Journal of Theoretical and Applied Information Technology
20th September 2015. Vol.79. No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

TOWARDS SECURE CLOUD COMPUTING USING DIGITAL SIGNATURE

[1]C. MERLIN PAULIESTHER, [2]DR.J.VISUMATHI

[1]Assistant Professor,Department of Information Tecnology, Sathyabama University

[2]Professor, Department of Computer Science, Jeppiaar Engineering College

E-mail: [1]merlin2781@gmail.com , [2]jsvisu@gmail.com

ABSTRACT

Cloud Computing is a new flair of computing in which real time scaling and virtualized resources are provided as services over the internet. The services provided by Cloud Computing can be grouped into three categories: software as a service, platform as a service, infrastructure as a service. Cloud technologies can help to reduce cost, reduce management responsibilities, increase agility and efficiency of organizations. There are various security issues for Cloud Computing as it comprises many technologies including networks, databases, operating systems, virtualization, resource scheduling, Transaction management, load balancing, concurrency control and memory management. Providing Data security is the crucial challenge in Cloud Computing . The Data security in Cloud Computing includes six aspects: Data-in-transit, Data–at-rest, Processing of Data, Data Lineage, Data Provenance, Data Remanence. Even though Many standards and solutions are developed by groups like The Cloud Security Alliance (CSA), and Open Web Application Security Project (OWASP), still there are Many challenges in Cloud Computing security. An architectural model is discussed to mitigate the data threats by enhancing key management system which aims to provide guaranteed computing dynamic environments for end-users.

Keywords: *VM Template, Key Management System, MultiCloud*

1. INTRODUCTION

A large scale distributed computing paradigm that is driven by economies of scale, in which a pool of abstracted, virtualized, dynamically-scalable, managed computing power, storage, platforms, and services are delivered on demand to external customers over the Internet. Cloud computing is today's trend, with almost all the organizations, institutions trying to cloud infrastructure. The cloud is emerging approach, to improve delivery models for IT capabilities.

Cloud computing offers dynamically scalable resources, as a service through the Internet. The third party, on-demand, self-service, pay-per-use, and seamlessly scalable computing resources and services offered by the cloud paradigm promise to lower capital cost and operational cost for hardware and software. Clouds can be categorized tracking the physical location from the viewpoint of the user into account. A public cloud is offered by third-party service providers and involves resources outside the user's premises. In case the cloud system is installed on the user's premise usually in the own data center this setup is called private cloud. A hybrid approach which is a combination of two or more cloud is denoted as hybrid cloud.

Cloud computing aims to provide scalable and inexpensive on -demand computing infrastructures with good quality of service levels. Cloud Computing is the implementation of distributed computing principals to obtain high quality applications through the Internet. The main expectation of the cloud computing is to provide scalable and low price on-demand computing infrastructures with good quality of service levels. Cloud computing provides computational resources like networks, servers, storage, applications, and platforms are offered 'as a service'. The definition of the cloud computing model "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 or service provider interaction" is introduced by NIST.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

S.No	Services	Providers
SaaS	Support running multiple instances of it. Develop software that is capable to run in the cloud.	Google Docs Mobile Me Zoho
PaaS	A platform which allows developers to create programs that can be run in the cloud. Includes several application services which allow easy deployment.	Microsoft Azure Force.com Google APP engine
IaaS	Highly scaled and shared computing infrastructure accessible using internet browser Consists of Database servers and storage	Amazon s3 Sun's Cloud Service

The advantages of using cloud computing are:

i) Reduced hardware and maintenance cost
ii) Broad network access
iii) Resource pooling
iv) Rapid elasticity
v) Measured Service
vi) Modern Data Center
vii) Virtualization technology

Cloud computing has two major participants, the end user and the cloud. In most scenarios, the end user is connected to the cloud via the internet.

It is also possible for an organization to have a private cloud in which a user is connected via an intranet . The end-user. Who also termed as the client sends requests to the cloud and the cloud service provider offer the service.

Multi-tenancy and elasticity are two key characteristics of the cloud model. Multi-Tenancy enables sharing the same service instance, among different tenants. Elasticity enables scaling up and down resources allocated to a service based on the current service demands. Both characteristics focus on improving resource utilization, cost and service availability.

Cloud computing products, also called cloud service delivery models, which are classified in service terms, like

i) Infrastructure-as-a-service (IaaS).

ii) Platform-as-a-service (PaaS)

iii) Software-as-a-service (SaaS).

Table 1: Service Models

Security is the major obstacle to open the cloud era for many organizations who maintains the sensitive data. Each service model has different possible implementations, which complicates development of standard security model for each service model. Some of the Data related risks are Secured Stored Data, Secured Data Transfer, Trustable Third Party, User Access control, Data Separation, Data can be collocated with the data of unknown owners (competitors and intruders) with a weak separation, Information about the location of the data is unavailable to users, Incomplete data deletion, Data backup done by distrustful third-party providers, Data may be located in different jurisdictions which have different laws.

Now the cloud environment revolves around three functional units:

i) Cloud service provider: It is an entity, which manages Cloud Storage Server (CSS), has significant storage space to preserve the clients' data and high computation power.

ii) Client/owner: It is an entity, which has large data files to be stored in the cloud and relies on the cloud for data maintenance and computation; it can either be individual consumers or organizations.

iii) User: It is a unit, which is registered with the owner and uses the data of owner stored on the cloud. The user can be an owner itself as well.

2. RELATED WORK

As stated the secure management of the resources associated with cloud services is a critical aspect of cloud computing. Cryptographic operations are one of the main tasks of security management. Hence, while cloud services provide ubiquitous computing, elastic capabilities and self-configurable resources at lower costs, they also entail performing several cryptographic operations (from a cloud Consumer perspective) for the following: Secure Interaction of the Cloud Consumer with various services and Secure Storage of data generated/processed by those services.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

The key management system (KMS) is required, since a lot of cloud consumers, cloud providers using keys for sharing data. There many approaches in key management like, key with consumers, key with cloud service providers, partial key with consumers and partial key with service providers, key with Trustable Third Party. This presents challenges to a cloud Consumer seeking to obtain the necessary security assurance from those cryptographic operations.

According to[1] National Institute of Standards and Technology, U.S. Department of Commerce (2013). Two broad two major categories of Cryptographic keys are

2.1 Secret Key

A key which is used to 1) perform encryption and decryption using symmetric cryptographic algorithms and 2)Using message authentication codes to assure data integrity (i.e., Hash based Message Authentication Code or HMAC) or A secret key is also termed as a symmetric key, since the same key is required for encryption and decryption..

2.2 Public/Private Key Pair

The mathematically related key pair used in asymmetric cryptography for authentication, digital signature, or key establishment. As the name indicates, the owner uses the private key of the key pair, It should keep secret, and should be protected at all times, while the public key can be published and used be the relying party to complete the protocol or invert the operations performed with the private key.

From these broad categories one can determine the most commonly used key models in a cloud computing environment like:
i) Public/Private Authentication Key Pair
ii) Public/Private Signature Key Pair
iii) Public/Private Key Establishment Pair
iv) Symmetric Encryption/Decryption Key
v) Symmetric Message Authentication Code (MAC) Key : A symmetric key is used to provide assurance for the integrity of data. There are three techniques:Using a symmetric encryption algorithm and a MAC mode of operation (e.g., CMAC using AES)Using a symmetric encryption algorithm and an authenticated encryption mode of operation (e.g., GCM or CCM using AES); and Use a hash-based MAC (HMAC).
vi) Symmetric Key Wrapping Key: Here symmetric key is encrypted with symmetric key or an asymmetric private key. A Key Wrapping Key is also called a Key Encrypting Key.

According to [2] architectural model distinguished into four designs

i) Replication of applications in which multiple application in distinct clouds produces multiple results on same dataset which helps to prove integrity of data

ii)Partition of the application System into tiers in which logics and data are stored in distinct clouds. This gives additional protection against data leakage due to flaws in the application logic.

iii)Partition of application logic into fragments, this pattern allows application logics got distributed to multi clouds This has two benefits. First, no cloud provider learns the complete application logic. Second, no cloud provider learns the overall calculated result of the application. Thus, this leads to data and application confidentiality.

iv) Partition of application data into fragments allows the data partitioned into a number of fragments and distributed in distinct clouds. None of the involved cloud providers gain access to all the data, which safeguards the data's confidentiality. Each of the introduced architectural designs gives unique security merits, which map to different application scenarios and their security needs.

According to [3] In June 2009 Craig Gentry from IBM implemented the first fully homomorphic encryption scheme that was able to perform many additions and multiplications using ideal lattices and bootstrapping technique. The scheme has proved the possibility of implementing fully homomorphic encryption and laid a solid ground for most recent fully homomorphic encryption schemes including Fully Homomorphic Encryption over Integers , by Marten Van Dijk et al. And Fully Homomorphic Encryption without Bootstrapping by Brakerski et al.

Gentry used ideal lattices to provide an additive and multiplicative homomorphism. The somewhat homomorphic scheme is then transferred into the fully homomorphic encryption scheme using the bootstrapping technique. The bootstrapping is represented as a Boolean circuit that refreshes the ciphertext to prevent the inherent noise factor from growing too large and hence make it difficult to get

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

the correct decryption. After the noise is reduced the number of additions and multiplication operations has no limitation; thus making the scheme fully homomorphic.

According to [4] multi cloud architectural model is used for data recovery procedure and data backup procedure.the queries from clients are buffered and replicated by replica scheduler, and stored in distinct clouds, later data can be recovered when it required.

According to [11] security assurance is provided by verifying the integrity of a large file, by spot checking a fraction of file based on meta data with clients and Proof of Retrievability (POR) by checking a fraction of the file based on the key with clients.

3. PROPOSED WORK

For protecting data in databases, one has to distinguish two security goals: general attributes, confident attributes, for example., personal data, sensitive authentication data. For protecting data in databases, we can partition data in one cloud and logics which used to analyze the data in another cloud.. Data and Logic are distributed in multiple distinct clouds to reduce the risk of malicious data manipulation and process tampering. To enhance the data security, the encrypted form of data is stored. The digital signature of VM Template provided by cloud is Authenticated by the public key of cloud providers. Cloud Provider creates single public/private signature key pair for each cloud consumer. By monitoring resource usage of distinct clouds, cost overhead can be minimized.

The above Figure.1 illustrates, the cloud Provider signs the VM template using the cloud Provider's private key once the VM template has been created.

Every time before running an application on VM, the cloud Consumer checks out a VM template, he/she can verify the digital signature on the VM template using the public key of the cloud Provider. The public key is given to the cloud Consumer and also to the verification engine in a secured manner as illustrated in Figure1.

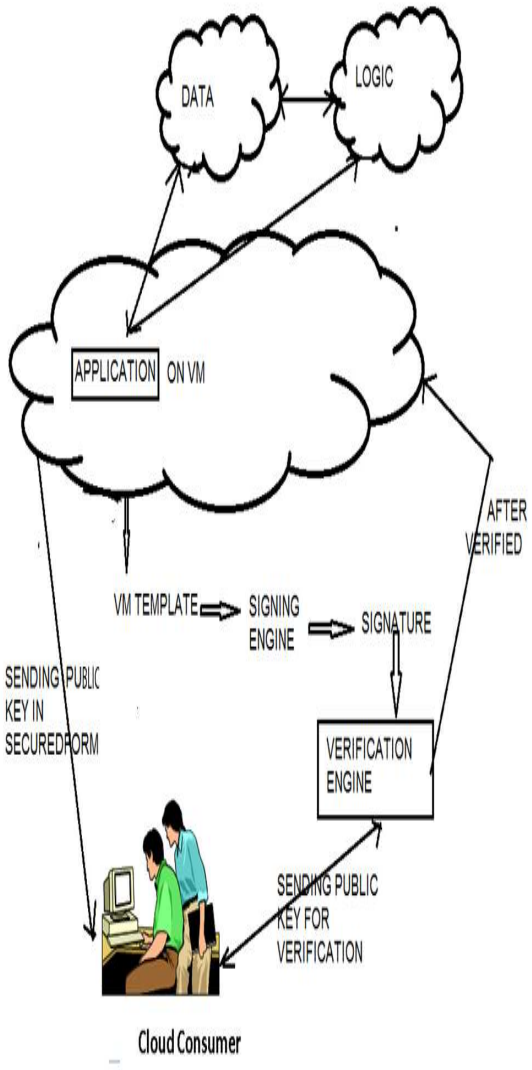

Figure 1: Multicloud approach with verification engine

This approach has the advantage that the cloud Provider is able to create and modify multiple VM templates, and all cloud Consumers can verify the source and integrity of the VM template via a digital signature verification. It also has the advantage of simplified key management. All that is required are the following:

- The Data, Logics and Application which run on that data using the Logics should be distributed in distinct clouds.
- The cloud Provider needs to create a single public/private signature key pair and protect the private key from unauthorized use and from unauthorized disclosure,

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

- The cloud Provider needs to provide the public key in a trusted manner to each cloud Consumer

- The cloud Consumer needs to protect the public key from undetected, unauthorized modification.

This architectural solution has many advantages like Lowering the risk of malicious data manipulation and process tampering, by distributing Data and Logic are distributed in multiple distinct clouds, Enhancement of data security using key agreement, Data Privacy by Authentication and secret sharing, Secure Cloud Computing using Trusted third Party as verification engine, Extending Secure Cloud Computing to Multi server Cloud Computing.

4. RESULTS AND DISCUSSIONS

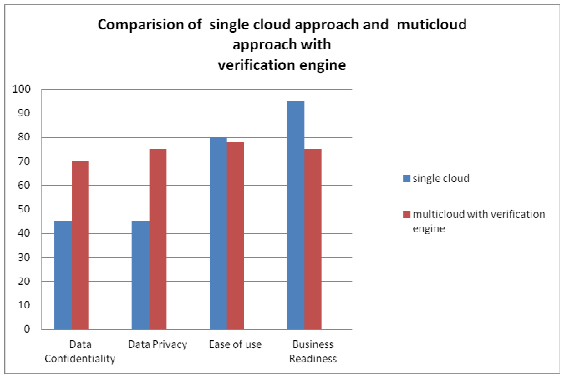

Figure 1: comparison of single cloud approach and Multicloud approach with verification engine

Multicloud approach with the verification engine has many advantages like

i) Separation of data and Logics helps lowering the risk of unauthorized data manipulation

ii) Data security is raised to a higher degree by cryptographic operations.

iii) Enhancement of Secure Cloud Computing by using a verification engine.

iv) Data Privacy by Authentication and secret sharing.

v)Readiness to use is high because of parallel execution in multiple distinct clouds which achieves the idea of Cloud computing very well.

The approach has some disadvantages as well. Even though the approach seems highly secure, there are several security issues with it:

1.The cloud Consumer has to communicate securely with the verification engine to provide the public key and to get the verification results.

2. We have to trust the verification engine which is also provided by another cloud service provider.

3.Since this approach needs an extra step to verify the VM It increases a great deal of process and Time. In spite of these difficulties we can achieve data confidentiality to a great extent and severity of Data threats can be lowered.

5. CONCLUSIONS

Cloud computing has the potential to become a major technology player in the deployment of the future Internet services. At present we are at the starting gate, and there are still many research and technology challenges that need to be addressed and adoption barriers that must be overcome. Fortunately, cloud solution architectures include technology components from different fields and many of these challenges in cloud computing have already been addressed to a certain degree by different research communities, mostly virtualization, Grid, and autonomic computing. These challenges will play a decisive role in the definition of the technology roadmap for the development of future IaaS cloud platforms.

In future, plan to fully implement our model, and various key algorithms has to be used to optimize the verification engine according to cloud consumers requirement.

REFERENCES:

[1] Ramaswamy, Michaela Iorga, and Santosh Chokhani,"Cryptographic Key Management Issues & Challenges in Cloud services," *NIST Interagency or Internal Report 7956* September 2013.

[2] Jens-Matthias Bohli, Nils Gruschka, Meiko Jensen,Luigi Lo Iacono,and Ninja Marnau, "Security and Privacy-Enhancing Multicloud Architectures", *IEEE Transactions on Dependable and Secure Computing*, vol. 10, no. 4, pp. 212 – 224, 2013.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

[3] C.Gentry, "A Fully Homomorphic Encryption Scheme", *PhD dissertation*, Stanford University, 2009.

[4] Yu Gu, Dongsheng Wang, and Chuanyi Liu, "DR-Cloud: Multi-cloud Based Disaster Recovery Service", *Tsinghua Science and Technology*, ISSN 1007-0214 02/10, vol.19, No.1, Feb 2014, pp.13-23.

[4]R. Curtmola, O. Khan, R. Burns, and G. Ateniese, "MR-PDP:Multiple-Replica Provable Data Possession," in *ICDCS '08: Proceedings of the 2008 The 28th International Conference on Distributed Computing Systems*, (Washington, DC, USA), pp. 411–420, *IEEE Computer Society,* 2008.

[5] Mukesh Singhal and Santosh Chandrasekhar, Tingjian Ge, Ravi Sandhu and Ram Krishnan, Gail-Joon Ahn, Elisa Bertino, " Collaboration in Multicloud Computing Environments: Framework and Security Issues " *Published by the IEEE Computer Society* 0018-9162/13.

[6] C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-preserving public auditing for data storage security in cloud computing," in *InfoCom2010, IEEE*, March 2010.

[7] C. Wang, S. S.-M. Chow, Q. Wang, K. Ren, and W. Lou, "Privacy-preserving public auditing for secure cloud storage." *Cryptology ePrint Archive, Report 2009/579*, 2009. http://eprint.iacr.org/.

[8] Z. Hao and N. Yu, "A multiple-replica remote data possession checking protocol with public verifiability," in Data, Privacy, and E-Commerce, 2010. *The Second International Symposium on, IEEE*,September 2010.

[9] P. Mell and T. Grance, "The NIST Definition of Cloud Computing, Version 15," Nat'l Inst. Of Standards and Technology, *Information Technology Laboratory*, vol. 53, p. 50, Website:
http://csrc.nist.gov/groups/SNS/cloud-computing/, 2010.

[10] Zhifeng Xiao et al, "Security and Privacy in Cloud Computing", *IEEE Communications surveys and & tutorials*, Vol 15, No.2, Second quarter 2013.

[11] Fawaz S. A1-Anzi et al, "Towards Robust, Scalable and Secure Network Storage in Cloud Computing", *IEEE 4th International Conference on Cloud Computing* (2014)