Volume 2, Issue 2, February 2012 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Integrating the Trusted Computing Platform into the Security of Cloud Computing System

Mr. Kailash Patidar[1] ,Mr. Ravindra Gupta[2] ,Prof. Gajendra Singh[3] ,Ms.Megha Jain[4] ,Ms.Priyanka Shrivastava[5]
1 *M.Tech Scholar Dept. of Computer Science, SSSIST SEHORE,*
3 *Head of Dept. Computer Science, SSSIST SEHORE,*
4 *M .Tech Scholar Dept. of Computer Science, MIT BHOPAL,*
5 *M .Tech Scholar Dept. of Computer Science, LNCT BHOPAL,*

Abstract: - **Cloud computing has become one of the fastest growing fields in computer science. As the new computing service pattern of cloud computing develops rapidly, the security problem of cloud computing has become a hot research topic. Before the user passes important data or computing task to 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. And the remote attestation mechanism in Trusted Computing is suited for the cloud user's verification need. Cloud computing basically provides people the way to share heterogeneous distributed resources and various services that belong to various organizations or sites. 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 to develop the cloud computing application environment. In this paper, we pay attention to the security requirements in cloud computing environment system. We proposed a method to build a trusted computing environment for cloud computing system by integrating the trusted computing platform into the security of cloud computing system. 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.**

Keyword: **- Distributed system, Cloud Computing, trusted service, trusted computing platform, trusted platform module.**

I. Introduction

Cloud Computing is a new computing model that distributes the computing missions on a resource pool that includes a large amount of computing resources. It is the result of development of infrastructure as a service (IAAS), platform as a service (PAAS), and software as a service (SAAS). With broadband Internet access, Internet users are able to acquire computing resource, storage space and other kinds of software services according to their needs. In cloud computing, with a large amount of various computing resources, users can easily solve their problems with the resources provided by a cloud. This brings great flexibility for the users. Using cloud computing service, users can store their critical data in servers and can access their data anywhere they can with the Internet and do not need to worry about system breakdown or disk faults, etc. Also, different users in one system can share their information and work, as well as play games together. Many important companies such as Amazon, Google, IBM, Microsoft, and Yahoo are the forerunners that provide cloud computing services. Recently more and more companies such as Sales force, Face book, YouTube, MySpace etc. also begin to provide all kinds of cloud computing services for Internet users. Cloud computing gets its name from the drawings typically used to describe the Internet. Cloud computing is a new consumption and delivery model for IT services. The concept of cloud computing represents a shift in thought, in that end users need not know the details of a specific technology. The service is fully managed by the provider. Users can consume services at a rate that is set by their particular needs. This on demand service can be provided at Cloud service providers are making a substantial effort to secure their systems, in order to minimize the threat of insider attacks, and reinforce the confidence of customers. For example, they protect and restrict access to the hardware facilities, adopt stringent accountability and auditing

procedures, and minimize the number of staff who has access to critical components of the infrastructure [5]. any time

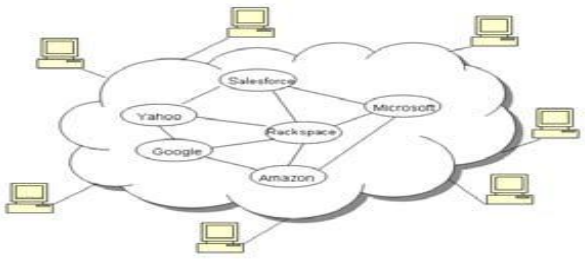

Figure1: cloud computing services

Nevertheless, insiders that administer the software systems at the provider backend ultimately still possess the technical means to access customers' VMs. Thus, there is a clear need for a technical solution that guarantees the confidentiality and integrity of computation, in a way that is verifiable by the customers of the service. 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.

II. Cloud Computing and Security

Cloud computing provides Internet-based services, computing, and storage for users in all markets including financial, healthcare, and government. This new approach to computing allows users to avoid upfront hardware and software investments, gain flexibility, collaborate with others, and take advantage of the sophisticated services that cloud providers offer. However, security is a huge concern for cloud users[2]. Cloud providers have recognized the cloud security concern and are working hard to address it. In fact, cloud security is becoming a key differentiator and competitive edge between cloud providers. By applying the strongest security techniques and practices, cloud security may soon be raised far above the level that IT departments achieve using their own hardware and software. To recognize the latest approaches to cloud security, you must first understand the fundamental Trusted Computing technologies on which these approaches are based. Then you'll learn how to apply them in the cloud.

III. Trusted Computing

One approach to achieve trustworthy computations in cloud infrastructures is to adapt existing trusted Computing solutions to the cloud computing paradigm or to use these solutions as building blocks in new cloud architecture models[1]. The most prominent approach to Trusted Computing technology has been specified by the Trusted Computing Group (TCG). The TCG proposes to extend common computing platforms with trusted components in software and hardware. 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. Thus, it provides the means to achieve verifiability and transparency of a trusted platform's software state. Trusted Computing, based on the TPM and its remote attestation feature, enables the establishment of trusted execution environments in commodity cloud infrastructures. However, the reliable and efficient attestation of the execution environment at run-time is a research problem to which no complete solution exists yet.

Trusted Platform Module: - Cloud providers have recognized the cloud security concern and are working hard to address it. In fact, cloud security is becoming a key differentiator and competitive edge between cloud providers. By applying the strongest security techniques and practices, cloud security may soon be raised far above the level that IT departments achieve using their own hardware and software. To provide stronger computer security than software alone can provide, TCG has defined the specification for the widely implemented Trusted Platform Module (TPM)[7]. The TPM is an international standard, hardware security component built into many computers and computer-based products. The TPM includes capabilities such as machine authentication, hardware encryption, signing, secure key storage, and attestation. Encryption and signing are well-known techniques, but the TPM makes them stronger by storing keys in protected hardware storage. Machine authentication is a core principle that allows clouds to authenticate to a known machine to provide this machine and user a higher level of service as the machine is known and authenticated. Attestation requires a bit more explanation. When this feature is used, the TPM monitors software as it is loaded and provides secure reports on exactly what is running on the machine. This monitoring and reporting are especially important in the virtualized environment of cloud computing where viruses and worms can hide in many places. However, these other TCG specifications can work without a TPM at a lower security level by using software only approach.

Trusted Network Connect: - TCG's Trusted Network Connect (TNC) architecture provides an industry standard approach to network security and network access control

© 2012, IJARCSSE All Rights Reserved

(NAC) that works with leading providers such as Microsoft and Cisco. The Trusted Network Connect (TNC) Work Group has defined and released an open architecture and a growing set of standards for endpoint integrity[7]. The TNC architecture enables network operators to enforce policies regarding endpoint integrity at or after network connection. The standards ensure multi-vendor interoperability across a wide variety of endpoints, network technologies, and policies.

IV. Trusted Network Connect (TNC) architecture

The Trusted Network Connect (TNC) architecture is a standards-based framework for Network Access Control (NAC) that bases network access decisions on security state information gathered from a wide variety of sensors across a multi-vendor environment. 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 [14]. The basic objective of TNC from the perspective of endpoint integrity is to deny network access to endpoints that do not meet certain minimum security criteria or quarantined during remediation to prevent further infection. Has strong user authentication allows guest access blocks the access of unsafe endpoints extends access control to clientless endpoints such as IP phones and printers coordinates security devices across the enterprise.

Trusted Storage: - TCG's Trusted Storage specification provides a manageable, enterprise-wide means for implementing full-disk encryption using hardware included right in the drive. These drives, known as self encrypting drives, simplify the enterprise encryption process for handling sensitive data, since all data, applications, and drivers are encrypted internal to the drive and key management is an integral part of the design.

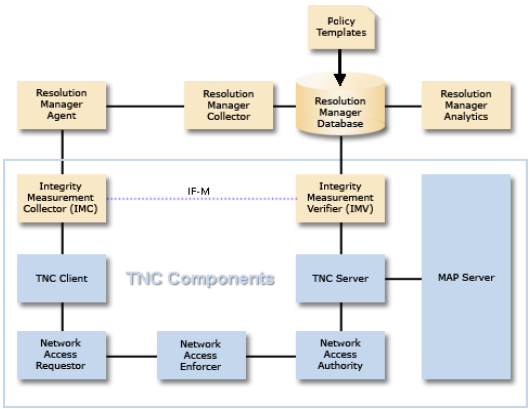

Figure 2: TNC Architecture

The hardware-based encryption can take advantage of the TPM if desired and does not require user intervention or impact system performance, unlike traditional software-only encryption schemes that require cycle time from the main processor. With a self-encrypting drive, when a drive is removed for any reason (maintenance, end of life or even theft), the data is completely useless to criminals since they don't know the encryption key.

V. Critical Areas for Cloud Computing

The Cloud Security Alliance (CSA) [2] has developed a 76-page security guide that identifies many areas for concern in cloud computing [3]. This environment is a new model which cannot be well protected by traditional "perimeter" security approaches. From this exhaustive document, we have selected six specific areas of the cloud computing environment where equipment and software implementing TCG specifications can provide substantial security improvements [14]. Areas for security concerns in cloud computing:-

(1) Data at rest
(2) Data in transit
(3) Authentication
(4) Separation between customers
(5) Cloud legal and regulatory issues and
(6) Incident response

Securing data at rest:-Cryptographic encryption is certainly the best practice and in many U.S. states and countries worldwide, it's the law for securing data at rest at the cloud provider. Fortunately, hard drive manufacturers are now shipping self encrypting drives that implement the TCG's Trusted Storage standards. Self-encrypting drives build encryption hardware into the drive, providing automated encryption with minimal cost or performance impact. Software encryption can also be used, but it is slower and less secure since the encryption key can be copied off the machine without detection.

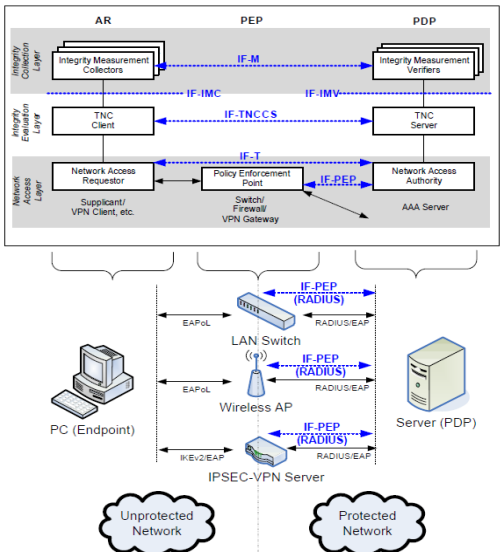

Figure 3 - Network-Based PEP in TNC Architecture

© 2012, IJARCSSE All Rights Reserved

Radius: **-** Since the TNC architecture is part of the authentication, authorization, and accounting (AAA) architecture, it is only natural that some of the same protocols from contemporary AAA implementations be pressed into service within the TNC framework. A key AAA protocol is RADIUS.

Securing data in transit:-Encryption techniques should also be used for data in transit. In addition, authentication and integrity protection ensure that data only goes where the customer wants it to go and is not modified in transit. Well-established protocols such as SSL/TLS should be used here. The tricky part is strong authentication, as described next.

Authentication:-User authentication is often the primary basis for access control, keeping the bad guys out while allowing authorized users in with a minimum of fuss. In the cloud environment, authentication and access control are more

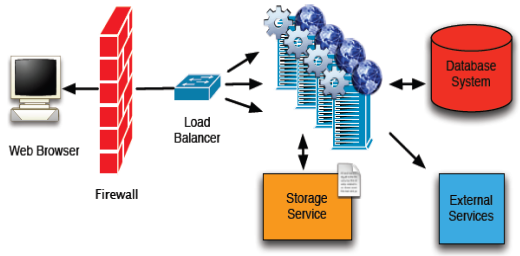

Figure 4: Cloud Web Architecture

Important than ever since the cloud and all of its data are accessible to anyone over the Internet. The TPM can easily provide stronger authentication than username and passwords [15]. TCG's IF-MAP standard allows for real-time communication between the cloud provider and the customer about authorized users and other security issues. When a user is fired or reassigned, the customer's identity management system can notify the cloud provider in real-time so that the user's cloud access can be modified or revoked within seconds. If the fired user is logged into the cloud, they can be immediately disconnected. Trusted Computing enables Authentication of client PCs and other devices, which also is critical to ensuring security in cloud computing.

Separation between customers:-One of the more obvious cloud concerns is separation between a cloud provider's users (who may be competing companies or even hackers) to avoid inadvertent or intentional access to sensitive information. Typically a cloud provider would use virtual machines (VMs) and a hypervisor to separate customers. TCG technologies can provide significant security improvements for VM and virtual network separation [9]. In addition, the TPM can provide hardware-based verification of hypervisor and VM integrity. The TNC architecture and standards can provide strong network separation and security.

Cloud legal and regulatory issues:-To verify that a cloud provider has strong policies and practices that address legal and regulatory issues, each customer must have its legal and regulatory experts inspect cloud provider policies and practices to ensure their adequacy. The issues to be considered include data security and export, compliance, auditing, data retention and destruction, and legal discovery [7]. In the areas of data retention and deletion, Trusted Storage and TPM access techniques can play a key role in limiting access to data.

Incident response: **-** As part of expecting the unexpected, customers need to plan for the possibility of cloud provider security breaches or user misbehavior. An automated response or at least automated notification is the best solution. TCG's IF-MAP (Metadata Access Protocol) specification enables the integration of different security systems and provides real-time notification of incidents and of user misbehavior.

VI. Future Work

In this paper, we argue that concerns about the confidentiality and integrity of their data and computation are a major deterrent for enterprises looking to embrace cloud computing. The TPM can be an independent entity that works on behalf of cloud computing customers. Inside every server in the cloud, the TPM and associated software can check what is installed on each machine and verify the machine's health. When it detects a problem, TNC technology can immediately restrict access to a device or server. For securing data at rest in the cloud or in clients that access cloud data, self-encrypting drives based on Trusted Storage provide the ultimately secure solution. Organizations that have already implemented TCG-based solutions can leverage their corporate investment in hardware, software and policies and re-use them for cloud computing. If cloud computing represents an organization's initial implementation of TCG-based technology used by the cloud provider, the rest of the organization should be re-evaluated for areas where TCG technology can provide improved internal security, including: activating TPMs, use of self-encrypting drives and network access control through TNC.Security of cloud computing model used authentication, confidentiality and integrity, this three techniques provided in cloud computing system security. We plan to implement a fully functional prototype based on our design and evaluate its performance in the near future.

VII. Conclusion

This work represents a new paradigm of information protection and security in cloud computing. We examined and defined a new trust model for cloud computing and addressed the core security challenge of utility cloud computing with multi-tenancy. We have shown that using trusted computing technologies in the cloud computing environment can benefit both operators and clients. Utility cloud computing can

© 2012, IJARCSSE All Rights Reserved

provide many benefits to companies wishing to reduce their IT expenses and overhead. Security of information in the cloud and the trustworthiness of the cloud environment is a major concern with IaaS clouds. We describe three example IaaS cloud computing applications: a cloud web server, a cloud datacenter, and a corporate virtual desktop. These applications benefit from the added security of using the TVEM and VTN to manage trust.

References

[1]. S. Berger, R. C´aceres, K. A. Goldman, R. Perez, R. Sailer, and L. van Doorn. vTPM: virtualizing the trusted platform module. In *Proc. of USENIX-SS'06*, Berkeley, CA, USA, 2006.

[2]. J. Heiser, and M. Nicolett, Accessing the Security Risks of Cloud Computing,G00157782, Gartner, Inc., Stamford, CT, 2008.

[3]. Survey: Cloud Computing 'No Hype', But Fear of Security and Control Slowing Adoption.http://www.circleid.com/posts/20090226 cloud computing hype security/.

[4]. T. Garfinkel, B. Pfaff, J. Chow, M. Rosenblum, and D. Boneh. Terra: A Virtual Machine-Based Platform for Trusted Computing. In *Proc. of SOSP'03*, 2003.

[5]. J. Leach. "The Rise of ServiceOriented IT and the Birth of Infrastructure as a Service," March 20, 2008; http://advice.cio.com/jim_leach/the_rise_of_service_ oriented_it_and_the_birth_of_infrastructure_as_a_se rvice.

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

[7]. 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.

[8]. Chiba, M., et. al., "Dynamic Authorization Extensions to Remote Authentication Dial In User Service (RADIUS)", RFC 3576, July 2003.

[9]. HALDAR, V., CHANDRA, D., AND FRANZ, M. Semantic remote attestation: a virtual machine directed approach to trusted computing. In VM'04: Proceedings of the 3rd conference on Virtual Machine Research And Technology Symposium (Berkeley, CA, USA, 2004), USENIX Association, pp. 3–3.

[10]. LIPNER, S. The Trustworthy Computing Security Development Lifecycle. In ACSAC '04: Proceedings of the 20th Annual Computer Security Applications Conference (Washington, DC, USA, 2004), IEEE Computer Society, pp. 2–13.

[11]. Amazon.AmazonWebServices:OverviewofSecurityP rocesses.http://awsmedia.s3.amazonaws.com/pdf/A WS Security Whitepaper.pdf,
   a. Nov. 2009.

[12]. TRUSTED COMPUTING GROUP. TCG Schema.http://www.trustedcomputinggroup.org/reso urces/infrastructure work group reference manifestrm schema specification version 10, November 2006.

[13]. TRUSTED COMPUTING GROUP. Summary of Features under Consideration for the Next Generation of TPM.http://www.trustedcomputinggroup.org/resourc es/summary of features under consideration for the next generation of tpm, 2009.

[14]. TRUSTED COMPUTING GROUP. TCG Storage ArchitectureCoreSpecification.http://www.trustedco mputinggroup.org/resources/tcg storage architecture core specification, April 2009.

[15]. TRUSTED COMPUTING GROUP. Trusted Computing GroupHomePage.https://www.trustedcomputinggrou p.org/home, 2009

© 2012, IJARCSSE All Rights Reserved