Review of Homomorphic Encryption on the Cloud for Secure Data Storage

Shubhangi Arora
M.Tech. Student, Department of Computer Science & Applications, Kurukshetra University, Kurukshetra-136119
Email: arora.shubhangi92@gmail.com
Monika Poriye
Assistant Professor, Department of Computer Science & Applications, Kurukshetra University, Kurukshetra-136119
Email: monikaporiye@gmail.com
Vinod Kumar
Assistant Professor, Department of Computer Science & Applications, Kurukshetra University, Kurukshetra-136119
Email: dcsavinod@gmail.com

----------**ABSTRACT**----------
Companies are showing their interest in storing data on the clouds. In the last few years, data increases in miraculous way. The security issues are also associated with storage of data in the cloud. So the cryptographic methods for the security of data find out that will provide confidentiality. Homomorphic encryption is one of the encryption methods for the cloud applications. The data is protected and managed in the cloud using homomorphic encryption. Homomorphic encryption also uses a updating method to reduce the bandwidth consumption while transfer of large encrypted files.

Keywords: Cloud Computing, Cryptography, Cloud Storage Security, Homomorphic Encryption

1. Introduction

Cloud computing manages the IT infrastructure in a scalable and flexible manner and also provides a cost effective solution. Cloud computing provides deployment platforms, software applications and computing resources on the demand of users and on the basis of pay-per-use the cloud applications. Because of these qualities, it has drawn the focus on the cloud computing in recent year. Many organizations adopt the cloud for their day to day operations(Anon., 2013).

The cloud hosted the applications over the internet. This approach becomes special because user can use the data from outsource and computation can be done using remote server that has enough resources to perform the task within much less time than the traditionally running applications on the user's machine. This is one of the major reasons of the research in the cloud computing technologies. However there have been issues of confidentiality and privacy of data being stored on the clouds. In a recent survey, many security discontinuity of cloud services such as, Drop box(Anon., n.d.), Last.fm(Anon., n.d.),(http://www.last.fm/, n.d.) and icloud(Anon., n.d.),(http://www.forbes.com/, 2012). A study (http://www.tappin.com/, 2012) indicates 72% of the IT professionals complain employees for mostly data loses, whereas the rest complain the Intruder. So the concern of inside attack increases on public clouds.

In a recent study (Anon., 2013), 79% employees use SaaS for their organization and 45% adopt IaaS. These numbers indicate a considerable growth and interest in cloud adoption. Mostly organizations are going to adopt cloud based applications and solutions because it gives benefits as compare to local traditional IT infrastructure. So, a large amount of data is moving to the cloud. Hence the needs of secure cloud storage options are growing.

2. Cloud Computing: A Security Perspective

In cloud computing, it allows resources to be available over a network. NIST defines cloud computing is a model for providing on-demand network access by a shared computing resources (e.g. servers, applications) that can be rapidly provided and released with minimum management effort or interaction service provider (Peter Mell, 2009).NIST defined five essential

characteristics, four deployment and three service models for cloud.

Essential Characteristics of the cloud

On-demand self-service:

It provides resources such as storage, network and server to customer without any manual interaction with the service providers. It also provides flexibility so that customers can make easily changes and facilitate quick deployment.

Broad network access:

The cloud offers services over the network using standard protocols so that the services can be easily accessed by the multiple client devices such as laptops, workstations, mobile phones and tablets. So the customers have the flexibility to select a platform of their choice in which they want to work with.

Resource Pooling:

The cloud is a multi-tenant model in which computing resources are pooled and the need of customers are fulfilled by the resources that are dynamically allocated. The customers are not aware of the actual physical location of a resource in the cloud. The physical location of the resource can be controlled at a higher abstraction level by specific certain geographical limits. For example a customer in its country can store data to be limited range with in physical infrastructure of the home country only.

Rapid Elasticity:

Additional resources can be easily provisioned or released as per the demand. In the cloud the resource availability appear virtually unlimited and resources can be requested in any quantity depending upon requirements. The cloud should handle the scaling as needed.

Measured Service:

In order to maintain a transparent record of the resource usage both for the providers and the consumers. The cloud systems often use a metering capability depending on the kind of service being provided. This helps many activities such as billing, setting quotas on resource usage, and auditing.

Deployment Models in Cloud Computing

Private Cloud:

The private cloud infrastructure is provided by a single organization for its exclusive use. The organization has more control over the underlying infrastructure and enhanced security. It may be managed by the organization or some third party.

Public Cloud:

The public cloud infrastructure is available for the public. The customers can more focus on their objectives in the public cloud. But it also raises many security concerns. Generally, this cloud is mostly managed by the providers themselves.

Community Cloud:

The community cloud infrastructure has a selected group or community of customers belonging to organization with related goals. It may be managed by one or more of the organizations or by some third party.

Hybrid Cloud:

The hybrid cloud infrastructure contains two or more forms of the public, private and community cloud infrastructures where communication among the different infrastructures is possible by using standardized or property of data and application communication methods.

Service Models in Cloud Computing

Software as a Service (SaaS):

It includes services where the consumers are given access to applications deployed on the cloud infrastructure of the providers. The applications are accessed using various device platforms through web browser, or some native applications interface. In this case the consumers do not have the control over the cloud infrastructure. Still they can specify certain limited configuration settings.

Platform as a Service (PaaS):

Cloud platform services or Platform as a service (PaaS) deliver a computing platform. It provides deployment of applications without the cost and complexity of buying managing the underlying hardware and software.

Infrastructure as a Service (IaaS):

Infrastructure as a service (IaaS) provides computer infrastructure. It provides virtualization platform as a service. There is no need to purchase servers, data centre space, software or network equipment, clients instead buy those resources as fully outsourced service. This service is typically billed on the amount of resource consumed.

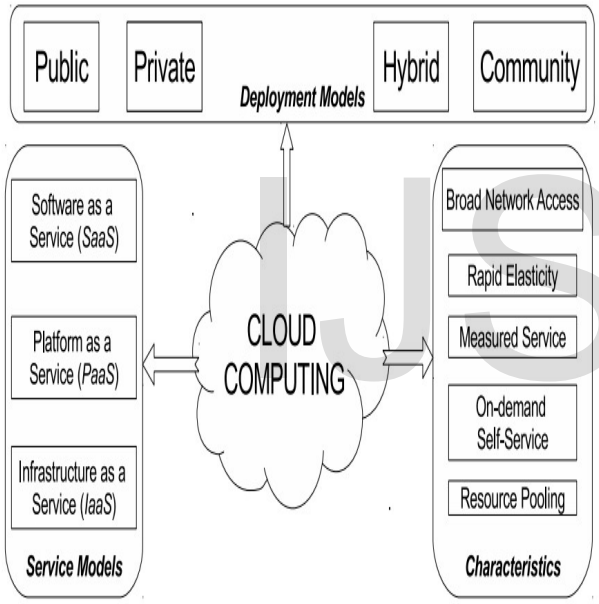

Fig 1: Cloud Computing Overview (M.K., 2013)

Recent works done in the context of cloud security is briefly described below.

3. Literature Review

Chen and Zhao provides an analysis(Devan Chen, 2012) of seven phase of data life cycle such as generation, use, transfer, share, storage, archival and destruction. It is used for data security. They have discussed key management as an important part in data storage. In data destruction phase, it is ensured that data is securely removed with the help of methods that makes the data unrecoverable, so that an attacker or hacker cannot take advantage of the sensitive information in the storage medium.

(M.A. AlZain, 2012) provides the information about single and multi-cloud models security issues. Authors have discussed the single cloud's security such as data intrusion, data integrity and service availability. Data integrity is ensured that it cannot get modified or corrupted during the transmission of data between cloud and data source. The scenarios involved the data integrity become more complicated by using of multiple clients and devices interaction with the cloud. In data intrusion, an attacker gains access to cloud service by stolen passwords of the authorized users so that it can damage the services. Availability of service is also another main factor to be considered.

KO, Jeon and Morales (Steven Y. Ko, 2011) have been proposed an execution model called HybrEx (Hybrid Execution) model. This model was developed to ensure the privacy and confidentiality. It operates by using the private cloud for sensitive data while the non-sensitive data and computations are performed with in the public cloud infrastructure of the organization. This model supports the application which works with public and private data. It also allows to add the additional storage resources or computing resources to the private clouds with maintaining the confidentiality or privacy of data. However, this approach provides security to the data but this model ignores the storage of sensitive data on the public clouds.

Jayodia, Litwin and Schwarz applies client side encryption for assuring privacy of data which is outsourced (Witold Litwin, 2011).This method use symmetric keys and diffie-hellman scheme for the protection of data and authentication of clients. At the client side, the keys are cached and also kept on the cloud as backup. These keys are kept hidden on the cloud. In a public share, it is produced by the owner which belongs to a two-share secret. This secret is a

type of key in which the client share is specific to the owner and each selected reader.

The authors provide security appraisal of cloud in (A Patrascu, 2012), 4 categories-computer network traditional security, cloud computing applications availability, data privacy by third- party and data-control by third party. The security provides solutions for some issues such as weakness of cloud provider, attacks on virtual machines, data leakage or stealing, authentication and authorization.

The critical applications are available in the cloud computing which involves vulnerabilities. This involves single point of failure, updation of cloud application and valid computation. The SLAs, audit ability and design are the issues of cloud infrastructure that are defined by the third-party to maintain the data privacy. The third-party data controls represent two issues related to the data usage by third-party and level of control by owner. This involves assurance of data deletion, fixed response time, losing of data access and cloud data stealing.

In cloud computing security and privacy guidelines (Wayne Jansen, 2011), NIST cites in security threats, it is a problem for the trust. It provides data isolation security concerns in multi-tenant environment of the cloud and sanitization of data measures are also defined.

Another survey (S. Subashini, 2011) by Subashini and Kavitha et al., have been proposed the security issues on the various service models of the cloud computing. There are some securities aspects with focus on data being stored in the cloud are presented below-

4. Data Locality

In the SaaS model, consumers of the cloud computing infrastructure use the tools and softwares provided by the SaaS service vendors for the processing of their business data. In fact, the customers are not aware about the storage of data and processing of data. But sometimes this is not acceptable because of various privacy laws established in many countries. So the location of data is very important in many organization applications. The certain confidential data cannot go outside from the European countries. Thus, the secure SaaS model should provide the reliability to the customer on the locality of the data.

5. Data Confidentiality

Data encryption is the common solution for the data confidentiality. An effective encryption depends on the key strength and encryption algorithm, both should be analyzed. The computational efficiency and processing speed of large encrypted data should be focused into study because the cloud computing environment contains large amount of data transmission. Hence key management is a major problem because of the large number of users is involved. Generally, key management is the responsibility of the data owner. Usually users hand over the key management to the cloud service providers due to the data owner is less expertise to manage the keys. The key management is more complex and difficult because of the large number of users.

6. Data Access

The cloud provider is responsible for the security of data access. Security policies must be designed by the category of the user who wants to access the data. Regular users should be allowed to access sensitive data and it must be assured that only privileged users can be accessed the data. The interruption of the data can be prevented by unauthorized users with the help of security policies of cloud computing.

7. Data Integrity

Data integrity can be easily maintained in the systems that have single database with the help of database constraints. However, multiple database and applications are maintained in a distributed system. Transactions are also performed on each and every database. Transactions are ensured by following ACID (Atomicity, Consistency, Isolation, and Durability) properties. A centralized transaction management is

used to perform those transactions securely. SaaS applications are based on multi-tenancy which is hosted by third party. XML is used in SaaS applications which are based on APIs. Almost all SaaS service providers define their APIs for web services without any support of transaction. So the data level can show into data exploitation due to the lack of integrity controls. Thus developers must provide that integrity of the data is not negotiated.

8. Data Deletion

Local data is generally deleted with less consideration but in case of cloud the data is stored into remote servers to the users which do not have physical approach, so data deletion is also important in case of cloud. A request to delete a particular data must be processed in secure manner to ensure that the data cannot be got back again. The cloud service provider should assure about data deletion because many organizations are storing their sensitive data in the cloud. An attacker can be misused the deleted data if data is not deleted securely because it can be recovered by attacker.

9. Data Isolation

Cloud infrastructure has multi tenancy property and various users share same physical storage location for data, so there may be possibility of data interruption. This can be attained due to some vulnerability or by inserting the vulnerability in the client code. It will permit interruption into others data. A SaaS model should be responsible for proper isolation among the data from different users.

10. CONCLUSION

In summary, there is a need of a framework that provide the protection and management of data stored over the clouds. This framework has the security concerns for the location of data, data protection when it is accessed from the cloud and also maintains the integrity of data. There are many homomorphic encryption algorithms which are used to maintain the security of data and updation of data. In future, there is need to focus on that homomorphic encryption algorithm that will reduce the bandwidth and time the transfer of large encrypted file.

References

A Patrascu, D.M.S., 2012. New directions in cloud computing a security perspective. In *9th international conference*., 2012. Communication(COMM).

Anon., 2013. *Ponemon research study infographic:Whos minding your cloud?* [Online] Available at: http://www.ca.com/us/collateral/white-paper/na/ponemon-research-study-infographic-whos-minding-your-cloud.aspx [Accessed 2 April 2016].

Anon., n.d. [Online] Available at: http://news.cnet.com/83011009_57483998-83/dropbox-confirms-it-was-hacked-offers-users-help/.

Anon., n.d. *http://www.last.fm/*. [Online] [Accessed 2 April 2016].

Anon., n.d. *https://www.dropbox.com/*. [Online] [Accessed 2 April 2016].

Anon., n.d. *https://www.icloud.com/*. [Online] [Accessed 3 April 2016].

Devan Chen, H.Z., 2012. Data security and privacy protection issues in cloud computing. In *Computer science and Electronics Engineering(ICCSEE)*., 2012.

http://www.forbes.com/, 2012. *Another apple disaster:The icloud gets hacked*. [Online] Available at: http://www.forbes.com/sites/timworstall/another-apple-disaster-the-icloud-gets-hacked/ [Accessed 3 April 2016].

http://www.last.fm/, n.d. [Online] Available at: http://www.last.fm/passwordsecurity [Accessed 2 April 2016].

http://www.tappin.com/, 2012. *Securing the clouds[infographic]*. [Online] Available at: http://www.tappin.com/blog/cloudsecurity-ingographic [Accessed 3 April 2016].

M.A. AlZain, E.P.S.A.T., 2012. Cloud computing security from single to multi-clouds. In *45th Hawaii International Conference*., 2012. System Science(HICSS).

M.K., M., 2013. *Secure Data Storage on the cloud using Homomorphic Encryption*.

Peter Mell, T.G., 2009. *The NIST definition of cloud computing*.

S. Subashini, V.k., 2011. Security issues in service delivery models of cloud computing. pp.1-11.

Steven Y. Ko, K.J.M., 2011. The hybrex model for confidentiality and privacy in cloud computing. In *3rd USENIX*. USA, 2011. Berkeley,CA,USENIX Association.

Wayne Jansen, T.G., 2011. *Security and privacy in public cloud computing*. United States.

Witold Litwin, S.J.S., 2011. Privacy of data outsourced to a cloud for selected readers through client side encryption. In *10th annual ACM conference on privacy in the electronic society*. NEW YORK, 2011. ACM.