ISSN (Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 1, January 2018

Survey Paper on Android Based Encrypted Message System

Vrushali Rajendra Sonar[1], Yash Uttam Semlani[2], Maaz Ahmed Munir Ahmed Shaikh[2] ,
Zeeshan Ansar Pawar[2], Rohit Manohar Saggam[2]

Guide, Department of Computer Engineering, AISSMS Polytechnic, Pune, India[1]

Student, Department of Computer Engineering, AISSMS Polytechnic, Pune, India [2]

ABSTRACT:-The ubiquitous use of wireless networks has significantly changed our lifestyle. Along with great comfort and efficiency, there are new challenges in the protection of confidential and / or private data contained in dispositive. The most difficult part lies in a dilemma: must be computationally unfeasible for opponents to decrypt data, the cryptographic operation should be effective for legitimate users and minimize the drainage of the battery. This paper proposes a new scheme of encryption and storage of address this challenge. In our system one user can upload any file to the system in the encrypted format or we can send any message to user.When any user want to that file/message user can enter the otp and the decrypted key to related that file,so user can easily view or download that file. Treat the data as a binary bit our encryption scheme (SE) generates a flow of by random bit extraction of current. The length of the Key stream depends on the user's security requirements. The bit is encrypted and encrypted text is stored in the mobile device, while the key stream is stored separately. This makes it computationally impossible to retrieve the original data stream of encrypted only.

KEYWORDS: Android, Encryption Scheme, Mobile Device.

I. INTRODUCTION

Mobile devices have become popular in the community for the ease it provides to the user, it's not only a way of communication but a technology which can help to store, transfer data. Important aspect which we cannot neglect is m-commerce which is now getting a hike in business. All of these benefits have raised the chances of theft to the devices and the data stored in it. Security has become great concern to the users as well as business which make use of such devices. The Encryption Scheme for Data Security in Mobile Devices was introduced in their paper they have investigated whether it is possible to implement a lightweight encryption algorithm which provides data confidentiality by exploiting the availability of a secure connection with a central server. The server is used to store a small amount of data, required to decrypt the confidential information. In case of loss of the device, the access to the company server is temporarily revoked. In our system one user can upload any file to the system in the encrypted format or we can send any message to user.When any user want to that file/message user can enter the otp and the decrypted key to related that file,so user can easily view or download that file.So we can easily maintain the security.

II.MOTIVATION

This system used maintain secure data. Send the file/message in the form encrypted form.Data should be accessed only authorized person only.

ISSN (Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 1, January 2018

III . LITERATURE SURVEY

D. Roselin, Selvarani and Dr. T. N. Ravi have introduced A Review on the role of Encryption in Mobile Database Security technique protection of data against accidental or intentional loss. limitations of resource constraint mobile Devices [1] Bhagat.A.R Prof. Bhagat.V.B have introduced mobile database review and security aspects concepts in that systems is the provision of sufficient security and privacy guarantees for the user data. Security need to improve[2]C. Galdi, A. Del Sorbo, and G. Persiano have introduced distributed certified information access for mobile devices techniques it is possible to securely distribute the load of the most time-consuming operations among a set of untrusted peers. For that sytem,Need more secure services for mobile device[3] Y. Jiang, C. Lin, M. Shi, and X. Shen have introduced The scheme offers the capability of multiple key sharing and distribution for current and future application scenarios, and a threshold mechanism that effectively improves flexibility and robustness of the key sharing and distribution process. For that processNeed more forward and backword secrecy techniques[4] V. Kher and Y. Kim have introduced Challenges, Techniques, and Systems for distributed system The main advantage of SIDS (running directly on the storage server or on the disk firmware) as compared to host-based IDS is that an intruder having full access to the host can disable a host-based IDS, whereas a SIDS can still continue to function properly and are independent of host (or OS) compromise. Need to more authentication[5] A. J. Nicholson, M. D. Corner, and B. D. Noble have introduced Mobile Device Security Using Transient Authentication system for This improves performance while still guaranteeing file keys are never exposed when the user is absent. This system need to improve cryptographic controls[6] P. E. Sevinc, M. Strasser, and D. Basin have introduced the Securing the Distribution and Storage of Secrets with Trusted Platform Modules system a protocol for securely distributing and storing secrets with TPMs. We specify the protocol in detail at the level of TPM commands and we informally analyze its security .Storage security id less[7] E. Zenner have study about Why IV Setup for Stream Ciphers is Difficult This means that in addition to choosing messages (which is not an advantage in our narrow stream cipher model), the adversary also is allowed to choose the IV that is used for the encryption, as long as he does not request the same IV twice (nonce-respecting adversary). In addition, general-purpose hash functions have the disadvantage that they might be more inefficient than required for our purposes[8]

IV.SCOPE AND OBJECTIVES

Scope:-
Protect data or message in mobile with encrypted form. Original data cannot with authorized person.

Objective:-
To maintain data securely for authorized user. To maintain data confidentiality of user data. To inform data owner about his stored data is secure or not. To protect data in mobile with encrypted form.

V.EXISTING SYSTEM

Lack of effective protection of confidential data on mobile devices it is an important concern that prevents mobile devices to be widely used as part of the networks personal area networks. The Encryption system proposed removes the barrier and allow employees to enjoy efficiency and convenience that mobile devices bring. That will lead to another prosperous valley of wireless networks and ubiquitous information. Physical attacks have proven to be effective in breaking some well-designed figures in practice. In existing system user can send any file or message in which can in general format, so anybody can easily read that file or message easily. So in this system, we cannot maintain the security of the system. Anybody can easily hack message or file, so this system is less secure.

ISSN (Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 1, January 2018

VI.PROPOSED SYSTEM APPROACH

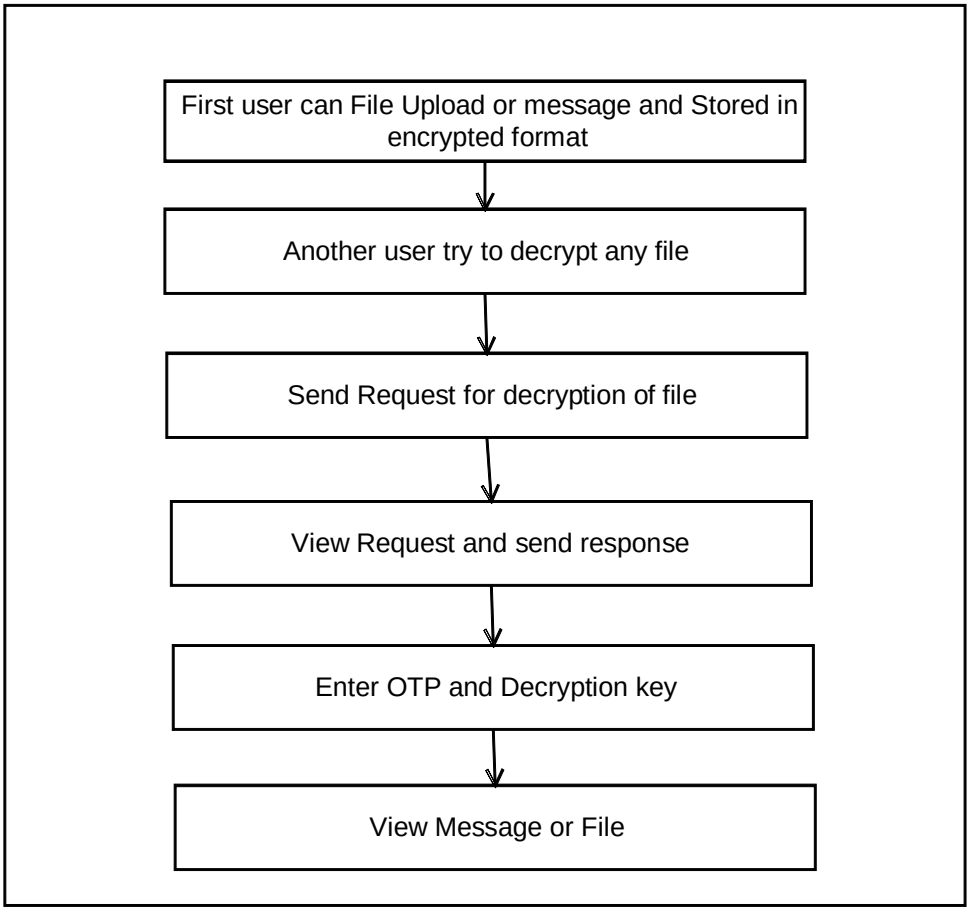


Fig.Architecture of Proposed System

Proposes a novel data encryption and storage scheme to address this challenge. Treating the data as a binary bit stream, our Encryption scheme generates a key stream by randomly extracting bits from the stream. The length of the key stream depends on the user's security requirements. The bit stream is encrypted and the cipher text is stored on the mobile device, whereas the key stream is stored separately. This makes it computationally not feasible to recover the original data stream from the cipher text alone. We are using one time key for decrypt data as well as session key generation technique. In our system when one user can send the message or file to the other person ,in an encrypted format. If another user can read that message or file, request for key for decrypt data to encrypted by authorized user, then this generate one time key generate.After entering that otp and key user can easily decrypt any file.

ISSN (Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 1, January 2018

VII.COMPARATIVE RESULTS

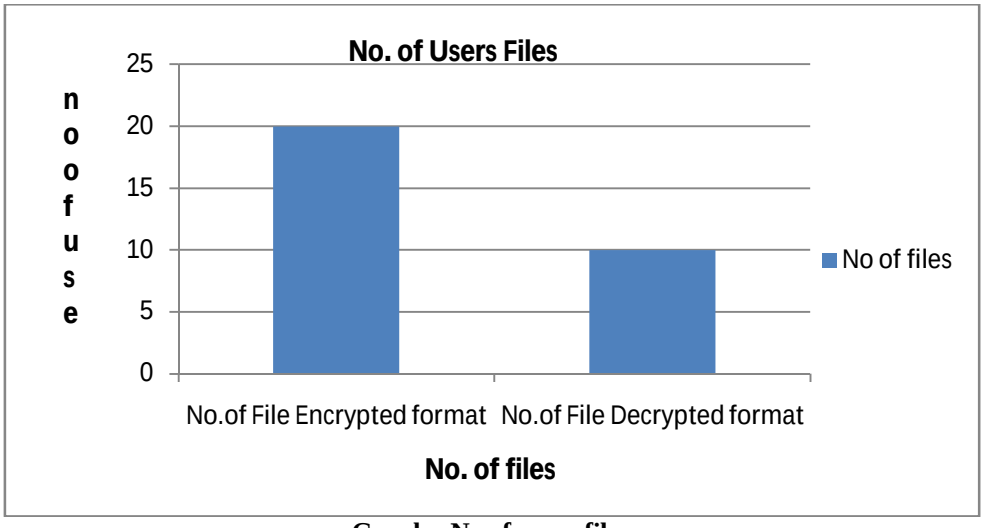
In our experimental setup, In table 1, find out number of message or file uploaded in encrypted format and message or file decrypted .In our experimental setup, in our system number message or file upload in encrypted format and number message or file decrypted.

Sr. No	Number of Message or File Upload in Encrypted format	Number of Message or File in Decrypted format
1	20	10

Table1: No. Upload and download Message or file

VIII.RESULTS

From above data, In graph 1,we can see the no. of file upload in encrypted format by 1 user and no of file decrypt in the graph; we see 20 files upload user and 10 users are decrypt the file in the graph.



Graph :No of users files

IX. CONCLUSION

Lack of effective protection of confidential data on mobile devices it is an important concern that prevents mobile devices to be widely used as part of the networks personal area networks. The Encryption system proposed removes the barrier and allows employees to enjoy efficiency and convenience that mobile devices bring. That will lead to another prosperous valley of wireless networks and ubiquitous information. One person can send the message or file to another person in encrypted format. After checking proper authentication and correct OTP another person can easily decrypt that file. Physical attacks have proven to be effective in breaking some well-designed figures in practice. Unfortunately, challenging designers to investigate theoretically of a cryptographic system against various attacks. To solve this problem, it will be a prototype implemented on top of reconfigurable hardware devices (i.e., FPGA). In particular we

ISSN (Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 1, January 2018

will study the behavior of our SE prototype under local non-invasive attacks, including time analysis and analysis of differential power (DPA).

REFERENCES

[1]J. Al-Muhtadi, D. Mickunas, and R. Campbell, "A Lightweight Reconfigurable Security Mechanism for 3G/4G Mobile Devices," *IEEE Wireless Communications*, April 2002.
[2]C. Galdi, A. Del Sorbo, and G. Persiano, "DistributedCertified Information Access for Mobile Devices," *Workshop in Information Security Theory and Practices*(WISTP'07), Crete, Greece, May 8-11, 2007.
[3]Y. Jiang, C. Lin, M. Shi, and X. Shen, "Multiple Key Sharing and Distribution Scheme with (n, t) Threshold for NEMO Group Communications," *IEEE Journal on Selected Areas in Communications*, Vol. 24, No. 9, Sep. 2006.
[4]V. Kher and Y. Kim, "Securing Distributed Storage: Challenges, Techniques, and Systems," *StorageSS'05*,Fairfax, Virginia, USA, Nov. 11, 2005.
[5]S. Rafaeli and D. Hutchison, "A Survey of Key Management for Secure Group Communication," *ACM Computing Surveys*, Vol. 35, Issue 3, Sept. 2003.
[6]A. J.Nicholson, M. D. Corner, and B. D. Noble, "Mobile Device Security Using Transient Authentication," *IEEE Transactions on Mobile Computing*, vol. 5, no. 11, pp. 1489-1502, Nov., 2006.
[7]P. E. Sevinc, M. Strasser, and D. Basin, "Securing the Distribution and Storage of Secrets with Trusted Platform Modules," *Workshop in Information Security Theory and Practices* (WISTP'07), Crete, Greece, May 8-11, 2007.
[8]E. Zenner, "Why IV Setup for Stream Ciphers is Difficult," in *Proceedings of Dagstuhl Seminar on Symmetric Cryptography*, Jan. 2007.