Towards Secure Data Distribution Systems in Mobile Cloud Computing: A SURVEY

Anusree Radhakrishnan[1] Minu Lalitha Madhav[2]

PG Scholar[1], Asst. Professor[2]
Dept. of Computer Science & Engineering, Sree Buddha College of Engineering, Pattoor, Alappuzha

---

ABSTRACT-*Electronic devices are developing day by day. Although their need increases compared to a desktop mobile devices has some of the demerits in the sense that they have limited computation capability and storage. So that they cant meet all the needs of the user. The solution is to integrate the mobile computing with the cloud computing technology. The new name Mobile cloud computing (MCC) opens an extended boundary for mobile users. But when we integrate the cloud computing concept with the mobile technology, the issues that present in the cloud computing is still there. Privacy, data integrity, authentication such terms should be maintained control. For to ensure it different cryptographic primitives can be used.*

Keywords - MCC, access control , data integrity, authentication, security

INTRODUCTION

Cloud computing provides immense storage for different clients. The main advantage of the cloud is the storage itself. Most of the organizations now a days depends on the clouds . So that they are not bothered about the economic cost of the storage hardware. Cloud provides low cost and good reliability. But here also when the data is shared we need to ensure that whether it is shared to the right person. According to a survey conducted in USA 90% of the citizen uses the cloud facility for storage purposes. Within this 90% about 80% of them are worried about the security of their data. Since the data is completely handled in the cloud the data security is completely depends on the ability of the technical team whom are handling the cloud. Any type of security loop hole will harm the trust of the cloud. Now a days it is quite common to use the cloud with the help of the mobile device. By a recent study the cloud will acquire 90 % of the citizens for their mobile devices. To offload storage to the cloud, there are many existing storage services for mobile devices, such as Dropbox, Box, iCloud, Google Drive, and Skydrive We are integrating the Mobile computing nad Cloud computing, surely there will be some security issues. In this survey we are looking for some of the security preserving paradigms in MCC environment. The following section is the literature review section of 5 papers. Along with it merits and demerits are also mentioned. Last the review section ends with a conclusion

LITERATURE REVIEW

In [1] Huaquan Wang proposes a provable data possession protocol. Recently the demand of the cloud computing increased due to its ability , flexibility and large storage capacity. . Normally in public clouds the user keeps the data in the server but they can't access the data remotely. Thus, information security is an important problem in public cloud storage, such as data confidentiality, integrity, and availability. Some cases the client can't check the possession of the data. This paper tells about a proxy provable data possession (PPDP). In public clouds, PPDP is a matter of crucial importance when the client cannot perform the remote data possession checking. Here it focuses on the PPDP system model, the security model, and the design method. Based on the bilinear pairing technique . It Verifies whether the server possess correct data.

Advantages

- ❖ The overhead at the server is low.
- ❖ Performance of PDP is bounded by disk I/O and not by cryptographic computation

Disadvantages

- ❖ Performance decreases as the no. of users increases

Dan Boneh describes a broadcast encryption in [2]. Some set S of the users will be listening to the broadcast channel. A broadcaster will encrypt the message. I order to decrypt it the user can use the private key. We can say that the system is collusion resistant in the sense that the users outside the broadcast can't collude the information. The broadcaster can encrypt to any subset S of his choice. In the file system the access control can be provided by this broadcast encryption.

Advantages

Each user only has to keep a single secret key

Disadvantages

It needs more storage and time for to implement.

Paper [3] is based on a novel remote based data possession checking protocol. Most of the data owners will outsource this data to cloud storage. But the security of the data is the main issue here. . To solve this problem some remote data possession checking protocols are used . But most of the techniques will not support the data dynamics. RDPC is a solution to the above problem. And it is based on homomorphic hash function. The scheme is secure against forgery attack, replay attack, reply attack. An operation record table is used to track the files. Optimised implementation of ORT is used here. It has Less computation + Communication cost. But Need to access the entire file block for each challenge

[4] describes an attribute based encryption. Hui Cui, Robert H. Deng describes AB scheme. Here the data owner will save all the data in the cloud and the data will be shared with the users having some specific credentials. In order to save the storage space duplicate copy of the data should be avoided. But most of the cases deduplication is not supported. But in this paper deduplication is supported. Where a private cloud is responsible for duplicate detection and a public cloud manages the storage. Compared with other schemes this AB schemes has some of the advantages. Firstly, it can be used to confidentially share data with users by specifying access policies rather than sharing decryption keys. Secondly, it achieves the standard notion of semantic security for data confidentiality while existing systems only achieve it by defining a weaker security notion.

[5] describes Cloud Security Using Service Level Agreements. It make use of some of the service level agreements. Users can specify the needs. And with the help of the security level agreement they can be provided. Te security level agreement consist of different security parameters in different point of view.

Advantages

- ❖ Customers visually comparing CSPs based on their offered secSLAs.

Disadvantages

- ❖ Nothing mentioned about advanced security metrics/Cloud secSLA notions
- ❖ e.g., uncertainty, end-to-end security evaluation

In [6] Giuseppe Ateniese says about a Proxy reencryption(PRE). A significant benefit brought by PRE is that each user only has to keep a single secret key and does not suffer from the key escrow problem. Concretely, in a PRE system, a data owner Alice can generate a re-encryption key to help Bob transform a ciphertext under her own public key to ciphertext of the same message under Bob's public key, such that Bob can decrypt it by using his own secret key to obtain the original message. However, the access control provided by a traditional PRE (including ID-based PRE) is in an "all or nothing" manner . Namely, a user with a corresponding re-encryption key can read all the data of the data owner, but a user without the re-encryption key cannot read any private data of the data owner. This is not applicable to the case that the data owner only wants to share part of his data with others. In order to realize flexible access control, a new variant of PRE can be used

Advantages

a) Implementation is simple

Disadvantage

a) Some area is error prone

CONCLUSION

MCC is an evolving technology in which many more features are adding to it.By analysing these features we can conclude that the only problem with the system is of security in data sharing. MCC has to follow a number of features such as data sharing access control, authentication ,integrity etc.

But we cant design one system with all these features. For all security related frameworks the main purpose should be to ensure the security of data. A number of security frameworks has already been designed to this proposed. By analysing 6 of these methods we could conclude that a lot of research are going on in the field of mobile cloud computing

REFERENCES

[1] Huaqun Wang, "Proxy Provable Data Possession in Public Clouds" JOURNAL OF L ATEX CLASS FILES, VOL. 6, NO. 1,.

[2] Dan Boneh, Brent Waters, Craig Genry, Collusion Resistant Broadcast Encryption With Short Ciphertexts and Private Keys," in ICNP '05, 2005.

[3] Hao Yan, Jiguo Li, Jinguang Han, "A Novel Efficient Remote Data Possession Checking Protocol in Cloud Storage " Carnegie Mellon University Research Showcase @ CMU.

[4] Hui Cui, Robert H. Deng, Yingjiu Li, and Guowei Wu, "Attribute-Based Storage Supporting Secure Deduplication of Encrypted Data in Cloud," JOURNAL OF L ATEX CLASS FILES, VOL. , NO. , MONTH 2016.

[5] Y. Xiang, W. Zhou, and M. Guo, "Cloud Security Using Service Level Agreements. Parallel Distrib. Syst., vol. 20, no. 4, pp. 567–580, 2009.

[6] Giuseppe Ateniese, Kevin Fu, Matthew Green, and Susan Hohenberger. "Improved proxy re-encryption schemes with applications to secure distributed storage. ACM Trans. Inf. Syst. Secur., 9:1–30, February 2016..