Survey Paper on Mobile Cloud Computing based Secure Data Management

Mr. Nilesh Bhalchandra Patil

Department of CSE, Vindhya Institute of Technology & Science, India

Abstract - **Cloud computing offers efficient computing experience and computational resources. For utilizing the service of cloud no need to install and maintain the software's and other resources in the local machine. Using simple internet connectivity any one can utilize the service of cloud. In addition of that it offers secure data hosting, transfer and sharing services. Therefore the security of the parked content in cloud storage is a primary and essential concern in cloud computing. Thus the security of the cloud is essentially strong and the private internet access area is also secured. But the data transmission among two secure networks is performed over un-trusted network. Therefore a secure data transfer service is required to design. On the other hand the mobile devices are built with efficient processing ability but their storage support is found smaller. Thus a data hosting service is desired to implement for mobile devices. This paper gives an overview of the state of mobile cloud computing and their secure cloud storage techniques for data management. Additionally, for specification of the paper, we suggest our solution along with problem identification.**

Keywords: Mobile cloud computing, Data security, Attribute based Encryption, Cryptography, Cipher-text Policy, Data Storage.

I. INTRODUCTION

The success of modern day technologies highly depends on its effectiveness of the world's norms, its ease of use by end users and most importantly its degree of information security and control. Cloud computing is a new and emerging information technology that changes the way IT architectural solutions are put forward by means of moving towards the theme of virtualization: of data storage, of local networks (infrastructure) as well as software [1-2].

The cloud is a new generation computing and it provides very effective services for utilizing it remotely without installation and maintenance. In this paper work the mobile cloud is key area of concern. Now in these days a number of applications are developed using the support of mobile devices and these applications are becomes more popular due to portable use of mobile device and tablets. Some of these applications are backup and storage management and some of them for contact and private data management. In this presented work a mobile cloud concept is desired to design which is capable to manage the entire kind of data with secure manner [3-4].

This mobile application is designed for the purpose of maintaining the online mobile data. The user can sign in their username and password. The online storage mobile data contain details about user data what they upload in cloud and also they can view the data simultaneously. In case user loss the mobile, they can retrieve all the data through web.

Therefore the private and sensitive data is managed over the cloud platform through the mobile device. But security on cloud and during data transmission through the public area network is leads to study about the cloud data security and network based data security.

II. BACKGROUND

A. Mobile Cloud Computing

Mobile Cloud Computing (MCC) is combination of two terms, mobile computing and cloud computing. Mobile computing is provision of applications on mobile devices. Cloud computing refers to getting paid services either in the form of infrastructure, platform or software through internet based cluster of distributed servers. Mobile cloud computing is provision of mobile applications using cloud to give more power to mobile devices towards computing, in spite of resource limitations in mobile devices [5].

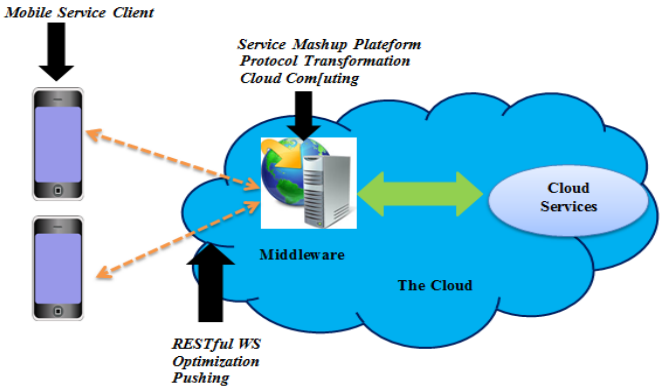

Figure 1: Mobile Cloud Computing Architecture

In above figure, architecture of MCC is presented. As per the architecture presented in above figure, middleware such as Simple Object Access Protocol (SOAP) or Representational State Transfer (REST) web services can be useful to consume the service and then delivering the results to the mobile client. The steps are as follows:

- ✓ The mobile client sends a HTTP GET request to the middleware.
- ✓ The middleware with interaction with the web service.
- ✓ Then middleware extracts the required service results from the original service result and prepares a new service results in particular format and returns this result to the mobile client. A middleware is required as cloud services don't support mobile devices [6].

B. Attribute Based Encryption

A crucial security feature of Attribute Based Encryption is collusion-resistance: An adversary that holds multiple keys should only be able to access data if at least one individual key grants access [7]. The goal is to contribute security and access control. Attribute-based encryption (ABE) contains a public-key based one to many other encryptions that allows users to encrypt and decrypt data based on user attributes. In that the secret key of a user and the cipher text are reliant upon attributes. In this type of system, the decryption of a cipher text is probable only if the set of attributes of the user key contest the attributes of the cipher text. Decryption is only desirable when the number of matching is at minimum a threshold value d. Collusion resistance is deciding security feature of Attribute-Based Encryption. An attacker that holds multiple keys should only be able to access data if at least one has their own key grants access [8].

In Sort we can say that-

ABE is

a. A form of Public-Key Cryptograph

b. Based on Identity-Based Encryption (IBE)

c. In ABE, messages are encrypted under arbitrary attributes.

d. The defined attributes are represented as regular ASCII strings. In turn, these strings are parsed and tokenized and a policy is created and later on verified.

e. Recipients can decrypt the message (cipher-text) only if their keys match specified attributes during the creation of the cipher-text

C. Cryptography

Cryptography is the art of achieving security by encoding messages to make them non-readable. Cryptography is the practice and study of hiding information. In modern times cryptography is considered a branch of both mathematics and computer science and is affiliated closely with information theory, computer security and engineering. Cryptography is used in applications present in technologically advanced societies; examples include the security of ATM cards, computer passwords and electronic commerce, which all depend on cryptography. One essential aspect for secure communications is that of Cryptography. Cryptography is the science of using mathematics to encrypt and decrypt data. Cryptography enables you to store sensitive information or transmit it across insecure networks (like the Internet) so that it cannot be read by anyone except the intended recipient [9].

D. Classification of Cryptography

Cryptography can be divided into three major category based on the use of key [10] [11].

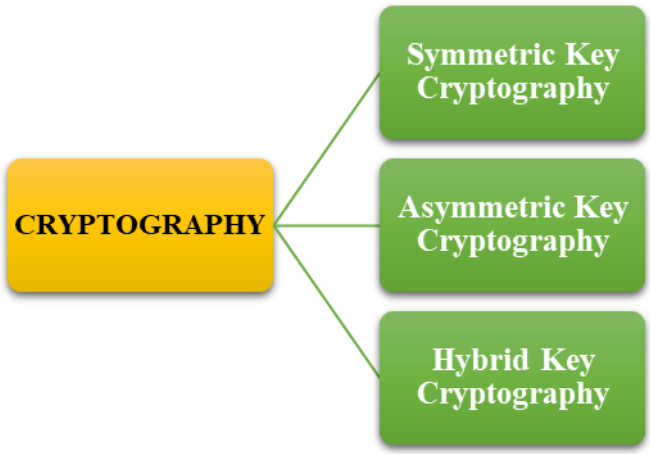

Figure 2: Cryptographic Classification

Symmetric Encryption (Private Key Encryption): In this type of encryption same key is used at the time of encryption and decryption. The key distribution has to be made before the transmission of the information starts. The key plays a very important role in this type of encryption. Symmetric encryption is known as secret key or single key, The receiver uses the same key which the sender uses to encrypt the data to decrypt the message,. This system was the only system used before discovering and developing the public key.

Asymmetric Encryption (Public Key Encryption): In this type of encryption different key is being used for encryption and decryption process. Two different key is generated at once and one key is distributed to other side before the transmission starts. ; Asymmetric encryption is the opposite of symmetric encryption in safety, since it doesn't require sharing the secret key between the sender and the receiver.

Hybrid Encryption (Combination of private and public): Hybrid encryption is a mode of encryption that merges two or more encryption systems. It incorporates a combination of asymmetric and symmetric encryption to benefit from the strengths of each form of encryption. These strengths are respectively defined as speed and security

III. LITERATURE SURVEY

The given section provides the understanding about the data management and security over the public mobile cloud. For that ABE concepts that are recently contributing in mobile cloud environment therefore a number of research articles and research papers are included in this section.

In order to address the problem of achieve a secure and dependable cloud storage service, **Anand Surendra Shimpi et al. [12**] propose a new secure framework. In addition to providing traditional computation services, mobile cloud also enhances the operation of traditional ad hoc network by treating mobile devices as service nodes, e.g., sensing services. The mobile services or sensed information, such as location coordinates, health related information, should be processed and stored in a secure fashion to protect user's privacy in the cloud. Authors present a new mobile cloud data processing framework through trust management and private data isolation. Finally, an implementation pilot for improving teenagers driving safety, which is called FocusDrive, is presented to demonstrate the solution.

Weiwei Jia et al. [13] design a secure mobile user-based data service mechanism (SDSM) to provide confidentiality and fine-grained access control for data stored in the cloud. This mechanism enables the mobile users to enjoy a secure outsourced data services at a minimized security management overhead. The core idea of SDSM is that SDSM outsources not only the data but also the security management to the mobile cloud in a trust way. Our analysis shows that the proposed mechanism has many advantages over the existing traditional methods such as lower overhead and convenient update, which could better cater the requirements in mobile cloud computing scenarios.

Ruixuan Li et al. [14] propose a lightweight data sharing scheme (LDSS) for mobile cloud computing. It adopts CP-ABE, an access control technology used in normal cloud environment, but changes the structure of access control tree to make it suitable for mobile cloud environments. LDSS moves a large portion of the computational intensive access control tree transformation in CP-ABE from mobile devices to external proxy servers. Furthermore, to reduce the user revocation cost, it introduces attribute description fields to implement lazy-revocation, which is a thorny issue in program based CP-ABE systems. The experimental results show that LDSS can effectively reduce the overhead on the mobile device side when users are sharing data in mobile cloud environments.

Effective methods are needed to verify the correctness of the data stored at cloud servers, which are the research issues the Provable Data Possession (PDP) faced. The most important features in PDP are: 1) supporting for public, unlimited numbers of times of verification; 2) supporting for dynamic data update; 3) efficiency of storage space and computing. In mobile cloud computing, mobile end-users also need the PDP service. However, the computing workloads and storage burden of client in existing PDP schemes are too heavy to be directly used by the resource-constrained mobile devices. To solve this problem, with the integration of the trusted computing technology, **Jian Yang et al. [15]** proposes a novel public PDP scheme, in which the trusted third-party agent (TPA) takes over most of the calculations from the mobile end-users. By using bilinear signature and Merkle hash tree (MHT), the scheme aggregates the verification tokens of the data file into one small signature to reduce communication and storage burden. MHT is also helpful to support dynamic data update. In this framework, the mobile terminal devices only need to generate some secret keys and random numbers with the help of trusted platform model (TPM) chips, and the needed computing workload and storage space is fit for mobile devices. Our scheme realizes provable secure storage service for resource-constrained mobile devices in mobile cloud computing.

The problem of simultaneously achieving fine-grainedness, scalability, and data confidentiality of access control actually still remains unresolved. **Shucheng Yu et al. [16]** addresses this challenging open issue by, on one hand, defining and enforcing access policies based on data attributes, and, on the other hand, allowing the data owner to delegate most of the computation tasks involved in fine-grained data access control to untrusted cloud servers without disclosing the underlying data contents. Authors achieve this goal by exploiting and uniquely combining techniques of attribute-based encryption (ABE), proxy re-encryption, and lazy re-encryption. This proposed scheme also has salient properties of user access privilege confidentiality and user secret key accountability. Extensive analysis shows that this proposed scheme is highly efficient and provably secures under existing security models.

IV. PROBLEM FORMULATION

Due to computational need and growing technology needs to invent new ways for data analysis and their importance in our life. Due to computer human interaction a huge amount of data daily generated some of them are essential and private and user want to secure for long time on the other hand some of the data is not much essential. In order to protect and preserve data on local machines and local storage is suspicious due to hardware faults and other physical damages thus cloud storage is required to creating backups and preserves the contents for long term. Additionally the storage of data needs security and privacy and protection from the other users and attackers thus a new secure storage and privacy preserving system is required for managing sensitive and private data with intermediate security from the attackers and malicious programs. Problem formulation

In order to provide the secure mobile cloud data storage services the following issues are considered.

- ✓ Mobile devices are built with efficient computing but the storage and backup is not much secure.
- ✓ Transmission of data between two secure devices is performed using public and untrusted network.
- ✓ Data in cloud is stored at random in the cloud space private and sensitive data can be mismanaged and produces the redundancy during their management.

V. SOLUTION DOMAIN

The proposed solution leads to solve the issue of small storage space for user data collection and also provides the solution during the data transfer and man in middle attack. Therefore the following solution is incorporated in this solution.

- ✓ Providing a secure and different level of data management scheme for private data storage and normal data storage
- ✓ Solution incorporate the additional security of private data management
- ✓ During data transmission is based in trust management and token based data exchange.

VI. CONCLUSION

Although mobile Cloud computing can be seen as a new phenomenon which is set to revolutionize the way we use the Internet, there is much to be cautious about. There are many new technologies emerging at a rapid rate, each with technological advancements and with the potential of making human's lives easier. However one must be very careful to understand the limitations and security risks posed in utilizing these technologies The key goal of the proposed survey work is to enhance the security of the mobile device from the unauthenticated data access, malicious programs and physical damage of the mobile device therefore by using the secure cloud data storage the mobile devices data is preserved. In addition of that the authentication system is improved for optimizing the data validity for long term storage.

REFERENCES

[1] Leavitt N, 2009, 'Is Cloud Computing Really Ready for Prime Time?', Computer, Vol. 42, pp. 15-20, 2009.
[2] Weinhardt C, Anandasivam A, Blau B, and Stosser J, 'Business Models in the Service World', IT Professional, vol. 11, pp. 28-33, 2009
[3] M. Sulochana and Ojaswani Dubey, "Preserving Data Confidentiality using Multi-Cloud Architecture", 2nd International Symposium on Big Data and Cloud Computing (ISBCC'15), Procedia Computer Science 50 (2015) 357 – 362.
[4] Ramgovind, Sumant, Mariki M. Eloff, and Elme Smith. "The management of security in cloud computing", In Information Security for South Africa (ISSA), 2010, pp. 1-7. IEEE, 2010.
[5] Khan, Abdul Nasir, ML Mat Kiah, Samee U. Khan, and Sajjad A. Madani. "Towards secure mobile cloud computing: A survey." Future Generation Computer Systems 29, no. 5 (2013): 1278-1299.
[6] Atul Gonsai, Mr. Rushi Raval, "Mobile Cloud Computing: A Tool for Future", International Journal of Computer Science & Engineering Technology (IJCSET), Volume 4, July 2013, PP. 1084-1090.
[7] Abdul Raouf Khan, "Access Control in Cloud Computing Environment", ARPN Journal of Engineering and Applied Sciences, PP. 613 - 615 Volume 7, No. 5, May 2012.
[8] Sushmita Ruj, Milos Stojmenovic, and Amiya Nayak, "Privacy Preserving Access Control with Authentication for Securing Data in Clouds", 12th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing, PP. 556 – 563, 2012.
[9] Stallings, William. Cryptography and network security: principles and practice. Pearson Education India, 2003.
[10] Manoj Kumar Pandey, Mrs. Deepty Dubey, "Survey Paper: Cryptography The art of hiding Information", International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), PP. 3168-3171, Volume 2, December 2013.
[11] Mohammed AbuTaha, Mousa Farajallah and Radwan Tahboub, "Survey Paper: Cryptography is The Science of Information Security", International Journal of Computer Science and Security (IJCSS), PP. 298- 309, Volume 5, 2011.
[12] Shimpi, Anand Surendra, and R. Chander. "Secure Framework in Data Processing for Mobile Cloud Computing." International Journal of Computer & Communication Technology, 2012, Volume-2, Issue-3
[13] Jia, Weiwei, Haojin Zhu, Zhenfu Cao, Lifei Wei, and Xiaodong Lin. "SDSM: a secure data service mechanism in mobile cloud computing." In Computer Communications Workshops (INFOCOM WKSHPS), 2011 IEEE Conference on, pp. 1060-1065. IEEE, 2011.
[14] Li, Ruixuan, Chenglin Shen, Heng He, Zhiyong Xu, and Cheng-Zhong Xu. "A Lightweight Secure Data Sharing Scheme for Mobile Cloud Computing", IEEE Transactions on Cloud Computing (2017).
[15] Yang, Jian, Haihang Wang, Jian Wang, Chengxiang Tan, and Dingguo Yu. "Provable data possession of resource-constrained mobile devices in cloud computing." JNW 6, no. 7 (2011): 1033-1040.
[16] Yu, Shucheng, Cong Wang, Kui Ren, and Wenjing Lou. "Achieving secure, scalable, and fine-grained data access control in cloud computing", In INFOCOM, 2010 proceedings IEEE, pp. 1-9, IEEE, 2010.