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

Securing Mobile User Data in Cloud Computing Environment

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

[1, 2] G.H Raisoni College of Engineering and Management, Pune, Maharashtra, India

Abstract: ***Mobile Cloud Computing (MCC) combines dynamic fields of cloud computing, portable computing, wireless communication infrastructure, location services and mobile web. Using mobile cloud computing the user can access unlimited computing power and storage space. Data stored by mobile user on the cloud should be secured both from unauthorized access and cloud provider. Additionally mobile devices assessing the data are constrained in terms of resource such as storage space and computing power, so communication cost must be reduced. For securing the data stored on the cloud our proposed system uses attribute based encryption in which only the authorized user can access stored data by satisfying required attributes. Complex cryptographic operations are performed by cloud provider and trusted authority i.e manager thus relieving mobile user from heavy computational load. Whenever a user leaves group of authorized users re-encryption is performed on the encrypted data by cloud provider without intermediate decryption while preserving the integrity and privacy of user data.***

Keywords: Mobile Cloud Computing, Cloud Computing, Security, Attribute Based Encryption, Re-Encryption

1. Introduction

Cloud computing is the delivery of computing as a service to users over Internet. Cloud computing provides scalable IT resources such as computing power, storage space, networking, software as a service to the users having access to Internet. In-stead of purchasing and operating these resources locally they can be rented on-demand and paid on pay-as-you-use basis. This reduces the capital cost of hardware and software and helps to increase capacity and capability on the fly [1]. Mobile cloud computing is a computing model in which mobile users can access unlimited computing power and storage space from the cloud [2]. Mobile user's data stored in the cloud resides on third party servers and can be read by cloud provider or hacked by man-in-middle during transaction. So data should be encrypted such that only authorized users can access it. Encryption on data requires complex cryptographic operations which impose computational, transactional and storage burden on resource constrained mobile devices. Major issues identified in mobile cloud computing environment are integrity, privacy and resource constraints, such as computing power and storage space. To address these issues our proposed system uses attribute based encryption [3] and re-encryption. Attribute based en-cryption is a type of encryption which allows users to access encrypted data by satisfying set of attributes instead of keys alone. A modified version of attribute based encryption has been proposed in which, load of computationally expensive cryptographic operations are performed by combined efforts of cloud provider, trusted authority and data owner which helps in relieving the burden on mobile devices. Re-encryption is a technique of re-encrypting the stored data, which is done to preserve Integrity of stored data in case of user revocation. Re-encryption in proposed system is performed without intermediate decryption step by cloud provider. This results in dissemination of newly generated keys to authorized member group to access encrypted data, thus avoiding unauthorized access by revoked users. Outline of our proposed system is as follows.

1) A protocol has been proposed for encrypting data stored in the cloud which allows authorized users to access data based on possession of required attributes. Cloud provider in unable to access data due to non-availability of attributes.
2) Modified version of attribute based encryption is used in which cryptographic operations requiring intensive computation such key generation and paring are per-formed by trusted authority, mobile data owner and cloud provider instead of mobile data owner alone.
3) Re-encryption is done on encrypted data in the cloud, whenever a user leaves authorized membership group. It is performed without intermediate decryption, re-moval of attributes on stored data.
4) Development of cloud app for accessibility of system on any platform connected to Internet.

2. Related Work

In Attribute-Based Encryption (ABE) [3], suggested by Ming Li, Shucheng Yu, Yao Zheng, Kui Ren, Sen, and Wenjing Lou, data owner can share encrypted data with multiple authorized users, by distributing keys having attribute-based access privileges. In this system users can encrypt and decrypt messages solely based on attributes. User attributes such as name, mobile number, social security number, location, role in an organization, etc. can be used for encryption and decryption of data. In a system with multiple data owners and user such technique would prove inefficient as each user would receive keys from multiple data owners; even though key has same set of attributes. It requires constant availability of data owner which hampers flexibility and mobility. Also being computationally expensive it cannot be used for resource constrained mobile devices.

A Role-Based Access Control (RBAC) model [4] proposed by Lan Zhou, Vijay Varadharajan, and Michael Hitchens uses a system in which, data objects are assigned access permissions. These permissions are mapped to appropriate roles and roles are mapped to users. Here the data owner

encrypts the data in such a way that only the users with appropriate roles as specified by a RBAC policy can decrypt and view the data. The cloud provider is not able to see the content of the data as a role is not assigned to it. A user is assigned only when the owner has encrypted and assigned data for that role. Whenever a user is revoked it is denied from accessing the encrypted data. One of the drawback of the system is that data owner is solely responsible for providing access to encrypted data which can place additional burden of computation on owner, also requires constant availability of data owner.

Public-Key Infrastructure (PKI) also known as asymmetric key cryptography is a class of cryptographic algorithms which require two separate keys which are linked mathematically, one of them is published publicly and other is kept secret. A public key is generally used to verify a digital sign or to encrypt plain text message. Private-key is used to create a digital sign or to decrypt cipher text message. Public-key algorithms are computationally expensive as they require factorization of large prime numbers or integers. This imposes an extra burden of computation and storage on data owner.

Zhifeng Xiao and Yang Xiao [5] in their work have reviewed current security and privacy issues in cloud computing environment. Security and privacy attributes such as integrity, confidentiality, availability, privacy-preservability and account-ability are five most representative issues identified in their work. Also existing cloud defence strategies, vulnerabilities that can be exploited by attackers and relationships between security issues are taken into account.

In this paper we have suggested a system to bridge above gaps by providing a unified solution for shared data in mobile cloud environment, preserving privacy of user on multiplatform mobile environment along with reducing burden of computation for mobile users.

3. Proposed System

The CSP provides storage for users on cloud servers which are geographically dispersed. Data stored at CSP can be accessed by user through Internet which is generally considered as insecure medium. Network can be accessed by users through ISP's and Mobile Network Operators. Mobile users access Internet via GPRS, 3G, 4G or Wi-Fi access points, but due to mobility and limited network coverage, mobile users suffers from constant connectivity.

Fig.1 shows proposed system architecture which shows, CSP in public cloud that administers the access to cloud resources, which includes requests for uploading and downloading the data. A Manager is a Trusted Authority that forms a part of organizations private cloud, also acts as a Cloud Auditor [6]. Manager maintains database consisting private keys of authorized mobile users, while the public keys are stored and distributed by the CSP itself. CSP is also responsible for reading and writing data from permanent or replicated data store on behalf of client. User data occasionally undergoes transformation from one version to another by a process called as re-encryption without intermediate decryption step. A mobile user acting as data owner provides access to stored data to other users having permissions and satisfying required attributes. Cloud is a highly scalable system where users are thou-sands or millions in number, constantly accessing the system. CSP is considered as honest entity, follows protocols and does not denies service to authorized users, but may read data out of curiosity. Also CSP has administrative privileges and can copy, modify or delete data of client. So to preserve integrity and privacy data should be stored and remain in encrypted form all the time. Also, the communication channel i.e the Internet through which user and CSP communicate is subjected to eavesdropping, so user data cannot be exchanged in plain text.

Algorithm

In the proposed algorithm modifications are proposed to base system i.e CP-ABE such that key functions are reassigned to different entities to achieve scalability and to reduce the mobile user communicational, computational workload. Generation of key pairs is done by combined efforts of data owner and Manager. Complex and expensive operation of pairing is done by CSP or Manager thus relieving mobile user resources. The cloud provider is unable to access stored data due to lack of required keys. Combination of Proxy based encryption with CP-ABE is used for automatic data re-encryption in case of user revocation. This dual-encryption scheme, combines cryptographic techniques to provide greater flexibility and access control.

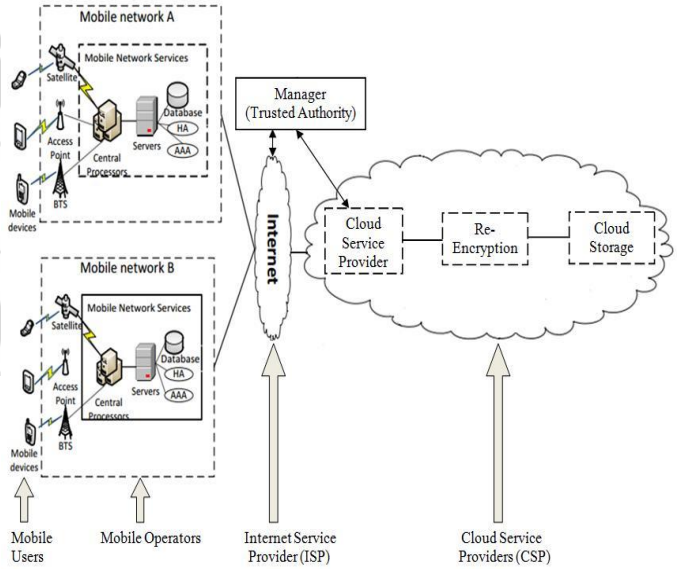

Figure 1: System Architecture

The algorithm is discussed below:

Let f be generator function, used to generate keys. Also defined α, β, v are set of random prime numbers of order p, used for key generation key generation.

Initial Setup ( ) → SK, PK, SSK, SPK, GSK, GPK
Mobile owner U_0 interested in storage of data on to the cloud generates secret key SK and public key PK by using

generator function *f* and random number β, which are further, used for generation of storage secret and public keys SSK and SPK respectively.

Data owner uses 256-bit AES symmetric key encryption to encrypt entire message, this key itself is now encrypted using proposed system. A Manager *M* then chooses random value α and computes f^{α} which forms storage secret key SSK by using same generator function *f*. It then performs paring operation calculate $e(f,f)^{\alpha}$ which is used to form storage public key SPK. To provide additional level of security data owner can also generate group keys for subset of users. Group keys GPK and GSK are computed by the owner by using the function *f*. The components of keys generated by user and manager are given as follows

$$SK = \{\beta\} \text{ and } PK = \{f^{\beta}, f^{1/\beta}\}$$
$$SSK = \{\alpha, f^{\alpha}\} \text{ and } SPK = \{f, f^{\beta}, f^{1/\beta}, e(f,f)^{\alpha}\}$$
$$GSK = \{v\} \text{ and } GPK = \{f^{v}\}$$

GPK is uploaded to cloud for public access while GSK is preserved with the data owner or optionally given to Manager for distribution amongst the authorized users.

Table 1: Symbolic Notations Legend

Symbol	Description
CSP	Cloud Service Provider
M	Manager (Trusted Authority)
A	Attributes Set
Ug	User Group
M	Plain text message
CT	Cipher text
RK	Re-encryption Key
SPK	Storage Public Key
SSK	Storage Secret Key
SK	Owner Secret Key
PK	Owner Public Key
GSK	Group Secret Key
GPK	Group Public Key
DSK	Data Secret Key

Encryption (SPK, GPK, m) → CT
Any user encrypting data can use publicly available storage public key SPK and encrypt message m. If the encryptor wish to restrict the encrypted data for a group of users *Ug*, then it can use group key GPK which is publicly available with CSP. Data encryptor also specifies set of attributes A to be required for decryption. Cipher text is formed by user and uploaded to cloud, shown as follows

$$CT_0 = \{v=0, C_{0msg}=m.e(f,f)^{\alpha s}, C_{0grp}=f^{vs}\}$$

Re-Encryption (CTx, RK) → CTy
Whenever a user leaves authorized member group *Ug*, access rights of user must be revoked. This results in formation new group key GSK generation and distribution among remaining authorized users of group *Ug*. The cloud provider is then requested to perform re-encryption on stored data by use of re-encryption key RK, which is computed either by data owner or Manager using group key GSK. The re-encryption key can be generated from group keys *v* and f^{v} used as version 0 and version x of cipher text.

$$RK\ 0 \rightarrow x = \{ v_x/v_0 \}$$

The cloud provider now computes new cipher text CT*x* by using this re-encryption key.

Data Key Generation (SSK, SSK, A) →DSK
Manager runs a key generation algorithm *f* to form data secret key DSK which requires storage public key SPK, storage secret key SSK, and set of attributes required to decrypt data.

Data secret key DSK is distributed among authorized member group *Ug* holding necessary attributes. DSK may also be given to data owner on demand for peer-to-peer distribution. The availability of data owner in not necessary during key generation, thus relieving from expensive cryptographic operations. Manager select a random number ð and calculates (α + ð) to form $f^{(\alpha+\delta/\beta)} = (f^{1/\beta})^{\alpha+\delta}$. Thus manager and data owner does not reveal their private keys to each other. As data owner is not participating in key generation, it need not requires to be available all the time. To calculate other subparts of key manager chooses random prime number $a_i \in Z_p$ for each attribute in set A.

$$DSK = \{ f^{(\alpha+\delta/\beta)}, i \in A: D_i = f^{a} . H(i)^{ai,} D'i=f^{ai}\}$$

Decryption (CT, DSK, SPK, GSK) → m
Any authorized user holding required set of attributes can download and decrypt CT by using data secret key DSK obtained from manager, SPK and GSK obtained from cloud provider to reveal plain text message m.

4. Implementation

The proposed protocol was implemented using Java Server Pages (JSP), MySQL Database and was deployed on commercially available JElastic Cloud, which is IaaS and PaaS service provider. An existing implementation of CP-ABE in Java was used as a baseline for system. An Instance of JElastic compute unit hosting Apache Server and MySQL database was user to run Java Application performing proposed functions. Clients are using either a desktop computer or mobile phone having minimum 1GB of RAM and processor of 1GHz were used to access the application hosted in cloud. The connection between app hosted in cloud and smartphone or desktop client was done through HTTP requests. Multiple iterations of encryption and decryption along with other proposed functions were run to evaluate the performance of algorithm. Table 2 shows the comparison of timing in milliseconds required for each operation of proposed system and base system.

Table 2: Performance of Base system and Proposed system

Function	Baseline System	Proposed System
Data Owner Setup	426	52
Manager Setup	n/a	50
Key Generation	743	102
Encryption by Owner	632	267
Encryption by CSP	n/a	200
Re-encryption	n/a	111
Decryption	1257	496

5. Conclusion

In this paper we have proposed a system for securing data of mobile user in the cloud. Cloud provider is unable to read stored data; authorized user may do so by satisfying required attributes. In this algorithm key generation and encryption process is done co-operatively by data owner, trusted authority and cloud provider, reducing the burden of mobile user. The user is not required to perform costly pairing operations as they are performed by manager and cloud provider. This helps in conserving the storage space, battery as well as computations required for wireless communication. Additionally in case of user revocation, re-encryption is performed with no intermediate decryption by the cloud provider, without hampering the data integrity. Our system uses a cloud application for increased availability on multiple mobile platforms.

References

[1] Peter Mell, Timothy Grance, ”The NIST Definition of Cloud Comput-ing,”National Institute of Standards and Technology, U.S Department of Commerce, NIST Special Publication 800-145, September 2011.
[2] Niroshinie Fernando, Seng W. Loke, Wenny Rahayu, ”Mobile Cloud Computing: A survey,” Future Generation Computer Systems 2013.
[3] 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.
[4] 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.
[5] Zhifeng Xiao and Yang Xiao, ”Security and Privacy in Cloud Com-puting,” IEEE Communications Surveys and Tutorials, Vol. 15, No. 2, Second Quarter 2013.
[6] Fang Liu, Jin Tong, Jian Mao, Robert Bohn, John Messina, Lee Bad-ger and Dawn Leaf, ”NIST Cloud Computing Reference Architecture,”
National Institute of Standards and Technology U.S Department of Commerce, NIST Special Publication 500-292, September 2011.
[7] Michael Hogan, Fang Liu, Annie Sokol, Jin Tong, ”NIST Cloud Comput-ing Standards Roadmap”National Institute of Standards and Technology, U.S Department of Commerce, NIST Special Publication 500-291, July 2011.
[8] Boyang Wang, Baochun Li and Hui Li, ”Oruta: Privacy-Preserving Public Auditing for Shared Data in the Cloud”.