International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

A Survey on Data Storage Security in Mobile Cloud Computing Environment

Manoj M. Chavan[1], Poonam Gupta[2]

[1]G.H Raisoni College of Engineering and Management, Pune, India

Abstract: ***Cloud computing is a utility computing which provides computing, networking, storage space as a service to users through Internet. Users can automatically provision and de-provision resources on demand, paying charges for the capacity they use. Mobile cloud computing combines the power of mobile with cloud computing thus providing the user with unlimited pool of resource from cloud without hampering mobility of user. A mobile user storing data on the cloud can be read by the cloud service provider or hacked by man-in-middle attack, thus affecting user privacy and integrity. So data stored on the cloud should be encrypted, disallowing unauthorized user to access stored data. Mobile devices are resource constrained since they are battery powered, have less processing power and have less storage space. Any algorithm or technique used for securing mobile users data should take into account above constraints for effective uses of cloud for mobile users. In this paper we have provided a survey of different techniques for secure storage of mobile user's data in the cloud, their merits and demerits for mobile environment.***

Keywords: Security, Mobile Cloud Computing, Cloud computing.

1. Introduction

Cloud computing provides access to large pool of computing, storage network resources to users on multi-tenant model and pay as you go basis, thus reducing the capital expenses occurred for purchasing, hosting, maintenance of resources locally [8]. Cloud computing for mobile users [3] provides access to unlimited resources hosted on the cloud, maintaining the flexibility and mobility. In mobile cloud computing processing and storage is done on the cloud instead of mobile itself, thus increasing the capacity and capability of mobile devices. Storing data on the cloud always imposes a security risk, as the data resides on third party servers, outside the user domain. Encrypting the data before storing it on the cloud is essential for mobile users along with maintaining mobility and reducing battery power usage. In this survey paper, we have covered number of techniques that can be used for securely storage of mobile user's data on the cloud.

2. Related Work

Mobile users data stored on cloud have to be protected against unauthorized access and integrity. The following section describes various techniques and algorithms used by data owner for securing data in cloud computing environment.

1) Symmetric Key Encryption

In symmetric key encryption user encrypts the data using secret key generated by a generator function. The same key used for encryption of plain text can be used for decryption of cipher text too. The secret key is disseminated to the users intended to access the shared data. Stream cipher and Block cipher are two types of algorithm used by symmetric key systems. Various algorithms such as Advanced Encryption Standard (AES)(approved by NIST in 2001), Data Encryption Standard (DES), 3DES, Blowfish, International Data Encryption Algorithm (IDEA) are used for encryption and decryption using symmetric key [2].

Merits: Simplicity, Difficult to crack without possession of secret key.
Demerits: Access to secret key reveals all information.

2) Public-Key Infrastructure (PKI)

Public key Infrastructure are set of cryptographic algorithms which requires generation of two separate but mathematically linked keys known as public key and private key. Private Key is usually kept secret by the owner and used for digitally signing a document and decryption of cipher text. Public key which is published publicly is used to verify a digital sign and to encrypt a plain text message. PKI performs factorization, transformation, transposition of large integer or prime numbers for creating the cipher text [2].
Merits: Theoretically impossible to crack cipher text without possession of proper key.
Demerits: Computationally Expensive, High memory footprints, Cannot be used for resource constrained mobile devices.

3) Role-Based Access Control (RBAC)

Data stored by single user and accessed by multiple users in the cloud requires assigning access rights to every user in authorized group [1]. In this model data objects are assigned permissions which are further mapped to roles based on Access Control List. These roles are further assigned to authorized users, thus providing access to stored data. Here the data owner encrypts the data in such a way that only authorized users with appropriate roles and owner specified RBAC policies, are able to view or decrypt data. Revocation of one of the user from authorized group results in denied access for unauthorized user.

Merits: Provides privacy and Integrity of stored data. Computationally secure.

Demerits: Data owner is solely responsible for providing access to shared data, also requires constant availability of data owner. Affects mobility of data owner and adds computation burden on mobile device.

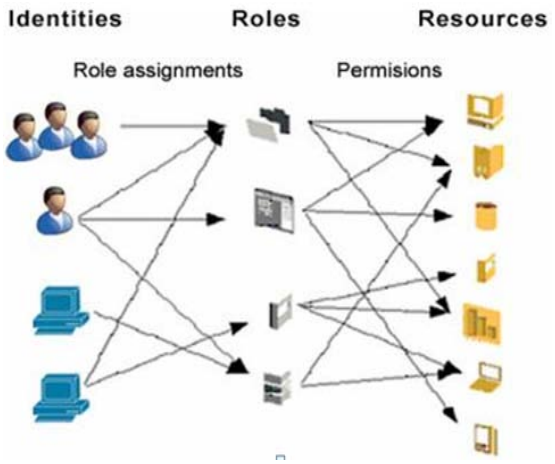

Figure 1: Role Based Access Control Method

4) Hierarchical Identity Based Encryption (HIBE)

Identity based encryption provides the users with private and public key pairs, without the requirement of certificates and CA. In this scheme, unique and public identifiers such as email id, mobile number and user_id can be used as a public key. The corresponding private key is generated by Private Key Generator (PKG) which has the knowledge of master secret key, called as root PKG. A refined version of Identity based encryption called as Hybrid Identity based encryption (HIBE) delegates the task of key generation to domain PKG, thus relieving the root PKG from expensive operation of key generation. Root PKG only generates private keys for domain PKG which in turn, working on behalf of root PKG is responsible for generation of private key for users in subsequent hierarchy [1].

Merits: Uses publicly available identifiers as public key, User and root PKG relieved from load of cryptographic operations

Demerits: Higher number of computation required.

5) Attribute-Based Encryption (ABE)

In this system data owner interested in sharing encrypted data with multiple users in group distributes keys having attribute-based access rights. Data are encrypted and decrypted by using set of user attributes instead of using single key. Unique user attributes (user id, mobile number, organizational role, department role), environmental attributes (user location, current time, type of client), Action (read, write) can be used for encryption or decryption of data to be stored on the cloud. Revocation of any user results in denied access for that set of attributes [4].

5.1) KP-ABE (Key Policy Attribute Based Encryption)

In key-policy attribute based encryption, owner encrypts the data and specifies set of attributes that can be used to decrypt the cipher text. Intended users get the key for decryption from trusted authority, which also specifies the access policy that specifies type of cipher text a user has access. User having and satisfying required set of attributes can decrypt the cipher text. This scheme is suitable for an organization that requires providing different level of access for different users.

5.2) CP-ABE (Cipher Policy – Attribute based Encryption)

In cipher policy attribute based encryption user encrypting the data requires to set attributes that can be used to decrypt a cipher text. A trusted authority disseminates attributes to intended users which allow access to shared data by possession of required attributes.

Merits: Instead of maintaining keys user are allowed to access stored data based on possession of certain attributes.

Demerits: Requires large amount of infrastructure to implement policies, Dynamic changing of attributes (user, environmental, action) leads to constant updating of access structure or policy. It is computationally expensive for resource constrained mobile devices.

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

A modified version of attribute based encryption called as hybrid attribute based encryption which provides an authorized user to access encrypted data on possession of required attributes. Additionally to reduce the burden of computation from the mobile user, the computationally expensive task of key-paring is done by the combined efforts of user, trusted manager and cloud provider, which helps in relieving burden of cryptographic operations from user alone. This also helps the mobile user in lowering the communication cost.

Merits: Optimized for mobile users, Reduces communication and computation cost, computationally very difficult to crack.

Demerits: No provision of backup manager.

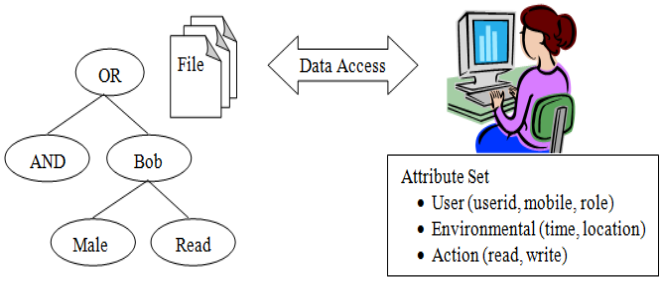

Figure 2: Attribute based encryption with attributes and access tree structure

7) Proxy based Re-Encryption

This scheme of secure data storage is especially optimized for mobile cloud computing environment. Data stored in encrypted form can be accessed by using keys disseminated by data owner and group key assigned for a group of users. In this system a user revocation results in denied access for revoked user by re-encrypting the stored data. Re-encryption is a process of converting a cipher text from one version to another without intermediate decryption step and creation of keys to access re-encrypted data. The new keys for accessing shared data are disseminated to remaining set of users in authorized group [7].

Merits: Store data securely, works efficiently in case of user revocation.

Demerits: Constant user revocation results in updating of keys thus denied access to authorized users during ongoing process.

8) Third Party Auditing

Third party auditing is used to check the integrity of shared data. There are three parties involved in this scheme: users,

cloud provider, third party auditor. Third party auditor, having more powerful communication and computation capability, lie in domain external to cloud provider or user, provides auditing service. They do not have direct access to shared data in spite of which they are able to publicly verify the integrity of shared data. TPA preserves identity of user, correctness of data along with public auditability [6].

Merits: Maintain integrity of data by TPA reduces the burden of mobile user.

Demerits: Failure or Compromise of TPA results in non-auditability of stored data.

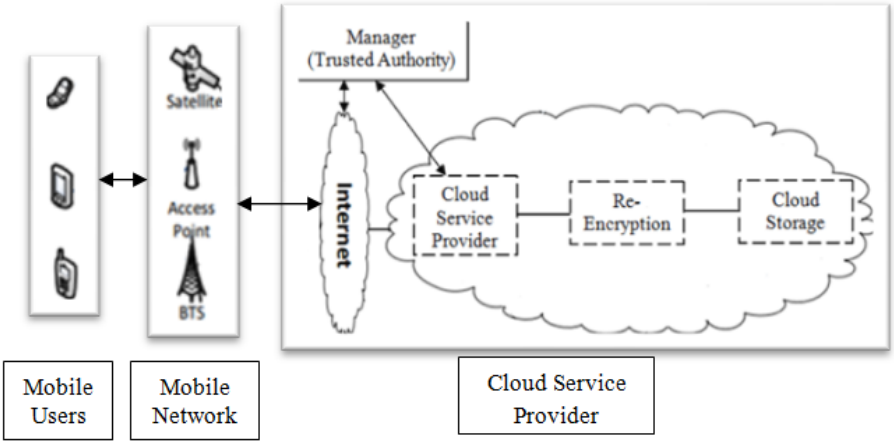

Figure 3: Proxy based Re-encryption in cloud with trusted third party Manager / Auditor

9) Trusted Hardware

Trusted hardware techniques make use hardware based security instead of relying on software based programs to secure user data. Specialized microprocessor's called as crypto-processor is used for storing cryptographic keys. Trusted platform Module (TPM) is a hardware technology used for secure execution by integrating the cryptographic keys in the microprocessor itself. Trusted Computing Group (TCG) gives the technical specification of TPM. Intel Trusted Execution Technology (TXT) [5] makes use of TPM and cryptographic techniques to measure the security of software, Operating System, platform components to make trust decisions. Also local as well as remote applications can make use of TPM for trusted execution. Platform Configuration Registers (PCR) is used by TPM for storing the actual measurements which are compared against the execution component to check integrity.

Merits: Trusted execution of software and applications without hampering integrity of stored data.

Demerits: Cost of hardware is considerable, requires up gradation of current hardware.

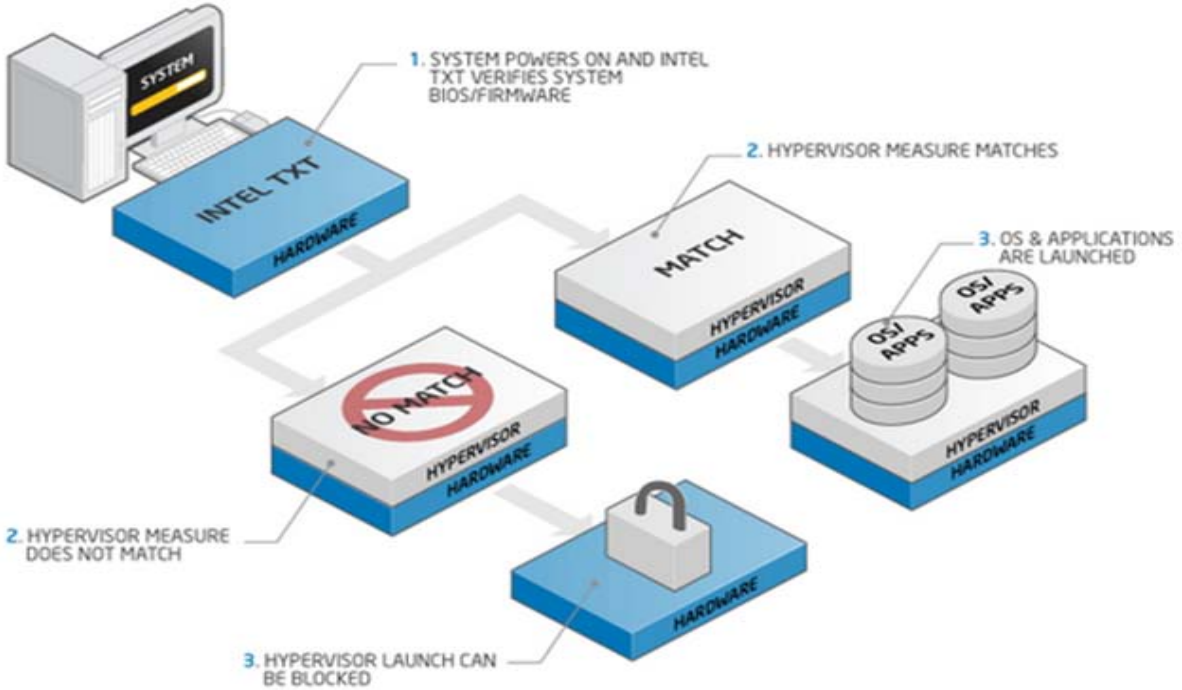

Figure 4: Intel trusted execution technology: adopted from Intel TXT whitepaper

3. Conclusion

Cloud Computing provides pool of configurable computing resources as a service for users. Mobile cloud computing is much more constrained then cloud computing due to use of mobile devices which are battery powered and has less storage space, computing power. Mobile users storing their data on the cloud service provider's servers need to secure it against unauthorized access so as to preserve integrity of data. Protocol used to secure user data should take into account the issues confronted by Mobile Devices. In this paper we have discussed various methods, techniques and algorithm that can be used for secured data storage in the mobile cloud computing environment. Also the merits and demerits 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 Attribute-Based 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: Privacy-Preserving Public Auditing for Shared Data in the Cloud".
[7] Piotr K. Tysowski, M. Anwarul Hasan "Re-Encryption-Based Key Management towards Secure and Scalable Mobile Applications in Clouds".
[8] National Institute of Standards and Institute, "The NIST Definition of Cloud Computing".
[9] National Institute of Standards and Institute, "NIST Cloud Computing Reference Architecture".