ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 10, October 2015

A Cloud-based System for Enhancing Security of Android Devices using Modern Encryption Standard – version II (MES-II) Algorithm: A Review

Deepika D. Agrawal[1,] Prof. Pravin Kulurkar[2]

M. Tech Research Scholar, Department of CSE, Vidarbha Institute of Technology, Nagpur, Maharashtra, India[1]

Assistant Professor, Department of CSE, Vidarbha Institute of Technology, Nagpur, Maharashtra, India[2]

ABSTRACT: The recent rapid growth of Data over the Internet through mobile devices increases security issues. Cloud data storage Security is one of the most important issue, data from Mobile are uploaded in Cloud and later used by the user as he needed. Many of the present mobile companies are already added some security features in it to enhance the quality of their product by satisfying the customer needs, still they are prone to less secure and contains some weakness. Most of the user uses mobile device which uses android application. One of the feature for securing the data by using encryption techniques, the present encryption based systems are very complex with respect to their functionality and are less secure as they are static, uniform and invariant. The objective of the proposed system is to make an mobile application which makes it specific to the user and provide the highest security level for data storage and to maintain its confidentiality by using Mobile Encryption Standard –II algorithm.
.

KEYWORDS: Android, Cloud , Confidentiality, Encryption, Security.

I. INTRODUCTION

In present era, Mobile communication plays an very vital role in daily life of people .Every person depend on the mobile phone .They have large amount of data stored in their mobile phone but due to memory space limitation we are not able to store all data in the mobile device so here the concept comes cloud which stores our data without any limitation on the internet .We can upload and download our data from mobile phone at any time using internet but as all our private data are stored somewhere in the cloud it don't assures us the security of our data. As we know that when data transferred from user into clouds means users will have to surrender the control of our Using cloud storage services is easy, but comes with its own security challenges. Do you know where your data is going? You store those files somewhere in the cloud.

Cloud storage providers have full access your data and control where it is stored. You don’t have much information about the infrastructure and the security mechanisms in place. And it might be that this storage isn’t in your country, which could cause legal concerns Sharing data everywhere has never been easier. The cloud allows you to have your files always there when you need them, no matter where you are. Upload your data to the cloud and access it from anywhere, even from your smart phone or tablet. And easily share with colleagues or partners.

The security of any data mainly depends on three goals,

1) Confidentiality: The confidentiality aspect refers to limiting the disclosure and access of information to only the people who are authorized and preventing those not authorized from accessing it. Through this method, a company

DOI: 10.15680/IJIRCCE.2015. 0310033

or organization is able to prevent highly sensitive and vital information from getting into the hand of the wrong people while still making it accessible to the right people.

2) Integrity: Integrity is another security concept that entails maintaining data in a consistent, accurate and trustworthy manner over the period in which it will be existent. In this case, one has to ensure that data is not changed in the course of a certain period. In addition, the right procedures have to be taken to ensure that unauthorized people do not alter the data.

3) Availability: The concept of availability refers to the up time maintenance of all resources and hardware. This means that all the hardware and resources one have are functional all the time. It can also involve carrying out of regular hardware repairs.

Now days, the illegal activities are increases by number of attackers. Attackers exploit the existing security infrastructure and their benefits for illegal activities. So it is very necessary to adopt the effective method to assure the security of data to make it confidential at individual level. Generally, there are two ways to guarantee user not to be destroyed: one is to encrypt user data by some popular algorithm or standards in the user mobile terminal, the another way is to provide the safety of the storage devices in the cloud by all kinds of security mechanisms such as firewalls, virtual private networks, intrusion detection system and other security policies and technical ways. But user trust himself only rather than service provider hence by encrypting the data before uploading in the cloud provides the security of data.

II. RELATED WORK

[1] Cao Wanpeng ,"Adaptive and dynamic mobile phone data encryption method", Author in this paper uses an adaptive and dynamic data encryption method to encrypt user data in the mobile phone before it is uploaded. Firstly, the adopted data encryption algorithm is not static and uniform. For each encryption, this algorithm is adaptively and dynamically selected from the algorithm set in the mobile phone encryption system. From the mobile phone's character, the detail encryption algorithm selection strategy is confirmed based on the user's mobile phone hardware information, personalization information and a pseudo-random number. Secondly, the data is rearranged with a randomly selected start position in the data before being encrypted. The start position's randomness makes the mobile phone data encryption safer. Thirdly, the rearranged data is encrypted by the selected algorithm and generated key. In this way author uses different Encryption method which possesses the higher security for data.

[2] Pratap P. Nayadkar," Automatic and Secured Backup and Restore technique in Android" In this paper, Author apply automatic as well as an encrypted backup technique for an Android device as per as security is concerned. Author uses aes algorithm for encryption and decryption purpose to enhance the security of android devices.

[3] Somdip Dey, Asoke Nath," Modern Encryption Standard (MES) Version-I: An Advanced Cryptographic Method", Author in this paper uses cryptography for secure data while transmitting from one place to another place. He proposed a new encryption standard which is the amalgation of two different encryption algorithms developed by nath.e. al namely TTJSA and DJSA in randomized fashion. The method is achieve by splitting the files , which is to be encrypted and encrypting the split section of the files in various ways using TTJSA and DJSA cipher methods.

[4] Xiao Zhang, Hong-tao Du , Jian-quan Chen, Yi Lin, Lei-jie Zeng," Ensure Data Security in Cloud Storage". Author in this paper focus on data security in cloud Storage. An economic choice is to use cloud computing and cloud storage instead of manage data center by itself. Small companies buy compute and storage service just like water and electronic. The difficulty is how to ensure their data in cloud storage. Cloud storage provider claims that they can protect the data, but no one believes them. In this paper, author presents a framework to ensure data security in cloud storage system. In the framework, we use SLA as the common standard between user and provider.

III. PROBLEM DEFINITION

Existing systems uses number of encryption methods. In existing system use algorithms like Elliptic curve Cryptography for image Encryption which protects images from unauthorized access. In all existing system we are not making any specific and unique information to secure the data over internet from mobile devices. Further, all above system make use of certain encryption algorithm to prevent the confidential data of mobile user from being decrypted. In this encryption system of mobile phones are static, uniform and invariant. Hence it decreases the difficulty to decrypt the user's private data and results in a low safety for the mobile phone encryption system.

IV. PROJECT OBJECTIVE

The objective of proposed techniques is

- To protect your data when it's stored in the cloud.
- The encryption and decryption will be done by Strong Encryption Algorithm named as Modern Encryption Standard (MES-II) -version II.
- It saves time and increase complexity for decryption.

V. INVESTIGATIONAL OUTCOME

To achieve the objective of this project, we have proposed technique called Modern Encryption Standard II Algorithm (MES-II) for encrypting and decrypting the data using mobile ID which takes the complete hardware information of mobile.The MES-II is an algorithm used in Cryptography which focus on how one can achieve high order data security. The present method on various types of plain text files MES–II can be used as independent encryption algorithm to encrypt any short message such as SMS, Password or encryption key etc. By using this algorithm we provide the security of data stored in cloud by means of encryption and decryption process.

VI. CONCLUSION

This review paper proposes a technique to prevent the android mobile data which is saved in the cloud such as Google drive, drop box, etc. we will use an MES-II algorithm for encryption and decryption of data which is fast and gives security at highest level .The MES-II algorithm method will be free from standard cryptography attack such as known plain text attack, brute force attack, and differential attack.

REFERENCES

[1] CAO Wanpeng1, BI Wei2, "Adaptive and Dynamic Mobile Phone Data Encryption Method", Communication ,China(Volume:11,Issue:1),IEEE, May 2014.

[2] Pratap P. Nayadkar ,"Automatic and Secured Backup and Restore Technique in Android", IEEE International Conference on Innovations in Information Embedded and Communication Systems (ICIIECS'15),March 2015.

[3] "Modern Encryption Standard (MES) Version-I: An Advanced Cryptographic Method", Somdip Dey, Asoke Nath, Proceedings of IEEE 2nd World Congress on Information and Communication Technologies (WICT- 2012), pp. 242-247.

4] Xiao Zhang, Hong-tao Du ,Jian-quan Chen, Yi Lin, Lei-jie Zeng," Ensure Data Security in Cloud Storage"2011 International Conference on Network Computing and Information Security.

[5] Gunjan Sekhon,Asoke Nath, "Modern Encryption Standard (MES) Version-II", Proceedings of IEEE International Conference on Communication Systems and Network Technologies, April 2013.

[6] Koblitz N, Menezes , The State of Elliptic Curve Cryptography[J]. Design, Codes, and Cryptography¾Special Issue on Towards a Quarter-Century of Public Key Cryptography, 2000, 19(2-3): 173-193.

[7] Molnard D, Schechter S. Self Hosting vs. Cloud Hosting: Accounting for the Security Impact of Hosting in the Cloud[C]// Proceedings of Workshop on the Economics of Information Security (WEIS 2010): June 7-8, 2010.Harvard University, MA, USA, 2010.

[8] CSA: Cloud Security Guide. Tech. Rep., Cloud Security Alliance[EB/OL][2009-04]http://www.clodsecurityalliance.org.

[9] ENISA: Cloud Computing: Benefits, Risks and Recommendations for Information Security. Tech Rep., European Network and Information Security Agency[EB/OL]. [2009-11-20]. http:// enisa.europa.eu.

[10] Advanced Symmetric key Cryptography using extended MSA method: DJSSA symmetric key algorithm: , Journal of Computing, Vol 3, issue-2, Page 66-71,Feb(2011)

BIOGRAPHY

Ms. D. Agrawal received the B.E degree in Computer science & Engg. from Amravati University, Maharashtra, India in 2011 and pursuing M. Tech(CSE).Her current interest is Cryptography and Network Security .

Prof .P. Kulurkar received the M Tech degree in Computer Science and Engineering from RGPV University, India. He is working as a Professor and HOD in the Department of computer science and engineering at Vidarbha Institute of Technology, Nagpur University, India. His current interest is Network security and data mining.