Volume 3, No. 9, September 2012
Journal of Global Research in Computer Science
ISSN-2229-371X
REVIEW ARTICAL
Available Online at www.jgrcs.info

COMPARATIVE STUDY OF VARIOUS EXISTING SECURITY SCENARIOS IN CLOUD COMPUTING ENVIRONMENT

Dr. R. Sridevi[*1] Vasavi Bande[2]
[*1]Associate professor, Computer Science and Engineering
Jawaharlal Nehru Technological University, Hyderabad, AP,INDIA
[1]sridevirangu@yahoo.com
[2]Associate professor, Computer Science and Engineering
Netaji College of Engineering and Technology, Hyderabad, AP, INDIA
[2]vasavi.bande@yahoo.co.in

Abstract:- The advantage of Cloud computing is ever lasting but it brings more issues including security, such as virtualization security, application security, identity management, access control and authentication. This paper focus on recent research pertaining to Cloud Security. This paper envisage on diverse security sphere parameters in cloud computing such as Framework, Risk Management, Compliance , Lifecycle Management, Interoperability, Business Continuity, Data Center Operations, Incident Response, Encryption and Key Management, Identity and Access Management, Virtualization, Static Access Security, Internet Access Security, Dynamic Access Security etc . We have used the classification and survey results not only to discover similarities but to explore the differences in the architectural approaches of cloud computing and also to identify areas requiring thorough research. Thus, it provide findings based on the detailed review and could assist in analyzing best fit scenario for a elegant secured cloud computing environment.

Keywords: Service provider, secret key, trusted service, ticket, encryption.

INTRODUCTION

Security has become a vital problem in distributed systems and network computing. In distributed computing different services are spread on different servers that are distributed in different places to squash forward the work efficiency. Even though the distributed computing technologies are fast developing but still not enough to earn information security and safety. Recently, a new trend attracts people's attention, in which users from diverse and multiple environments hope to use the distributed computing more efficiently, just like using the electric power. Thus, cloud computing has become a new idol to meet this demand. Cloud computing simply means Internet computing, generally the internet is seen as collection of clouds, thus the word cloud computing has emerged 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 or service provider interaction.

Cloud computing enables consumers to access resources online through the internet, from anywhere at any time without worrying about technical and physical management or maintenance issues of the original resources. Besides, Resources of cloud computing are dynamic and scalable. Cloud computing is independent computing and it is totally unlike from grid and utility computing. Google Apps is the chief example of Cloud computing, it enables to access services via the browser and can be deployed on millions of machines over the Internet. Resources are accessible from the cloud at any time and from any place across the world using the internet. Cloud computing is cheaper than other computing models. The maintenance cost involved is zero since the service provider is responsible for the availability of services and clients are free from maintenance and management issues of the resource machines. Due to this feature, cloud computing is also known as utility computing or simply IT on demand. Scalability is key attribute of cloud computing and is achieved through server virtualization.

This new, web-based generation of computing uses remote servers placed in extremely protected and secured data centers for storage of data and management, so that organizations need not pay for or look after their interior IT solutions. After creation of a cloud, deployment of cloud computing changes with reference to the requirements and for the purpose it will be utilized. Cloud providers use virtualization technologies combined with self service abilities for computing resources via network infrastructure. In cloud environments, several kinds of virtual machines are deployed on the same physical server as infrastructure.

There are three major types of services in the cloud environment i.e Software as a service, Platform as a Service, and a Infrastructure as a service. The cloud model has different dimensions that participate in complicating its security problem. The cloud model has two key characteristics, Multi-tenancy which results in virtualization of the boundaries among the hosted services of different tenants and thus, we need to solidify such boundaries with new category of security controls, and elasticity which requires secure services' migration and secure service placement strategies. Now a days the available security mechanisms are suitable for single cloud provider and single cloud user, in the near future if the cloud moves to multi provider environment security then it would become the most difficult problem. To address this problem section II we describe about the research that is being done by different researchers .

COMPARATIVE STUDY OF EXISTING APPROACHES

In 2011 Mahbub ahmed et al [1], introduced a mechanism for providing trust and security in SAAS. According to his idea the control over data, user's registration, and access to the outsourced data will be under the control of data owner. The data owner issues a trust ticket for the registered user and the data owner keeps record of each registered user. The data owner sends the trustID, user's public key, capability list to the CSP. Hence the registered user when submits the request for the CSP and it will be identified by the CSP whether he is a valid user or not. They devised an algorithmic protocol for the deployment of a data owner-generated Trust Ticket. This Trust Ticket is an idea of trust from the perspective of a data owner's control over data and a registered user. In this mechanism da ta owner encrypts the data with secret key (KO) and outsources the encrypted data to a CSP. A data owner shares KO with a user at the end of that user's registration. A data owner is the issuer and distributor of the Trust Ticket during a user's registration.

In this mechanism the registered user capability list will be stored by the CSP as well as the data owner which will be used to identify invalid users if the registered user submits different authority rights. In the algorithmic protocol for Trust Ticket deployment, triple verifications of a registered user and triple encryptions of data is established as a data owner's notion of trust. Here the data owner can change user's access right and trust ticket expiration and he can also update data by changing the secret key K0 shared with users. Unless a data owner makes any changes, a registered user uses the Trust Ticket and KO for a data owner's data service from a CSP. They assumed that a registered user does not share KO with a CSP in any way. However, they have not yet devised a mechanism to counter a malicious situation of a user's sharing KO with a CSP.

Based on the presentation held in December 2011 in the 14th International Conference on Computer and Information Technology (ICCIT 2011)[2] similar areas were explored. According to Aashish Bharadwaj's discussion IT services are now moving towards cloud dissimilar to traditional solutions where there is physical control. As the Cloud Computing moves the application software and databases to the large data centers, the management of the data and services may not be fully reliable. Even though we are having lot of advantages of cloud computing still security and privacy issues became strong fence for user's acceptance of Cloud systems and Cloud services. Their presentation suggests that more security strategies should be deployed in the Cloud environment to achieve these goals as well as privacy acts should be modified to adapt a new relationship between users and providers. Privacy should be taken into account when designing cloud services. It is not recommended to try to insert security at a later stage in the design process. They suggested that Identity management is important as it is possible that customers hold multiple accounts with the service providers like e-bay, Gmail etc. So in this scenario intense precautions should be applied to identify the entities. In their discussion they mentioned that the Dynamic mapping Association N Discovery System (DIMANDS) is an identity management solution for large scale heterogeneous network environments and it is based on an innovative Distribute Hash Table (DHT) overlay infrastructure which combines the routing capabilities of DHT networks and the security benefits of individual Identity Providers (IdPs). According to him in the near future the identity management problem will become more complex and will have to deal with not only with the management of users' identities but also with interconnected devices, machines and software components. According to them the observed security domains in cloud computing are Cloud Computing Architectural Framework,

Governance and Enterprise Risk Management, Legal and Electronic Discovery, Compliance and Audit, Information Lifecycle Management, Portability and Interoperability, Traditional Security, Business Continuity, and Disaster Recovery, Data Center Operations, Incident Response, Notification, and Remediation, Application Security, Encryption and Key Management, Identity and Access Management, Virtualization, Server Access Security, Internet Access Security, Database Access Security.

In the view of Ling Li Lin Xu Jing Li Changchun Zhang [4] now a day's most service providers think to improvise their income. This is done in lieu of improving the security with the help of audit mechanism as the internal audit incurs cost as well as with the help of internal auditing team will get the internal behavior and process of service providers and as a result operating process of those providers will be exposed in the audit results. Apart from internal audits even external audits may not be accepted by the service providers because they are supporting the auditing only for static data. So to support dynamic data auditing these people introduced dynamic verifiable data possession (DPDP), in which the correctness about the audit result can be strictly guaranteed.

In the view of Ling Li Lin Xu Jing, Li Changchun Zhang. To increase the cloud storage service usage, two prerequisites are essential. The first one is the availability of service supply for the end user including large storage space, and the scalability. Based on the prerequisites as mentioned above they built a service supply platform based on open source software Eucalyptus in their research work. It is mainly used for convenient storage service supply to their campus. They introduced the cloud storage service architecture which is composed of three entities users, service providers and the TPA. They proposed an idea of bringing in the TPA mechanism into the file sharing system and analyzed the reliability of the system. But it has to be tested with larger storage case.

According to Joel Ahmed M.Mondol et al in 2011 [3**],** a new research strategy towards delivering cloud computing security using reconfigurable computing has been discussed. In his presentation four different solutions were proposed in which all together can allow trusted computing while keeping the data secured. The solution discussed is to introduce possible hardware solutions that can increase trust in cloud computing by keeping control of data in the hands of the data owner. If the physical hardware is associated with the user, the issues with anonymity are greatly reduced and increased security measures can be built around the concept. This hardware is directly associated with the user

and this FPGA device is separate from the cloud. The FPGA device allows ownership of identity to be non reproducible from the third party client. The idea of security is gained through direct participation of the client and their willingness to ensure security and not singularly dependent on the security commitment of the cloud service vendor(CSV). As FPGA devices are located in the client side of the computation it prevents malicious internal cloud service providers to tamper with the PAAS and IAAS layer.

This layer is invisible to the CSV and its operators. Yet its presence and execution can be agreed upon by both CSU and CSV. The problems associated with the virtualization technology can be removed as the FPGA based trust tools clients are essentially tied to the FPGA hardware. The solutions mentioned are Trusted cloud computing platform, User enabled security groups, Data security, Verifiable attestation. The four different solutions implemented on hardware provide security solutions for four different areas Trusted Platform, User Enabled Collaboration Mechanism using Security Groups, Finally Data Security, Cloud Service User and Cloud Service Vendor (CSV) attestation. These solutions can be either implemented in a collective manner on the cloud as a security suite or individually based on the requirement of the cloud user. All four of these solutions ensure that the security is enabled by the Client, the owner of the data.

A study based on Sherif El-etriby, Eman ,M. Mohamed et al [5] has evaluated eight modern encryption techniques namely RC4, RC6, MARS, AES, DES, 3DES, Two-Fish, and Blow-Fish with two independent platforms namely desktop computer and Amazon EC2 Micro Instance cloud computing environment. The algorithms are evaluated based on the randomness testing by using NIST statistical testing in cloud computing environment. This evaluation uses Pseudo Random Number Generator (PRNG) to determine the most suitable technique and analysis the performance for selected modern encryption techniques.

They implemented Cryptography algorithms using Java Cryptography Extensions (JCE). According to them In Amazon EC2, the evaluation of eight modern encryption techniques show that RC6, AES, DES and Blowfish results were slightly better than other encryption methods, Which the pervious methods have more than P-value in very safe area.

Based on their research they suggested that AES encryption method is suitable algorithm for Amazon EC2 environment, and based on time of encryption method Blow-Fish and DES are suitable.

Similar work has been proposed in the paper by Uma Somani, Kanika Lakhani, Manish Mundra et al [6], to overcome the security problems with the cloud computing Uma somani along with her team proposed digital signature with RSA algorithm. In digital signature technique the data and the document will be compressed into a few lines by using hashing algorithm. These few lines are called as message digest. Digital signature is produced with the encryption of the Message digest with the sender's private key.

The steps involved in implementation are as follows.

a. Hashing algorithm will be applied on the document to get the message digest.
b. The generated Message digest is encrypted with the sender's private key.
c. The Digital signature is then encrypted with the receiver's public key, and then at the receiver's side the receiver will decrypt the cipher text into plain text with his private key and verifies the signature with the sender's public key. Digital Signature scheme is useful to detect forgery and tampering in the fields like financial transactions.

In 2011 canh Ngo,Peter Membrey et al [7] Canh Ngo has presented the ongoing research on developing security framework in multi provider cloud computing environments and infrastructure services provisioned on demand which aims to deliver a security infrastructure to support consistent trust establishment, Identity management, access control and security context management.

Now a days most of the currently available commercial cloud services are built and organized with single provider and single customer with simple security and trust model but in order to create multi provider heterogeneous environment new architectural models should be developed. These new models should support new security approaches to create consistent security issues in virtualized multi provider cloud environment and it should provide complex access control and trust relations among the various cloud actors. He defined security infrastructure reference model for on demand services provision systems which include common security service, Authentication and Identity Management, Security Context Management System, Trust Management, SLA Management.

As the cloud provider is offering multi tenant environment implementing different security policies it is difficult and suggested that cloud providers should be able to hand over such services to customers in associating with their clouds.

According to Canh Ngo's security reference model the identified dynamic access control service components are Identity management, authorization service, DACS management service and CSSI gateway in which the trust is created from the most fundamental hardware such as BIOS and then to the OS and then virtualization platform which hosts virtualized services and DACI itself. This DACI is implemented in GEYSERS project and their further research includes implementing bootstrapping protocol in TPM.

In 2010, Zhidong Shen, Qiang Tong in 2nd International Conference on Signal Processing Systems[8] discussed about a method to build a trusted computing environment for cloud computing system by integrating the trusted computing platform into cloud computing system. In the view of Zhidong Shen, in cloud computing environment the trusted root has not been defined clearly. The creation and protection of certificates are not secure enough for cloud computing environments. He expressed that in the current scenario we have to work a lot to protect our sensitive data as number of threats are growing and hackers are

developing new kinds of attacks and many technology researchers support the development of trusted computing (TC) systems embedded with data security mechanism into their core operations, rather than implementing it by using add-on applications.

Trusted Computing Platform (TCP) operates through a combination of software and hardware. manufacturers add some new hardware to each computer to support trusted functions, and then a special TC operating system mediates between the hardware and any TC enabled applications. TCP provides two basic services, authenticated boot and encryption, which are designed to work together.

An authenticated boot service monitors what operating system software is booted on the computer and gives applications sure way to tell which operating system is running. It does this by adding hardware that keeps a kind of audit log of the booting process. When the machine starts booting, the TC hardware computes the cryptographic hash of the code in the Boot ROM and it writes that hash into the tamper-resistant log. Before it brings in the next block of code, the code from the Boot ROM computes the hash of the next block and appends it to the end of the tamper-resistant log. In turn, each chunk of code adds to the log the hash of the next chunk that will load. This process continues until the entire OS is booted, at which point the tamper-resistant log contains a record what can establish exactly which version of which OS is running. Integrating different hardware modules with cloud computing system is a challenging work and need more deep research.

FINDINGS BY ANALYSIS

The table 1. Reviews the various mechanisms suitable for providing security in virtualized cloud computing environment to find out the better solution for security based trusted computing, dynamic security etc. It also describes the strength of each research work and identifies the areas where it has to be improvised.

Table 1. Analysis of different mechanisms based on their Findings.

Related Area Under review	Mechanism used	Strength of the Method	Implementability	Suitability for usage through findings
Reference paper[1]	Algorithmic protocol for trust ticket deployment	Triple verifications	Data owner has to work hard to provide security even though data is placed in cloud	If the Registered user shares the secret key with the CSP security violations will arise.
Reference paper [2]	Dynamic Identity Mapping Association N Discovery System (DIMANDS)	Only validated providers can issue requests to retrieve information from DIMANDS.	Not sufficient	Only Identity management is not enough for providing complete security
Reference paper [3]	FPGA device	Trusted cloud computing platform, User enabled security groups, Data security, Verifiable attestation.	Its possible to implement	We have to provide Security for the Hardware device
Reference paper [4]	dynamic provable data possession	Correctness of the audit is guaranteed	possible	Has to be tested with large data storage
Reference paper[5]	Surveyed on different encryption algorithms	Gave results about different encryption algorithms	Implemented and tested different encryption algorithms	Only tested with Amazon EC2
Reference paper[6]	Digital signature with RSA algorithm	Easy to implement	possible to implement	Has to be tested with large data storage
Reference paper[7]	Dynamic access control Infrastructure	provides security in virtualized multi provider cloud environment	(DACI)Implemented in GEYSERS project	Bootstrapping protocol has not yet checked.
Reference paper[8]	Trusted computing platform with trusted platform model	Trace mechanism	possible	Integrating different hardware modules with cloud computing system is a challenging work and need more deep research.

CONCLUSION

Based on the review carried out in this paper, we conclude, that in multi provider cloud environment cannot provide complete security. To offer complete security trust assessment work would be carried out under the supervision of TPM. According to the method prescribed, it is clear that dynamic access control is achieved with the help of DACI mechanism. It is evident that this method exhibits better results in terms of dynamic access control under multi provider environment as compared to other mechanisms.

As a futuristic scope we suggest that the strength of the proposed algorithm must be based on implementing secured bootstrapping protocol which is created from the most fundamental hardware such as BIOS and then to the OS and virtualization platform which hosts the virtualized services.

REFERENCES

[1]. Mahbub Ahmed, Yang Xiang,Trust Ticket Deployment: A Notion of a Data Owner's Trust in Cloud Computing, IEEE 2011.

[2]. Aashish Bharadwaj, Vikas Kumar, Cloud Security Assessment and Identity Management, ICCIT 2011 22-24 2011.

[3]. Joel Ahmed, M.Mondol Cloud security solutions using FGPA IEEE 2011.

[4]. Ling Li Lin Xu Jing Li Changchun Zhang , Study on the Third-partyAudit in Cloud Storage Service, International Conference on Cloud and Service Computing, 2011.

[5]. Sherif El-etriby, Eman ,M. Mohamed, Modern Encryption Techniques for Cloud Computing Randomness and Performance Testing.

[6]. Uma Somani, Kanika Lakhani, Manish Mundra, Implementing digital signature with RSA algorithm to enhance the data security of cloud in cloud computing,IEEE 2011.

[7]. Canh Ngo,Peter Membrey, Security Framework for Virtualized Infrastructure Services Provisioned On-demand 2011.

[8]. Zhidong Shen, Qiang Tong, The Security of Cloud Computing System enabled by Trusted Computing Technology IEEE 2010.

Short Bio Data for the Author

 **Dr. Sridevi Rangu** obtained B.E (Computer Science and Engineering) from Madras University, chennai, and M.Tech (Computer Science and Technology) from Andhra University Visakapatnam in 1999 and 2003 respectively. She is having nearly 12 years of teaching experience. Since November, 2006 she is working as an Associate professor in JNTU Hyderabad. She pursued Ph.D. from faculty of Computer Science and Engineering JNTU Hyderabad in December, 2010. Areas of research interest are Network security, Intrusion Detection and Computer Networks. She is Guiding 6 Ph.D students in the area of network security and guided more than 25 M.tech students. Published 10 research papers in various International Journals and conferences. She achieved best Paper Award in ICSCI-2008**,** Pentagram Research Center, Hyderabad, India, 2008.

 Vasavi Bande, is M.Tech in Computer Science from Jawaharlal Nehru Technological University,A.P., India. She is presently working as Associate Professor in Department of Computer Science and Engineering, Netaji Institute of Engineering and Technology , Hyderabad, A.P, India. She has authored 7 research papers to date and are published in reputed and indexed International Computer Science Journals. Her area of research include Cloud computing, Network Security, Data Mining, Web Technologies and Emerging Technologies. She can be reached at vasavi.bande@yahoo.co.in

