",2016 International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT)

[5] Technical white paper," WhatsApp Encryption Overview", 2016.

[6] Ahmet, Can Gemicioglu, Kaan Onarlioglu,Michael Weissbacher, Collin Mulliner, William Robertson, and Engin Kirda," BabelCrypt: The Universal Encryption Layer for Mobile Messaging Applications"

[7] Amirmohammad Sadeghian, Mazdak Zamani, Bharanidharan Shanmugam," Security Threats in Online Social Networks." Published in: Informatics and Creative Multimedia (ICICM), 2013 International Conference on 4-6th September 2013.

[8] Calvin Li, Daniel Sanchez, Sean Hua, "WhatsApp Security Paper Analysis" , https://www.whatsapp.com/security/WhatsApp-Security, Apr 5, 2016

[9] Rohit Minni, Kaushal Sultania, Saurabh Mishra, "An Algorithm to Enhance Security in RSA", IEEE - 31661 4th ICCCNT 2013 July 4-6, 2013, Tiruchengode, India.