ISSN:0975-9646

Security and Privacy Issues in Trusted Cloud Computing Secure Architecture

Shalini Agarwal [#1], Arun Singh Chouhan [*2]

[#1]M.Tech Scholar, Department of Computer Science& Engineering
Chandravati Education Charitable Trust Group Of Institute, Bharatpur India

[2#]Associate Professor ,Department of Computer Science& Engineering
Vyas Institute of Engineering & Technology, Jodhpur, Rajasthan, India

Abstract— **Cloud computing is the latest and most widely used utility computing that provides a flexible, cost-effective, scalability and consumer, business-oriented service over the Internet. No doubt in this era of cloud computing there is a risk often outsourced to a third party, which is now very difficult to maintain data security and privacy, data-driven and service availability. The Trusted Cloud computing is very necessary among the consumers and key stakeholders of cloud computing. The Secure architecture gives the basic key management, key distribution and Digital certificates. The Virtualization, Web2.0 and Service Oriented Architecture (SOA) also their security issues which we will discuss in the research paper.**

Keywords— **Cloud Computing, Security, Threats, Key Distribution**

I. Introduction

Cloud computing is the latest technology that creates the utility computing made easy and its service, deployment models are very finely work for rapid elasticity and broad network access. The cloud computing meaning and roles can be different and vary from people or stakeholders. No doubt security and privacy policies they want a complete emphasis on their application areas means consumer that using public cloud application, a medium-scale organisation using a customized suite of business applications on a cloud platform, and a government agency with a private cloud for internal database sharing. The shift of each category of user to cloud systems brings a different package of benefits and risks. In this scenario some real value that the user seeks to secure or protect the data. For an individual point of view, the value at risk can range from loss of public emancipation of the contents of bank accounts. For a business point of view the value runs from core trade secrets to continuity of business operations and public reputation. Much of this is hard to estimate and translate into standard metrics of value.

II. Trusted cloud Computing Characteristics

Trusted cloud computing can be viewed as a computer security architecture that is designed to protect cloud systems from malicious intrusions and attacks, and ensure that computing resources will act in a specific, predictable manner as intended. A trusted cloud computing system will protect data in use by hypervisors and applications, protect against unauthorized access to information, provide for strong authentication, apply encryption to protect sensitive data that resides on stolen or lost devices, and support compliance through hardware and software mechanisms.

In a cloud computational system, multiple processes might be running concurrently. Each process has the capability to access certain memory locations and to execute a subset of the computer's instruction set. The execution and memory space assigned to each process is called a protection domain. This domain can be extended to virtual memory, which increases the apparent size of real memory by using disk storage. The purpose of establishing a protection domain is to protect programs from all unauthorized modification or executioners interference.

A trusted computing base (TCB) is the total combination of protection mechanisms within a computer system, which includes the hardware, software, and firmware that are trusted to enforce a security policy. Because the TCB components are responsible for enforcing the security policy of a computing system, these components must be protected from malicious and un-trusted processes. The TCB must also provide for memory protection and ensure that the processes from one domain do not access memory locations of another domain. The security perimeter is the boundary that separates the TCB from the remainder of the system. A trusted path must also exist so that users can access the TCB without being compromised by other processes or users. Therefore, a trusted computer system is one that employs the necessary hardware and software assurance measures to enable its use in processing multiple levels of classified or sensitive information. This system meets the specified requirements for reliability and security.

Another element associated with trusted computing is the trusted platform module (TPM). The TPM stores cryptographic keys that can be used to attest to the operating state of a computing platform and to verify that the hardware and software configuration has not been modified. However, the standard TPM cannot be used in cloud computing because it does not operate in the virtualized cloud environment. To permit a TPM version to perform in the cloud, specifications have been generated for a virtual TPM (VTM)4 that provides software instances of TPMs for each virtual machine operating on a trusted server. Trusted computing also provides the capability to ensure that software that processes information complies with specified usage policies and is running unmodified and isolated from other software on the system. In addition, a trusted computing system must be capable of enforcing mandatory access control (MAC) rules. MAC rules are discussed in more detail later in this chapter.

Numerous trust-related issues should be raised with, and satisfied by, a cloud provider. They range from concerns about security, performance, cost, control, availability, resiliency, and vendor lock in. Following are some of the critical questions that should be asked to address these concerns:

III. Secure Execution Environments and Communications

All paragraphs must be indented. All paragraphs must be justified, i.e. both left-justified and right-justified.

A. Secure Execution Environment

Configuring computing platforms for secure execution is a complex task; and in many instances it is not performed properly because of the large number of parameters that are involved. This provides opportunities for malware to exploit vulnerabilities, such as downloading code embedded in data and having the code executed at a high privilege level.

In cloud computing, the major burden of establishing a secure execution environment is transferred from the client to the cloud provider. However, protected data transfers must be established through strong authentication mechanisms, and the client must have practices in place to address the privacy and confidentiality of information that is exchanged with the cloud. In fact, the client's port to the cloud might provide an attack path if not properly provisioned with security measures. Therefore, the client needs assurance that computations and data exchanges are conducted in a secure environment. This assurance is affected by trust enabled by cryptographic methods. Also, research into areas such as compiler-based virtual machines promises a more secure execution environment for operating systems. Another major concern in secure execution of code is the widespread use of "unsafe" programming languages such as C and C++ instead of more secure languages such as object-oriented Java and structured, object-oriented C#.

B. Secure Communications

As opposed to having managed, secure communications among the computing resources internal to an organization, movement of applications to the cloud requires a revaluation of communications security. These communications apply to both data in motion and data at rest.

Secure cloud communications involves the structures, transmission methods, transport formats, and security measures that provide confidentiality, integrity, availability, and authentication for transmissions over private and public communications networks. Secure cloud computing communications should ensure the following:

 Confidentiality — Ensures that only those who are supposed to access data can retrieve it. Loss of confidentiality can occur through the intentional release of private company information or through a misapplication of network rights. Some of the elements of telecommunications used to ensure confidentiality are as follows:

- Network security protocols
- Network authentication services
- Data encryption services
- Integrity

Ensures that data has not been changed due to an accident or malice. Integrity is the guarantee that the message sent is the message received and that the message is not intentionally or unintentionally altered. Integrity also contains the concept of non-repudiation of a message source. Some of the constituents of integrity are as follows:

- Firewall services
- Communications Security Management
- Intrusion detection services
- Availability — Ensures that data is accessible when and where it is needed,

and that connectivity is accessible when needed, allowing authorized users to access the network or systems. Also included in that assurance is the guarantee that security services for the security practitioner are usable when they are needed. Some of the elements that are used to ensure availability are as follows:

- Fault tolerance for data availability, such as backups and redundant disk systems
- Acceptable logins and operating process performances
- Reliable and interoperable security processes and network security mechanisms

IV. Public Key Infrastructure and Encryption Key Management

To secure communications, data that is being exchanged with a cloud should be encrypted, calls to remote servers should be examined for imbedded malware, and digital certificates should be employed and managed. A certification process can be used to bind individuals to their public keys as used in public key cryptography. A *certificate authority (CA)* acts as notary by verifying a person's identity and issuing a certificate that vouches for a public key of the named individual. This certification agent signs the certificate with its own private key. Therefore, the individual is verified as the sender if that person's public key opens the data.

The certificate contains the subject's name, the subject's public key, the name of the certificate authority, and the period in which the certificate is valid. To verify the CA's signature, its public key must be cross-certified with another CA. (The X.509 standard defines the format for public key certificates.) This certificate is then sent to a repository, which holds the certificates and *certificate revocation lists (CRLs)* that denote the revoked certificates. Digital certificates are discussed in more detail in the following sections.

The integration of digital signatures and certificates and the other services required for e-commerce is called the *public key infrastructure (PKI)*. These services provide integrity, access control, confidentiality, authentication, and non-repudiation for electronic transactions. The PKI includes the following elements:

- Digital certificates
- Certificate authority (CA)
- Registration authorities
- Policies and procedures
- Certificate revocation
- No repudiation support
- Time stamping
- Lightweight Directory Access Protocol (LDAP)
- Security-enabled applications

V. KEY MANAGEMENT

Obviously, when dealing with encryption keys, the same precautions must be used as with physical keys to secure the areas or the combinations to the safes. The following sections describe the components of key management.

VI. KEY DISTRIBUTION

Because distributing secret keys in symmetric key encryption poses a problem, secret keys can be distributed using asymmetric key cryptosystems. Other means of distributing secret keys include face-to-face meetings to exchange keys, sending the keys by secure messenger, or some other secure alternate channel. Another method is to encrypt the secret key with another key, called a *key encryption key*, and send the encrypted secret key to the intended receiver.

These key encryption keys can be distributed manually, but they need not be distributed often. The X9.17 Standard (ANSI X9.17 [Revised], “American National Standard for Financial Institution Key Management [Wholesale],” American Bankers Association, 1985) specifies key encryption keys as well as data keys for encrypting the plain-text messages. Key distribution can also be accomplished by splitting the keys into different parts and sending each part by a different medium. In large networks, key distribution can become a serious problem because in an N-person network, the total number of key exchanges is $N(N–1)/2$. Using public key cryptography or the creation and exchange of session keys that are valid only for a particular session and length of time are useful mechanisms for managing the key distribution problem. Keys can be *updated* by generating a new key from an old key. If, for example, Alice and Bob share a secret key, they can apply the same transformation function (a hash algorithm) to their common secret key and obtain a new secret key.

VII. CONCLUSION

We conclude here our paper with cloud computing security architecture is a critical element in establishing trust in the cloud computing paradigm. Confidence in using the cloud depends on trusted computing mechanisms, robust identity management and access control techniques, providing a secure execution environment, securing cloud communications, and supporting trusted cloud computing architectures.

REFERENCES

[1] NIST Special Publication 800-14, “Generally Accepted Principles and
Practices for Securing Information Technology Systems,” September 1996.

[2] U.S. Department of Defense Information Systems Agency, “Virtual Machine Security Technical Implementation Guide,” http://iase.disa.mil/stigs/stig/vm_stig_v2r2.pdf.

[3] Cloud security: A comprehensive guide to secure cloud computing. John Wiley & Sons, 2010.

[4] NIST Special Publication 800-30, “Risk Management Guide for Information Technology Systems,” July 2002.