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. 8, Issue 2, February 2019

Mobile Self Encryption System

Viraj Jagtap[1], Tushar Ingale[1], Vaibhav Walke[1], Sahil Satpute[1], A. S.Khandagale[2]

Diploma Students, Department of Information Technology, A.I.S.S.M.S Polytechnic, College of Engineering Pune, Maharashtra, India[1]

Professor, Department of Information Technology, A.I.S.S.M.S Polytechnic, College of Engineering, Pune, Maharashtra, India[2]

ABSTRACT: On web user stored there data on server. The data will be in different form. The stored data need to be stored on server in secure format in a way that no one can recognize that data. Proposed system store user data from mobile to server and for security data will be encrypted form and while at the time of data access user have to enter OTP and decryption key then only user will get the file.The key and OTP will get on user's second mobile no. that is given at the time of registration. If key matched user will get decrypted file.If user mobile device is lost then there is no issue to access stored data on server. User will get file from anywhere. Proposed system increase data security for user's mobile data.The proposed system is developed in Android platform.

KEYWORDS: AES, Data security, Mobile devices,Self Encryption,.

I. INTRODUCTION

1.1 BACKGROUND

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 Self-Encryption (SE) 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.Portability makes mobile devices prone to being stolen or lost. It is very challenging to protect the weakly encrypted information on a mobile device, which might end up in the hands of an adversary, who could then use powerful cryptanalysis tools to break the encryption. Therefore, security solutions developed for general distributed data storage systems cannot be adopted directly for this new frontier.

1.2 MOTIVATION:

In existing system presented security issues of Mobile database system as well as Mobile network and discussed the solutions for it. They classified the security issues in four different areas such as Security of mobile device, security of operating system on mobile device, security of mobile database and security of mobile network. They also identified a set of vulnerabilities on mobile database and provided some techniques to decrease the side effect of vulnerability of mobile database

II. REVIEW OF LITERATURE

1."**Role of Encryption in Mobile Database Security", D. RoselinSelvarani and Dr. T. N. Ravi Volume 3, Issue 12, December 2014** In this paper the authors presented security issues of Mobile database system as well as Mobile network and discussed the solutions for it. They classified the security issues in four different areas such as Security of

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. 8, Issue 2, February 2019

mobile device, security of operating system on mobile device, security of mobile database and security of mobile network. They also identified a set of vulnerabilities on mobile database and provided some techniques to decrease the side effect of vulnerability of mobile database [12].

2. **Mobile Database Review andSecurity Aspects" Bhagat.A.R Prof. Bhagat.V.B, JCSMC,Vol. 3, Issue. 3,March2014, pg.11741182** In a mobile database application a part or a replica of the database is locally installed on the mobile device. This is a significant difference compared to a conventional client-server application where all data is centrally stored in a database server. The approach with a mobile database provides the necessary autonomy to the mobile device to work independently from the central database. The client application can work with the mobile database asynchronously, and needs to connect to the central database only when it is necessary to synchronize. This approach has several advantages compared to a conventional approach where the clients do not use local storage[11].

3. **"Distributed Certified information Access for Mobile Devices,"** C. Galdi, A. Del Sorbo, and G. Persiano, *Workshop in Information Security Theory and Practices*(WISTP'07), Crete, Greece, May 8-11, 2007. this paper we describe a primitive, which we call, Certified Information Access, in which a database answers to a query by providing the information matching the query along with a proof that such information are consistent with the actual content of the database.Adv:-We have shown that it is possible to securely distribute theload of the most time-consuming operations among a set of Untrusted peers[2].

4. **"Multiple Key Sharing and Distribution Scheme with (n, t) Threshold for NEMO Group Communications,"** Y. Jiang, C. Lin, M. Shi, and X. Shen, *IEEE Journal on Selected Areas in Communications*, Vol. 24, No. 9, Sep. 2006.**In this paper, a novel secure key** sharing and distribution scheme for network mobility (NEMO) group communications
is proposed. 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. Both forward and backward secrecy are guaranteed by compulsive key refreshment and automatic key refreshment mechanisms,
which provide dynamic in-progress group communication joining/ leaving and periodic keys renewal, respectively**.** Adv:- 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. Adv:- 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[3].

5. **"Securing Distributed Storage: Challenges, Techniques, and Systems,"** V. Kher and Y. Kim *StorageSS'05*,Fairfax, Virginia, USA, Nov. 11, 2005The rapid increase of sensitive data and the growing number of government regulations that require long-term data retention and protection have forced enterprises to pay serious attention to storage security. In this paper, we discuss important security issues related to storage and present a comprehensive survey of the security services provided by the existing storage systems 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 [4].

III. SYSTEM OVERVIEW

Proposes a novel data encryption and storage scheme to address this challenge. Treating the data as a binary bit stream, our self-encryption (SE) scheme generates a key stream by randomly extracting bits from the stream. The proposed system user store his mobile data file on server that will be in encrypted format. When user want to download the file that time user have to enter OTP if OTP matches then user will get decryption key on second mobile no. of user if user enters that key and key matched then file will download.

Advantages:

1An unauthorized user try to access data with key then he/she first send request for key to decryptdata.

2. Data stored on server so user will get anywhere that 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. 8, Issue 2, February 2019

3. If mobile lost key and OTP will send on another mb.

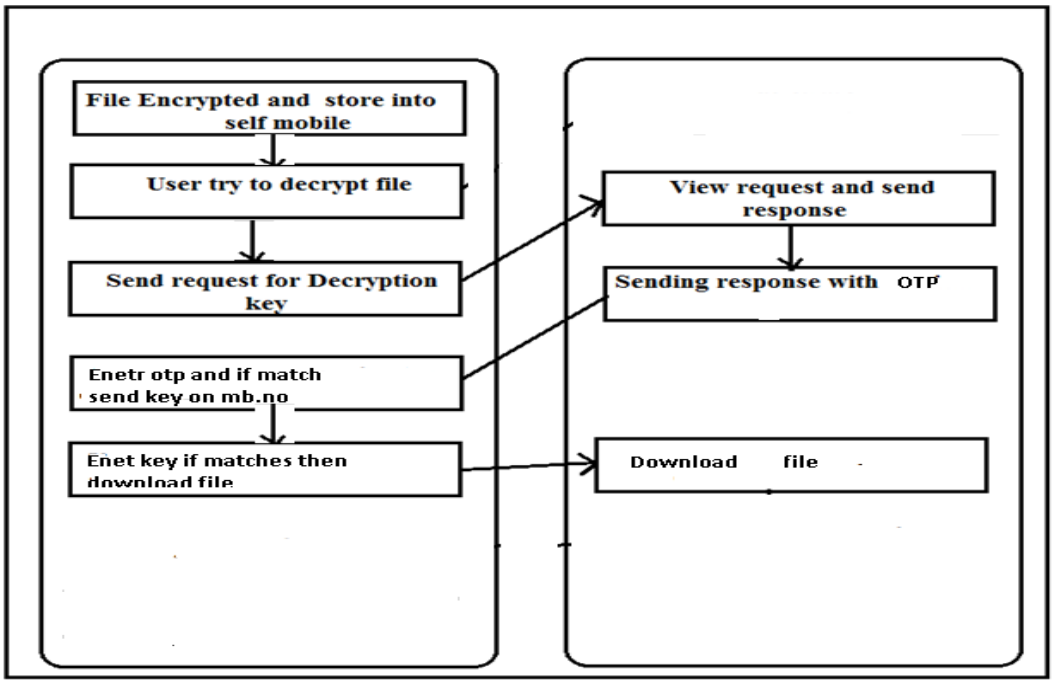

Fig. 01 System architecture

IV. ALGORITHMS

Algorithm 1: Advanced Encryption standard.

Encryption:
step 1:128 bit data block
step 2-key expansion
step3: add round key
step4:sub byte ,shift row,mix columns ,add round key
step5:sub byte ,shift rows, add round key
step6-128 but encrypted block

Decryption:

step1-128 but encrypted block
step2-key expansion
step3-add round keys ,shiftrows,subbytes
step4-add round keys ,mix columns, shift rows ,sub bytes
step5-add round key
step6-128 bit block.

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. 8, Issue 2, February 2019

V. CONCLUSION

Present a novel scheme for storing mobile data securely on server. If in case mobile device is lost user will get secure data on another mobile number of user. User will get OTP and decryption key on second mobile number of user. User has to enter key within session time. Here stored data on cloud is in encrypted format. So no one can recognize that stored data on server.In futurepdf data will store on server from android application

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.
[9] IAMR Group of Institutions, "Security in Mobile Database Systems", Para1, May 28, 2011. Accessed : Sep. 5,
[10] A Review on the role of Encryption in Mobile Database Security,D. RoselinSelvarani
and Dr. T. N. Ravi Volume 3, Issue 12, December 2014
[11]Bhagat.A.R Prof. Bhagat.V.B,JCSMC, Vol. 3, Issue. 3,March2014, pg.1174–1182 Mobile Database Review andSecurity Aspects
[11] Mobile Database Review and Security Aspects pg.11741182 Bhagat.A.R Prof.Bhagat.V.B,JCSMC, Vol. 3, Issue. 3,March 2014
[12] A Review on the role of Encryption in Mobile Database Security, D. RoselinSelvarani and Dr. T. N. Ravi Volume 3, Issue 12, December 2014
[13]IAMR Group of Institutions, Security in Mobile Database Systems, Para1, May 28, 2011.
[14]E. Zenner, Why IV Setup for Stream Ciphers is Difficult, in Proceedings of Dagstuhl Seminar on Symmetric Cryptography, Jan. 2007.
[15] 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 (WISTP07), Crete, Greece, May 8-2011.