© 2016 IJSRSET | Volume 2 | Issue 5 | Print ISSN: 2395-1990 | Online ISSN : 2394-4099
Themed Section: Engineering and Technology

Security Enhancement Using P-Encryption Approach for Safer Clouds

A. Reyana, M. Amutha

Department of Computer Science and Engineering/Nehru Institute of Engineering and Technology, Coimbatore, TamilNadu, India

ABSTRACT

Millions of people use public cloud storage to share and exchange files, but at times due to their openness it restricts the usage. Here we apply data encryption which enables the users to access cloud in a risk free manner.

Keywords: Filtering, P-Encryption, Authentication, Security

I. INTRODUCTION

Users choose cloud because of its convenient and easy usage. The undermine existing IT Policies, restricts the client in sharing confidential data. Nowadays, organizations apply web filtering to block access to web storage providers preventing cloud, thus storage applications getting installed. Some of these Cloud storage services are Drop box, Google Drive, etc, These tools let people access their files from anywhere on any device. However these services are flexible and easy to deploy, by making data more accessible it also makes it more easily exposed to hackers.

With Cloud removing the need for end-users to own systems, we also experience a change in mindset, from a focus on systems security to a focus on data security and protection. To know who, what, why, etc., is more emergency with the impending data explosion. Thus the data security and protection measures comes a demand which will enable the cloud service providers and administrators to inspect, monitor and analyze the data access and movements within large scale cloud computing environment.

II. II. METHODS AND MATERIAL

1. Security in Cloud

Today's users are working everywhere and it is essential to make sure that their data protection also works everywhere. As already the flow of data is across more devices and over more infrastructures it becomes tedious to identify whether approved users are only using the public cloud. Thus a systematic approach is required in securing the data on wherever it flows, independent of whether it is stored internally in public cloud or accessed from mobile devices.

Hence the security in cloud should manage various cloud storage accounts, its password complexity, and access to data and written policies in maintaining organizations confidentiality. It is widely acknowledged that data and intellectual property are among the mass valuable assets for most businesses today. So protecting its security, integrity and confidentiality is a critical priority, and also enables its value and competitive advantage in the performance of every organization.

Every enterprise needs information, and to serve these needs the information must be widely accessible and applied to create values. Too much or too less of security may result in the loss of opportunity or leads. Thus it is essential to follow best security a practice, as resource sharing dramatically simplifies infrastructure planning is the promise of 'cloud computing'.

Applications available in LAN only could even be infiltrated from the outside so placing an application over the internet is always a security risk. This is the unique situation of cloud computing. Implementation

IJSRSET162596 | Received : 20 October 2016 | Accepted : 31 October 2016 | September-October-2016 [(2)5: 445-448]

of cloud computing could require millions of dollars in infrastructure and applications development but it still places itself at risk for different types of attacks. a) Protecting the Users: Above everything else, cloud computing or any type of online application format should consider protecting its users. Developers should make sure that data related to the user should not be mishandled and could be extracted just by one. b) Data Security: The hardware component for cloud computing on the other hand requires a different type of security consideration. The location of data center should not only be selected because of its proximity to controllers and intended users but also on its security from external problems. c) Recovery and Investigation: Cloud computing security should not only focus itself on prevention. Ample resources should also be focused on recovery if the unfortunate event really strikes. Even before disaster happens, certain plans have to be in place to ensure that everyone will be working in unison towards recovery.

2. Cloud Architecture

The majority of cloud computing infrastructure consists of reliable services delivered through data centers and built on servers with different levels of virtualization technologies. The services are accessible anywhere that provides access to networking infrastructure. The Cloud appears as a single point of access for all the computing needs of consumers. Commercial offerings are generally expected to meet quality of service requirements of customers. Open standards are critical to the growth of cloud computing, and open source software has provided the foundation for many cloud computing implementations.

3. Types of Cloud

Public cloud: Public cloud or external cloud describes cloud computing in the traditional mainstream sense, whereby resources are dynamically provisioned on a fine-grained, self-service basis over the web services, from an off-site third-party provider who shares resources and bills on a fine-grained utility computing basis. Hybrid cloud: A hybrid cloud environment consisting of multiple internal and/or external providers "will be typical for most enterprises". Private cloud: Private cloud and internal cloud are neologisms that some vendors have recently used to describe offerings that emulate cloud computing on private networks. These products claim to "deliver some benefits of cloud computing without the pitfalls", capitalizing on data security, corporate governance, and reliability concerns.

4. Related Works

The increased use of smart phones and tablet PC's represent a major shift in the way people collaborate. If the employees are allowed to use their devices, it opens up a wealth of opportunities for increased employee comfort and productivity. Thus as long as there is data ready to be accessed and share there are external services that overlay restrictive procedures. It has been identified that too much of security issues arrived due to hacking by external hackers rather than employees within an organization.

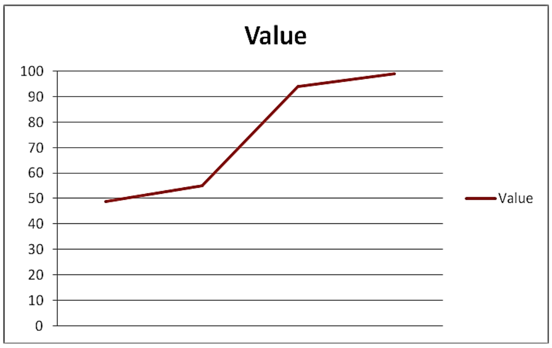

Figure 1. Survey Rating on Hacking

Legacy management infrastructures is based on dedicated relationships and constructs that are not well suited to cloud environments as they are continuously launched and decommissioned. Therefore it requires monitoring and management tools that are adaptable and customizable.

Cloud computing presents a number of challenges, which includes: Companies using public clouds do not have the ownership of the equipment hosting the cloud environment; also do not have the full visibility or control. Users of public Cloud services must integrate with an architecture defined by the cloud provider. Applications of all sizes may appear in the environment, consume an unpredictable amount of resources them disappear at any time. Pricing Resources is the challenge for both the public and private cloud environments. Exceeding budgets can be a risk. Hybrid clouds, which combine both public and private cloud services, sometimes with traditional infrastructure elements, present their own set of management challenges. These include security concerns if sensitive data lands on public cloud servers, budget concerns around overuse of storage or bandwidth and proliferation of mismanaged images. Managing the information flow in a hybrid cloud environment is also a significant challenge. On premises clouds must share information with applications hosted off premises by public cloud providers and this information may change constantly. Hybrid cloud environments also typically include a complex mix of permissions and limits that must be managed consistently.

III. IMPLEMENTATION AND RESULT

In general, the sensitive information is protected when they are in a database or specific application. Once they are open to attack they can be easily misplaced, lost or stolen. Today data are encrypted only if an application or device explicitly does it. Otherwise it is a clear text and is unprotected by default.

P- Encryption protects data at rest, in transit and in the cloud while moving around the network. This approach is largely transparent to users and for users with appropriate permissions to access files, the data always remains accessible even though it is encrypted. The encryption is managed and stored locally in the cloud by allowing users to define, manage their own encryption key. The users can secure their files using this encryption keys and access them any time behind the firewall or in the cloud. Encryption takes place on the client before any data is synchronized. There by need not worry on the security of the cloud providers. Central keys give authorized users or group access to files.

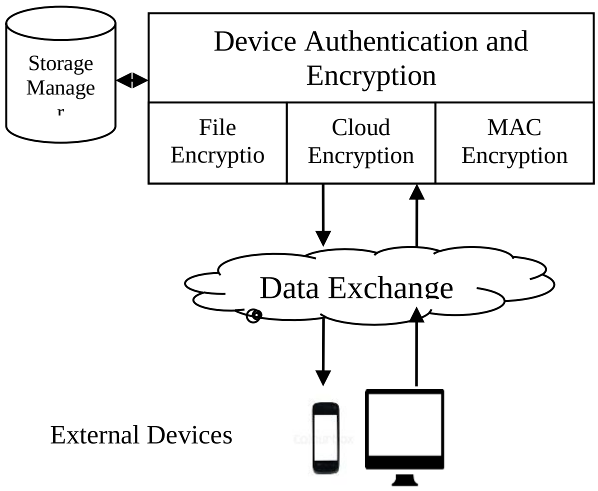

Figure 2. P-Encryption Architecture

1. Storage Managers

A central management for all the data encryption, this includes wide range of IT environments. Efficiently manages keys and policies throughout the organizations business. The functions include: Managing, Storing, Sharing, exchanging, retrieving a key, password recoìvery and compliance reporting features.

2. Device Authentication and Encryption

Encrypts all data by protecting users against unauthorized access, loss or theft. It also helps in emergency data recovery. Operating system is encrypted thereby it is faster, easier more reliable and saves times this enables three set of encryption.

1.

2. File Encryption: Centralized keys given to users or groups beneficial for teams and project group as it encrypts documents and data as network file shares to ensure that only right uses get access to decrypt and read the information.

Cloud Encryption: File uploaded to cloud are encrypted before allowed for access in other devices. The tools like's ios, android are used.

MAC Encryption: Files stored in Hard disk are also protected i.e., files protected in removable media, network file shares and also in cloud.

3. Data Exchange

Ensures the secured data exchange with business partners and customers even without installation of application for encryption. This helps in encryption and decryption of data on the same media, track files to check whether copied or moved to removable storage.

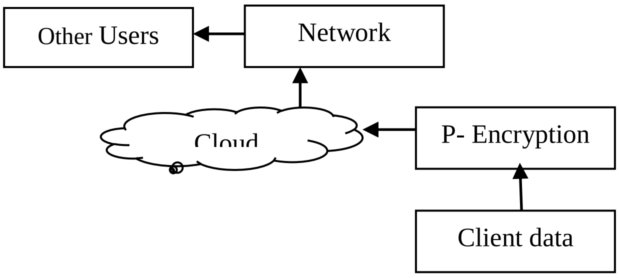

Figure 3. Synchronization of Data in Cloud

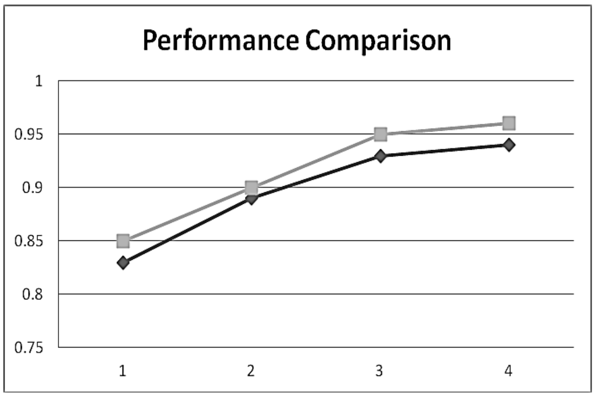

Figure 4. Performance Comparison

The result of the above implementation suggests that P-Encryption method provides better performance in security issues while data exchange in cloud environments, thereby protecting unauthorized access and helps in keeping data safer on clouds.

IV. CONCLUSION

With P-Encryption cloud storage does not matter from where the files are accessed, the data remains encrypted and secured. All files are kept encrypted through transit and decrypted locally when required. Encryption keys are nowhere shared with the cloud. This also saves time, easy to manage and ensures that human mistakes won’t put the data at risk.

V. REFERENCE

[1]. Rajkumar Buyya, “Introduction to the IEEE Transactions on Cloud Computing”, *IEEE Transactions on Cloud Computing*, Vol. 1, No. 1, January-June 2013.

[2]. Kevin Hamlen, Murat Kantarcioglu, Latifur Khan, Bhavani Thuraisingham “ Security Issues for Cloud Computing” ,*Technical Report*, UTDCS-02-01Feb 2010.

[3]. Hao, Chen, and Ying Qiao. "Research of Cloud Computing Based on the Hadoop Platform," *Chengdu, China: 2011*, Pp. 181 – 184, 21-23 Oct 2011.

[4]. Ren, Yulong, and Wen Tang. "A Service Integrity Assurance Framework for Cloud Computing Based on Mapreduce."*Proceedings of IEEE CCIS2012. Hangzhou: 2012*, Pp 240 – 244, Oct. 30 2012-Nov. 1 2012

[5]. K. Chitharanjan, and Kala Karun A. "A Review on Hadoop — HDFS Infrastructure Extensions", *Jeju Island: 2013*, Pp. 132-137, 11-12 Apr. 2013.