Enhancement of the Cloud Data Storage Architectural Framework in Private Cloud

Dr. K. Subramanian[1], M.Mohamed Sirajudeen[2]

[1]Department of Computer Science, V.S.S Government Arts College, Pulankuruchi, Pudukottai, Tamil Nadu, India.
[2]Corresponding Author, Department of Computer Science, J.J College of Arts and Science, Pudukottai, Tamil Nadu, India.

Abstract— *The data storage in the cloud typically resides in a service providing environment collocated with data from different clients. The institutions or organizations moving the sensitive and regulated data into the cloud in order to maintain the account for the means by which the access data is controlled and the data is kept secure. Data can take many forms. The cloud based application development; it includes the application programs, scripts, and configuration settings, along with the development tools. For deployed applications, it includes records and other content created or used by the applications, as well as account information about the users of the applications. Access controls are one means to keep data away from unauthorized users; encryption is another. Access controls are typically identity-based, which makes authentication of the user's identity an important issue in cloud computing. In this research paper focus the cloud data storage architectural frame work of encrypted data.*

Keywords— Data, Secure, Cloud storage and access control.

I. INTRODUCTION

In general, the procedures for protecting data at rest are not as well standardized, however, making the interoperability an issue due to the predominance of proprietary systems. The lack of interoperability affects the availability of data and complicates the portability of applications and data between cloud providers. Currently, the responsibility for cryptographic key management falls mainly on the cloud service subscriber. Key generation and storage is usually performed outside the cloud using hardware security modules, which do not scale well to the cloud paradigm. NIST's Cryptographic Key Management Project is identifying scalable and usable cryptographic key management and exchange strategies for use by government, which could help to alleviate the problem eventually. Protecting data in use is an emerging area of cryptography with little practical results to offer, leaving trust mechanisms as the main safeguard [1].The data sanitization practices that a cloud provider implements have obvious implications for security. Sanitization is the removal of sensitive data from a storage device in various situations, such as when a storage device is removed from service or moved elsewhere to be stored. Data refinement also applies to backup copies made for recovery and restoration of service, and also residual data remaining upon termination of service. In a cloud computing environment, data from one subscriber is physically commingled with the data of other subscribers, which can complicate matters. For instance, many examples exist of researchers obtaining used drives from online auctions and other sources and recovering large amounts of sensitive information from them [3].

First of all, there are currently no standards for cloud-based storage or computing. This can make porting an infrastructure from one vendor to another dicey at best, and may mean you're subject to the whims of an infrastructure provider. This is a key issue that emerging cloud-based storage solutions will address, but nonetheless is a major challenge today. Once solutions are available from major vendors, more services with common APIs will become available, and developers will come up with mappings between other popular APIs (such as Amazon S3, and potentially even XAM).

The cloud-based storage solutions still fall short of meeting all IT storage needs. The biggest gap is where databases are concerned. While Amazon S3 started life looking very much like a widely distributed, extremely flat database, it has never been capable of meeting traditional enterprise database needs: It is not relational in the traditional sense, it lacks DBMS tools, and because it is designed to support loosely coupled applications, it does not support high loads of guaranteed, consistent transactions expected in traditional database environments. More importantly, without a distributable database, the cloud looks like a poor place for databases applications that depend on access to single instances of databases in the cloud will never be able to benefit from load balancing, scalability, and improved availability; all of which may imply the use of multiple copies of data or stateless redirection of data connections.

This is an area of critical importance in which next-generation cloud-based storage vendors must begin to innovate.

In this paper, to give the attention of segmentation of encrypted cloud data into two major components such as the encryption key (EK) and the cloud data(CD), thereafter the EK and CD will store in different cloud servers situated perpendicular (orthogonal) with each other.

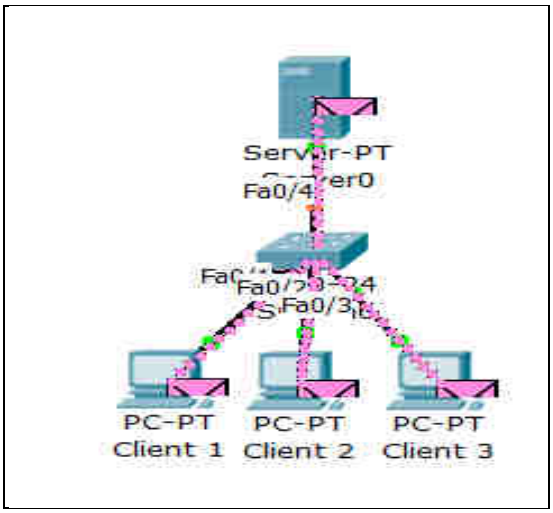

Fig.1.1: General Cloud Data Storage Frameworks

The above figure 1.1 illustrates the general storage mechanism of the data transfer between the clients and server. The standard data storage mechanism is focus on the data either it will encrypt neither form nor original form, it occupies in the same server or single server. It causes more security risks for highly sensitive data. In order to avoid such kind of risk as well as to improve the authenticated access by using this proposed cloud storage management.

II. RELATED WORK

Moving data and applications to a cloud computing environment operated by a cloud provider expands the insider security risk not only to the cloud provider's staff, but also potentially among other customers using the service.

For example, a denial of service attack launched by a malicious insider was demonstrated against a well-known IaaS cloud [2]. The architecture of the software systems used to deliver cloud services comprises hardware and software residing in the cloud. The physical location of the infrastructure is determined by the cloud provider as is the implementation of the reliability and scalability logic of the underlying support framework.

Virtual machines often serve as the abstract unit of deployment and are loosely coupled with the cloud storage architecture. Applications are built on the programming interfaces of Internet-accessible services, which typically involve multiple cloud components communicating with each other over application programming interfaces.

Many of the simplified interfaces and service abstractions belie the inherent complexity that affects security. Data must be secured while at rest, in transit, and in use, and access to the data must be controlled. Standards for communications protocols and public key certificates allow data transfers to be protected using cryptography.

Procedures for protecting data at rest are not as well standardized, however, making interoperability an issue due to the predominance of proprietary systems. The lack of interoperability affects the availability of data and complicates the portability of applications and data between cloud providers.

While outsourcing relieves operational commitment on the part of the organization, the act of engaging a cloud provider's offerings for public cloud services poses risks against which an organization needs to safeguard itself. The analysis must include factors such as the service model involved, the purpose and scope of the service, the types and level of access needed by the provider and proposed for use between the organizational computing environment and provider services.

The service duration and dependencies, and the strength of protection offered via the security controls available from the cloud provider [4]. The Cloud data storage of encrypted key along with data store architectural framework is depicted in the following figure 1.2.

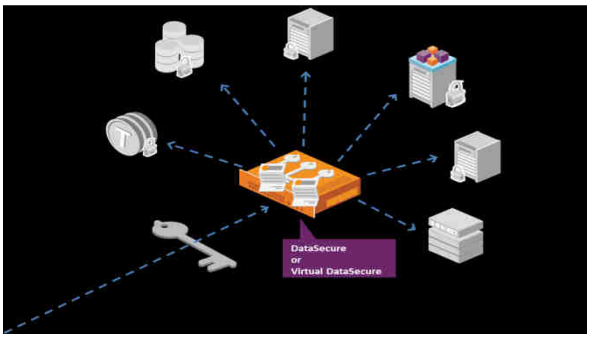

Fig.1.2: Encrypted Key and Data Storage architectural frame work

III. PROPOSED WORK

The basic principle of the proposed architectural framework mainly focuses on the storage of encrypted message in private cloud. There are different mechanism of secure data transmission is proposed by different cryptographic algorithms for example. RSA (Rivest, Shamir and Aldemin), AES (Advanced Encryption Standard), DES (Data Encryption Standard).

In the largest part of the storage mechanisms for encrypted message /content in the cloud service Provider (CSP) is habitually to locate in the same server. But in the proposed architecture is depicted in the following figure 1.3. Distribution of Content. The encrypted cloud data will be segmented into the data content and the encryption key.

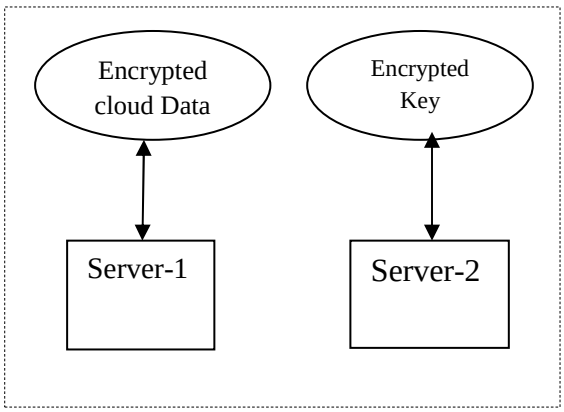

Fig.1.3: Distribution of Content.

The locality of the content storage will be allocated the cloud servers to place in perpendicular (orthogonal) with each other (Figure 1.4).

Let us assumes that, he messages/information comes out from different clients (P1) via the cloud will be encrypted (in the below equation 1), and then the encrypted data is allocated in one server (depicted in the equation 2 and 3) and the encryption key (EKP1) is allocated in another server.

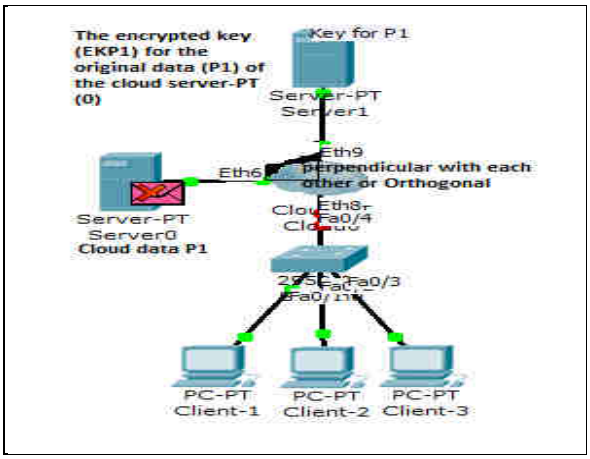

Fig.1.4: Locality allocation of Data storage

Whenever the respective data stored such mechanism is required for another user under the private cloud is access with the help of index maintained by the primary cloud service provider (Figure 1.5and Figure 1.6).

$$C_T = CD + EK \quad \text{---------- 1}$$

$$S1 = \sum_{i=1}^{n} CD \quad \text{---------- 2}$$

$$S2 = \sum_{i=1}^{n} EK(P1) \quad \text{---------- 3}$$

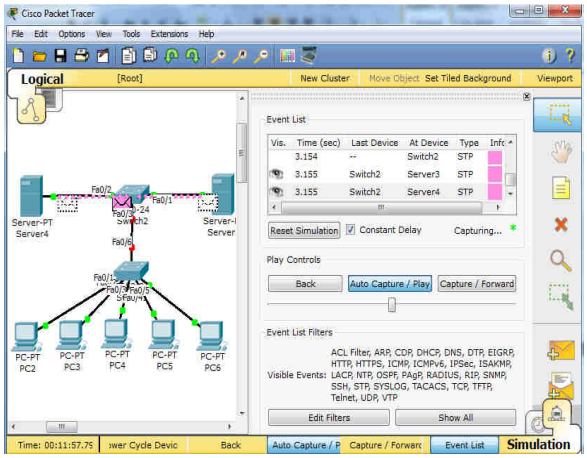

Fig.1.5: Data transmission under private cloud

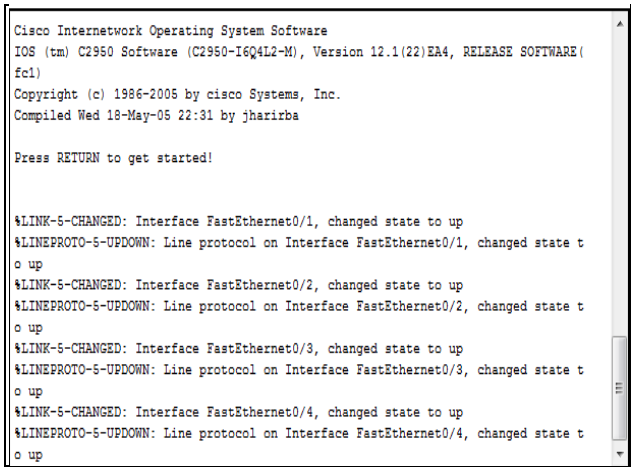

Fig.1.6: Data Transmission Initiation

IV. CONCLUSION AND FUTURE WORK

At the moment, the secure cloud data transmission in the modern era is the challenging task and every researcher try to solve it in their own way. In this research work, the prime objective is the achievement of secure way of cloud transmission by using the principles of enhancement of storage architectural framework along with the new dimension of encryption in the future work.

REFERENCES

[1] Andy Greenberg, IBM's Blindfolded Calculator, Forbes Magazine, July 13, 2009, <URL: http://www.forbes.com/forbes/2009/0713/breakthroughs-privacy-super- secret-encryption.html>.

[2] Marco Slaviero, BlackHat Presentation Demo Vids: Amazon, part 4 of 5, AMIBomb, August 8, 2009, <URL: http://www.sensepost.com/blog/3797.html>

[3] Craig Valli, Andrew Woodward, The 2008 Australian Study of Remnant Data Contained on 2nd Hand Hard Disks: The Saga Continues, The 6th Australian Digital Forensics Conference, Perth, Western Australia, December 1-3, 2008, <URL: http://conferences.secau.org/proceedings/2008/forensics/Valli%20and%20Woodward%202008%20remnant%20Data%20saga%20continues.pdf>

[4] Bee Leng, A Security Guide for Acquiring Outsourced Service, GIAC GSEC Practical (v1.4b), SANS Institute, August 19, 2003, <URL: http://www.sans.org/reading_room/whitepapers/services/a_security_guide_for_acquiring_outsourced_service_1241>.

[5] Haroon Meer, Nick Arvanitis, Marco Slaviero, Clobbering the Cloud, Part 4 of 5, Black Hat USA Talk Write-up, SensePost SDH Labs, 2009, <URL: http://www.sensepost.com/labs/conferences/clobbering_the_cloud/amazon>.