Trusted System In Cloud Environment

Arif Mohammad Abdul
Department of Computer Science
GITAM University
Hyderabad, INDIA

M Balraju
Department of Computer science
VIDYA VIKAS Institute of Technology.
Hyderabad, INDIA

Sudarson Jena
Department of Information Technology
GITAM University
Hyderabad, INDIA

Abstract-*Cloud security has gained increasingly emphasis in the research community, with much focus primary concentrated on how to secure the operation system and virtual machine on which cloud system runs on. A trust management system will match the service providers and the customers based on the requirements and offerings.* In this paper, we proposed a new method to build a secure and trusted computing system for cloud environment. *It includes some important security services, including authentication, confidentiality and integrity, are provided in cloud computing system.*

Keywords-- **Cloud Computing, IaaS, Trusted System, Trusted Computing Group, Trusted Computing platform.**

I. Introduction

With the development in networking technology and the increasing need for computing resources, many companies have been prompted to outsource their storage and computing needs. This new economic computing model is commonly regarded as cloud computing [1]. Cloud computing provides a facility that enable large scale control sharing and inter operation among resources that are dispersedly owned and managed [2]. The opportunities afforded by cloud computing are too attractive for the consumers to ignore in today's highly competitive service environments. The way to realizing these opportunities, however, is not free of obstacles. In cloud computing, with a large amount of various computing resources, users can easily solve their problems with the resources provided by a cloud.

Cloud computing has many new characteristics compared with traditional computing mode. Cloud security Alliance (CSA) describes these characteristics as: abstraction of infrastructure, resource democratization, services oriented architecture, elasticity/dynamism of resources and utility model of consumption & allocation [3]; NIST summarizes these characteristics as: on-demand self-service, ubiquitous network access, resource pooling, rapid elasticity and pay per use [4]. Since these cloud facilities are shared resources and generally located in the data center of Cloud Security Provider (CSP), they are under the full control of CSP. Security devices in cloud are also owned and controlled by CSP. On the other hand, customers have no control over the facilities on which their businesses run [5].

They should be security duty separation in cloud computing between CSP and customers. The mechanism of security duty separation must be based on what services the security provides the customers.

Cloud services are currently marketed on their different categories namely Infrastructure as a Service (IAAS), Platform as a Service (PAAS), and Software as a Service (SAAS) [6].The interrelationship and logical boundaries between these three cloud services delivery models where depicted in the cloud reference model in fig. 1.

Tim Mather et al. further detailed the security responsibility between CSP and the customers [7]. CSP must be responsible for the security of computing platforms and applications they provide. Trust the measure concern of the consumers and provider of services that participate in cloud computing environment. In this paper, we proposed a new method to build a secure and trusted computing system for cloud environment.

Cloud computing developed from the grid computing technology and paid attention to provide distributed service to different users. A typical cloud model described by Frank Gillett[8] is shown in Fig. 1 that model does not seen to address end-to-end management. Ultimately, the cloud service infrastructure must provide end-to-end service assurance to meet both service creation and service delivery platform user requirement.

A current means for establishing trust in computing platforms is the Trusted Platform Module (TPM), a core component of the root of trust for the platform. A root of trust is a component of a computing platform that is implicitly trusted to provide a specified set of controlled functions to measure and pass control to other platform component.

Krautheim's Locator Bot(LoBot)[9,10]uses the VTPM to root trust for a virtual environment in a PVI; however, the VTPM implementation has several issues that make it problematic to use as a root of trust for cloud virtual environments. Traditional trusted computing platform like Terra[11]

Take a compelling approach to this problem. For example, Terra is able to prevent the owner of a

physical host from inspecting and interfering with a computation. Terra also provides a remote attestation capability that enables a remote party to determine upfront whether the host can securely run the computation. This mechanism reliably detects whether or not the host is running a platform implementation that the remote party trusts. These platforms can effectively secure a VM running in a single host. However, many providers run data centers comprising several hundreds of machines, and a customer's VM can be dynamically scheduled to run on any one of them. This complexity and the opaqueness of the provider backend create vulnerabilities that traditional trusted platforms cannot address.

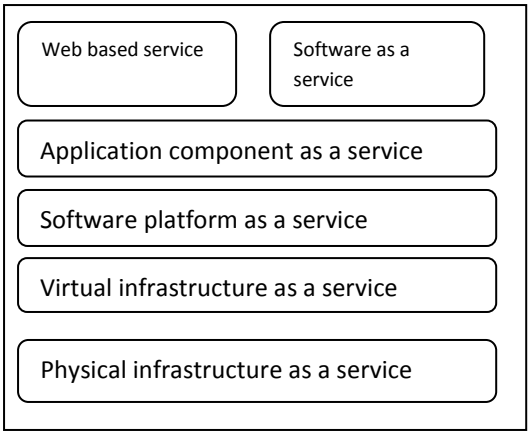

Figure 1 Cloud Computing Model

The rest of the paper is organized as follows. Section 2 presents related work on trusted cloud. Section 3 presents trusted cloud computing. The section 4 of this paper presents trusted computing platform. The architecture of trust network computing is discussed in section 5, The section 6 of this paper presents trusted storage. Section 7 concludes the paper.

II. Related Work on Trusted Cloud

The issue of establishing trust in the Cloud has been discussed by many authors. Much of the discussion has been centred on reasons to "trust the Cloud" or not to. Paper [11] discusses factors that affect consumer's trust in the Cloud and some of the emerging technologies that could be used to establish trust in the Cloud including enabling more jurisdiction over the consumers' data through provision of remote access control, transparency in the security capabilities of the providers, independent certification of Cloud services for security properties and capabilities and the use of private enclaves. The issue with jurisdiction is echoed [9], who further suggest some technical mechanisms including encrypted communication channels and computation on encrypted data as ways of addressing some of the trust challenges. The use of hardware based attestation mechanisms to improve transparency into the enforcement of critical security properties. Cachin [12] contains a survey of security issues in the context of cloud storage services and recent research addressing these issues; Armbrust [13] is a more general survey of cloud computing. Both of these papers point out some of the same challenges that motivate our work. Trusted cloud computing platform (TCCP) which enables laaS providers to serve a closed box execution environment that guarantees confidential execution of guest VMs. This system allows a customer to verify if its computation will run securely, before requesting the service to launch a VM. TCCP assumes that there is a trusted coordinator hosted in a trustworthy external entity, however, it is impossible to make the backend of the cloud visible to the third part. Moreover, TCCP lacks the mechanism to protect cloud user's data, once the cloud backend nodes are compromised. Our mechanism is different. TSSC allows the cloud users to indirectly measure the cloud backend, which relies on a remote attestation delegation service (RDS) provided by the cloud provider. So, TSSC can seamlessly cooperate with the current cloud architecture. Further, TSSC provide sealed storage to reduce the leakage risk of cloud user's sensitive data. Krautheim[15] provides a Private Virtual Infrastructure (PVI) that shares the responsibility of security in cloud computing between the service provider and client, decreasing the risk exposure of both. The challenge of PVI is similar to TCCP, which need exposure of every implementation detail to the cloud user and lacks sealed storage ability.

III. Trusted Cloud Computing

3.1. Trusted Computing

Trust in cloud computing is more complex than in a traditional IT scenario where the information owner owns his own computers. Before the user uses the cloud, the user of the cloud may want to verify the trusted status of the platform which actually carries out the computing task in the cloud. Trust is the major concern of the consumer and provider of services that participate in a cloud computing environment [16].The remote attestation mechanism in Trusted Computing is suited for the cloud user's verification need. Since cloud computing share heterogeneous distributed resources via the network through in the open Internet Technology environment, thus it makes security problems necessary for us, trusted computing environment including some important security services, authentication, confidentiality and integrity for cloud computing system. Trust is the basis of secure interaction between human society and cyberspace [17].Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released

with minimal management effort or service provider interaction.'[18].

Trusted computing implies a redesign of systems architecture in such a way as to support its factorization into relatively discrete components with well-defined characteristics. This permits, in particular, rational decisions based upon reasonable expectations of behavior. Any such systems thinking must be motivated by an analysis of risks so that effort is expended where it may give the best return and an awareness of the limitations of such risk assessment. The most prominent approach to Trusted Computing technology has been specified by the Trusted Computing Group (TCG) and Trusted Platform Module (TPM).

3.2. Trusted Computing Group

The Trusted computing Group (TCG) [19] proposed a set hardware and software technologies to enable the construction of trusted platforms. Trusted Computing Group (TCG) is a not-for-profit organization formed to develop, define and promote open, vendor-neutral, industry standards for trusted computing building blocks and software interfaces across multiple platforms [20]. The main idea of TCG is to assure computing platform trusted based on a hardware protected cryptograph module named Trusted Platform Module (TPM) and related software stacks [21].

The approach described here is largely the result of the work of an industry consortium (the Trusted Computing Group, TCG), it informed by a history of research, largely in the area of high-assurance systems, from government and academe. TCG's approach is distinctive in that previous trusted systems were usually bespoke and highly expensive the current work aims to touch every computing device.TCG believes that the general objective of trusted computing is to enhance the security of computer system. The main objective in current stage is to ensure data integrity, secure storage, and remote attestation for trusting platform. The TCG proposes to extend common computing platforms with trusted components in software and hardware.

IV. Trusted Computing Platform

In particular the hardware extension, called Trusted Platform Module (TPM) acts as a hardware trust anchor and enables the integrity measurement of the platform's software stack at boot-/load-time and the secure reporting of these measurements to a remote party. A platform is regarded as trusted if it always behaves as expected. This expectation can be assured by a transitive trust mechanism: a computing platform can only boot from Core Root of Trust Measurement (CRTM), and CRTM is supposed to be trusted. After that, CRTM conveys system control to next executables only when it believes the code is trusted, and the trust boundary is extended. This process is iterated to form a trust chain as CRTM->BIOS->OS Loader->OS-> Applications, over which a platform is assured to be trusted. Another important mechanism of trusted computing platform technology is platform attestation. Attestation is a mechanism by which a computing platform proves to a third party that it is trusted. The challenge to attestation is to define a set of reasonable and measurable metrics that can be used to determine whether a computing platform is trusted. To provide stronger computer security than software alone We will require 2 platforms

1. Strongly identify themselves using public key cryptography, involving a secret key strongly tied to the platform itself, and
2. Strongly identify their current configuration and running software using cryptographic hashes of object code, and other mechanisms.

TPM can be implemented wholly in software, but some of its behaviors such as the strong protection of a platform-specific unique secret key require protections which can be achieved only through a hardware device. The TPM, with its embedding in the PC platform, is then intended to provide three roots of trust:

i) Root of trust for measurement (RTM) a trusted implementation of a hash algorithm, responsible for the first measurement on the platform whether at boot time, or in order to put the platform into a special, trusted state;

ii) Root of trust for storage (RTS) a trusted implementation of a shielded location for one or more secret keys probably just one, the storage root key (SRK);

iii) Root of trust for reporting (RTR) a trusted implementation of shielded location to hold a secret key representing a unique platform identity, the endorsement key, (EK) [22].

These are described as roots of trust because they are each inherently indivisible: all subsequent trust decisions are based upon these [24]; they are the basis of an inductive chain. Trust chain mechanism based on a root of trust is one of the most primary key technologies. One trusted computer system is composed of root of trust, trusted hardware platform, trusted operating system and trusted applications.

V. Architecture of Trust Network Computing

The TNC architecture is part of the larger Trusted Computing Architecture promoted by the Trusted Security Group with the purpose of creating more secure computing environments [21].The stated goal of the trusted platform approach is to prevent all software-based attacks — that is, there should be no way that the trusted platform can be com- promised simply through participating in network protocols.

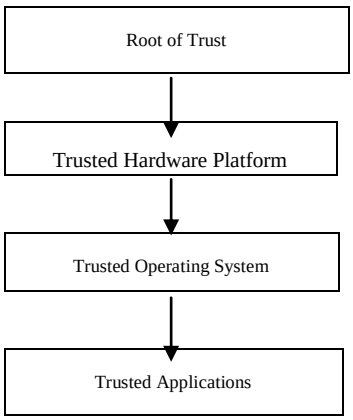

Figure 2 Trusted Systems

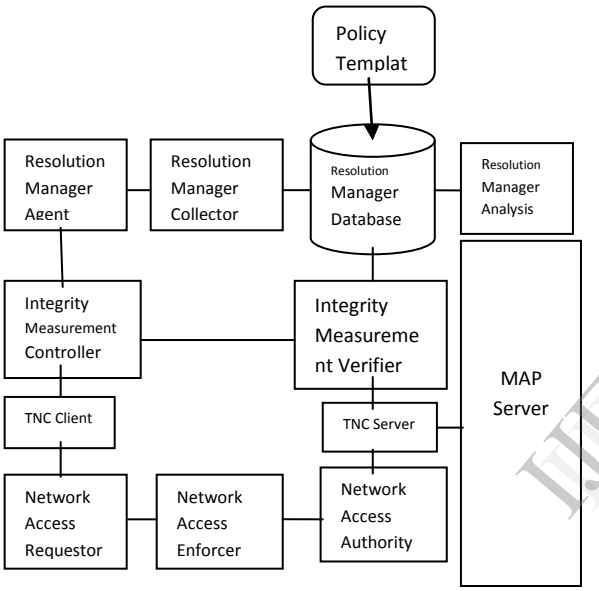

Figure 3 TNC Architecture

For us, trusted systems are those upon whose correct (or predictable) operation we rely. If they fail to live up to our expectations, we may expect bad consequences. In a strong sense, this idea of trust is somewhat orthogonal to that of security: we may use trusted components to build secure systems. Trust on its own does not entail security: merely, predictable behavior. We would not generally try to build secure systems from untrustworthy components, but the author can think of a handful of examples where this may work [19, 25].

Establishing trust in the Cloud is a fundamental requirement especially for Cloud's potential future as an Internet scale critical infrastructure [26]. Cloud users coming from different backgrounds and have different requirements. For example, users could be non-technical end-users, or organizations that could have a well established enterprise infrastructure and might be interested in outsourcing part of its complex infrastructure. Establishing trust in the Cloud should consider the requirement of all these users, by providing them with different models. Each model should provide different levels of transparency in context of technical complexities and trust establishment. In addition, trust models are not only beneficial to Cloud's users, but also to Cloud providers, collaborating Cloud-of-Cloud, and external auditors. For example, trust assessment helps in exposing components that must be trusted or are assumed to be trusted in a Cloud; can be used in computation of a trust value for a given Cloud and thus enable comparison between alternative Cloud providers; a Cloud provider can assess its own resources' trustworthiness, which enables the Cloud to realize its trust level; and when Cloud providers collaborate then they can define certain levels of trust for resources involved in the collaboration.

VI. Trusted Storage

Cloud storage enables users to remotely store their data and enjoy the on-demand high quality cloud applications without the burden of local hardware and software management. Though the benefits are clear, such a service is also relinquishing users' physical possession of their outsourced data, which inevitably poses new security risks toward the correctness of the data in cloud. In order to address this new problem and further achieve a secure and dependable cloud storage service, we propose in this paper a flexible distributed storage integrity auditing mechanism, utilizing the homomorphic token and distributed erasure-coded data. The proposed design allows users to audit the cloud storage with very lightweight communication and computation cost. The auditing result not only ensures strong cloud storage correctness guarantee, but also simultaneously achieves fast data error localization, i.e., the identification of misbehaving server. Considering the cloud data are dynamic in nature, the proposed design further supports secure and efficient dynamic operations on outsourced data, including block modification, deletion, and append. Analysis shows the proposed scheme is highly efficient and resilient against Byzantine failure, malicious data modification attack, and even server colluding attacks.

There are many products on the market which will encrypt one's storage devices (whether discs, tapes, memory sticks, etc.), and increasingly many application do- mains are seeing a need for this.

Trusted Platform can bring to this approach is that the key for encrypting the drive can be stored using the TPM, and sealed so that it is released only when the legitimate platform configuration is seen. This is intended to mean that a stolen disc (or a disc extracted from a laptop) cannot be decrypted, because the correct context to do so will not exist at the attacker's system. The stolen laptop will still boot, but the attacker needs login

credentials in order to access the disc's contents. This is the approach taken by Microsoft's Bitlocker.

VII. Conclusion

Cloud providers need to safeguard the privacy and security of personal data that they hold on behalf of organizations and users. We have analyzed the trusted computing in the cloud computing environment and the function of trusted computing platform in cloud computing. Our proposed approach are to extend the trusted computing technology into the cloud computing environment to achieve the trusted computing requirements for the cloud computing and then fulfill the trusted cloud computing.

VIII. References

[1] Xin Yang, Qingni Shen, Sihan Qing "A Way of Key Management in Cloud Storage Based on Trusted Computing" International Federation for Information Processing 2011.

[2] S.Berger, R.Caceres, K.A.Goldman, R.Pervez, R.Sailer and L.van Doom. VTPM: Virtualizing the Trusted Platform Module.In Proc. Of USENIX-SS'06, Berkeley, CA, USA,2006.

[3] Cloud Security Alliance. Security Guidance for Critical Areas of Focus in Cloud Computing.

[4] Peter Mell, Tim Grance. Effectively and Securely Using the Cloud Computing Paradigm. NIST, Information Technology Laboratory,3-19-2009 .http://csrc.nist.gov/groups/SNS/cloud-computing-v26.ppt

[5] Xiao-Yongli, Li-Tao Zhou, Yong Shi, "A Trusted Computing Environment Model in Cloud Architecture" IEEE 11 July 2010.

[6] C.Vecchiola, S.Pandey, R.Buyya, "High Performance Cloud Computing:A view of Scientific Applications" in 10th International Symposium on Pervasive Systems, Algorithms and Networks, Kaohsiung, Taiwan, pp.4-16, 2009.

[7] Tim Marher, Subra Kumaraswamy and Shahid Latif "Cloud Security and Privacy" published by O'Reilly Media, Inc., 1005 Gravenstein Highway North, Sebastopol, CA 95472.

[8] Frank E.Gillet, "Future View: The new Technology Ecosystem of Cloud. Cloud services and cloud Computing" Forrester report Aug 2008.

[9] Krauthiem, F.J., Phatak, D.S., Sherman, "A.T.: Private Virtual Infrastructure: A Model for Trustworthy Utility Cloud Computing". TR-CS-10-04. University of Maryland Baltimore County, Baltimore, MD (2010)

[10] Krauthiem, F.J: "Private Virtual Infrastructure in Cloud Computing". In: Workshop on hot topics in Cloud Computing, San Diego, CA (2009)

[11] T. Garfinkel, B. Pfaff, J. Chow, M. Rosenblum and D. Bonch. Terra: " A Virtual Machine-Based Platform for Trusted Computing. In Proc. Of SOSP'03, 2003

[12] C Cachin, L Keidar, and A. Shraer, "Trusting the Cloud," ACM SIGACT News, 40(2):81-86, June 2009.

[13] M. Armbrust, A Fox, R. Griffith, A D. Joseph, R. H. Katz, AKonwinski, G. Lee, D. A Patterson, A. Rabkin, 1. Stoica, and M.Zaharia, "Above the Clouds: A Berkeley View of Cloud Computing,"Technical Report EECS-2009-28, University of Cal ifornia at Berkeley, February 2009.

[14] N. Santos, K. P. Gummadi, and R. Rodrigues, 'Towards Trusted Cloud Computing," Proc. HotCloud, June 2009.

[15] F. J Krautheim, "Private Virtual Infrastructure for Cloud Computing," Proc. HotCloud, June 2009.

[16] Zhidong Shen, Qiang Tong. The Security of Cloud Computing System enabled by Trusted Computing Technology. Proc.International Conference on Signal Processing System.

[17] MELL,P., and GRANCEE,T. The NIST Definitionof Cloud Computing 2009.

[18].S.ChangXiang,Z.HuanGuo,W.HuaiMin"Research on Trusted Computing and its Development".

[19] Anderson, R.Cryptography and competition policy: Issues with trusted computing. In Proceedings of the Workshop on Economics and Information Security, 2003.

[20] S. Berger, R. Cáceres, D. Pendarakis, et al., "TVDc: Managing security in the Trusted Virtual Datacenter," ACM SIGOPS Operating Systems Review, vol. 42, no. 1, pp. 40-47, January, 2008.

[21]TRUSTED COMPUTING GROUP TCStorageArchitectureCoreSpecification .http://www.trusted co

[22] Brickell, E., Camenish, J. and Chen, L. The DAA scheme in context, in Mitchell, 2005.

[23] TCG. https://www.trustedcomputinggroup.org

[24] Vaughan-Nichols, S. J. How trustworthy is trusted computing?, Computer 36(3): 18–20,2002.

[25] Arbaugh, B.Improving the TCPA specification, IEEE Com- puter 35(8): 77–79,2002.

[26] Alves, T. and Felton, D. TrustZone: integrated hardware and software security, White paper, ARM, 2004.