Applying Encryption Algorithm for Data Security and Privacy in Cloud Computing

Mohit Marwaha[1], Rajeev Bedi[2]

[1] Computer Science And Engineering, Punjab Technical University, Beant College of engineering and Technology Gurdaspur, Punjab, India

[2] Computer Science And Engineering, Punjab Technical University, Beant College of engineering and Technology Gurdaspur, Punjab, India

Abstract

Cloud computing is the next big thing after internet in the field of information technology; some say it's a metaphor for internet. It is an Internet-based computing technology, in which software, shared recourses and information, are provided to consumers and devices on-demand, and as per users requirement on a pay per use model. Even though the cloud continues to grow in popularity, Usability and respectability, Problems with data protection and data privacy and other Security issues play a major setback in the field of Cloud Computing. Privacy and security are the key issue for cloud storage. Encryption is a well known technology for protecting sensitive data. Use of the combination of Public and Private key encryption to hide the sensitive data of users, and cipher text retrieval. The paper analyzes the feasibility of the applying encryption algorithm for data security and privacy in cloud Storage.

Keywords: *Cloud Storage, Cipher text retrieval, encryption algorithm.*

1. Introduction

Cloud computing is a flexible, cost- effective and proven delivery platform for providing business or consumer IT services over the Internet. Cloud computing supports distributed service oriented architecture, multi-users and multi-domain administrative infrastructure, it is more prone to security threats and vulnerabilities. At present, a major concern in cloud adoption is its security and Privacy. Intrusion prospects within cloud environment are many and with high gains. Security and Privacy issues are of more concern to cloud service providers who are actually hosting the services. In most cases, the provider must guarantee that their infrastructure is secure and clients' data and applications are safe by implementing security policies and mechanisms. While the cloud customer must ensure that provider has taken proper security measures to protect their information. The issues are organized into several general categories: trust, architecture, identity management, software isolation, data protection, availability Reliability, Ownership, Data Backup, Data Portability and Conversion, Multiplatform Support and Intellectual Property.

2. Cloud Computing Framework

Service Models: These three are the most widely used service models of cloud computing.

2.1 Software as a service.

Software-as-a-Service (SaaS): It is also referred as software available on demand, it is based on multi-tenant architecture. Software like word processor, CRM (Customer Relation Management), etc. or application services like schedule, calendar, etc. are executed in the "cloud" using the interconnectivity of the internet to do manipulation on data. Custom services are combined with 3rd party commercial services via Service oriented architecture to create new applications. It is a software delivery for business applications like accounting, content delivery, Human resource management (HRM), Enterprise resource planning (ERP) etc on demand on pay-as-you go model[1].

2.2 Platform as a Service.

Platform-as-a-Service (PaaS): This layer of cloud provides computing platform and solution stack as service**.** Platform-as-a-Service provides the user with the freedom of application design, application development, testing, deployment and hosting as well as application services such as team collaboration, web service integration and database integration, security, scalability, storage, persistence, state management, application versioning, without thinking about the underlying hardware and software layers by providing facilities required for completion of project through web application and services via Internet.

2.3 Infrastructure as a Service.

Infrastructure-as-a-Service (IaaS): Infrastructure as a service delivers a platform virtualization environment as a service. Instead of purchasing servers, software, data center space or network equipment, clients can buy these resources as outsourced service. In other words the client uses the third party infrastructure services to support its operations including hardware, storage, servers and networking components.

3. Cloud Deployment Models

There are three types cloud Deployment models that widely used are:

3.1 Public.

It is referred as external cloud or multi-tenant cloud, this model represents an openly accessible cloud environment in this cloud can be accessed by general public. Customer can access resources and pay for the operating resources. Public Cloud can host individual services as well as collection of services

3.2 Private.

It is also known as internal cloud or on-premise cloud, a private cloud provides a limited access to its resources and services to consumers that belong to the same organization that owns the cloud. In other words, the infrastructure that is managed and operated for one organization only, so that a consistent level of control over security, privacy, and governance can be maintained.

3.3 Hybrid.

A hybrid cloud is a combination of public and private cloud. It provides benefits of multiple deployment models. It enables the enterprise to manage steady-state workload in the private cloud, and if the workload increases asking the public cloud for intensive computing resources, then return if no longer needed.

3.4 Community.

This deployment model share resources with many organizations in a community that shares common concerns (like security, governance, compliance etc). It typically refers to special-purpose cloud computing environments shared and managed by a number of related organizations participating in a common domain or vertical market [12].

4. Issues in Cloud Data Storage.

Cloud Computing moves the application software and databases to the large data centers, where the management of the data and services may not be fully trustworthy. This unique attribute, however, poses many new security challenges which have not been well understood. In this article, we focus on cloud data storage security, which has always been an important aspect of quality of service. To ensure the correctness of users' data in the cloud.

A. Trust: Trust is defined as reliance on the integrity, strength, ability and surety of a person or thing. Entrusting your data on to a third party who is providing cloud services is an issue. Recent incidents like In April of 2012 Amazon's Elastic Compute Cloud service crashed during a system upgrade, knocking customers' websites off-line for anywhere from several hours to several days. That same month, hackers broke into the Sony PlayStation Network, exposing the personal information of 77 million people around the world. And in June a software glitch at cloud-storage provider Dropbox temporarily allowed visitors to log in to any of its 25 million customers' accounts using any password or none at all. These issues have certainly created doubts in mind of cloud consumers and damaged the trust ability of Consumers [4].

B. Privacy: Different from the traditional computing model, cloud computing utilizes the virtual computing technology, users' personal data may be scattered in various virtual data center rather than stay in the same physical location, even across the national borders, at this time, data privacy protection will face the controversy of different legal systems. On the other hand, users may leak hidden information when they accessing cloud computing services. Attackers can analyze the critical task depend on the computing task submitted by the users [9].

C. Security: Cloud service providers employ data storage and transmission encryption, user authentication, and authorization. Many clients worry about the vulnerability of remote data to criminals and hackers. Cloud providers are enormously sensitive to this issue and apply substantial resources to mitigate this problem.

D. Ownership: Once data has been relegated to the cloud, some worry about losing their rights or being unable to protect the rights of their customers. Many cloud providers address this issue with well-skilled user-sided agreements. According to the agreement, users would be wise to seek advice from their favourite legal representative [10].

E. Performance and Availability: Business organizations are worried about acceptable levels of performance and availability of applications hosted in the cloud.

F. Legal: There are certain apprehensions for a cloud service provider and a client receiving the service like location of the cloud provider, infrastructure and physical location of the data and outsourcing of the cloud provider's services etc.

G. Multiplatform Support: More an issue for IT departments using managed services is how the cloud-based service integrates across different platforms and operating systems, e.g. OS X, Windows, Linux and thin-clients. Usually, some customized adaption of the service takes care of any problem. Multiplatform support requirements will ease as more user interfaces become web-based.

H. Intellectual Property: A company invents something new and it uses cloud services as part of the invention. Is the invention still patentable? Or there can be issues like cloud service provider can make claim for that invention or leak the information to the competitor.

I. Data Backup: Cloud providers employ redundant servers and routine data backup processes, but some people worry about being able to control their own backups. Many providers are now offering data dumps onto media or allowing users to back up data through regular downloads.

J. Data Portability and Conversion: Some people have concerns like, switching service providers; there may be difficulty in transferring data. Porting and converting data is highly dependent on the nature of the cloud provider's data retrieval format, particular in cases where the format cannot be easily revealed. As service competition grows and open standards become established, the data portability issue will ease, and conversion processes will become available supporting the more popular cloud providers. Worst case, a cloud subscriber will have to pay for some custom data conversion.

These are certain areas in which cloud computing requires to excel and solve problem related to it. Out of all the problems Security, Privacy and Intellectual property put the major threats on growth of cloud computing that are needed to be worked upon.

5. OVERVIEW OF OUR APPROACH

Our goal is to build up a repository to facilitate the data integration and sharing across cloud along with preservation of data confidentiality. For this we will be using an encryption technique to provide data security on data storage [16].

Objective of our System.

1. To develop a system that will Provide Security and Privacy to Cloud Storage

2. To Establish an Encryption Based System for protecting Sensitive data on the cloud and Structure how owner and storage Service Provider to operate on encrypted Data

3. To Create a System where the user store its data on the cloud the data is sent and stored on the cloud in encrypted form As in normal cases in cloud computing when a user login to the cloud and they store data on cloud storage device the data stored on the server cloud is not much secure as it can be readable to anyone which have permission to access and Leaving data vulnerable,

4. To Develop a retrieval System in which the data is retrieved by the user in encrypted form and is decrypted by the user at its own site using a public and private key encryption both the keys working at the user level.

6. Conclusion

Our research indicates that that Security and Privacy are the major issues that are needed to be countered, efforts are being made to develop many efficient System That can Provide Security and privacy at the user level and maintain the trust and intellectual property rights of the user. Our method States Encryption is one such method that can provide peace of mind to user and if the user have control over encryption and decryptions of data that will boost consumer confidence and attract more people to cloud platform.

References

[1]http://en.wikipedia.org/wiki/Cloud_computing.
[2] Rich Maggiani, solari communication. "Cloud computing is changing how we communicate".
[3] Randolph Barr, Qualys Inc, "How to gain comfort in losing control to the cloud".
[4] Greg Boss, Padma Malladi, Dennis Quan, Linda Legregni, Harold Hall, HiPODS, www.ibm.com/ developerworks/websphere/zones/hipods
[5] http://www.roughtype.com.
[6] Tharam Dillon, Chen Wu, Elizabeth Chang, 2010 24th IEEE International Conference on Advanced Information Networking and Applications ,"Cloud computing: issues and challenges".
[7]June13,2009,http://server.zol.com.cn/183/1830464.html.
[8] Elinor Mills, January 27,2009. "Cloud computing security forecast: clear skies".
[9] Jianchun Jiang, Weiping Wen, "Information security issues in cloud computing environment", Netinfo Security,doi:10.3969/j.issn.1671-1122.2010.02.026.
[10] Jianchun Jiang, Weiping Wen, "Information security issues in cloud computing environment", Netinfo Security,doi:10.3969/j.issn.1671- 1122.2010.02.026. of virtual machines" In Proc. Of NSDI'05, pages 273-286, Berkeley CA, USA, 2005. USENIX Association.

[11] Eucalyptus Completes Amazon Web Services Specs with Latest Release.
[12] Open Cloud Consortium.org.
[13] July 27,2009. Available from http://fx.caixun.com/.
[14] Jack Schofield. Wednesday 17 June 2009 22.00 BST, http://www.guardian.co.uk/technology/2009/jun/17/cloud-computingjack- schofield.
[15] Gartner. "Seven cloud-computing security risks".
[16] Ranjita Mishra "A Privacy Preserving Repository for Securing Data across the Cloud".

First Author Mohit Marwaha completed BTech from Beant College of Engineering and Technology in 2008 Pursuing MTech from Beant College of Engineering and Technology I have published two papers one in an international jouranal and other in an international conference and is presently working with Beant college of Engineering and Technology as Assistant Professor. Area of Research is security on cloud computing.

Second Author Rajeev Bedi completed B.Tech Computer Science and Engineering in 2000 and M.Tech. Computer Science and Engineering in 2008 from Punjab Technical University, Jalandhar and Pursuing PhD from CMJ University Shillong. Currently Working as Assistant Professor in Beant College of Engineering and Technology, Gurdaspur since 2004. I am Reviewer of IJCSIT journal. I have 13 publications in different Internationl, National Journals and Conferences. My current research interest is Cloud Computing.