A SECURITY-FOR TRUSTED CLOUD COMPUTING

Punam A.Patil[*]

Nilesh S. Vani[**]

ABSTRACT

Internet is an important part, but there are several network security issues. To overcome those issues, trusted computing proposed. In trusted computing platform secure storage is important functionality and key management is important technology in secure storage. Cloud computing is recognized as an alternative to traditional information technology. Cloud computing –the fastest growing fields in computer world. This work is an investigation of the works to enhance the security level of authentication and authorization for trusted and cloud computing environment.

Keywords: ***Trusted Computing Platform; Cloud Computing; Secure Storage***

[*] Research Scholar, M.E. (II year), Computer Engineering Department, GF's Godavari College of Engineering, Jalgaon-Maharashtra (India)

[**] Assistant Professor, Computer Engineering Department, GF's Godavari College of Engineering, Jalgaon-Maharashtra (India)

1. INTRODUCTION

Today, the internet is an important part in our lives, spreading over every corner. The trusted computing technology includes security, storage, identity attestation and trusted platform, remote integrity measurement, storage and reporting etc. [1] the trusted computing is an active research in the field of information security.

Cloud Computing is a technology. Cloud computing is a type of computing that relies on sharing computing resources rather than having local servers or personal devices to handle applications. In cloud computing, the cloud service providers are able to deliver various services to cloud users with the help of powerful datacenters. One of the most fundamental services offered by cloud providers is data storage [2].

The main objective of this work is an investigation of the works to increase the security level especially in a trusted cloud computing environment. The paper is structured as follows: In section 2 introduce the basic concepts of trusted computing and cloud computing mechanism.

Section 3 introduces the existing scheme and analysis related to trusted and cloud computing. Section 4 describes the propose works. Finally, gives the concluding remark and future research work in section 5.

2. BASIC CONCEPTS

A. Trusted Computing

Trusted computing is a term that refers to technologies for resolving computer security problems.

Trusted Platform Module

Cloud provides have recognized the cloud security concern and are working hard to address it.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.

Trusted Network Connect

TCG's Trusted Network Connect (TNC) architecture provides an industry standard approach to network security and network access control (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. 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 . Cloud computing is a new computing model that distributes the computing missions on a resource pool that includes a large amount of computing resource .It is the result of development of infrastructure as a service (IAAS),platform as a service (PAAS),and software as a service(SAAS) .

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 drivers ,known as self – encrypting drivers.Simply the enterprise encryption process for handling sensitive data,since all data ,applicatons ,and drivers are encrypted internal to the drive and key management is an integral part of the design.

B. Cloud Computing

Cloud Computing is a type of computing -"a type of Internet-based computing," that relies on sharing computing resources rather than having local servers or personal devices to handle applications.

Salesforce
Microsoft
Yahoo
Rackspace
Google
Amazon

Fig 2.1 cloud computing services [2]

3. RELATED WORK

The traditional information security measures include firewall, Intrusion Detect System (IDS) and anti-virus .They are all passive defense technologies to ensure network security.The trusted computing platform Alliance was formed in Oct.1999 by Compaq,HP,IBM,Intel and Microsoft.In 2003 TCPA was renamed Trusted Computing Group.TPM is viewed as functionality equivalent to a high-end smart card.Usually TPM is a small chip soldered to the motherboard. Trusted Computing Platform (TCP) is a computing platform which contains TPM and the matched trusted software (Trusted Software Stack-TSS).

In [1] [7], Zhang Xing etc. find the key synchronization problem in the TCG key hierarchy authorization management system. To solve the problem, they presented a new AuthData management scheme. Although the improved scheme overcomes the key synchronization problem.

In [1], Song Cheng etc., In order to effectively solve the key synchronization problem in TCP key management mechanism; they proposed a security-enhanced trusted key authorization management mechanism. The main idea is that a data item (child key information) is added in the parent key object node. Improved key hierarchy authorization management is shown in fig.3.1

When a user creates a new TPM key object, the KCM first performs all actions as before, and then TPM computes the key information and stores the information in parent key object node. When a user wants to update an AuthData for a key object, after the user can be authorized to operate the key object he first inputs new AuthData instead of old one, and then TPM anew computes the key information. Finally TPM stores the information in its parent key node instead of the old one. When an owner wants to use his key object, he first inputs the key AuthData, then TPM validates the AuthData and computing the key information, and then determines whether the user has right to operate the key.

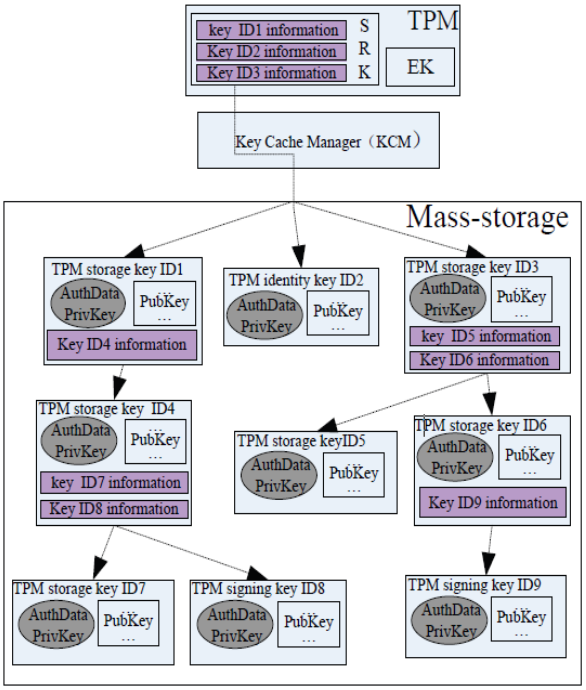

Fig 3.1 Protected storage object hierarchy based on timestamp [1]

4. ANALYSIS

One approach to achieve trustworthy computations in cloud infrastructure 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 .The TCG proposes to extend common computing platforms with trusted components in software and hardware

According to the introduction, the privacy part of the key pair and the corresponding authorization data is secret stored in key object node as a whole by encrypting them using parent key.

In [1], Song Cheng et al. to address the key synchronization problem and enhanced the trust and security of the trusted storage. To solve the problem they proposed a security enhanced trusted key authorization management scheme, the basic idea of which is to add child key information in parent key. That scheme includes: Security enhanced Trusted Key Management Scheme, Key Creating Flows Key AuthData Update Flows.

In the analysis done in [4], it investigates the access control mechanism in the cloud. That work has focused on the existing control access mechanism in cloud computing environments. Finally, they conclude that security features provided by service providers in a cloud computing are not totally trustful.

In [3], Xuefeng Liu et.al designs a secure data sharing scheme, Mona, for dynamic groups in an untrusted cloud. In Mona, a user is able to share data with others in the group without revealing identity privacy to the cloud. Additionally, Mona supports efficient user revocation and new user joining. More specially, efficient user revocation can be achieved through a public revocation list without updating the private keys of the remaining users, and new users can directly decrypt files stored in the cloud before their participation.

Moreover, the storage overhead and the encryption computation cost are constant. Extensive analyses show that proposed scheme satisfies the desired security requirements and guarantees efficiency as well.

4. FUTURE WORK

We plan to implement 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.

Modules:

1. Security Storage
2. Security-enhanced Trusted Key Generation
3. Authentication
4. Authorization

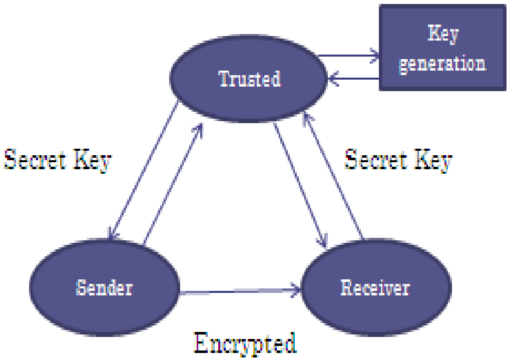

Fig.4.1 Key Generation, Authentication Authorization.

5. CONCLUSION

Security features provided by service providers in a cloud computing is not totally trustful. For this purpose proposed new scheme.

This scheme can effectively solve the key synchronization problem and disadvantages in the existing scheme, so the trust and security of the trusted storage is further enhanced.

This work has focused on the existing control access and security mechanisms in cloud computing and trusted computing environments.

REFERANCES

[1] Song Cheng, Li Jing, Peng Weiping and Tian Xinji, "A Security Enhance Key Authorization Management Scheme for Trusted Computing Platform," IEEE, *pp. 1573–76, 2012.*

[2] Kailas Patidar, Ravindra Gupta, Gajendra Singh, Megha Jain, Priyanka Shrivastava "Integrating the Trusted Computing Platform into the Security of Cloud Computing System" *volume 2, Issue 2,February 2012.*

[3] Xueteng Liu, Yuqing Zhang, MemberIEEE, Boyang Wang and Jingbo Yan Yan, "Mona: Secure Multi – Owner Data Sharing for Dynamic Groups in the Cloud

IEEE Transactions on Parallel and Distributed Systems volume l. 24, No. 6 June 2013.

[4] Mauro José A. de Melo and Zair Abdelouahab, "A Study of Access Control in Cloud Computing", Journal of Computers and Technology Volume 3 No. 3, Nov-Dec, 2012.

[5] Rajan Sameer, Jairath Apurva, "Cloud Computing The Fifth generation of Computing", International Conference on Communicati n Systems and Network Technologies, 2011

[6] TRUSTED COMPUTING GROUP. Cloud Computing and Security –A Natural Match GroupHomePage. https://www.trustedcomputinggroup.org/home, April 2010

[7] Zhang Xing, Zhang Xiaofei, Liu Yi and Shen Changxiang. A New AuthData Management Scheme. Journal of Wuhan University(Natural Science Edition). Vol. 53(5), PP. 518-522, Oct. 2007.