International Journal of Research
eISSN: 2348-6848 & *pISSN:* **2348-795X** *Vol-5 Special Issue-13*
International Conference on Innovation and Research in Engineering, Science & Technology
Held on 23rd & 24th February 2018, Organized by Tulsiramji Gaikwad Patil College of Engineering & Technology, Nagpur, 441108, Maharastra, India.

A Review on Data Storage Security in Cloud Computing Environment for Mobile devices

Samta Ukey,Jayant Adhikari,Rajesh sir
[1]*M.Tech Student TGPCET, Nagpur.*
[3,2]*Assistent Profesor, CSE Dept, TGPCET, Nagpur*

***Abstract*:**Cloud computing is a platform which provides different capabilities which are not just limited to storage, networking and computing capability as a service to users through Internet. Users can automatically request and release these resources on demand, by paying charges for the quantity and quality of service they use. Cloud computing for Mobile which is also referred as Mobile Cloud Computing is combination of mobile with cloud computing that provides user with unlimited access to the pool of different resources from cloud without affecting mobilization of user with his Mobile. As with its advantages it comes with the risk of data read by the cloud service provider or been grabbed by someone else using man-in-middle attack, thus affecting user privacy and integrity and losing users trust further over the service. These issues can be solved by implementing different techniques like encryption, avoiding unauthorized access to user to have access to stored data. Any algorithm or technique used for securing data should consider few important points like Mobile devices are battery powered and have less processing capability and have less storage space. In this paper we reviewed different techniques for secure storage of user's data in the cloud, their advantages and disadvantages for mobile cloud computing environment.

Keywords: Mobile data Security, Cloud Computing for Mobile, Cloud computing.

*****

I. Introduction

As we know Cloud computing is platform that provides access to huge pool of computing, storage network resources to multiple users in multi-tenant architecture and apply charges as per your usage and quality of service requested, this results in reducing the total capital expenses spent for purchasing, hosting and maintaining of resources if not locally [8]. Mobile Cloud computing for users using Mobile devices [3] provides facility and infrastructure to have access to unlimited resources hosted on the cloud, maintaining the flexibility, transparency and mobility. Here with mobile cloud computing the processing of any algorithm and storage of data is performed on the cloud instead of mobile device itself, thus virtually increasing the capacity and capability of mobile devices to process the data. Storing any type of data on the cloud environment had always shown a security risk, as the data will not reside on your servers but resides on third party servers, outside the user domain to which as sometime you are unaware of. Encrypting or applying any similar technique to the data before storing it on the cloud is essentially very important for mobile device users along with acceptable mobility and reducing battery power usage and consuming minimal processing of Mobile device. In this review paper, we have highlighted number of techniques and processes that can be used for securely storing user's data on the cloud environment.

II. Related Work

Number of Mobile device users are increasing day by day and thus looking at advancement in cloud-computing seems users data stored on cloud have to be protected against unauthenticated and unauthorized access. The following information describes various techniques, Processes and algorithms that can be used by owner of data for securing data in Mobile cloud computing environment.

1) Symmetric Key Encryption

Here in symmetric key encryption user can encrypt his mobile data using secret key generated by some generator function residing on his mobile device or on remote server. The same key which is used for encryption of plain text will be used for decryption of cipher text as well. The secret key is shared to the only intended users to have access to the shared data. Block cipher and Stream cipher are two types of algorithm available for symmetric key encryption systems. Different algorithms such as Advanced Encryption Standard (AES) (approved by NIST), Data Encryption Standard (DES), 3DES, International Data Encryption Algorithm (IDEA) are used for encryption and decryption using symmetric key [2].

Advantages: Simplicity in use, Difficult to crack without knowledge of secret key.

Disadvantages: Access to secret key gives all information of data.

2) Public-Key Infrastructure (PKI)

Public key Infrastructure are unique set of different algorithms generally referred as cryptographic algorithms that requires generation of two separate but mathematically and functionally linked keys. These keys are referred as public and private key. The Private Key as the name suggest is kept secret by the owner and used for digitally signing a document and decryption of encrypted text.

Public key is the key which is publicly available to all users is used to verify a digital sign and to encrypt given plain text message. However only the valid receiver having valid Private key is now able to decrypt the text correctly. PKI

International Journal of Research
eISSN: 2348-6848 & pISSN: 2348-795X Vol-5 Special Issue-13
International Conference on Innovation and Research in Engineering, Science & Technology
Held on 23rd & 24th February 2018, Organized by Tulsiramji Gaikwad Patil College of Engineering & Technology, Nagpur, 441108, Maharastra, India.

performs different operations like mathematical factorization, transformation, transposition of large integer or prime numbers for creating the cipher text [2].

Advantages: Theoretically it is impossible to crack down cipher text if you don't have correct key.

Disadvantages: High memory usage, Cannot be used on mobile devices due to high computation requirement.

3)Role-Based Access Control (RBAC)

This is also known as Responsibility based access control technique. Data in cloud environment is generally stored by single user and can be accessed by multiple users in the same environment but this requires assigning different access rights to every user who wants or should have access to it [1]. Here within this architecture data which is referred as data objects are given permissions which are further then mapped to role based or responsibility based Access Control List. These roles and responsibilities are further assigned to only authorized users, hence giving access to data stored in system. Here the owner of the data encrypts the data in a way that allows only valid users with appropriate responsibilities and owner specified RBAC policies, can decrypt the data.

Advantages: Provides privacy and Integrity of data stored in cloud environment and is also computationally secure.

Disadvantages: Owner of data is whole and sole responsible for providing access to shared data.

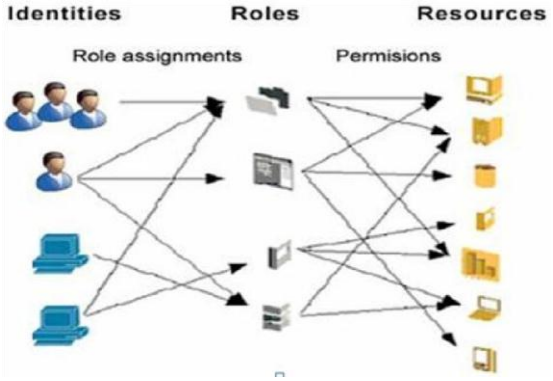

Fig.1: Role cum Responsibility Based Access Control Technique

4)Hierarchical Identity Based Encryption (HIBE)

It's an encryption technique where Identity of data object is used to encrypt with private and public key pairs, without the actual need of Certificate Authority and their certificates. In this technique, publicly available unique user identifiers such as his email id, mobile number and Facebook-id can be used as a public key. The related private key for this public key is generated by Private Key Generator (PKG) which has the all information of master secret key referred to as root PKG. A modified latest version of Identity based encryption which also widely used now a days is referred as Hybrid Identity based encryption (HIBE). Root PKG is only responsible for generating private keys for given domain PKG which in turn [1].

Advantages: Publicly available identifiers are used as public key

Disadvantages: Large computation power is required.

5) Attribute-Based Encryption (ABE)

In this system the group of users to whom data should be accessible must poses some attribute defined by data owner. The Data to be shared is encrypted and decrypted at other end by using set of user defined attributes instead of relying on single key for encryption. Similar to HIBE publicly available Unique user attributes (user id, department role, organizational role), environmental attributes such as current user location, current time zone, type of clientinterface in use, type of operation (read, write) and similar can be used for ciphering or deciphering of data to be performed in the environment. Removing any attribute of any user results in revoking access for that set of attributes of given data [4].

5.1) CP-ABE (Cipher Policy – Attribute based Encryption) In cipher policy attribute based encryption technique user ciphering the data requires to have set of attributes applied to data that can be used to decrypt a cipher text. A trusted authority sends or distributes these attributes to intended users for decryption purpose which also allow access to shared data by having these required attributes.

Advantages: No need to maintain keys instead user is allowed to access data based on possession of certain attributes.

Disadvantages: Very large amount of infrastructure is required to implement security policies, dynamically changing environment and related attributes (user, environmental, action) leading to constant update of access structure or policy. And is mostly avoided due to its computationally expensive for resource constrained mobile devices.

5.2) KP-ABE (Key Policy Attribute Based Encryption) Here, the data owner encrypts the data and then specifies set of different attributes that can be used to decipher text. In this case valid users get the key for decryption from trusted authority within or outside system as per system configuration, this includes the access policy defining type of access the user will have. The Users satisfying all the required set of

International Journal of Research
eISSN: 2348-6848 & pISSN: 2348-795X Vol-5 Special Issue-13
International Conference on Innovation and Research in Engineering, Science & Technology
Held on 23rd & 24th February 2018, Organized by Tulsiramji Gaikwad Patil College of Engineering & Technology, Nagpur, 441108, Maharastra, India.

security-attributes can decipher text. This technique is best suitable for all organization that try to provide different access levels to all users within that organization.

6) Hybrid Attribute-Based Encryption (H-ABE)

An updated flavor of attribute based encryption technique is called as hybrid attribute based encryption. Provides access to only those authorized user to access having required attributes. Further to overcome the burden of large-processing from the mobile user, the Processing expensive work of paring the key is performed by the mutually clubbed efforts of user, cloud provider and trusted manager. This also helps the mobile user in reducing the communication cost otherwise in other case would be much higher.

Advantages: Well Optimized for specific mobile users, reduced communication, storage and computation cost, difficult to crack the code.

Disadvantages: No Backup provision due to lack of backup manager.

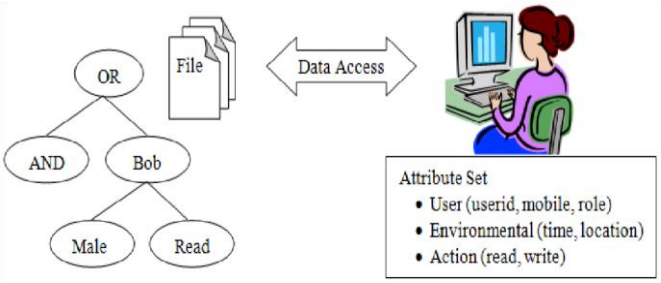

Fig. 2: Attribute and Access tree structure encryption

7) Proxy based Re-Encryption

The scheme we are discussing now focuses on securing data storage is especially optimized for the purpose of cloud computing environment for mobile devices. The Data stored here is in encrypted form and can be accessed by using keys distributed by data owner and unique group key assigned for a group of users by the system administrator based on some rules. In this system if a user revokes access it results in denial of access to the data for specific user by re-encrypting the stored data without affecting access to other users. Re-encryption process is defined as conversion of a cipher text from one version to another without intermediate decryption step or any intermediate results and creation of set of different keys to access newly encrypted data. [7].

Advantages: Data store is secured, works efficiently in case of user revokes the access.

Disadvantages: Frequent user revocation results in change of keys thus access is denied to valid and authorized users during ongoing operation.

8) Third Party Auditing

This is one of the widely used technique now a days where audits are carried out to check the integrity of any shared data. This process is executed between following three parties: Third Party auditor, users and cloud service provider. The Auditor, which acts as Proxy to entire system has large and powerful communication, storage and computation capability, which lie in domain external to cloud service provider and user accessing the data. Auditors do not have any direct or indirect access to shared data in spite of just they are able and has to publicly verify the integrity of shared data. They have to also preserve identity of user and correctness of data along with public auditability [6].

Advantages: Ease of use is maintained for mobile users as integrity of data maintained by TPA.

Disadvantages: Failure or Hack of TPA results in loss of data security.

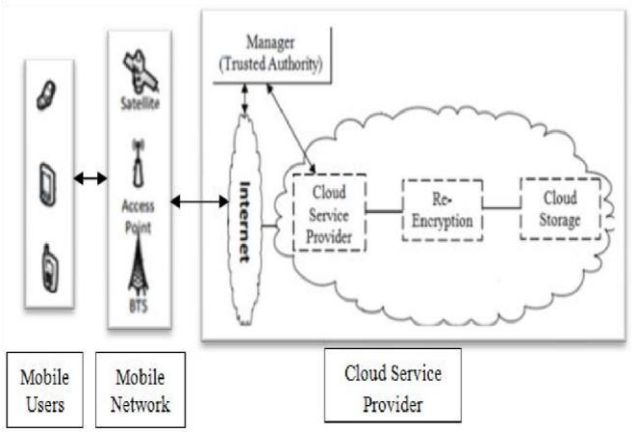

Fig. 3:Re-encryption in cloud environment with trusted third party Manager / Auditor acting as Proxy

9)Trusted Hardware

These are one of the most advanced technique of data security over cloud environment where this techniques make use hardware based security instead of depending on system or application software based programs to secure data. For this purpose specialized processor's i.e. Microprocessors in this case called as crypto-processor are used for manipulating cryptographic keys. Hardware based technology called the Trusted platform Module (TPM) is used for securing data by executing encryption algorithms within microprocessor itself using cryptographic keys. Trusted Computing Group (TCG) is responsible for giving

us the technical specification of TPM required for configuring the environment. Intel Trusted Execution Technology (TXT) [5] is an example of such system which uses TPM to analyze and quantify the security of software, Operating System and various other system resources and platform components to make trust decisions. No matter Local or Remote applications can leverage benefit of TPM for trusted execution. Processor registers called as Platform Configuration Registers (PCR) is used for storing and comparing the actual measurements against execution component to check integrity.

Advantages: Execution of software and applications in trusted manner without affecting integrity of stored data.

Disadvantages: Hardware cost is considerably high, up gradation of existing hardware is required.

[9]National Institute of Standards and Institute, "NIST Cloud Computing Reference Architecture".

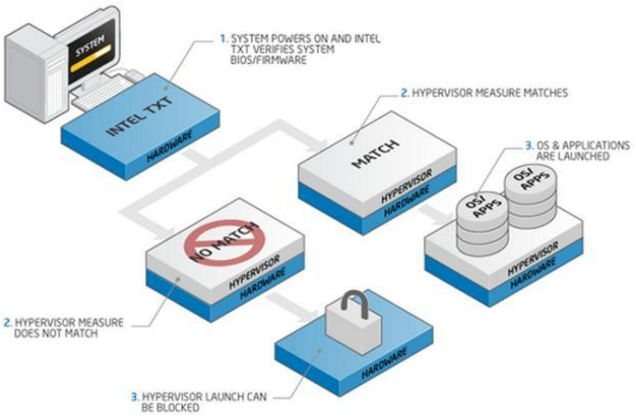

Fig. 4: Trusted Execution technology by Intel:

adopted from Intel TXT whitepaper.

III. Conclusion

Cloud computing here in with our context of Mobile-Mobile Cloud Computing provides set of configurable computing resources as a service for users such as Processors, Memory and Storage devices etc. Mobile cloud computing has much constraints over cloud computing due to device specific capabilities which are battery powered and has less storage space, processing power. To preserve integrity of data of users accessing data stored on cloud using their Mobile devices the data must be secured by all possible means. In this paper we have discussed various techniques, processes and algorithm that can be used for securing data storage in the cloud computing environment been accessed by Mobile devices. And discussed advantages and disadvantages of each scheme are given.

REFERENCES

[1] Lan Zhou, Vijay Varadharajan, and Michael Hitchens, "Achieving Secure Role-Based Access Control on Encrypted Data in Cloud Storage," IEEE Transactions On Information Forensics And Security, Vol. 8, No. 12, December 2013.

[2] Zhifeng Xiao and Yang Xiao, "Security and Privacy in Cloud Computing," IEEE Communications Surveys & Tutorials, Vol. 15, No. 2, Second Quarter 2013.

[3] Niroshinie Fernando, Seng W. Loke, WennyRahayu,"Mobile cloud computing: A survey,"Future Generation Computer Systems (2013)

[4] Ming Li, Shucheng Yu, , Yao Zheng, KuiRen, and Wenjing Lou, "Scalable and Secure Sharing of Personal Health Records in Cloud Computing Using AttributeBased Encryption," IEEE Transactions On Parallel And Distributed Systems, Vol. 24, No. 1, January 2013.

[5] "Intel Trusted Execution Technology" Hardware-based Technology for Enhancing Server Platform Security, White Paper.

[6] Boyang Wang, Baochun Li and Hui Li, "Oruta: PrivacyPreserving Public Auditing for Shared Data in the Cloud".

[7] Piotr K. Tysowski, M. AnwarulHasan "Re-EncryptionBased Key Management towards Secure and Scalable Mobile Applications in Clouds".

[8] National Institute of Standards and Institute, "The NIST Definition of Cloud Computing".

[9] G.Rajesh Babu, Ananth Kumar ,"Security In Inter Cloud Data Transfer" International Journal of Innovative Research in Computer Science & Technology (IJIRCST)
ISSN: 2347-5552, Volume-2, Issue-5, September-2014.