A TPM-based Secure Multi-Cloud Storage Architecture grounded on Erasure Codes

Emmy Mugisha, Nanjing University of Science and Technology, Nanjing, China
Gongxuan Zhang, Nanjing University of Science and Technology, Nanjing, China
Maouadj Zine El Abidine, Nanjing University of Science and Technology, Nanjing, China
Mutangana Eugene, Nanjing University of Science and Technology, Nanjing, China

ABSTRACT

In cloud storage systems, data security management is becoming a serious matter. Big data and accessibility power is increasingly high, though the benefits are clear, such a service is also relinquishing users’ physical possession of their outsourced data, which inevitably poses new security risks toward the correctness of the data in cloud. As a result, cloud storage security has become one of the driving components in Cloud Computing regarding to data manipulation trust on both hosting center and on-transit. This paper proposes a TPM-Based Security over Multi-Cloud Storage Architecture (MCSA) grounded on Erasure Codes to apply root of trust based on hardware authenticity. An erasure codes such as Reed-Solomon, is capable of assuring stability in storage costs with best practice to guarantee data accessibility failure recovery. A Multi-Cloud Control Node manages other Control Nodes evolved in the cloud; this work introduces TPM-Based Security functions per Control node in the architecture. This concept will resolve a number of storage security issues, hence Cloud Computing adoption.

KEYWORDS

Cloud Clients, Cloud Storage Vendor, Control Nodes, Erasure Codes, Multi-Cloud, TPM-Based Security

INTRODUCTION

Nowadays, the volume of data produced to be stored is growing higher as detailed in Sakr, Liu, Batista, & Alomari (2011). The growth is revealed when the volume of data is so huge to manage on available systems. The content of large daily weather radar reports, traffic surveillance equipment records, commercial transactions, medical daily reports, and distributed sensor reports are classic examples. Cloud storage providers play a significant role handling these advancement records of other organs flexibly with cost effectiveness, compared to constructing their own infrastructure.

A pay-as-you-go model was introduced for economic realm (Armbrust, Fox, Griffith et al., 2009). The model suggests a user to pay when the service is available (on-demand concept). As a result, users are at the mercy of their cloud service providers (CSP) for the availability and integrity of their data (Trust, Cloud, & With, 2009; Ren, Wang, & Wang, 2012). Although the cloud infrastructures are much more powerful and reliable than personal computing devices, broad range of both internal and external threats for data integrity still exist.

On the other hand, since users may not retain a local copy of outsourced data, there is still room for providers to behave unfaithfully toward the cloud users regarding the status of their outsourced data. For example, to increase the profit margin by reducing cost, it is possible for provider to discard
rarely accessed data without being detected in a timely fashion (Juels & Kaliski, 2007). Similarly, CSP may even attempt to hide data loss incidents so as to maintain a reputation (Ateniese, Burns, Curtmola et al., 2007; Shah, Baker, Mogul, & Swaminathan, 2007; Swaminathan & Baker, 2008). Therefore, although outsourcing data into the cloud is economically attractive for the cost and complexity of long-term large-scale data storage, it’s lacking of offering strong assurance of data integrity and availability may impede its wide adoption by both enterprise and individual cloud users.

Recent works based on this idea has been revised; RACS which uses a proxy server as a broker to manage transactions between customers and cloud storage providers (Abu-Libdeh, Princehouse, & Weatherspoon, 2010).

STRATOS is another implementation of Multi-Cloud. It focuses on automatic cloud provider selection for resource allocation to process running on multiple cloud providers (Pawluk, Simmons, Smit, Litoiu, & Mankovski, 2012). To achieve various data management strategies, it separates data control and execution. This data management is robust and elastic (Ghoshal & Ramakrishnan, 2012).

In order to achieve the assurances of cloud data integrity, availability and enforce the quality of cloud storage service, plus efficient methods that enable on-demand data correctness verification on behalf of cloud users, have to be designed. This work considered erasure coding as a method for distributing data over multiple cloud storage providers. Nevertheless, there is no comprehensive security analysis of the capabilities and potentials of this method in the context of Multi-Cloud storage services. This research provides a general architectural concept for applying erasure coding in combination with hardware TPM-Based security in Multi-Cloud Storage Architecture. The idea is to introduce TPM-Based Security solutions to vulnerable nodes, impacting data accessibility across multiple cloud storage providers based on hardware root of trust.

The Trusted Platform Module (TPM) is a hardware chip designed to enable commodity computers to achieve greater levels of security than was previously possible. There are 100 million TPMs currently in existence (Ryan, 2009). These are commonly in high-end laptops made by HP, Dell, Sony, Lenovo, Toshiba, and others. The TPM stores cryptographic keys and other sensitive data in its shielded memory, and provides ways for platform software to use those keys to achieve security goals. The TPM offers three kinds of functionality: secure storage, platform measurement and reporting and platform authentication. For secure storage, user processes can store content that is encrypted by keys only available to the TPM. In platform measurement and reporting; a platform can create reports of its integrity and configuration state that can be relied on by a remote verifier. In platform authentication, a platform can obtain keys by which it can authenticate itself reliably.

The rest of the paper is organized as follows: Section 2 introduces the Erasure Codes, comparison to replication, our design goal on Cloud Storage Security. A detailed description of our scheme and implementation are provided in Sections 3 and 4 respectively. Section 5 gives a conclusion the whole work.

**Erasure Coding Technique**

In recent years, erasure codes have moved to a fore data failure prevention over storage systems with segmented multiple storage disks. In the storage disks, a k-of-n systematic Maximum Distance Separable (MDS) erasure codes takes k data blocks and produces n – k parity blocks m, such that any subset of k blocks can reconstruct the k data blocks (original data) (Plank, Jianqiang & Schuman, 2009).

Moreover, redundant blocks are considered as linear combinations of data blocks. *Stripe* is the set of the k data blocks and m parity blocks i.e., If $a$ & $b$ are data blocks \{D0, D1, ..., Dk-1\}, then, two parity blocks can be produced; $a+b$ and $a-b$, \{P0, P2, P3, ..., Pm-1\}.
Play That Funky Password!: Recent Advances in Authentication with Music
www.igi-global.com/chapter/play-that-funky-password/123529?camid=4v1a

Toward Proactive Mobile Tracking Management
www.igi-global.com/article/toward-proactive-mobile-tracking-management/140671?camid=4v1a