A Trusted Evidence Collection Method Based on the Trusted Third-Party for Cloud Platform

Lili Wu[1,2,*], Jing Zhan[1,2,*], Yong Zhao[1,2], Jun Hu[1,2], Ming Li[3]

1Beijing Key Laboratory of Trusted Computing
Beijing University of Technology
Beijing, China
2National Engineering Laboratory for Critical Technologies of Information Security Classified Protection
Beijing University of Technology
Beijing, China
3The Third Research Institute of Ministry of public security
Shanghai, China

Abstract —The characteristics of cloud computing, such as highly centralized resources, dynamic extensibility, and layered service mode, make the trusted evidence collection on the cloud platforms becomes very complex, this article introduces a trusted third party, and proposes a trusted evidence collection method based on the technology of trusted computing. Security features provided by TPCM (Trusted Platform Control Module) are used to introduce a CPTECA (Cloud Platform Trusted Evidence Collection Agent) in each layer of cloud platform respectively. The Agent monitors the entity in real-time using TPCM, and objectively collects the trusted evidence on the cloud Platform. Finally, the paper implements a CPTECA functional prototype based on the LSM (Linux Security Module).

Keywords-Trusted Computing; Cloud Computing; Trusted Third Party; TPCM; Trusted Evidence; Trusted Evidence Collection

I. INTRODUCTION

In recent years, cloud computing with its characteristics of resource rent, application hosting and service outsourcing has quickly become the most popular technology in the computer field. However, cloud computing usage with convenient and easy and low cost while bringing more serious security threats to the traditional model. SaaS provider Salesforce.com was under strong attack in 2007, resulting in a large number of tenant's privacy data leak [1]; In March 2011, In 2013 Google's large customer data leaked when EverNote was breached, leading to nearly fifty million users were required to reset the password to ensure that their personal information will not be illegally obtained; In June 2013, the National Security Agency and the FBI proposed a "prism" project that monitors the secret information by hacking into the data centers of Microsoft, Google, apple, yahoo and so on. The increased incidents of cloud security make the contradiction between user requirements and provider credibility unavoidable.

Security and privacy is the shared concern of the cloud computing users. Guarantee the credibility of the cloud platform is urgent in a growing number of security risks [2-7]. So how to obtain and protect the credible evidence on the cloud platform, will also become an important research content of cloud computing.

Study abroad mainly has the following research on credible evidence collection, Chen et al. [8] designed a separate monitor between software and hardware on the cloud platform, to provide customers with the VM runtime evidences and reports; Run Test [9] proposed a new service integrity attestation system for verifying the integrity of dataflow processing in multi-tenant cloud infrastructures in application layer, using the consistency and inconsistency statistics of dataflow processing nodes as the credible evidence of cloud services. Rep Cloud [10] evaluates the cloud services by making the subjective trust as the credible evidence; Ruebsamen and Reich [11] think that data can be collected at the network, hardware, host operating system, hypervisor, virtual machines and cloud management system (CMS). It describes possible sources for evidence data collected across the different architectural layers.

Domestic credible evidence collection research mainly divided into the software, terminal platform, and credible evidence collected from cloud platform. On the credible evidence collection of software, Gu et al. [12] defined the software credible evidence as the information related to software running status. On the trusted evidence collection methods, trusted evidence collection agents TECA was used in the kernel layer of operating system, and using the TPM integrity measurement function to collected the integrity of files in specified software as credibility, and using the TPM security function to protect results. Cai et al. [13] proposed a multi-level tree structure based on source custom software trusted evidence representation model, to avoid the problem of undue expanding in single evidence model, but the evidence collection methods are not unified, which varies based on the characteristics of a software object. As the software reliability problem, Hao [14] used the software behavior trace as software trusted evidence, and made the software isolation into virtual machine environment and intercepted the form of its system call as the evidence collection. On the terminal platform trusted evidence collection, Tan et al. [15] used a trusted evidence collection agency in application layer to collect evidence when collected trusted evidence in running environment of the trusted terminal. Trusted evidence including process state, memory, CPU, network ports, disk information, strategies, data, etc., and based on TPM to protect trusted storage of evidence. On the trusted evidence collection of cloud platform, Song proposes a SCE system [16], which made the trust of service as trusted evidence, and obtained the evidence through monitoring the running state of the service. Liu et al. [17], Xin et al. [18] and Yang et al. [19], and many other researchers [20-24] all used trusted computing technology to monitor the IaaS service, and obtained its integrity attributes as trusted evidence.

Study on home and abroad of trusted evidence collection mostly focused on the IaaS layer, lack of cross-layer unified objective and trusted evidence collection of tools and methods. To enhance the credibility of cloud platform, this paper introduced a trusted evidence collection method on cloud platform for the third-party. This method can provide an objective and comprehensive trusted evidence for the trusted third party, and also provide a trusted validation, audit and assessment for the cloud platform. Using the security features provided by TPCM, we introduced CPTECA respectively in each layer of Cloud platforms. The Agent monitors the entity in real-time using TPCM, and objectively collects the trusted evidence on the Cloud Platform. TPCM integrity function ensured the confidentiality and integrity of trusted evidence collected. Finally, the paper implements a CPTECA functional prototype based on the LSM.

II. TRUSTED COMPUTING TECHNOLOGY

Trusted chain and trust root both are the core elements of trusted computing, TCG specification of Trusted Platform Module (TPM) is the trust root of trusted computing platform hardware, and it provides the protected secure storage, security chip of password computing power. TPM has independent executable unit and RAM memory, its random number generator and key generation components can provide functions that generated random number and key, and its password function parts, such as cipher coprocessor, HMAC engine and engine SHA-1, provides hardware password supported for reliable measurement and reporting mechanism. Secondly, TPM internal nonvolatile memory can save some status information or key information permanently as supported for the trust store, and provided protected areas known as the Platform Configuration Register (PCR), which used to store the measurements generated by building trusted chain, and to prove platform configuration to users through reporting the information in the PCR by specific TPM commands. However, the TPM has the problems of starting point and passive measure.

Thus china proposed Trusted Platform Control Module (TPCM) in the standard draft of "the Trusted Platform Control Module Scheme”, which put forward the idea of the TPM as an active device, changing the thinking of the TPM as a passive device, and realizing the Trusted Platform Control Module for active Control of computing platform. TPCM as the active device of computing platform starts before CPU, and builds trust chain that makes TPCM module as trust root. The Root of Trust for Measurement(RTM) designed in TPCM, increases the safety problem of trusted measurement root, and makes all trusted root implanted chip inside, and gets more stronger physical protect, and solved the problem of trusted measurement root out of control caused by tampering BIOS, so it strengthen safety reliable measure root.

TPCM chips consists of execution engine, nonvolatile storage unit, volatile memory cell, random number generator, cipher algorithm engine, key generator, timer and other parts, as shown in Figure 1. And input and output bridge units map these functional components into slice address space of CPU.

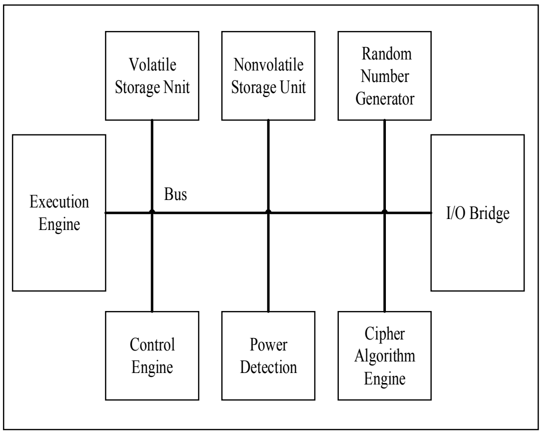

Figure.1TPCM Composition

In TPCM, power system was designed independent of the CPU, so TPCM could run as main equipment starting before CPU, and became the starting point of the system reliable measure, which could measure all parts including the BIOS, and could establish a trust chain starting with TPCM.

On the trusted computing platform based on TPCM, TPCM executed firstly, and when TPCM started, the CRTM which was core measurement root in TPCM measured the BIOS integrity, and stored the measurement results in PCR inside of TPCM. TPCM matched the measurement results and the benchmark in internal storage of TPCM, if true, TPCM sent electrical signals to the power controller, and then the main board platform started, then CPU started and BIOS code executed, then the BIOS guided, then the operating system started, and then a series of process performed. Trust would pass through this process, until the entire computing environment had setup.

PCR expand operation was defined as , symbol || notate connection, and x was the current operation that measure data block.

III. CLOUD PLATFORM TRUSTED EVIDENCE COLLECTION MECHANISM BASED ON TRUSTED COMPUTING

Based on the fundamental support of trusted computing and TPCM security functions, and combined with the structure features of cloud platform, this paper proposed a cloud platform trusted evidence collection mechanism based on trusted evidence collection agent, as shown in Figure 2.

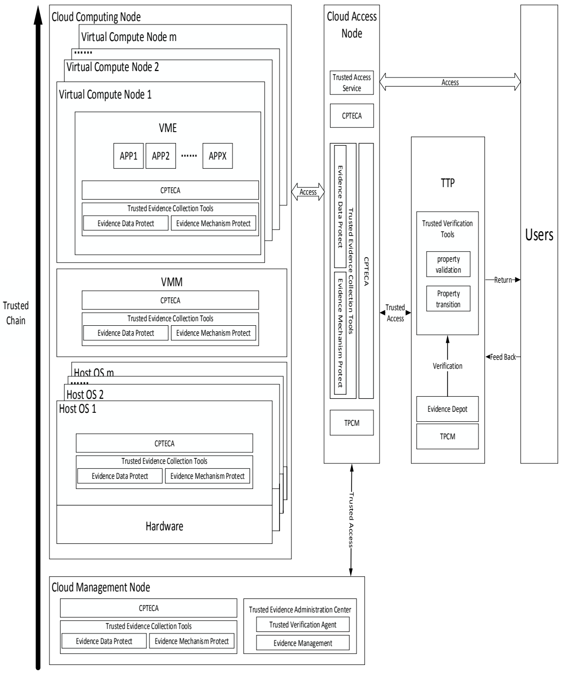

Figure.2 Trusted Evidence Collection Architecture of Cloud Platform

In the cloud platform trusted regulatory system, structure mainly includes three entities: cloud service providers, users, trusted third party. And the cloud platform according to the node types was divided into cloud computing environment node, cloud management node, and cloud access node. Cloud computing environment node processes all tasks for resources and environments submitted by cloud user, such as computing, storage, application and so on. Cloud access node made cloud users connect cloud platform and use cloud services. Cloud management node unified managed and preprocessed data that transmitted through cloud computing environment node, and waited for the third party requests. After users requested to the third party, the trusted third party requested to trusted evidence management center, and then trusted evidence would be collected by trusted agent, log, user feedback and etc., and would go back to the trusted third party.

A. *Cloud Platform Source Trusted Evidence*

Sources of evidence in cloud platform includes many aspects, such as the network layer, host system layer, virtual layer, IaaS, SaaS, PaaS, cloud computing management system (CMS) and so on, and the corresponding evidence includes network resources, load information, performance counters, all kinds of monitoring information, the VM run data, VM snapshot, running environment log (e.g. application logging) and etc..The cloud management system is a huge source of evidence. It is the center control component of cloud infrastructure, and provides for user login, cloud services using, access, configuration, resource allocation, policy, location and many other information.

B. *Trusted Evidence Collection Methods in The Cloud Platform*

Trusted evidence has three characteristics: objectivity, comprehensiveness and availability. According to these characteristics, in this paper, the trusted evidence collection agents CPTECA is introduced into the virtual layer, the VMM, the system layer of the host and the cloud management system in the cloud platform, it is used to monitor the entity of each layer instantly and collect the data.

TABLE 1. ALGORITHM FOR RECORDING THE STATE OF EVIDENCE

```
Algorithm1. Algorithm for recording the state of evidences
Record($e_s$,$t$).
        Input：$hashvalue$, $e_s$ =( $e_1$, $e_2$,…$e_j$)
            For $i$=1 to $j$ do
                        $r_i$=$hash(e_i)$;
                        $hashvalue$ ($e_i$)= $r_i$;
                        $record(e_i,t)$=<$e_i,t$, $r_i$, $sig(AIK_{priv,}$, $r_i \| t)$>;
                        $recordList(e_i)$= $recordList(e_i)$∪{$record(e_i,t)$};
                        $record(e_s,t)$= $record(e_s,t)$ ∪$r_i$;
            $Log(e_i)$= $hash(e_i \| Log(e_i))$;
     Output：$record(e_s,t)$, $recordList(e_s)$.
```

In the cloud platform, the collection of trusted evidences is the process of measuring the evidences. The trusted evidence is measured and recorded by the integrity measurement and trusted reporting mechanism of TPCM. In TPCM, identification key AIK denotes as $\{AIK_{pub}, AIK_{priv}\}$, sig(k, x) stands for signing the message using the key k, PCR expanding operation is , it is defined as . For each trusted evidence, TPCM extended operation maintains a state Log(x), symbol || denotes for connection operation, where x is the data block which is measured in current operation.

The state record of evidence e_i in time t is Record(e_i, t)= <e_i, t, hash(e_i || t), sig(AIK_{priv},, hash(e_i || t))>.

Algorithm for recording the state of evidence Record (e_s, t), as shown in Table 1.

IV. THE RELIZATION OF THE TRUSTED EVIDENCE COLLECTION AGENTS

In this paper, combining dynamic pile technology and hooks (Hook) technology, a functional prototype of trusted evidence collection agency of cloud computing is realized in Ubuntu based on LSM.

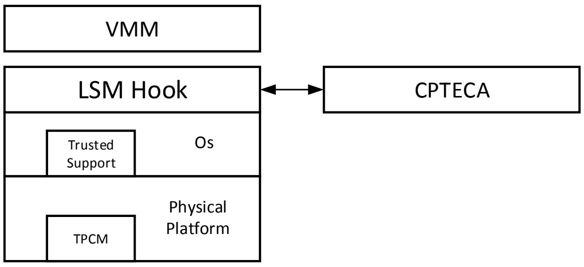

Figure.3Trusted evidence collection agent of cloud computing

In the Linux system, in order to support the scalable Linux kernel access control mechanism, the LSM provides a series of hook functions related to the system security. The hooks technology is a powerful process monitoring technology, by installing hooks and monitoring the transmission of system call in the process, it realizes the monitoring of system call sequences. Through implanting the related hook functions of Linux kernel, we can dynamically intercept the system call from different applications in cloud platforms, and furthermore, providing the trusted technology support to realize the collection of trust evidence in the cloud platform.

V.ANALYSIS OF PERFORMANCE

The process of trusted evidence collection is in fact the measurement process of trusted evidence. Increasing the trusted evidence collection agents, will inevitably increase the delay of the system, and the main delay time result from the time of evidence measurement. Therefore, the time of trusted evidence collection mechanism, is mainly the time of trusted evidence measurement. Using a hash table, only measure the modified files, while for the unmodified files, read directly the recent measurements from a hash table, so it can greatly reduce the measurement time overhead. In reference [25], the experiment platform is Linux system, the kernel 2.6.26, and using the trusted chip under TPCM environment, the time unit of measurement process is us. As a result of the measurement process, time consumption is in the acceptable range.

VI. CONCLUSIONS

In this paper, we introduce trusted evidence collection method on cloud platform for the third-party. This method can provide an objective, comprehensive and credible evidence for the trusted third party, while providing a credible validation, audit and assessment for the cloud platform. We use the security features provided by TPCM to introduce CPTECA in each layer of Cloud platforms respectively. The Agent monitors the entity in real-time using TPCM when objectively collecting the trusted evidence on the Cloud Platform. TPCM integrity function ensures the confidentiality and integrity of credible evidence collection. Finally, the paper implements a CPTECA functional prototype based on the LSM, and analyzes the future research work on using the collecting credible evidence to prove and evaluate the credibility of the cloud platform.

CONFLICT OF INTEREST

The authors confirm that this article content has no conflicts of interest.

ACKNOWLEDGMENT

This work was supported by: "Trusted Evaluation Technology of Cloud Platform Based on the Third-party" from China “863(SQ2015AA0101327)” and “National Major Subject of Science and Technology” (2012ZX03002003) and “The Specialized Research Fund for the Doctoral Program of Higher Education by The Ministry of Education” (2013110312000) and (20131103120001).

REFERENCES

[1]. http://voices.washingtonpost.com/securityfix/2007/11/salesforcecom_acknowledges_dat.html,2014.
[2]. Laprie J C. “Dependable computing and fault tolerance: Concepts and terminology”, Proc of 15th IEEE Int Symp on Fault-Tolerant Computing（FTCS-15），ANN Arbor，Michigan, pp.2-11,1985.
[3]. TCG. “Specification architecture overview specification. Revision 1.4 ”，2007.
[4]. ISO/IEC 15408-1-2005 “Information technology-security techniques -evaluation criteria for IT security，Part 1, Introduction and general model”, 2005.
[5]. NSTC. “Research challenges in high confidence systems”,Proceedings of the Committee on Computing Information and Communications Workshop，1997.
[6]. Avizienis A，Laprie J C，Randell B. “Fundamental concepts of dependability”3rd Information Survivability Workshop（ISW-2000），Boston，Massachusetts, pp.38-56,2000.
[7]. Avizienis A，Laprie J C，Randell B，et al, “Basic concepts and taxonomy of dependable and secure computing”, IEEE Transactions on Dependable and Secure Computing 1, 2004, 11-33.
[8]. ChenChen, PetrosManiatis, “Adrian Perrig. Towards Verifiable Resource Accounting for Out sourced Computation”, pp.16–17, 2013.
[9]. Juan Du, Wei Wei, XiaohuiGu,et al. “RunTest: Assuring Integrity of Dataflow Processing inCloud Computing Infrastructures”, pp.13–16, 2010.
[10]. AnbangRuan, Andrew Martin. “RepCloud: Achieving Fine-grained Cloud TCB Attestationwith Reputation Systems”,STC’11,October 17, 2011, Chicago, Illinois, USA. ACM,pp. 3-14,2011.
[11]. Thomas Ruebsamen, Christoph Reich. “Supporting Cloud Accountability by Collecting Evidence Using Audit Agents”. In: 2013 IEEE 5th International Conference on Cloud Computing Technology and Science (CloudCom).
[12]. Gu Liang. “Runtime Software Trustworthiness Evidence Collection Mechanism Based on TPM”. Journal of Software ,2012.
[13]. CAI Si-Bo, ZOU Yan-Zhen, SHAO Ling-Shuang, et al. “Framework Supporting Software Assets Evaluation on Trustworthiness”. Journal of Software ,2010.

[14]. Hao Rui. "RESEARCH ON SOFTWARE TRUSTWORTHINESS BASEDON VIRTUALIZED TRUSTED PLATFORM" ,2013.

[15]. TANLiang, CHEN Ju, Zhou Mingtian. "ACTA ELECTRONICA SINICA",2013.

[16]. TaoSong. "Modeling and Methods of Trusted Services under Network Environment" ,2010.

[17]. Chuanyi Liu, Lin Jie, Tang Bo, Journal of Software (2014)

[18]. Siyuan Xin, Yong Zhao, Yu Li. " Property-Based Remote Attestation Oriented to Cloud Computing", in: 2011 Seventh International Conference on Computational Intelligence and Security, Sanya, Hainan, China, pp.1028-1032,2011.

[19]. Yang Yang. "The Research and Design of Remote Attestation Based on Cloud Computing Environment",2012.

[20]. E. Kanimozhi, "Trusted cloud—a solution for cloud cartography,"JournalofGlobalResearchinComputerScience, vol.3, no.11, pp. 44–51, 2012.

[21]. T. Ristenpart, E. Tromer, H. Shacham, and S. Savage, "Hey, you, get offofmy cloud: exploring information leakage in third-party compute clouds," inProceedings of the 16th ACM Conference on Computer and Communications Security (CCS '09), pp. 199–212, 2009.

[22]. PRINCE MAHAJAN, SRINATH SETTY, SANGMIN LEE, et al. "Depot: Cloud Storage with Minimal Trust". ACM, Transactions on Computer Systems, 29(4), 2011, 1-38.

[23]. Shams Zawoad. SecLaaS. "Secure Logging-as-a-Service for Cloud Forensics". ACM, pp.219-230,2013.

[24]. Yan Zhu, Huaixi Wang. "Dynamic Audit Services for Integrity Verification of Outsourced Storages in Clouds", ACM, 1550-1557,2011.

[25]. Lili Wu. "An efficient method of Secure Startup and Recovery for Linux". Advances in Information Sciences and Service Sciences,2013.