A Study of Cloud Computing, Its Issues and Encryption

Syeda Huda Fatema[1] Prof. V.Kala[2]
[1]Student [2]Associate Professor
[1,2]Department of Computer Engineering
[1,2]Maharashtra Institute of Technology, Aurangabad, Maharashtra

Abstract— Cloud computing is the dynamic delivery of information technology resources and capabilities as a service over the Internet. Cloud computing is a style of computing in which dynamically scalable and often virtualized resources are provided as a service over the Internet. Virtualization is the core concept supported in the cloud computing. Resources are provided to the cloud users in a virtualized manner. Cloud providers are maintaining the user's data in cloud environment. The data which is stored in the provider's server could cause security and privacy issue in cloud storage. Lots of research is going on to provide security to the user's data. Leakage of user's confidential information stored in the database can cause disaster; hence there is a need of extra layer of security for the confidential information. Since the database is stored in a third party server, there is a need to prevent the exposure of information to the datacenter owner. There are many encryption techniques are used to protect the data in cloud.

Key words: Cloud Storage, Data Protection, Confidentiality, Encryption

I. INTRODUCTION

At its simplest, cloud computing is the dynamic delivery of information technology resources and capabilities as a service over the Internet. Cloud computing is a style of computing in which dynamically scalable and often virtualized resources are provided as a service over the Internet [1].cloud computing has become the most effective field in the industry and in research. The requirement for cloud computing has increased in recent days due to the utilization of software and hardware with less investment. [2]. Virtualization is the core concept supported in the cloud computing. Resources are provided to cloud users as virtualized manner. Virtualization and cloud computing can be used quite successfully to improve the resilience of an IT environment. Because, they provide the means to recover quickly from component or system malfunctions. They quickly take back up of essential applications and data. Virtual machines can be migrated from one physical server to another in a live migration; virtual machine images can be restarted in a different location to provide for disaster recovery. Cloud providers are maintaining the user's data in cloud environment. The data in the provider's hands could make security and privacy issue in cloud storage. With cloud computing, all users‟ data are stored on the cloud. So cloud users have to think about their data like: security of the data in the cloud, Access control and authentication of the cloud [3]. Data protection in the cloud storage is the core security problems. Data protection is concerned with data confidentiality, integrity, authentication, availability and so on. Data confidentiality means that only authorized persons can use the data. Data integrity refers to information that has not been modified or remains untouched. Authentication refers to the process of verifying whether the incoming user is authorized or not. Data availability refers to the ability to guarantee to use the data in time when needed and also refers to the availability of cloud service provider on-demand. [4]

Privacy and security are the main issues being faced in Database as a service in cloud computing. The Database-as-a service is an emerging service in cloud computing. The leading companies are doing research on Database-as-a-Service as well as security concerns regarding the service. Another problem with the database is that it contains all the information at one place, so if anyone gets access to the database then he/she can make misuse of information. So the information stored in the database needs to be encrypted. Despite of the above methods, there are still possibilities of an attack on the database. So the customer's private information is not secured in the cloud environment. Lots of research is going on to provide security to the user's data. Leakage of user's confidential information stored in the database can cause disaster; hence there is a need of extra layer of security for the confidential information. Since the database is stored in third party server, there is a need to prevent the exposure of information to the datacenter owner

II. CLOUD COMPUTING MODELS

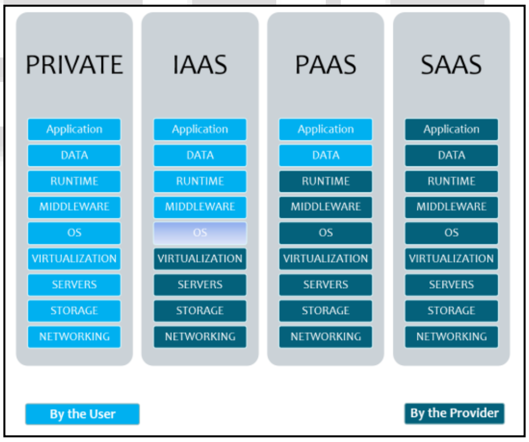

Fig. 1: Cloud Computing Models

– SaaS: To use the provider’s applications running on a cloud infrastructure and accessible from various client devices through a thin client interface such as a Web browser.
– PaaS: To deploy onto the cloud infrastructure consumer-created applications using programming languages and tools supported by the provider(java, python, .Net)
– IaaS: To provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications.

III. DATABASE MANAGEMENT IN CLOUD

The management of data is very important aspect of companies. Enterprises Interested to get benefits of cloud paradigm, outsource their data to database service provider and access their data via internet. This data management model is referred as database as a service (DaaS). DaaS is one of the most important applications of SaaS delivery model. DaaS model offers many benefits to enterprises like it saves the cost of database administration, offers reliable storage and efficient processing of query over the powerful machines of cloud service provider. In DaaS model, companies store business critical data through internet into the database that is managed by the service provider's database administrators (DBA). Database administrators have to have full control to the database to perform responsibilities of DBA like database backup, database restore, recovery of database in case it crashed and also to analyze the performance of the database. [5]

IV. Cloud storage issues

A. Trust

Data, when stored in the cloud, needs not only to be confidential but also should be accurate every time it is retrieved after uploading or a modification. There should not be a loss of integrity of the data. This is a valid scenario when third party storage services are compromised by the malicious agents. The data that is being provided by the corrupted service might not be accurate or fresh. This can be sometimes very hard to detect and can sometimes lead to considerable information leakage before being discovered. Hence it is the duty of the cloud service user to trust the cloud provider that what they provide is accurate inside the boundary of integrity check. The guidelines have been agreed upon between the service provider and the user. The guidelines might not be correct when the service provider's infrastructure has been compromised or encountered an error. [6]

B. Data Possession

This problem is loosely related to one of the other issues looked into how to trust the data stored on the service provider. When data is retrieved from the service provider on performing an integrity check, it would be very hard to determine how the data was stored in the service providers system. This is to ensure that the data is not leaked to a third party to whom the service provider is outsourcing the data, when the agreement for service is being agreed upon by the service provider and customer. The present service providers give hardly any kind of security on where and how the data is being stored and how secure is the methods. [7]

C. Data history

One of the significant features with local data storage is the presence of metadata features which allow users to view the history of a data object. This allows the systems to provide data integrity checks and rollback capabilities when a corruption or compromise is detected in the system. These features are almost non prevalent in the existing cloud system, and if present there are substantial security vulnerabilities associated with it because of the scale of the service. [7]

V. Cryptography

Cryptography is the science and study of secret writing. A cipher is a secret method of writing, whereby plaintext (or cleartext) is transformed into cipher text (sometimes called a cryptogram). The process of transforming plaintext into ciphertext is called encipherment or encryption; the reverse process of transforming ciphertext into plaintext is called decipherment or decryption. Both encipherment and decipherment are controlled by a cryptographic key or keys. [8]

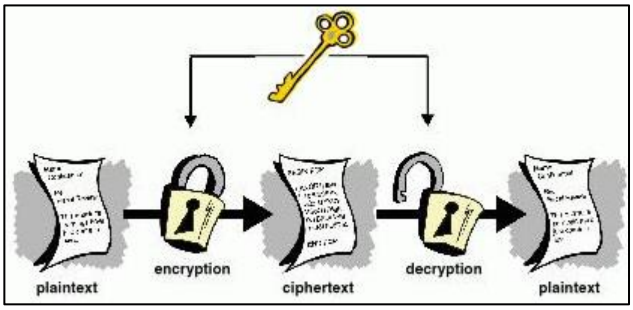

Fig. 2: Cryptography

Many encryption algorithms are widely available and used in information security. Encryption algorithms are classified into two groups: Symmetric-key (also called secret key) and Asymmetric-key (also called public-key) encryption. Symmetric key encryption is a form of cryptosystem in which encryption and decryption are performed using the same key. It is also known as conventional encryption. Asymmetric encryption is a form of cryptosystem in which encryption and decryption are performed using the different keys – one a public key and one a private key. It is also known as public-key encryption. A Key is a numeric or alpha numeric text or may be a special symbol. The Key is used at the time of encryption takes place on the Plain Text and at the time of decryption takes place on the Cipher Text. The selection of key in Cryptography is very important since the security of encryption algorithm depends directly on it. The strength of the encryption algorithm relies on the secrecy of the key, length of the key, the initialization vector, and how they all work together. Asymmetric encryption techniques are about 1000 times slower than Symmetric encryption which makes it impractical when trying to encrypt large amounts of data. Also to get the same security strength as symmetric, asymmetric must use a stronger key than symmetric encryption technique. [9]

VI. Related work

This section describes the research works which are related to ensure the confidentiality of data in cloud storage.

Dr. Nashaat el-Khameesy and Hossam Abdel Rahman in proposed [10] a security policy and procedures explicit to enhance the Data storage security in the cloud. They had a Control Access Data Storage (CADS) that included the necessary policies, processes and control activities for the delivery of each of the Data service offerings. The collective control Data Storage encompasses the users, processes, and technology needed to maintain an environment that supports the effectiveness of specific controls and the control frameworks. The security, correctness and availability of the data files being stored on the distributed cloud servers. It must be guaranteed by Providing Security Policy and Procedure for Data Storage, Defense in Depth for Data Storage in the cloud, Correctness Verification and Error Localization computing. All these recommendations are only theoretically proposed.

B. Raja Sekhar et al. of [11] introduced the Ciphertext policy attribute-based encryption (CP-ABE) which is a promising cryptographic solution to ensure the data security and integrity in cloud storage. It allows data owners to define their own access policies over user characteristics and enforce the policies on the data to be distributed. It provides a way of defining access policies based on various characteristics of the requester, background, or the data object. Especially, ciphertext-policy attribute based encryption (CP-ABE) enables an encryptor to define the attribute set over a universe of attributes that a decryptor needs to possess in order to decrypt the ciphertext, and enforce it on the contents. Thus, each user with a different set of attributes is allowed to decrypt several pieces of data per the security policy.

To have efficient cloud storage confidentiality, Dr. L. Arockiam used [7] encryption and obfuscation as two different techniques to protect the data in the cloud storage. Based on the type of data, encryption and obfuscation can be applied. Encryption can be applied to alphabets and alphanumeric type of data and obfuscation can be applied to a numeric type of data. Applying encryption and obfuscation techniques on the cloud data will provide more protection against unauthorized usage. Confidentiality could be achieved with a combination of encryption and obfuscation.

R. Anitha et al. of proposed [2]a method for providing protection to the data stored at the data server through metadata. This process provides protection using a cipher key which is created from the features of metadata. In this model, the time required for generating the cipher key is proportional to the number of attributes in the metadata as well the algorithms used for cipher key generation. Their plan enforced safety by providing two novel features;

1) Security is provided by the proposed design, where the encryption and decryption keys cannot be compromised without the involvement of data owner and the metadata data server (MDS).
2) The cipher key generated using the modified feistel network holds good for the avalanche effect as each round of the feistel function depends on the previous round value. This approach is time consuming for the generation cipher key.

VII. Conclusion

Cloud computing is a profitable computing service to an individual and enterprise customers. But due to some of the security problems in it, people might be reluctant to use it. Once the issues are resolved, the cloud computing will be the trillion dollars business in the computing world. The Data storage on un-trusted cloud makes data security as a challenging problem. Data security in the cloud is ensured by the confidentiality of sensitive data. The use of internet and network is growing rapidly. So there are more requirements to secure the data transmitted over different networks using different services. To provide the security to the network and data, different encryption methods are used.

References

[1] David E.Y. Sarna," Implementing and Developing Cloud Computing Applications", Taylor and Francis Group LLC, chapter 1, pp-2, January 2010.

[2] R. Anitha, P. Pradeepan, P. Yogesh, and Saswati Mukherjee, "Data Storage Security in Cloud using Metadata", 2nd International Conference on Machine Learning and Computer Science(IMLCS'2013), Kuala Lumpur (Malaysia), pp 26-30 August 2013.

[3] Dr. L. Arockiam, S. Monikandan, "Data Security and Privacy in Cloud Storage using Hybrid Symmetric Encryption Algorithm", International Journal of Advanced Research in Computer and Communication Engineering, Volume 2, Issue 8, pp 3064-3070 August 2013.

[4] Dr.L. Arockiam, S. Monikandan, Dr. Sheba K Malarchelvi," Obfuscrypt: A Novel Confidentiality Technique for Cloud Storage", International Journal of Computer Applications, Volume 88, Issue 1, pp 0975 – 8887 February 2014.

[5] Atiq Ur Rehman, M.Hussain, "Efficient Cloud Data Confidentiality for DaaS", International Journal of Advanced Science and Technology, Volume. 35, pp 1-10, October 2011.

[6] Prince Mahajan, Srinath Setty, Sangmin Lee, Allen Clement, Lorenzo Alvisi, Mike Dahlin, and Michael Walfish, "Depot: Cloud storage with minimal trust", 9th USENIX Symposium on Operating System Design and Implementation, pp 1-26, 2010.

[7] Dr. L. Arockiam, S. Monikandan," Efficient Cloud Storage Confidentiality to Ensure Data Security", 2014 International Conference on Computer Communication and Informatics (ICCCI -2014), January 2014.

[8] Dorothy Elizabeth Rob, ling Denning," Cryptography and Data Security ", Addison-Wesley Publishing Company, Inc, chapter 1, pp-1, January 1982.

[9] Gurpreet Singh, Supriya," A Study of Encryption Algorithms (RSA, DES, 3DES and AES) for Information Security", International Journal of Computer Applications, Volume 67,Issue19, pp 33-38, April 2013.

[10] Nashaat el-Khameesy, Hossam Abdel Rahman, “A Proposed Model for Enhancing Data Storage Security in Cloud Computing Systems”, Journal of Emerging Trends in Computing and Information Sciences, Volume 3, Issue 6, pp 970-974. June 2012.

[11] B. Raja Sekhar, B. Sunil Kumar, L. Swathi Reddy, and V. Poorna Chandar “CP-ABE Based Encryption for Secured Cloud Storage Access”, International Journal of Scientific & Engineering Research, Volume 3, Issue 9, pp 1-5, September 2012.