Chapter 108
High-Throughput Encryption for Cloud Computing Storage System

Yaser Jararweh
Jordan University of Science and Technology, Jordan

Nawaf Abdulla
Jordan University of Science and Technology, Jordan

Ola Al-Sharqawi
Jordan University of Science and Technology, Jordan

Lo'ai Tawalbeh
Jordan University of Science and Technology, Jordan

Mohammad Alhammouri
Jordan University of Science and Technology, Jordan

ABSTRACT

In recent years Cloud computing has become the infrastructure which small and medium-sized businesses are increasingly adopting for their IT and computational needs. It provides a platform for high performance and throughput oriented computing, and massive data storage. Subsequently, novel tools and technologies are needed to handle this new infrastructure. One of the biggest challenges in this evolving field is Cloud storage security, and accordingly we propose new optimized techniques based on encryption process to achieve better storage system security. This paper proposes a symmetric block algorithm (CHiS-256) to encrypt Cloud data in efficient manner. Also, this paper presents a novel partially encrypted metadata-based data storage. The (CHiS-256) cipher is implemented as part of the Cloud data storage service to offer a secure, high-performance and throughput Cloud storage system. The results of our proposed algorithm are promising and show the methods to be advantageous in Cloud massive data storage and access applications.

1. INTRODUCTION

In recent years, Cloud computing has become one of the most significant trends in the IT industry; it provides a whole new platform for high throughput computing and massive data storage needs. Cloud data storage services are among the essentials when building data centers and providing services, such as data backup, file synchronization, and resource sharing. Cloud storage may be accessed through

DOI: 10.4018/978-1-4666-6539-2.ch108

a web-based user interface, or a web service application programming interface (API). This way a Cloud user can access their data at any time and from anywhere, without the need to install a physical storage device on their own machines. Cloud storage providers allow their customers to pay for the storage they actually use (pay-as-you-go), where the providers are designated with the task of maintaining client data using such techniques as data replication, data backup, etc. These features allow customers to focus on their core business.

1.1. Cloud Storage Architecture

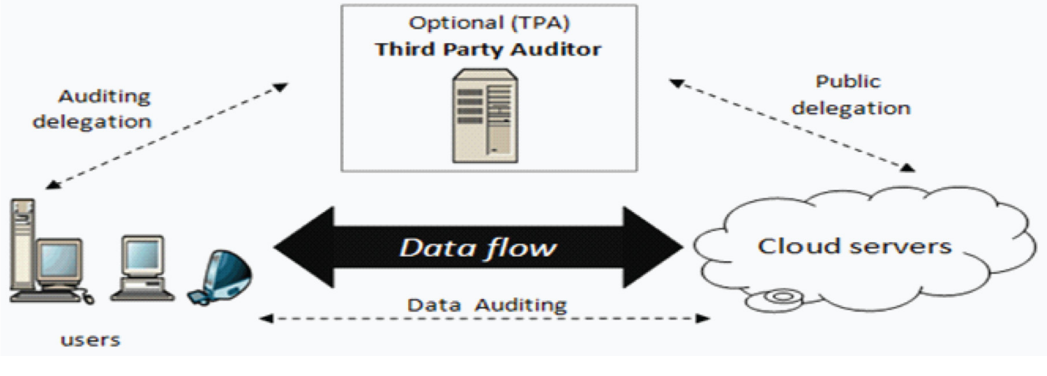
In Wang, Wang, Ren, and Lou (n.d.) provide a network based architecture cloud storage services as depicted in Figure 1. The architecture is composed from the following components:

- **Users:** The component that own and stores data in the Cloud, it can be either an enterprise or an individual customer;
- **Cloud Server (CS):** An entity which provides the data storage service. It commands a significant amount of storage space and computation resources, which are subsequently managed by a Cloud Service Provider (CSP);
- **Third Party Auditor (TPA):** An optional entity which has means and capabilities that a regular user may not have. It is entrusted to assess and expose risks of Cloud storage services on behalf of the users upon request.

In Cloud data storage, users store their data onto a set of Cloud servers, which in turn are running in a simultaneous, distributed, and cooperative manner, as illustrated in Figure 1. Data redundancy can be implemented, and along with some type of erasure correcting code, further fault-tolerance and recovery options can be provided, in case of server crash, as user data grows in size and importance. Since Cloud data resides at CSP's address domain away from user's local site, threats or concerns can come from two different sources; internal and external:

- **Internal attacks:** A CSP can be self-interested, untrusted, or possibly even malicious. It can move data which is rarely accessed to a lower tier of storage than agreed, for monetary reasons (Juels, Burton, & Kaliski, 2007). Additionally, it may attempt to hide data loss incidents due to management errors, Byzantine failures, and so forth (Ateniese, Burns, Curtmola, Herring, Kissner, Peterson, & Song, 2007; Shah, Baker, Mogul, & Swaminathan, 2007; Shah, Swaminathan, & Baker, 2008);
- **External attacks:** These may come from outsiders who are beyond the control do-

Figure 1. Cloud storage system architecture (Wang, Wang, Ren, & Lou, n.d.)



Related Content