CLOUD COMPUTING SECURITY: ENABLE BY TRUSTED COMPUTING

[1] MR. Chintan V. Shah, [2] Ms. Pooja K. Shah

[1] Asst.Professor of IT Engineering, SVBIT, GTU
[2 1] Asst.Professor of CE Engineering, SVBIT, GTU
Chintan.shah@bapugkv.ac.in, pooja.shah@bapugkv.ac.in

Abstract— **Cloud computing is a collection of resources and services offered by the Internet. Cloud services are delivered from data centers located throughout the world. Cloud computing helps its customers by providing virtual resources via the Internet. General example of cloud services is Google apps, provided by Google and Microsoft SharePoint. The rapid growth in the area of "cloud computing" also increases the serious security issues. Security remained a constant problem for open systems and the Internet, when we talk about cloud security genuinely suffering Cloud service requires security measures in three domains: data storage, processing and transmission. In this paper, we are focusing on security measures required for cloud computing. We proposed a method to build a secure computing environment for the system by integrating cloud computing platform of confidence in the cloud. We propose a model system in which cloud computing system is combined with trusted computing platform with trusted platform module. In this model, some important security services, including authentication, confidentiality and integrity, are provided in cloud computing system.**

Keywords— **cloud computing, cloud computing security, trusted service.**

I. INTRODUCTION

Cloud computing and distributed systems were uses widely, security becomes really important problem and we need to put more focus in future [1]. To get full benefit of cloud computing, we must check the data, application and systems are fully secured, so cloud infrastructure will not rendering any sensitive data of organization. Risk associated with cloud computing, such as privacy, data integrity, security and recovery of data etc., it is main barrier of accepting cloud computing for organizations [2]. Cloud computing provides a facility to use same resource (data) from different locations without configuring client machine. So security is major concern in any cloud computing architecture because it is necessary that only authorize person can access and secure behavior can accept. In other words, users in cloud and the cloud computing infrastructure are trusted by each other's and whatever communication done between them, also trusted by each one.

Cloud computing is combination of local system and remote servers which are accessible by internet or intranet, that's why to implement a security in cloud will be complicated. The security should provide assurance to users that data are secured to access but on other hand, we need to make sure that security is not be much complicated that users do not put into awkward situation. There should be balance between security and convenience [3].The dependable and secure computing includes not only security and confidentiality, but also reliability, availability, safety and integrity [4]. In this model, we are integrating Secured Computing Platform (SCP) which is based on Module for Secured Platform (MSP). The SCP is used in authentication and integrity in cloud computing infrastructure. With help of SCP, we can improve the security and remove complexity from users. Basically CSP is hardware modules and will improve the performance of cryptographic computation. Our aim is also to design middle ware so our cloud application can use easily security function.

II. WORK OF CLOUD COMPUTING SECURITY

A. Cloud computing's existing security model

To obtain maximum security of cloud computing system, some tools and technologies are using. The cloud computing security can be provided as security services. Security message and secured messages can be transported, understood, and manipulated by standard web services tools and software. This mechanism is a good choice because the web service technology has been well established in the network-computing environment [1]. With the help of this mechanism, we can secure cloud computing security but there may be some disadvantages. As for example, with help of certificates, are not enough to secure cloud computing. One problem with cryptography, when it is using the performance will be down. And also we cannot trace and monitor users that how many users are participating in cloud.

B. Security challenges for cloud

There are various security issues for cloud computing as it encompasses many technologies including networks, database, operating systems. Therefore, security issues for many of these system and technologies are applicable to cloud computing.

For example, data security involves encrypting the data as well as ensuring that appropriate policies are enforced for data sharing [4].

The cloud includes different users from different locations which have different security policies. For considering these criteria, it is a challenge to build secure cloud computing environment.

In the next section, we are proposing the mechanism of secured computing platform.

III. TRUSTED COMPUTING TECHNOLOGY

A. Trusted Computing Technology

Today, the biggest problem in computer technology is data security and privacy and this problem become nastiest because users are working or storing with sensitive data. Hackers are introducing new types of attack on system every day. In this case, it is very challengeable task to secure our data. Many researchers are developing trusted system that integrated with application. In this system, Trusted Computing (TC) system will cryptographically lock the hardware that providing resource to application and resource and other side provide decryption key to take decision about trusted connection. The trusted word defined as "A trusted component, operation, or process is one whose behavior is predictable under almost any operating condition and which is highly resistant to subversion by application software, viruses, and a given level of physical interference."[5]

B. The Secured Computing Platform

The SCP handled by a combination of hardware and software: manufacture adds new hardware to support to trust computing functions and design special operating system that becomes mediator between hardware and application to support trusted computing. SCP provides two types of service: authentication and encryption, both will work together. With authentication only trusted person can log into the system and use resources and also we need to track of log of the boot process.

IV. CONSTRUCT TRUST CLOUD COMPUTING SYSTEM USING SCP

With help of trusted computing, we can provide a way to establish secure environment in cloud. The basic purpose of developing this model is that provide the privacy as much we can and build trust in the cloud. Cloud computing is a distributed system model and act as a likely important role in e-business environments or research. Web service technology has been developed quickly and adopted by users in mean time. Cloud computing service has been integrated with web technology in that case we need to provide trusted computing system to secure data and application.

A. Authentication cloud computing environment with LDAP

In cloud computing, different users want to join cloud so they have to prove their identities before join cloud. Because cloud computing should involve in large amount of data, users and they are connected with each other. So authentication is important and also complex, we use LDAP to aid the process for authentication in cloud computing.

The LDAP is based on MSP which is hardware and it can prevent attack from different sources such as hardware attack or software attack. MSP hold a private key and that provide protection for information which stores in cloud computing environment. Certificates will store in hardware so it is not easy to attack on hardware and this way MSP should provide trust to users.

When users have full information about them (identification) so it is easy to trace the users and that mechanism will implement for cloud and get the record of users and trace them. LDAP will store user's personal key and with help of this key we can proved user's identity. Each cloud computing service will keep record of user's information. By using LDAP mechanism in cloud computing, the trace of participants will be done easily.

B. Person Based Access Control Model in cloud computing environment

There are too many users in cloud computing system that wants to access the resources. Every users have own purpose and goal to using cloud resources. If cloud computing deals with each user, it will be more difficult to control. So in other words, we need to reduce complexity, so we need to classify into such groups or classes. When user should register them into one or more class in cloud computing for accessing resources, and get some rights to access those resources. So when user tries to access cloud, they have to prove their identity and as per identity, acknowledge class/group and access source.

To attain the objective of trusted computing, users has to come from trusted platform, and take the safety mechanism on the platform for the privacy and security for their own. The user has its own id, message/password and secret key to get right to use LDAP. User has to hold decryption key to protect own data and privacy.

When the machine starts, the trusted computing hardware calculates the cryptographic hash of the code in ROM and writes to the log. Before it works on the block of code, the ROM code calculates the hash of the next block and adds it to the end of the log book. This process will continue until whole OS is not loaded, at some point log contains records that can establish the exact version of the operating system is running. The trusted computing contains part is called certifying, with the help of certificate for trusted computing hardware to know via its log what software configuration is running and then OS can verify the application's configuration. If we trust TC and OS, we can know the application's configuration. A configuration certificate can provide to any addressee such as class/group or the program running on another computer in the cloud computing environment. Addressee can verify this certificate and check whether it is up-to date so user can know the configuration of system.

With the help of remote attestation function, use the LDAP can notify their identities and information relevant to the

remote machine on which they want to access resources. Each environment has the objective clarifying the mechanism of the entity accessing information about their identity, role and other safety information.

Permission and role is also associate with cloud computing. When the user will request for resource the system will check whether user can able to access those resource that allocated when user was registered before it access.

The other important factor is encryption. This function will encrypt data and only decrypt on the other machine that hold the decryption key or machine holding such type of trusted configuration. These types of services, we can establish with help of software and hardware. If such person doesn't have proper configuration or decryption key and tries to decrypt the connection so such user can able to do that but as audit, we need to register those entry into log book.

C.Data Security in cloud based on LDAP

With LDAP, the various entities can communication in network with secure way. LDAP generate random keys and session keys. The random key generated by physical hardware and it is just better than software program. The MCP provides the encryption key and session key to the communicators in cloud computing.

The precious data stored in computer can be accessed by encrypted key which is generated by MCP. When access data, the user will pass authentication first, and encryption key store in hardware so it will not easy to bypass or attack on those keys.

D.The trace of user's behavior

Users have full information about their identity and role. The cloud computing system can use some mechanism to trace the users and their origin. Because in MCP the user's identity is proved by user's personal key and this mechanism is integrated by the hardware. When the user login into system, user's identity will be recorded and verify, it also stores the visitor information. So if the LDAP configuration is integrated into cloud application, the trace of users, including the user and other resources. If participant perform some illegal operation that will be recorded into log book and can know where it was perform, they will tracked and punish them. Monitoring function has to integrate into cloud application so we can also track that what participant can do and what they perform.

V. CONCLUSION

We reviewed the trusted computing in the cloud environment and function of confidence computing platform in the cloud. The advantages of our suggested approach is to extend trusted computing technology in the cloud computing environment to achieve the requirements of trusted computing to cloud computing and then fulfill the trusted cloud computing. LDAP is used as hardware configuration for the cloud computing service. In our approach, LDAP offers some important security function such as authentication, security for sensitive data and data protection

The LDAP provides cloud computing a secure base for achieve trusted computing. But how to integrate this entire module i.e. hardware and software is big task and required more research. We developed Secured Computing Platform, which is based on Module for Secured Platform and can provide flexible security service to the users.

REFERENCES

[1] Zhidong Shen, Qiang Tong, "The Security of Cloud Computing System enabled by Trusted Computing Technology", the 2nd international conference on Signal Processing System, 2010

[2]http://www-03.ibm.com/security/cloud-security.html

[3] Jason Reid Juan M. González Nieto Ed Dawson, "Privacy and Trusted Computing", Proceedings of the 14th International Workshop on Database and Expert Systems Applications, IEEE, 2003

[4] Algirds Avizienis, Jean-Claude Laprie, Brian Randell, and Carl Landwehr, "Basic Concepts and Taxonomy of Dependable and Secure Computing", IEEE transactions on dependable and secure computing, vol.1, No.1, January-March, 2004

[5] Dr.Rao Mikkilineni, Vijay Sarathy, "Cloud Computing and the Lessons from the Past", the 18th IEEE international Workshops on Enabling Technologies: Infrastructures for Collaborative Enterprises, on page(s):57-62, 2009

[6] ISO/IEC. Information technology - Open Systems Interconnection - Evaluation criteria for information technology, 1999. Standard ISO/IEC 15408.

[7] Frank E. Gillett, "Future View: The new technology ecosystems of cloud, cloud services and cloud computing" Forrester Report, August 2008.

[8] Farhan Bashir Shaikh; Haider, Sajjad," Security threats in cloud computing", Internet Technology and Secured Transactions (ICITST), 2011