IaaS Cloud Computing using Distributed Protocol

Supriya F. Rathod[1], M.Tech. scholar[1], Department of Computer Science & Engineering, Government College of Engineering, Amravati, *rathod.supriya4@gmail.com*

Prof. Pushpanjali Chouragade[2], Assistant Professor[2],Department of Computer Science & Engineering, Government College of Engineering, Amravati , *pushpanjalic3@gmail.com*

,

Abstract - Cloud Computing provides various economical benefits. Security issues are raised while working with cloud computing. In this paper we propose a novel technique that will allow consumer to work in cloud environment. Firstly we present theoretical analysis of selected technique and identified issues in IaaS cloud computing. Secondly we propose scattered Trust Protocol for IaaS Cloud Computing in order to make connection between users more secure. This is a distributed protocol that makes user feel comfortable in cloud computing platform. We follow the rule of safety responsibility division between the property of consumer and provider. We make the consumer actual owner of the system. In our protocol, following specification of Trusted Computing Group (TCG) and Trusted Platform Module (TPM) Chip of the consumer are utilized. The protocol is for the Infrastructure as a Service IaaS**.**

Index Terms - Trusted cloud computing, cloud computing, trusted computing, cloud security and trust, virtualization

.1. INTRODUCTION

As the name denotes, the word cloud means the collection of various users that uses internet services to communicate. It hides the basic abstraction for the users of cloud computing and yields a problem free thought for embracing the IT services from cloud service provider (CSP). In cloud computing there may be the participation of three entities: Cloud Infrastructure, Cloud Service Provider and Cloud Consumer. But, the two major entities used for the cloud computing model are Cloud Service Provider (CSP) and Cloud Service Consumer (CSC). Organizations exploit Cloud computing services in some delivery models. There are three services used in cloud computing that are: First, Software as a service (SaaS), Second, Platform as a Service (PaaS), Third, Infrastructure as a Service (IaaS).

Infrastructure as a Service (IaaS) model is an important layer for cloud environment where physical resources are placed, to obtain multi operation performance. It is needed to check that virtual structure for security. The literature studied for this, yields strong clue that there is a lack of such systems that lets the consumer to check the virtual environment for integrity and privacy. At IaaS layer all the security methods for safety of environment are performed by the service provider, so consumer has to trust in his infrastructure. There arises some queries for consumers to trust on. It is very tough for the customer to trust on the infrastructure provided by the other providers. This work proposes a Distributed Trust Protocol (DTP) that supports the security over VM of provider. Our proposed protocol is distributed between the provider and the consumer. In this protocol client stores the hash values of VM components (BIOS, Boot Loader and OS) in its PCRs of TPM at client side. TPM measures (hashes) all the software and firmware components, including the boot loader, and operating system kernel etc. before they are loaded and stores hash values in PCRs of TPM. In this DTP, TPM at consumer side is linked with VM hosted at provider side. After linking, consumer VM will be initialized as per the TCG's Trusted Boot Process. Therefore by using consumer's infrastructure the integrity of VM is checked. The basic element of working our protocol is hardware called Trusted Platform Module (TPM). The completed work is then combining with terms of Trusted Computing Group (TCG). This prediction is used to support for research work which authors are using the de facto hardware module for growing the trust in cloud computing environment. The cloud computing provides three service models that are IaaS, PaaS and SaaS.

1.1. Infrastructure as a Service (IaaS):

This is the important model for our research. This IaaS model must provides the services on cloud such as computing infrastructure of processing, storage and network resources. On this resources users can place and run there software. Its main functionality is to provide minimum purchasing and managing cost of basic hardware infrastructure. The main example of IaaS is Amazon Elastic Compute Cloud (EC2) used by various users. The main purpose of this model is to provide consumer storage, networking and processing facility and also provides some fundamental resources. This resources are used by consumer to store and run their software in the cloud computing environment. The consumer is not able to manage and control all the cloud infrastructure but they has control over operating systems, storage of software, deployed applications, and also can choose networking mechanism. Examples are Amazon EC2, GoGrid, and Flexiscale.

1.2. Platform as a Service (PaaS):

PaaS is a software model where applications are placed and works on demand. It reduces the cost of software purchasing, housing and deployment. The security in this model is a shared by the provider and the subscriber. The Amazon Simple Storage Service is an example of PaaS. The capability provided to the consumer is to produce cloud infrastructure consumer-created applications using programming languages and tools supported by the provider of languages e.g., Java, Python, .Net. In this model consumer is not able to manage and control the networks, servers, etc. But the consumers are able to manage over the applications and application hosting situation configurations. Examples are Google App Engine, Microsoft Azure, Amazon SimpleDB/S3.

1.3. Software as a Service (SaaS):

The SaaS model provides software/application for use on demand. This model can decrease the cost of software, repairing cost and operational cost. The security is the responsibility of the cloud provider in this model. The capability provided to the consumer is to use the applications running on a cloud infrastructure and other users can access various client devices through a medium such as a Web browser e.g., web-based email. The consumer does not control the any cloud infrastructure, network, servers, operating systems, storage. Examples are Google Docs, Salesforce, NetSuite, facebook, YouTube. This says that the cloud computing is collection of PaaS, SaaS and IaaS models. The employees working for an organization can be users or providers of cloud computing services in accordance with the organizational scope and the control over the IT environment. When a cloud is made available to the general public, it is called public cloud. Similarly, the term private cloud is used to refer the internal data at the organization level. Similarly, the term hybrid cloud is a model where a private cloud and a public cloud are combined to make one model. The four commonly used cloud models are:

Public Cloud*:* It is generally supported by the publicly available cloud model. That are operated and managed by the government organizations, academia and business enterprises or even a mix of them.

Private Cloud*:* It is supported and handled within a single organization or an enterprise for its workers or users.

Hybrid Cloud*:* It is a combination of two or more different cloud infrastructure (*i.e.*, public or private) to share the cloud entities but manages its unique entity.

Community Cloud*:* It is a cloud infrastructure entirely within the community users of a particular organization for a common reason. This model can be owned, operated and managed by themselves or third party consumers.

2. LITERATURE SURVEY

There are several methods through which trust in cloud computing can be improved. Firstly, by distributing the duty of security between consumer and provider. Method of duty separation is considered authors have designed a Multi Tenancy Trusted Computing Environment Model (MTCEM). In the MTCEM methodology, consumer is always concern about security of VM. While provider is always concern about the security of Host and VMM (Virtual Machine Monitor). Researcher of IBM implemented full specifications of TCG's TPM and provided a software based TPM called vTPM (Virtual TPM). This allows VM to takes tasks of TPM running in IaaS model of cloud computing environment. This generates trust of user on the virtual environment of cloud computing but the vTPM is always under the control of provider which creates risk for consumer. The security issue between the provider and consumer is cut by using PVI. There is one more way to improve trust by allowing consumer to know about the reliability of the particular platform. To establish this purpose authors have suggested Trusted Virtual Environment Module (TVEM). The virtual environment on provider's infrastructure provides this TVEM software that makes the consumer of system verify the host platform. After conforming the results, then that result is send to the consumer. In cloud environment, consumer requires the acknowledgement report about the reliability of lent VM. For configuring system the agreement with consumer is required, for this a system presented through which reliability of infrastructure can be measured irregularly. It also provides remote confirmation cloud computing environment.

The primary motivation for adopting cloud is its features such as providing low cost, overall security of the outsourced services. It also provides various services to the users such as resource management, storage, etc. The organization must be aware of the security issues while adopting the cloud. The security of cloud infrastructure is depends on cryptography. The business data of an organization must be confined with suitable and consistent policies or measures. While the enterprise data is confined in its own data center or in the cloud architecture. The cloud computing is becoming a popular and attractive paradigm with lots of benefits; however, there are some specific questions relating to its ability to support forensic investigation. The author mainly discussed the cloud characteristics, models, and architecture.

The forensic investigation has its roots for data recovery to finding digital evidence from law enforcement perspective. In cloud computing, the forensic readiness is not thoroughly considered by most of the organizations, so there is a need to revisit or develop new procedures to meet the current cloud requirements. Moreover, the forensic investigation has pros and cons, which need to be understood during forensic readiness. Similarly, the forensic investigation finding in virtual machines (VMs) has mixed approach of advantages and disadvantages. Therefore, the forensic investigator community is required to develop new procedures and techniques to overcome the cloud computing forensic analysis challenges. The data confidentiality, authentication and access control issues in cloud computing have been addressed by proposing a framework to increase the cloud reliability and trustworthiness in. A cryptographic algorithm Diffie-Hellman for secure communication, in contrast to key distribution management. Such a system normally consists of three modules: administration, authentication and encryption modules. Each module has different, but interconnected, functions. The administration module is used by the cloud provider for user registration and administration. While the authentication module is used for authentication of users, and encryption module is used for data encryption. The authentication provided here is a two-way process that involves consumer ans providers. First step involves the user login and password, and then it creates the one-time password and sends it on the user mobile or email for authentication. Once this password is created and supported by the system, then the system authenticates the user and provides access to the system.

3. REQUIREMENT FOR CONSUMER'S INFRASTRUCTURE

This architecture provides the distribution between cloud consumer and provider. This can make user to feel comfortable in the cloud environment. Figure, illustrates that what components are needed for the cloud consumer. While developing the prototype for consumer infrastructure we used Ubuntu of Canonical as an operating system. PKCS#11 is a Public-key Cryptography Standard No. 11. It's a platform independent API to support cryptographic operation at software level. A Software based TPM Emulator is installed at the machine of consumer which is based on java implementation of Trusted Software Stack (TSS). TCG device driver library TOOL is meant for the low level communication with TPM. In emulated TPM, simulation of hardware tpm driver is done by a linux kernel module i.e. tpmd_dev and provide the device /dev/tpm and also forwards commands to daemon service i.e. tpmd. This daemon is actual implementation of TPM Emulator.

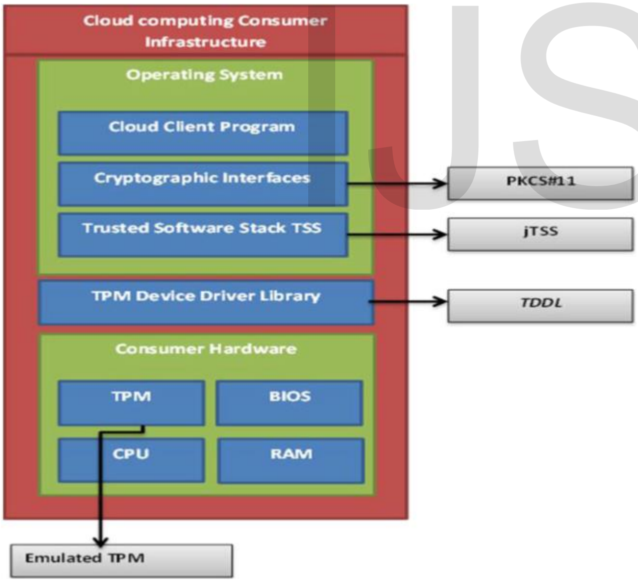

Figure: Requirement for consumer's Infrastructure

4. REQUIREMENTS FOR PROVIDER'S INFRASTRUCTURE

This section gives the brief idea about the infrastructure of provider. Here virtualized environment (VE) is presented for providing the overall base to the cloud of provider environment. This VE is not completely under control of provider of cloud services. This says that both part i.e. User VM and Management VM are physically under control of provider. But, consumer can directly access to his or her virtual machine and can performs some integrity operations by using his or her infrastructure. This seems that consumer locating at distinct places can check the integrity of VM at its initialization time by current VM integrity checking protocol. Authentication or integrity report of user VM is then passed to the consumer.

In this construction, Core Root of Trust for Measurement (CRTM) is initialized at the start up time of the VM which is supported by the each user VM presented at provider's platform. Similarly, for the platform verification process of TPM where Qoute TPMO operation is used, here TPM ExtendO operation is used to consider the reliability of VM components. In this figure, all the components of user VM that form Trusted Building Blocks (TBB) are shown. Here authors have implemented user VM with all the components that maintenance the principal boot of complete virtual machine.

These components mainly involve the CRTM, TCG BIOS, Trusted GRUB, and OS boot loader, some applications at providers system, TPM, some management software and Operating System. This architecture contains the executable code in the form of CRTM that remains continuous in the platform invoked by the CPU. In actual CRTM is one of the part of BIOS that measures all the initial mechanism of the system. This supports the trusted computing in virtualized environment of our system. After CRTM is invoked by the CPU it then executes the process of trusted boot by using the mechanism of SHA-1 of the BIOS component and it gives output in the form of hash value which is then extended by using PCR_EXTEND 0 functions into the protocol module of the user. After completing this process Trusted GRUB is initialized, measured and gives its control to execute. Trusted GRUB is the improvement of GNU GRUB which supports the implementation of SHA-l algorithm in the software. It generally consists of two steps during boot process i.e. step l and stage2. Step 1 we have already seen. Now in step 2 OS kernel is loaded which is a most important task of model.

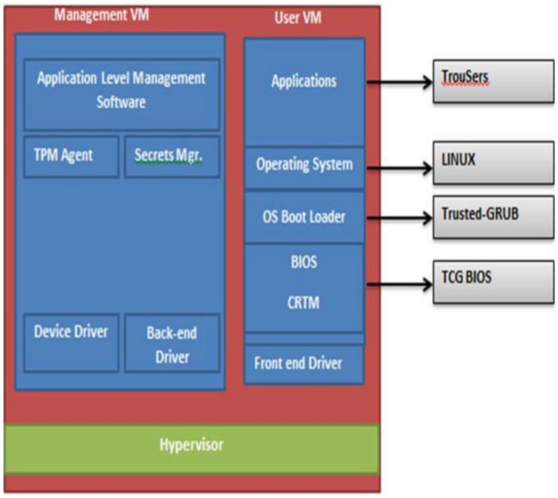

Figure: Requirement for Provider's Infrastructure

This level is also responsible for the trust made on the provider by consumer in the form of chain and Trusted GRUB is used to measure the Operating Systems and to pull out the PCR value to the user TPM at consumer’s side. All this communication made by consumer and providers system involves the hash value, loading of working units and addition into PCRs. This process is carried out by using components of host VM i.e. TPM Agent component of providers module.

5. THE TRUST PROTOCOL

Trusted Platform Module (TPM) is annoyance proof chip that performs some cryptographic operation to produce random numbers and to create session keys. The key generated by TPM is Endorsement Key (EK) consist of 2048 bit RSA key. This EK makes the platform to be distinctively recognized during the operation of TPM. This then raises some privacy issues of the users of the particular systems. To moderate this privacy issues another key is generated referred as Attestation Identity Key (AIK) which is also consist of 2048-bit and is created as an another EK. It is used to mark data created from TPM. Unlimited numbers of AIKs are generated by TPM as it has capability to produce the keys. In this part authors have presented the Trust Protocol which is distributive in nature. This protocol is distributed between consumer and provider. For connecting consumer and provider we require some connection this may be public internet network which is not secure for communication. To make this communication secure for both we are using IPsec protocol which is considered as a safe communication. In this communication we have used some keys which are created from a respective TPM.

List of keys with symbols used in the protocol:

- Attestation Public Identity Key (AIKpub)
- Endorsement Key (EKpr) private key
- Session Key (S)
- {} AIKpub Encrypted with AIKpub
- Number Once Generated (nonce N)
- Public Key of Provider Kpub
- Private key of Provider Kr

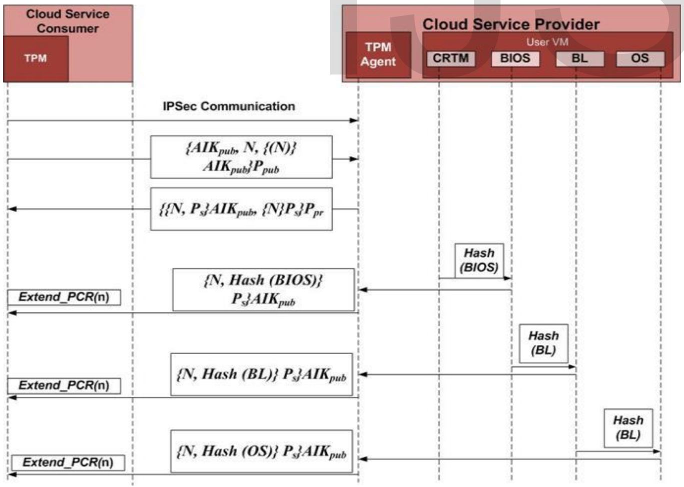

Figure: Distributed Trust Protocol

In the step 1 of protocol, consumer generates communication message by sending nonce N and Attestation Identity Key (AIKpub) produced publically and then sends this message for encryption by using the key of provider (P pub) generated publically. In the second step, further process of encryption is carried out which involves encryption of session key with the AIKpub. So that the session is devoted to the consumer, and message is encrypted with the private key of provider (P pr). So that consumer can say that the coming message is from the provider. In the third step, VM at consumer side is start when the VM at provider side is prepared. It then boots the TCG's Trusted Boot Process. In the boot process of VM process value of the VM components are calculated by using consumer's TPM then these values are provided to the consumer after completing the process of encryption of message with the AIKpub. After finishing all this process the VM is again restarted and the whole procedure is repeated and then compares the new value with previous values. If both the measurement values are same then VM starts normally, if not then consumer is notified.

6. CONCLUSIONS

In this seminar, we have concluded Distributed Trust Protocol (DTP) for IaaS Cloud Computing. In literature we started searching different techniques that have been exploited for establishing user trust in cloud computing but our protocol is unique and novel that combines consumer with provider.

REFERENCES

[1] Ubaidullah Alias Kashif, Zulfiqar Ali Memon, Abdul Rasheed Balouch, Jamil Ahmed Chandio, "Distributed Trust Protocol for IaaS Cloud Computing," Proceedings of 2015 12th International Bhurban Conference on Applied Sciences & Technology (IBCAST) Islamabad, Pakistan, 13th - 17th January, 2015

[2] F. J. Krautheim, D. S. Phatak, and A. T. Sherman, "Introducing the trusted virtual environment module: a new mechanism for rooting trust in cloud computing, " in Trust and Trustworthy Computing, ed: Springer, 2010, pp. 211-227.

[3] D. Schellekens, B. Wyseur, and B. Preneel, "Remote attestation on legacy operating systems with trusted platform modules, " Electronic Notes in Theoretical Computer Science, vol. 197, pp. 59-72, 2008.

[4] D. Wallom, M. Turilli, A. Martin, A. Raun, G. Taylor, N. Hargreaves, and A. McMoran, "myTrustedCloud: trusted cloud infrastructure for security-critical computation and data management, " presented at the Proceedings of the WICSA/ECSA 2012 Companion Volume, Helsinki, Finland, 2012.

[5] R. Sailer, X. Zhang, T. Jaeger, and L. Van Doorn" Design and Implementation of a TCG-based Integrity Measurement Architecture" in USENIX Security Symposium, 2004, pp. 223-238.