ATLANTIS PRESS

Advances in Engineering Research, volume 139

2nd International Conference on Electrical Engineering and Automation (ICEEA 2018)

Trusted Evidence Index System of Cloud Platform

Lili Wu[1], Zhengmin Li[2, 3], Tao Chen[1*] and Jinliang Hou[4]

[1]Department of Engineering Physics, Tsinghua University, Beijing 100084, China

[2]National Computer Network Emergency Response Technical Team/Coordination Center of China, Beijing 100029, China

[3]Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China

[4]Zshield Inc, Beijing 100191, China

[*]Corresponding author

***Abstract*—Trusted evidence collection is an important content in the study of the cloud platform trustworthiness. Trusted evidence index system and collection model should not only meet the description of cloud platform trusted evidence, but also solve the problems of model expansion by the massive evidence instance on the cloud platform. Based on the characteristics of data in the cloud, such as huge amounts and diversity of usage scenarios, source of evidence, and service types, we proposed the definition of credibility and trusted evidence on the cloud platform, and put forward a customized model of trusted evidence. According to the different sources and properties of trusted evidence, the model can describes and stores trusted evidence, and it provides an efficient method of data description and access for the subsequent remote attestation.**

Keywords—cloud computing; trusted evidence; trusted evidence attribution; index system; trusted evidence model

I. INTRODUCTION

Cloud computing is widely regarded as an important growth point of IT industry since the Internet boom, and has a huge growth of market prospects. According to IDC predictions, service revenue of cloud computing will be as high as $72.9 billion in 2015, and over the next five years, cloud computing services will continue to maintain strong growth momentum, the average annual growth rate will reach 27.6%, and it is four times of the traditional IT industry. The foreign well-known IT companies Google, Amazon, IBM, Microsoft, HP, Dell and Oracle are vigorously developing and promoting the cloud computing. In China Tencent, Baidu, Sina, Sohu, Alibaba, Shuguang, Huawei and other well-known IT enterprises are also actively promoting the construction and the application of the cloud platform. The government is also strengthening the construction of the center of the cloud computing, including Beijing, Shanghai, Wuxi, Shenzhen, Tianjin, Wuhan, Changsha, Jinan, Qingdao and other major areas of cloud computing center has been built or under construction.

However, cloud computing provides the using with convenient and easy and low cost as well as bring 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 reveal; In March 2011, Google's large user data leak; EverNote was breached in 2013, nearly fifty million users are asked 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 monitoring the secret information, such as emails, chats, videos and photos in whole American citizens, by entering into the data centers of Microsoft, Google, apple, yahoo and so on. The increasing incidents of cloud security make the contradiction between user requirements and provider credibility become clear.

Cloud computing is facing tremendous challenges in offering the security and privacy. 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. So how to obtain and protect the credible evidence on the cloud platform, will also become an important research content of cloud computing. Therefore, prove the credibility of the cloud platform is very important to the development of cloud computing, trusted evidence is the key factors of cloud platform, and how to accurately definite, divide, describe and store the trusted evidence on cloud platform has also became the important problem to be solved.

II. RELATED WORK

J.C. Laprie[1] puts forward the concept of dependable computing in 1985. Over the years, people propose many different expressions on the concept of trusted computing from different angles. Trusted Computing Group (TCG) thinks that system is credible, which is able to run fully comply with its preset program, and the behavior that contrary to the intentions of its designers and programmers will be appeared at a little possibility[2]. TCG's concept about "trusted computing" was from the view of the user's (subject), emphasized the predictability and consistency with the setting goals of object's behavior. ISO/IEC15408 defined that the behavior of a trusted component, operation or process is predictable under any operating conditions, and can resist the damage caused by the application software, virus, and certain physical interference[3]. This definition emphasizes the predictability, antiviral reliability and anti-interference ability of object's behavior from the view of the object. Microsoft's Bill Gates thinks that the trustworthy computing is to provide a reliable computing environment just like People's Daily use of the power system, and puts forward the four basic attributes of trusted computing, named the reliability, security, confidentiality and business integrity. Bill Gates emphasized the reliability and safety of software. The Science and Technology Commission(NSTC) thinks that the high confidence information system is a measure of predictability whether the system behavior conforms to the setting expectations or not, and thinks that trusted system has

many features, including the functional correctness, crisis-prevention, fault-tolerant, real-time and security[4]. NSTC also emphasizes the predictability and conformity with the set goals of the object's behavior.

Avizienis[5] put forward the attribute model of dependability in 2000, and proposed the concept framework of dependability, which includes availability, reliability, safety, confidentiality, integrity, maintainability. Avizienis[6] pointed out that the security of software is constituted by confidentiality, integrity and availability.

Literature [7] expressed the software behavior in the form of algebraic description of the software behavior traces. The software behavior trace is the behavior sequence of sequential relationship which is produced by an actual software operation, and behavior trace is software behavior that can be detected, if every behavior of the software can be detected, and the behavior traces are equal to the software behavior. System call sequences generated by the privilege program are the specific form of behavior trace, and they can reflect the characteristic of software behavior.

Literature [8] completed the record of trusted evidence except the input and output in file size. It thinks a software object O as a collection of files, and trusted evidence is the state and operation of the object and the related object, and then the collection of all operations is the expression of trusted evidence in software runtime. The set method is simple and intuitive.

Based on least trust, Literature [9] designed a cloud data storage depot, and guaranteed the consistency of the cloud data by Fork - Join - Causal consistency during the time in data storage and updated. Literature [10] designed a reliable monitoring called Observer which is between software and hardware of the cloud platform, and provided the evidence and reports of VM runtime for customers. Literature [11] proposed a SecLaaS to ensure confidentiality by recording/store VM logs, history logs and access control. Based on fragmentation structure and the hash table, literature [12] proposed a dynamic audit service to verify the storage integrity of an incredible outsourcing, these two methods can also ensure the integrity of the cloud data in the condition of cloud services are not credible. A measurement mechanism about the credibility of service was proposed in ref. [13], it established a cloud service metrics list through the cloud service runtime measures, and provided measurements to Proving.

Based on the characteristics of data in the cloud, such as huge amounts and diversity of usage scenarios, source of evidence, and service types, we proposed the definition of credibility and trusted evidence on the cloud platform, and put forward a customized model of trusted evidence.

III. THE DEFINITION OF CLOUD PLATFORM CREDIBILITY AND TRUSTED EVIDENCE

Trusted system refers to the behavior is always carried out in accordance with the expected targets. In addition to providing reliable cloud services, trusted cloud platform also must specify the properties of platform in the aspects of safety and maintainability, clear to ensure the security of privacy and data for users. Based on the characteristics of cloud platform and combining with the definition of trusted system, we can get the definition of the cloud platform credibility.

Definition 1, Cloud Platform Credibility refers to the behavior of cloud service providers are always carried out in accordance with the expected targets.

Definition 2, Trusted Evidence is the basis data without specifically analyzing and processing, and can be directly or indirectly tested by the hardware and software to perform the remote authentication on cloud platform.

Based on the definition, trusted evidence has the characteristics of objectivity, relevance, and availability. And then define the specific properties of trusted evidence, such as confidentiality, integrity, availability, reliability, scalability and maintainability, etc.

IV. INDEX SYSTEM OF TRUSTED EVIDENCE FOR CLOUD PLATFORM

According to the definition of cloud platform credible and trusted evidence, we can build the index system of credible evidence that cover cloud platform properties, such as security, reliability, availability and maintainability.

Based on the reference of clouds safety standards and guidelines of CSA groups, we put forward a cloud platform confidence index system, including the first-level indicators such as cloud platform security, reliability, availability and maintainability, secondary indexes such as password service, server configuration, network configuration, the third-level indicators such as password algorithm, password usage patterns, and the key length. As shown in Table I.

TABLE I. INDEX SYSTEM OF TRUSTED EVIDENCE FOR CLOUD PLATFORM

Index System of Trusted Evidence for Cloud Platform		
The first-level indicators	***The second-level indicators***	***The third-level indicators***
Security	Password service	Password algorithm, password usage patterns, key length, key management mechanism, signature mechanism
	Server configuration	Geographical location information, TPM, antivirus software, IDS, firewall, key file protection, white list management, Hypervisor and guest OS
	Network configuration	The link layer security, network IDS, firewall, content filtering, wireless network protection
	VM security	Virtual network monitoring and security scanning, VM traffic detection, VM fault location
	Multi-tenant data protection	File system, storage mode, data recovery strategy, data reconstruction, residual data recovery, data storage encryption, data transmission encryption, data using encryption, backup frequency,

Index System of Trusted Evidence for Cloud Platform		
The first-level indicators	***The second-level indicators***	***The third-level indicators***
		reduction rate, data integrity check, data recovery point, data export testing, data deleting, data leakage, data isolation
	Bug	The result of a recent bug scanning, bug and patch information, bug release time, bug severity, patch release time, patches of time
	Authentication and access control	Identity management, authentication services, authorization services
	Security isolation	Storage isolation, network isolation, tenant isolation, resource isolation
Reliability	Fault-tolerant backup	File system redundancy backup, copy of the deposit, the heartbeat report mechanism, snapshot mechanism, failure processing
	Failover	Services mean time between failures, mean time to recovery service failure
	Incident response	Severity classification, response time, the proportion of event in a certain period of time, to the user's report (report time, report content), the average time of the incident, the specific event data
Availability	Service availability	Service request failure rate, service cycle, specific service function, service object
	Service flexibility and load balance	CPUs, CPU speed, storage capacity, the number of VM, VM storage and bandwidth, message processing ability, application processing ability
	User-friendliness	The interface friendly, operation simplicity
Maintainability	Change management	Announcement time and content, test frequency and result, changes in the key security components
	Log management and forensics	Log availability (strategy violation log, event log, authorized users, subject logs, incident response log), log correctness
	Safety management system	Management system, formulate and publish, post setting, staffing, authorization and approval, communication and cooperation

In terms of security, we focus on the properties of password service, virtual machine security, multi-tenant protection, bug, authentication and access control, and security isolation, including password algorithm, password usage patterns, key length, key management mechanism, signature mechanism and so on.

In terms of reliability, we focus on the properties of incident response, fault recovery and fault-tolerant backup, including file system redundancy backup, copy of the deposit, the heartbeat report mechanism, snapshot mechanism, failure processing, etc.

In terms of availability, the main focus on the properties of service reliability, flexibility and load balancing, user friendly service, including service cycle, specific service function, service object, CPUs, etc.

In terms of maintainability, we focus on the properties of safety management system, log management and forensics, change management, including test frequency and result, authorization and approval, subject logs and so on.

V. THE TRUSTED EVIDENCE MODEL OF CLOUD PLATFORM

The different service architecture of cloud platform, determines the source and the type of the trusted evidence are different also. The content and organizational structure of evidence instances which come from different sources are often different, we need to provide a unified management mechanism for these different evidence instances. However, to establish a sufficient model for describing all instances will often bring the problem of excessive inflation, as once there is a new heterogeneous instance, there is need to extend the data model.

Therefore this paper according to different sources and properties proposes a customizable model of evidence. It can descript and extract the trusted evidence for the subsequent remote attestation. The Trusted Evidence Tree Model (TETM) is based on source-custom to describe trusted evidence. As shown in Figure I.

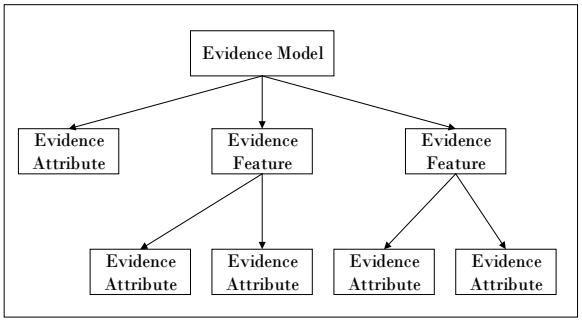

FIGURE I. TRUSTED EVIDENCE MODEL.

A single model of evidence can be described by a triple < EM_INFO EM_NODE, EM_VALTYPE >. As shown in Figure 2, among them:

EM_INFO refers to a model of evidence, described by a triple < EM_ID EM_NAME, EM_SRC >. EM_ID is the unique identifier of the evidence model, EM_NAME is the name of the evidence model, and EM_SRC is the source of model.

EM_NODE is used to refer to the all grubbing node, and it contains two types of nodes: leaf nodes and non-leaf nodes. Non-leaf node is called feature of evidence which can be nested, and it is a more detailed description of the parent's characteristics. Leaf node is called attribute of evidence, it is atomic and can't be subdivided. Evidence features is the comprehensive of evidence attributes, only evidence attribute is a calculation unit.

EM_VALTYPE defines the type of attribute value, and each attributes corresponding to a value type.

From the above, we can get the description of evidence model. As shown in Figure II.

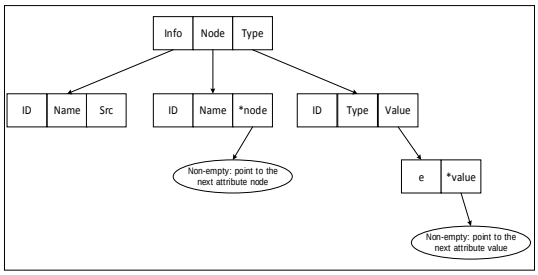

FIGURE II. DESCRIPTION OF EVIDENCE MODEL

Considering the same meaning of evidence attributes may exist in different evidence Model, we need to establish a synonymous link for such evidence attributes. According to the attributes between the synonymous, we can get more measurements of evidence attribute in the multiple evidence models. This article uses the binary relation to express the synonymous link between evidence attributes. As the formula (1) shown,

$$\Sigma\Psi N=<EM\_NO\Delta E1, EM\_NO\Delta E2> \quad (1)$$

EM_NODE1 and EM_NODE2 have the same meaning, but belong to two different models of evidence.

VI. CONCLUSIONS

This paper proposed the definition of credibility and trusted evidence on the cloud platform, and put forward a customized model of trusted evidence. The model uses a multi-level tree structure based on the source-custom to express the trusted evidence. Using this evidence model has the following advantages, (1) the evidence model based on the actual information of evidence, and as the custom-source, evidence is more in line with the actual situation. (2) Evidence model is easy to extend. Build the model respectively for different sources of evidence, when captured a new information source of evidence, directly to build the simulation, and it does not affect the defined model before. (3) Evidence model is easy to manage. Using multiple models instead of a large model of evidence, we can avoid the problem of overexpansion which a single model has.

According to the different sources and properties of credible evidence, the model can describes and stores credible evidence, and it provides an efficient method of data description and access for the subsequent remote attestation.

ACKNOWLEDGMENT

The authors appreciate the project Z161100001116010 supported by Beijing Municipal Science & Technology Commission.

REFERENCES

[1] Laprie J C. Dependable computing and fault tolerance: Concepts and terminology[C]//Proc of 15th IEEE Int Symp on Fault-Tolerant Computing(FTCS-15), ANN Arbor, Michigan, pp.2–11, June,1985.

[2] TCG. Specification architecture overview specification, Revision 1.4[S], August 2007

[3] ISO/IEC 15408-1-2005 Information technology-security techniques - evaluation criteria for IT security,Part 1, Introduction and general model[S], 2005

[4] NSTC. Research challenges in high confidence systems[C]//Proceedings of the Committee on Computing, Information, and Communications Workshop, 1997

[5] Avizienis A, Laprie J C, Randell B. Fundamental concepts of dependability[C]//3rd Information Survivability Workshop (ISW-2000),Boston,Massachusetts, October 24-26,2000

[6] Avizienis A, Laprie J C, Randell B, et al, Basic concepts and taxonomy of dependable and secure computing[J]. IEEE Transactions on Dependable and Secure Computing. pp.11–33, January, 2004.

[7] Hao Rui. RESEARCH ON SOFTWARE TRUSTWORTHINESS BASED ON VIRTUALIZED TRUSTED PLATFORM,2013

[8] Gu Liang: Runtime Software Trustworthiness Evidence Collection Mechanism Based on TPM. Journal of Software,2012

[9] PRINCE MAHAJAN, SRINATH SETTY, SANGMIN LEE, ALLEN CLEMENT, LORENZO ALVISI, MIKE DAHLIN, and MICHAEL WALFISH. Depot: Cloud Storage with Minimal Trust. ACM, Transactions on Computer Systems, Vol. 29, No. 4.

[10] Chen Chen, Petros Maniatis, Adrian Perrig, Towards Verifiable Resource Accounting for Outsourced Computation, AVM,16–17 March 2013

[11] Shams Zawoad. SecLaaS: Secure Logging-as-a-Service for Cloud Forensics. ACM,8–10 May 2013

[12] Yan Zhu, Huaixi Wang. Dynamic Audit Services for Integrity Verification of Outsourced Storages in Clouds, ACM,21-25 March 2011

[13] TaoSong: Modeling and Methods of Trusted Services under Network Environment, 2010