Secure Encryption Mechanism in Multi –Mobile Cloud Computing

Nisha Mohan P M[1] Anju Rachel Oommen[2]
[1,2]Assistant Professor
[1,2]Department of Computer Science and Engineering
[1,2]Mount Zion College of Engineering, Kadammanitta, Kerala.

Abstract— Mobile Cloud Computing is a form where applications and mobile data are downloaded stored and hosted using cloud computing technology. The homomorphic encryption allows making calculations on encrypted data without decrypting it. It does not provide proper security. This paper describes a new technique which provides secure encryption in multi-mobile cloud computing environment, i.e. Multi Mobile Encryption Mechanism (MMEM). Using this mechanism to improve the availability, integrity and confidentiality of information stored in the different cloud providers by using the multi-mobile cloud

Key words: cloud computing, multi-mobile, MMEM, security

I. Introduction

Cloud computing is a internet – based computing that provied computer processing resources and data to computers and other devices on demand. It is a flexible, commercial, and complete delivery platform for providing business or consumer IT services of the Internet[2]. Mobile cloud computing is a new prototype that allows users to fully consume mobile technologies more than the resources calculation limit. It ensures business offers for mobile network operators as well as cloud providers [1]. Multi mobile cloud computing at its simplest, refers to an infrastructure where both the data storage and data processing happen outside of the mobile device.

The major concern of the multi – mobile cloud is security because many attackers regularly try to take benefit to take access data stored in the remote cloud servers. Multi-mobile cloud allows among others to decrease the risk of data loss, it duplicates the capital and allows separating the security responsibilities across multiple servers.

The focus of this paper, propose a mechanism, MMEM (Multi-Mobile Encryption Mechanism) to produce a security platform that provides the availability, integrity and confidentiality of information stored in the different cloud providers by using the multi-mobile cloud. MMEM propose a virtual storage space system to construct a cloud of clouds. This allows explanatory the boundaries of individual clouds using many reliability and security techniques.

II. Security concern in multi-mobile cloud computing

A. *Multi- Mobile Cloud Computing:*

Mobile Cloud Computing is a form where applications and mobile data are downloaded stored and hosted using cloud computing environment. The Mobile Cloud computing is mainly used to transport our personal data from the mobile device to remote cloud servers. This mechanism permitted altering our lives because all data, applications, and services that would be accessible anytime.

Multi-mobile cloud at rest suffers in circumstances of security because the data stored in the cloud are often personal. So they are under fire by attackers to use special vulnerabilities in computer networks in classifying to remove this data.

B. *Security Issues:*

The multi-mobile cloud computing has grow to be very accepted and used by numerous applicants. Despite the big advances in constructing of mobile devices, they still suffer several limitations like battery lifetimes, capacity of storage, computational power. Many issues also attacks the multi-mobile cloud to get maximum maturity using in banking transactions, sharing and storing of personal data.

Illegal server attack: As the flow of data circulating between users and cloud servers is running scared through internet, various attackers pass themselves as genuine cloud servers to get back all the flow of data.

Brute force attack: Data encryption requires extensive computing power. It requires users to use little encryption keys.

Counterfeit attack: It help the attackers to create a fake signature during data exchange between one entity to another in a network.

III. Proposed mechanism

In the proposed paper Multi-Mobile Encryption Mechanism (MMEM) is used for improving the availability, integrity and confidentiality of information stored in the different cloud providers by using the multi-mobile cloud. The architecture consists of four clouds and each cloud uses its personal interface. The architecture is presented in client machines as a software library allowing reading and writing data stored in the cloud.

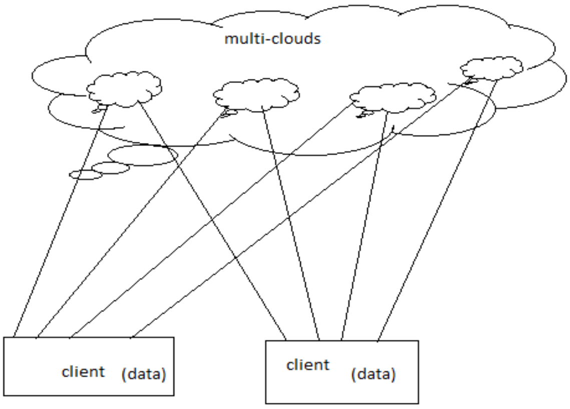

Fig. 1: Architecture of MMEM

The architecture uses one algorithm

MMEM-CA (Confidential and Available): This algorithm encrypts data before storing them in the Multi-Clouds with a symmetric encryption. The data is divided in to block as f+1 blocks are necessary to recover the original data, f or less block don't give any information about the data stored in the Multi-cloud

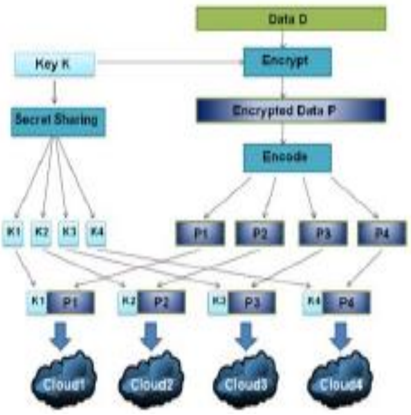

Fig. 2: MMEM-CA Algorithm

IV. Conclusion

The MMEM mechanism has developed a security architecture that can produce a signature to make sure the integrity and reliability for a data encryption scheme. Here we develop a fully homomorphic encryption scheme to be more well-organized in a multi-mobile cloud computing environment. As a future work, we can add a homomorphic crypto system in MMEM algorithm, exactly in the secret sharing scheme to give improved results while dealing with sensitive data.

References

[1] Maha Tebaa, Said El Hajji, « Secure Cloud Computing through Homomorphic Encryption», International Journal of Advancements in Computing Technology (IJACT) Volume5, Number16, 2013.

[2] Mohammed A. Al Zainand and al. «A Survey on Data Security Issues in Cloud Computing: From Single to Multi-Clouds», Journal of Software, Vol 8, No 5 (2013), 1068-1078, 2013.

[3] Monali Shrawankar and al. «Comparative Study of Security Mechanisms in Multi-clouds . Environment», International Journal of Computer Applications (0975-8887) Volume 77, No.6, 2013.\

[4] N. Fernando, Seng W. Loke, W. Rahayu, "Mobile cloud computing: Asurvey", Future Generation Computer Systems 29, pp. 84–106, 2013.

[5] D. Ardagna, "Cloud and Multi-Cloud Computing: Current Challengesand Future Applications", IEEE/ACM 7th International Workshop onPrinciples of Engineering Service-Oriented and Cloud Systems, 2015.