Volume 5, Issue 3, March 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Security of Key in Cloud Using Cryptography

Priya Sharma
Department of Computer Science & Engineering,
Greater Noida Institute of Technology, UPTU, India

Abstract— Cloud Computing provides new visualization to the world. Cloud Computing transforms the way by which information technology (IT) is consumed and managed, promising improved cost efficiencies, and the ability to scale application on demand. Cloud Computing allow user to store large amount of data in cloud storage and use as when required. Since Cloud Computing is rest on internet, security issues like privacy, data security, confidentiality and authentication is encountered. Customer information stored at cloud needs to be protected against potential intruders as well as cloud service provider. Organizations are transferring important information to the cloud that increases concerns over security over data. Cryptography is common approach to protect the sensitive information in cloud. Cryptography involves managing encryption and decryption keys. In this paper we have given a encryption and decryption algorithm to manage key in the cloud.

Keywords— Cloud Computing, Data Storage, Cloud Computing Security, Cryptography and Encryption.

I. INTRODUCTION

Cloud Computing provides means of computation, data access, software, and storage services that conceal the physical location and configuration. Cloud Computing is new utility of the century, which many enterprise wants to incorporates in order to improve their way of working. It implies sharing of computing resources to handle application. Cloud Computing offers compact capital expenditure, operational risks, complexity and maintenance, and increased scalability .The most widely used definition of cloud computing model is introduced by NIST [1] as "a model for enabling convenient, on demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort of service provider interaction".
Since cloud computing is a service available on net, so there are various issues that can be raised like user privacy, data stealing and leakage, unauthorized access and various hackers attacks.
According to a Gartner survey [2] on cloud computing revenues, the cloud market was worth USD 56.8B in 2009, expected to be USD 68B in 2010 and will reach USD 148 B by 2014. This revenues imply that cloud computing is a promising platform. On the other side this increases the attackers interest in finding existing vulnerabilities in the model. Internet -based online services like Amazon simple storage service (S3) and Amazon Elastic Compute Cloud (EC2) provides huge amount of storage space.

II. CLASSIFICATION OF CLOUD COMPUTING

It can be classified in following two ways:
1.Deployment Model
2.System Model

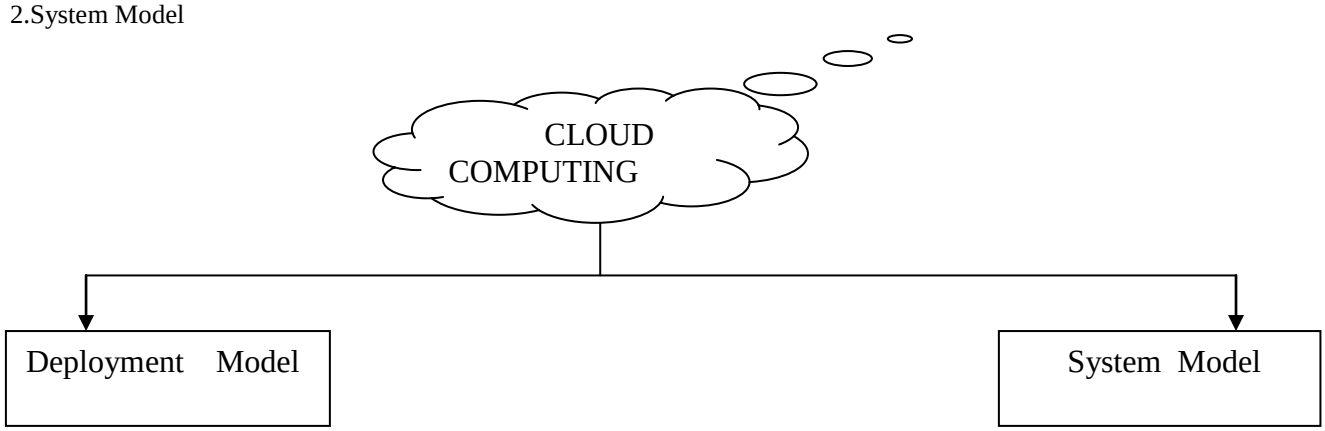

Fig 1:Types of cloud computing

A. Deployment models

Based on the deployment the cloud can be of following types. Different types are clouds are described below:

1) Public cloud: The cloud vendor hosts the computing infrastructure at its own premises and the customer don't have any control on where the computing infrastructure is hosted. The computing infrastructure is open for use by general public or different organizations share this computing infrastructure.

2) Private cloud: Computing infrastructure is not shared between the organizations. [8] Private Cloud users are considered as trusted by the organisation, in which they are either employees, or have contractual agreements with the organisation. It is dedicated to a particular organization and is therefore more secure but expensive than public clouds

3) Hybrid cloud: The cloud infrastructure in hybrid cloud is a synthesis of two or more unique cloud infrastructures that are bounded together by some standardized technology that empowers application and data portability.

4) Community cloud: In community cloud, consumers from organization that have related or imparted concerns solely utilize the cloud infrastructure. Community cloud may be supervised, managed and worked by a third party such as one organizations or a community of organizations or some consolidation of them.

B. Service models

1) Software as a Service (SaaS): In SaaS model consumer has the proficiency to utilize applications of supplier that are running on a cloud infrastructure. A program interface can be used to access the applications through various client devices. Operating systems, storages, servers, networks or other underlying cloud infrastructures are not overseen by the consumer.

2) Platform as a Service (PaaS): Consumer is given the capability to deploy onto the cloud infrastructure created by the consumer or applications acquired that are created using services, libraries, programming languages and tools supported by the provider. The underlying cloud infrastructure including storage, operating systems, servers, network controlled by the consumer..

3) Infrastructure as a Service (IaaS): Consumer has the capability to provision computing resources like networks, storage, processing etc. where the consumer can deploy and run arbitrary software, which can include applications and operating systems.

IaaS : Rackspace , Amazon web services, Jayent, sun's cloud services

PaaS : Google App Engine , Force.com, Windows Azure,

SaaS : Salesforce.com , Google Gmail , Microsoft 365 , Mobileme, Google docs , Zoho

Fig 2: Example of different service model

III. CHARACTERISTICS OF CLOUD COMPUTING

Various characteristics of cloud computing are [7]:

A. On demand Self Service

Without the human interaction with each service provider a consumer can provision computing capabilities automatically as and when required, for example server time and network storage.

B. Broad Network Access

Various client platforms like laptops, tablets, mobile phones can be used to access these capabilities that are available over the network.

C. Resource pooling

Multiple consumers are served with the providers pooled computing resources using a model, with different virtual and physical re- sources dynamically assigned and reassigned depending on the demand of consumer.

D. Rapid elasticity

A user can quickly acquire more resources from the cloud by scaling out . They can scale backing by releasing those resources once they are no longer required.

E. Measured service

Resources usage is metered using appropriate metrics such monitoring storage usage, CPU hours , bandwidth usage etc.

IV. AMAZON SIMPLE STORAGE SERVICES (AMAZON S3) SECURITY

Amazon Simple storage service (s3) allows us to retrieve data at any time, from anywhere on the web. Amazon S3 stores data as objects within buckets. An Object can be any kind of file: a text file, a photo, a video etc. When we add a file to Amazon S3, we have the option of including metadata with the file and setting permission to control access to the file. For each bucket, we can control access to the bucket, view access logs for the bucket and its objects, and choose geographical region where Amazon S3 will store the buckets and its contents.

A. Data Access

Access to data stored in Amazon S3 is restricted by default, only buckets and object owners have access to the Amazon S3 resources they create. There are several ways to control access to buckets and objects:

- Identify and Access Management (IAM) Policies
- Access Control List (ACLs)
- Bucket Policies

B. Data Transfer

For Maximum Security, we can securely upload/download data to Amazon S3 via the SSL encrypted endpoints.

C. Data Storage

Amazon S3 provides multiple options for protecting data at rest. For customers who prefer to manage their own encryption keys, they can use a client encryption to encrypt data before uploading to Amazon S3.

V. LITERATURE REVIEW

A. Introduction

One of the most challenging problems of cloud service solicitation is to persuade users to trust the security of cloud service and upload their sensitive data. Although cloud service providers always maintain that their services are well-protected by complex encryption algorithms and mechanisms, but note that traditional cloud systems still cannot convince users that even if the cloud servers are compromised or breached, the data are still protected securely [3]. Key management is the toughest part to manage in cryptosystems. In order to manage the encryption keys securely, keys should never be stored in the same place as encrypted data. Enterprises need to maintain secure storage of the encryption keys while employing the encryption in their cloud environment. The keys which are used for encrypting sensitive data should be managed efficiently by periodic key rotation, and then data should be re-encrypted with new keys. Employee's access should be limited to what is needed to complete their tasks.

B. Cryptographic Key Management Challenges in the Cloud

One of the critical aspect of cloud computing is the secure management of the resources that are associated with cloud services. One of the main tasks of secure management is cryptographic operation. Hence, while self-configurable resources, elastic capabilities and ubiquitous computing is provided by cloud services at a lower cost, they also involve performing several cryptographic operations.

C. Types of key management scheme

Selective distribution of keys and encryption that is utilized for security of critical information is a essential system for restricting access to data. Data information is given to encryption algorithm and a few transformations are performed on it. A figured content is produced in this procedure. There is no other way to recover the original message from the figured content other than by knowing the right decryption key [4].

There are three different methodologies to group key management:

- Centralized key management protocols: In this protocol single entity controls the whole group.
- Decentralized key management protocols: In this protocol a large group is separated into small subgroups and these subgroups are overseen separate subgroup administrators, which minimizes the issue of concentrating the workload in a lone spot.
- Distributed key management protocols: In this architecture the key management task is performed by the members themselves and no explicit KDC is required [6].

D. Issues with key management in cloud Systems

To manage the key is the toughest part in cryptosystems. Some of the issues with encryption key management in the cloud are:

- There is always a possibility of insider attack, in the cloud platform. Without the knowledge of end users keys can be accessed or stolen by employees.
- The keys need to be managed properly for all accounts. The challenge is to index proper accounts quickly and effectively with their respective keys.
- Another concern with key management is availability. How the keys will be accessed if a system goes offline? In order to retrieve keys there needs to be key cache, even in the event that a system goes offline.
- A very common fault in cloud servers is Byzantine failure [3]. When this kind of fault occurs a storage server can fail in arbitrary ways.
- The other common attacks in clouds is server colluding and data modification in which the storage servers can be compromised by the adversary, as a result of which files can be modified.

E. Solution to the security issues

Enterprises require to use encryption in their cloud environment, in order to manage the encryption keys securely, while maintaining secure offsite storage of their encryption keys.

Encryption keys and encrypted data should never be stored in the same place. The keys used for encrypting sensitive customer data should be managed efficiently by cyclic key replacement, and re-encryption of data with new keys.
More access should be not be given to employees than what is needed to complete their tasks.
Byzantine failure is very common fault in cloud servers, in which a storage server can fail in arbitrary ways. The system responds in an unpredictable way on occurrence of a byzantine failure [5]. At the point when a Byzantine failure has happened, the framework may react in any unpredictable way, unless it is proposed to have Byzantine fault tolerance. The cloud is also prone to data modification and server colluding attack in which the storage servers can be compromised by the adversary, as a result of which data files can be modified as long as they are internally consistent. For providing secure storage of data in cloud storage server, the data should be encrypted.

VI. ENCRYPTION AND DECRYPTION PROCESS

A. Encryption process

Step 1- Store each character of key separately
Step 2- Assign a position (n) to each character
Step 3- Determine the ASCII value of each character.
Step 4- Calculate a value X, using following formula:

X= (c+k+n)%256

c-character, k-shared key, n-position

Step 5- Now, determine the ASCII character of the X (decimal value resulted from the above formula). This would be the cryptogram text.

B. Decryption process

Step 1- Determine the ASCII value of the cryptogram text character.
Step 2- Use same shared encryption key.
Step 3- Assign the position n of the cryptogram text.
Step 4- D=((c-k-n)+256) %256

c-character, k-shared key, n-position.

Step 5 Generate the ASCII character of the corresponding decimal value in the result from the above given formula. This would be the original plain text.

VII. CONCLUSION

If a single KDC is used it may become a point of failure. In addition to it because of the large number of users it becomes difficult to maintain a single key distribution centre. Therefore in this proposed work we try to emphasize on decentralized approach in clouds while distributing secret keys and attribute to users.
The toughest part in cryptosystems is to manage key. There is always a possibility of insider attack or outsider attack, in the cloud platform. Keys can be accessed or stolen by employees without the knowledge of end users. Our aim is to provide secrecy to the data as well as keys that are stored in cloud systems. Our proposed technique provides better data security and key management in cloud systems. This technique also provides better security against byzantine failure, server colluding and data modification attacks.

ACKNOWLEDGMENTS

I take the opportunity to thanks all those, who have contributed to the completion of this work and helped me with valuable suggestions for improvement .
I express my deep gratitude to my guide , Mr Rajesh Pathak (HOD), for their valuable support , help and guidance during the project work and providing me with best facilities and atmosphere for the work and encouragement .

REFERENCES

[1] Peter Mell , and Tim Grance ," The NIST Definition of Cloud Computing ," 2009 , http://www.wheremyserver.co.nz/storage/media/faq-files/clouddef-v15.pdf, accessed April 2010.
[2] Frank Gens, Robert P Mahowald and Richard L Villars(2009, IDC Cloud Computing 2010).
[3] Vukolic, Marko. "The Byzantine empire in the intercloud." ACM SIGACT News 41.3 (2010): 105-111.
[4] Rafaeli, Sandro, and David Hutchison. "A survey of key management for secure group communication." ACM Computing Surveys (CSUR) 35.3 (2003):309-329.
[5] Agbaria, Adnan, and Roy Friedman. "Overcoming Byzantine Failures Using Checkpointing." University of Illinois at Urbana-Champaign Coordinated Science Laboratory technical report no. UILU-ENG-03-2228 (CRHC-03-14) (2003).
[6] Liu, C.L. Introduction to Combinatorial Mathematics. McGraw- Hill, New York, 1968.
[7] Yogita Gunjal, Prof. J. Rethna Virjil Jeny," Data Security and Integrity of Cloud Storage in Cloud Computing", in the year of April 2013,
[8] Ang Li, Xiaowei Yang , Srikanth Kandula and Ming Zhang ," Comparing public cloud providers ,"IEEE Internet Computing , Vol. 15, no. 2 ,pp.50-53,2011.

