International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

Development of Mobile Data Encryption Mechanism in Cloud Environment

Jitesh S. Zade[1], Prof. Piyush Ingole[2]

[1, 2] Department of Computer Science & Engineering, G. H. Raisoni College of Engineering, Nagpur, India

Abstract: ***The use of mobile is not limited to calling only. The multiple use of application leads to requirement of comparatively large storage capacity which is big constraint of mobile device. Cloud storage can be used to overcome this problem as it provides online storage to users. Still it is quite risky to allow the control of their data to service provider of cloud. We have proposed a mobile data encryption mechanism using MES(Modern Encryption Standard) algorithm to enhance the security level in cloud environment by encrypting the mobile data before storing it on cloud is proposed to enhance the mobile data security on cloud***

Keywords: cloud computing, confidentiality, encryption, decryption.

1. Introduction

One of the fastest growing industry in most countries in the world, which plays an important role in daily life is mobile communication. The continuous and large use of application increases the requirement of comparatively large storage capacity which is big constraint of mobile device. Use of cloud storage better option to handle this problem which provides storage service to users. Still it brings certain risk as the users have to surrender the control of their data to cloud service provider.

Cloud computing implies to the delivery of computing resources over the Internet. Rather than keeping data on their own hard drive or updating applications for their needs, they use a service at different location, to use its applications or to store their information over the Internet. There are benefits to users include reliability, scalability and efficiency. Scalability means that processing capacity and unlimited storage offered by cloud environment. Cloud computing is reliable and efficient as it provide access to documents and applications anywhere in the world by mean of the Internet as well as allows organizations to ease up resources to focus on innovation and product development. It is observed that cloud computing may lead to “function creep" which uses data by cloud providers that were not predictable when the information was collected originally and for which consent has typically not been attained. Security is the major issues which slow down the growth of cloud. Allowing the control of important data to another company is troublesome; such that the consumers need to be attentive in understanding the risks of data violation in this new environment.

It is clear that the security issue has played the key role in hampering acceptance of Cloud computing. Running software and storing data, on another hard disk using unknown CPU is not that much trustful. Botnet which is a well known security issues, data loss, phishing, causes serious threats not only to software but also to data of organizations. An Improved mechanism is required to minimize new security challenges which is introduced by the pooled computing resources and Multi-tenancy model in cloud computing. The services which are provided by Cloud are relatively cheaper for hackers who can use Cloud to organize botnet and start an attack.

2. Related Work

First Farhad Soleimanian Gharehchopogh and Meysam Bahari suggest four different methods for providing security in cloud environment in [1]. One of them is data fragmentation, in which the fragmented tables are divided into two groups’ i.e. Main data tables and Tables which determine communications (relations) for preserving confidentiality and increasing user trust. Second is Data Trust Third Party (TTP), which provides the increasing rely in levels and more important layers and creating proper solutions to keep security, accuracy and integrity in data and communication validity. Third method proposed is Fragmented data in secure space, where use Public Key Infrastructure (PKI) have been suggested for applying secure communications through IPSec or SSL. Forth method is using applied security methods of database server in Client/Server model which includes methods like User management, Access Control, Masking and Monitoring, Encryption.

In [2], the problems in previous keyword searching method have been discussed and the new method has been proposed in order to make the process of data retrieval on cloud more secure and efficient. In this method the Elliptical Curve Cryptography (ECC) has been implemented so that without compromising security of the cloud server and privacy of the users the objective of secure and efficient cloud server can be obtained.

Data partitioning technique with cryptography ensure cloud storage security, integrity and error identification. Cloud storage integrity checking concept is suggested to enhance the integrity of cloud storage. The overall System model is consist of three layers namely user machine, Third Party Auditor (TPA) and cloud storage servers. Partitioning method implemented at third party auditor [3].

The Cipher Cloud is a framework has been proposed in [4]. This framework allows users to put their data in confidential manner on public cloud servers. The data sent from a client to a cloud server or from a cloud server to a client is kept

completely confidential and encrypted. It is a two-step encryption process which is used by Cipher Cloud.

An application of a method to execute operations on encrypted data without decrypting them has been proposed in [5]. Homomorphic Encryption systems are used to perform operations on encrypted data without knowing the private key (without decryption), the client is the only holder of the secret key.

In [6], encryption mechanism like RSA, DES and latest version AES have been focused and also the modern Cryptography concept to data security in cloud have been given.

The combination of linear and elliptical cryptography methods have been used in encryption algorithm which has three security checkpoints: authentication, key generation and encryption of data[7].

Key Rotations are used in Data Encryption and Decryption Algorithms for Data Security in Cloud System which includes data encryption to encrypt critical data before sending to the cloud server[8]. the block level data encryption is exploits by using 256 bit symmetric key with rotation. The requested data from cloud server can be reconstructed by a client using shared secret key.

Cloud Storage Encryption (CSE) Architecture have been proposed which allows to encrypt data and to index it in a manner that ensures the protection of data during transportation. Also it allows the search process in the form of encrypted data and the retrieval of data in a safe manner[9].

To improve cloud data storage security, Data Partitioning Technique, Data Integrity Checking for data storage, and end users can stores their data in cloud has been done with help of cryptographic tool for secure data storage. remote data integrity checking concept has been proposed in order to enhance the performance of cloud storage[10].

3. Analysis

Papers are reviewed and studied related security of data on cloud environment. The reviewed techniques are different from each other.

In “Secure and efficient retrieval method”, The scheme implemented is ECC algorithm which is efficient in terms of cost and security. Due to such lightweight and efficient scheme it can be easily accessible through mobile devices like cell phone, tablet with browsing capacity to gives its users anytime anywhere service. The authentication level in this scheme makes it more robust and secure to defend with the intruders and for intruders only encrypted copy is available[2].

In “Partitioning Data and Domain Integrity Checking for Storage - Improving Cloud Storage Security Using Data Partitioning Technique”, the partitioning of data helps storing of the data in easy and effective manner. And implementation of chunks concept leads to quick retrieval and store. It also gives way for flexible access and there is less cost in data storage. Cloud storage integrity can become efficient to ensure integrity of stored data the space and time is also effectively reduced during storage [3].

The Cipher Cloud is a framework method, Cipher Cloud encrypts the data, making its ownership exclusive to its owner and makes it independent from the facts of where the data might be stored or who manages it. Even in cases of take over and change of ownership, only the user will be able to decrypt the given data. Additionally the data is kept safe during transit using HTTPS TLS 1.0 standard making it difficult for anyone to sniff the data [4].

In Homomorphism encryption algorithm, enables providing results of calculations on encrypted data without knowing the raw data on which the calculation was carried out, with respect of the data confidentiality [5].

The Data Security based on Elliptical Curve Cryptography and Diffie Hellman method in Cloud Architecture provides a four step procedure for ensuring authenticity of user. The first step is to establish the connection, second is account creation, third is authentication and last one is data exchange [6].

In Key rotation method, with data encryption, data owner can utilize the benefits of file split ingot reduce storage and computational overheads. On the other hand, to reduce the burden of data owner, trusted third party is introduced for verification of authorized users to access the data from cloud server[8]. By using Cloud Storage Encryption (CSE) Architecture, Policy encryption / decryption and access method have been identified in order to show how data can be transfer to cloud computing storage environment. The integrated work flow between encryption point, decryption point and searchable encryption has been presented as CSE Architectural components and interaction between components is explained [9].

4. Proposed System and Architecture

Fig 1. shows the system workflow. The entire analysis of proposed system will be analyzed by means of simulation and real time application.
The work is supposed to be progress in following steps:

- First phase include the initiation of hardware and user data collection module. The data collected by this module is used for authentication purpose of user as well as the device (hardware device).
- The third phase includes the data rearrangement module that will process the data which we got from integration module.
- In fourth phase the data will be given to encryption module which will apply the MES algorithm to give the final output has to be transferred on cloud for storing. Finally the performance and results of whole system will be analyzed and conclusions will be taken as shown in fig2, fig3, fig4.

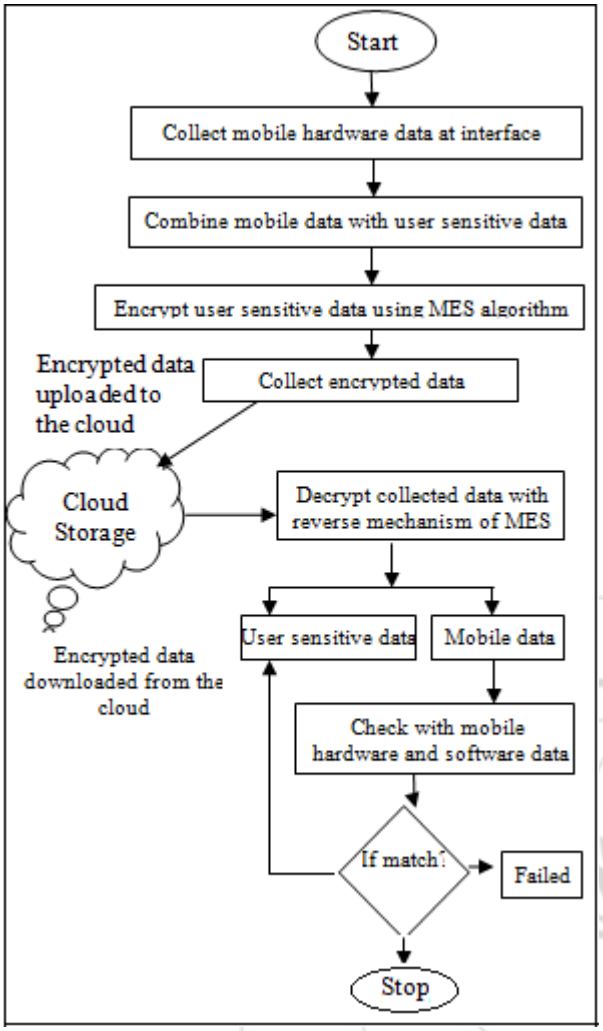

Figure 1: Research Flow Design

5. Results and Discussion

In initial phase of project the basic scenario of the whole system has been designed. The first snapshot particularly gives the view about how the user initiate with an application.

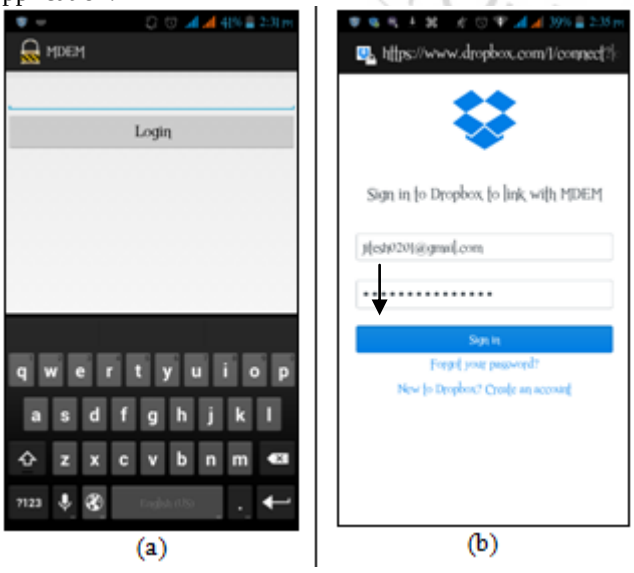

Figure 2: Initial Login Window

Fig 2(a) gives the initial view of an application which consists of one Login buttons. In Fig 2(b), user need to enter the login details to login to the particular account. Fig 3(a), shows the application request to access the cloud services so that user can store his/her data.

Fig. 3(b). shows the main working window, where we can select file to upload, download and delete, also view the list of files present on cloud.

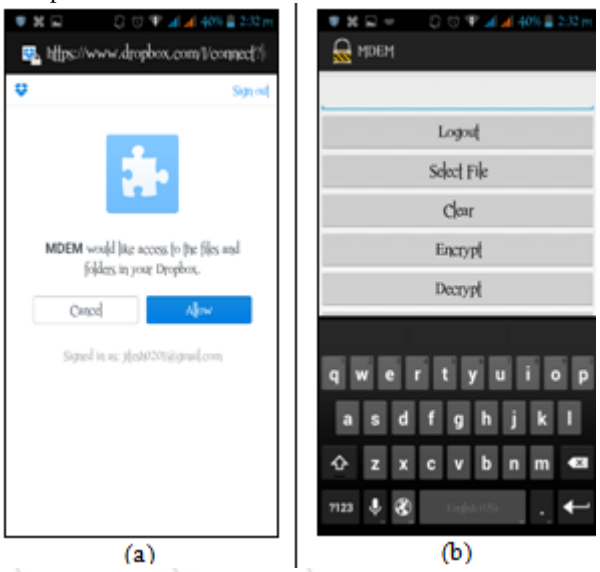

Figure 3: (a) Access Permission to Cloud, (b) MDEM Mail Window

Fig. 4.(a) shows the path where the original file is located in the mobile storage that is to be uploaded to the cloud after encrypting it. In Fig. 4.(b) the message shows that the file is encrypted successfully.

The encrypted data file is now ready to upload on cloud storage. To upload encrypted data file we just need to click on upload button in the mail window. Fig. 5.(a) shows the upload in progress. The cloud storage contains number of files, and if we want to see the list of files on cloud, we just

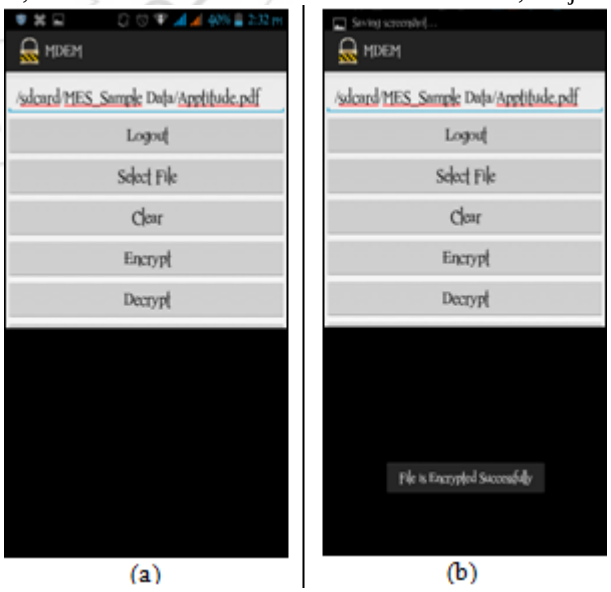

Figure 4: (a) Select file to upload, (b) Encryption of data file

need to click on List on Cloud Button from main window, it will show the complete list of files present on cloud storage. Fig. 5.(b) shows the list of files present on cloud storage.

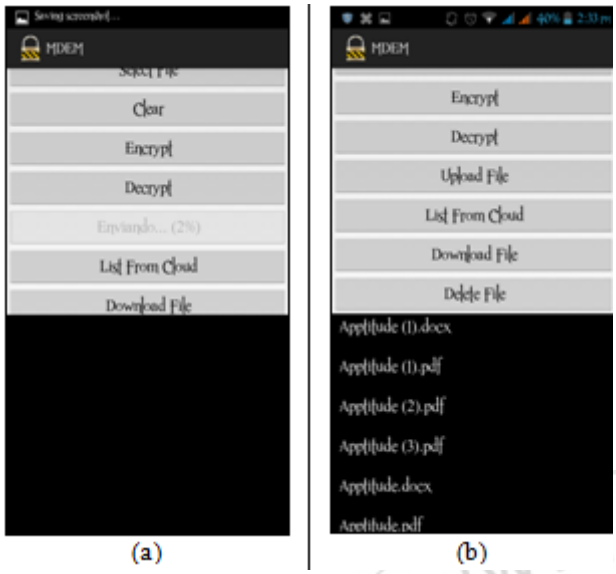

Figure 5: (a) Uploading of encrypted file, (b) List of files on cloud

The data file, selected from device storage is encrypted and the uploaded to cloud successfully. If we want to download any data file from cloud, we just need to do the reverse process. List the files from cloud, select the particular file we want and then click on download button. The selected file will be stored in the device storage. After that we need to decrypt that file. The downloaded file will be open in same device from which it is uploaded to cloud. The same file can be downloaded on other device but, the file will not be decrypted. The file gets damaged if decrypted in any other device. Fig. 6 shows the snapshot showing message "File Decrypted Successfully". We can delete he file from cloud.

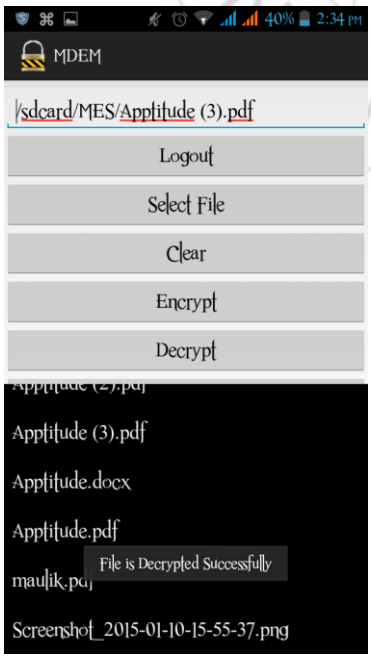

Figure 6: Decryption of selected data file

6. Conclusion

This paper reviewed various security mechanisms. Based on the analyzed parameters, various encryption algorithm can be used in alone or in combination to improve the security of user data at cloud storage. In proposed system, a lightweight encryption algorithm for mobile devices is designed .The proposed work gives an efficient mechanism to enhance the security for mobile data using MES.

References

[1] Farhad Soleimanian Gharehchopogh and Meysam Bahari , "*Evaluation of the C methods in cloud computing environments* ", International Journal in Foundations of Computer Science & Technology (*IJFCST*), Vol. 3, No.2, March 2013

[2] Akshay D. Kapse, Piyush K. Ingole, "*Secure and Efficient Retrieval of Data in Cloud*", International Journal of Application or Innovation in Engineering & Management (IJAIEM), 2014.

[3] Santosh Jogade, Ravi Sharma, Prof. Rajani Kadam, "*Partitioning Data and Domain Integrity Checking for Storage - Improving Cloud Storage Security Using Data Partitioning Technique",* International Journal of Emerging Research in Management &Technology ISSN: 2278-9359,Volume-3, Issue-3, March 2014.

[4] Manpreet Kaur, Rajbir Singh, "*Implementing Encryption Algorithms to Enhance Data Security of Cloud in Cloud Computing*", International Journal of Computer Applications, Volume 70– No.18, May 2013.

[5] Maha TEBAA, Saïd EL HAJJI, Abdellatif EL GHAZI, "*Homomorphic Encryption Applied to the Cloud Computing Security*", Proceedings of the World Congress on Engineering 2012 Vol I WCE 2012, July 4 - 6, 2012, London, U.K.

[6] Vijendra Rajendra Augustine, Prof. Prabhaker L. Ramteke, "*Data Storage Security in Cloud Environment with Encryption and Cryptographic Techniques*", International Journal of Application or Innovation in Engineering & Management (IJAIEM) ,2013.

[7] Neha Tirthani, "*Data Security in Cloud Architecture Based on Diffie Hellman and Elliptical Curve Cryptography",* IACR Cryptology ePrint Archive 2014

[8] Prakash G L ,Dr. Manish Prateek and Dr. Inder Singh, "*Data Encryption and Decryption Algorithms using Key Rotations for Data Security in Cloud System",* International Journal Of Engineering And Computer Science ISSN:2319-72423 Issue 4 April, 2014.

[9] Hamdan M. Al-Sabri, Saleh M. Al-Saleem, "*Building a Cloud Storage Encryption (CSE) Architecture for Enhancing Cloud Security*", IJCSI International Journal of Computer Science Issues, Vol. 10, Issue 2, No 1, March 2013.

[10] Swapnil V. Khedkar , A. D. Gawande, "*Data Partitioning Technique to Improve Cloud Data Storage Security",* (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (3) , 3347-3350, 2014.

[11] Abdeladim Alfath, Karim Bai A, Salah Barna, "*Cloud Computing Security: Fine-grained analysis and Security approaches*", IEEE Conference, 2013.
[12] Mohammed A. AlZain, Ben Soh and Eric Pardede, "*A New Approach Using Redundancy Technique to Improve Security in Cloud Computing*", Cyber Security, Cyber Warfare and Digital Forensic (CyberSec), 2012 International Conference on , vol., no., pp.230,235, 26-28 June 2012.
[13] K. Sriprasadh, Saicharansrinivasan , O. Pandithurai, A. saravanan, "*A Novel Method to Secure Cloud Computing Through Multicast Key Management",* Information Communication and Embedded Systems (ICICES), 2013 International Conference on , vol., no., pp.305,311, 21-22 Feb. 2013.
[14] C. Selvakumar, G. Jeeva Rathanam, M. R. Sumalatha, "*PDDS: Improving Cloud Data Storage Security*", Advance Computing Conference (IACC), 2013 IEEE 3rd International , vol., no., pp.7,11, 22-23 Feb. 2013
[15] Somdip Dey, Asoke Naths, "*Modern Encryption Standard (MES) Version-1: An Advanced Cryptographic Method",* IEEE Conference Publications, vol., no., pp.242,247, 2012
[16] BAO Haiyong, WEI Guiyi, SHAO Jun, *et al., "Efficient Signature-Encryption Scheme for Mobile Computation[C]",* Proceedings of 2011 International Conference on System Science and Engineering (ICSSE): June 8-10, 2011. Macao, China : 390-393, 2011.
[17] M. Armbrust, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, *"A View of Cloud Computing,"* ACM Trans. On Communications, vol. 53, no. 4, pp. 50- 58, April 2010.
[18] F.B. Shaikh, and S. Haider, *"Security Threats in Cloud Computing,"* in Proc. FInternational Conf. for Internet Technology and Secured Transactions (ICITST), pp. 214-219., 2011
[19] Wanpeng, Cao; Wei, Bi, "*Adaptive and Dynamic Mobile Phone Data Encryption Method"*, IEEE Magazine, Communications, China , vol.11, no.1, pp.103,109, Jan. 2014
[20] Faraz Fatemi Moghaddam, Omidreza Karimi, Maen T. Alrashdan, "*A Comparative Study of Applying Real-Time Encryption in Cloud Computing Environments*", IEEE 2nd International Conference on Cloud Networking (CloudNet), 2013.