An Integrated Secure Cloud Storage Architecture for Ensuring Integrity of Data using Hybrid Encryption Schemes in Cloud IoT Environment

Prof. Y. Sunil Raj, Dr. S. Albert Rabara & Mr. V. K. Sanjeevi

Assistant Professor, Department of Computer Science, St. Joseph's College (Autonomous), Trichy, India
Associate Professor, Department of Computer Science, St. Joseph's College (Autonomous), Trichy, India
Research Scholar, Department of Computer Science, St. Joseph's College (Autonomous), Trichy, India

ysrsjccs@gmail.com, a_rabara@yahoo.com, vksanvi@gmail.com

Abstract
Cloud computing revolutionize the way internet is used during the past few decades. As providing everything in an outsourced fashion, it provides infrastructures such as storage too. Though everything makes it easy for as to store and access data in a fastest and easy manner, their exist security risks if not handled become more dangerous. Strengthening of security in cloud storage is need of the hour, as it is the future technology which is changing the way business is done. This paper analysing the existing security mechanisms and algorithms, could present a novel architecture for enhancing the security of storage. In order to enhance the security, systematicuse of a hybrid algorithm along with a hashing technique is proposed. The validity of the mechanism have been analysed and ensured that if implemented will present better results to the cloud architecture.

Keywords: Cloud Storage, Data Integrity, Encryption, Hashing, DNA, MD5

I. Introduction

Cloud computing being a major technology which outsources almost every as services, is hiding the presence of chief corner stone called Internet. Without its presence, probably Cloud would be existing inside the womb of simpler networks waiting for the birth of Internet. The support of this great giantInfrastructure, Software, and Platform were distributed as service in low cost. Among these infrastructure would encapsulate things such as storage, networking, computation and virtualization.

In this IoT era, data is generated by most living and artificial objects. The data generated by the IoT is shared over the internet, and will be stored on cloud storage. This have become very essential because scaling the size of local storage will be more expensive. As a result most organizations have started using cloud storage for business related transactions. A number of research have been done and architectures have been devised. [Raj et. al., 2019]. Security issues can be resisted with a good architecture. Being a good architecture is alone not enough to secure data. It also requires other security mechanisms to protect the data. The work first analysis the issues that exists in the cloud that allows the data integrity to be affected.

1.1. Security Issues

As everything is available public, security of data becomes the major issue. Also every data is copied to a remote machine adds still more security risks. Therefore using proper security mechanism is very essential to keep the data safe and secure, preventing it from security attacks.

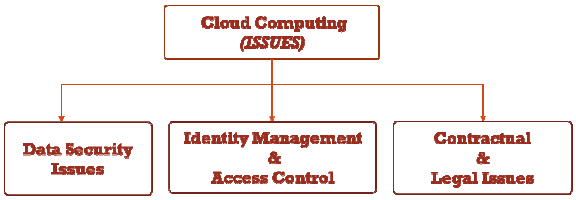

Fig. 1.1 Security Issues in Cloud Computing

The security attacks can be classified as storage based attacks, access control based attacks, identity attacks, contractual and legal issues. Among these analysing storage related attacks could enhance the security of storage, as it is where data stays for a long period of time. Major issues related to data storage are depicted in Fig 1.2.

Fig. 1.2. Data related Issues

1.1.1 Data in-transit

The communication among the entities with a secured communication channel like Transport Layer Security, may give rise to the following issues such as data lineage and data provenance.

Data Lineage: Data lineage is related to the origin of the data and where it moves over a time period. **[Bhadauria,**