Research on ATN-based Trusted Cloud Computing Security Model *

Shaoyu YANG*, Shiqing WANG

College of Information Engineering, Zhengzhou University, Zhengzhou 450000, China

Abstract

In cloud computing environment, the trust relationship between resources is hard to define. By analyzing the layered framework for cloud service, we find a regulation for building the trust within the two strange entities. Along with this regulation, we propose a 3-layer trust framework for evaluating trust relationship in cloud computing. Combined with trust computing and automated negotiation trust mechanism, a property-based negotiating trust model was established by improving the property-based trust attestation. Discussing the four security properties, this model can provides safe and high-efficient security underpinning for cloud service.

Keywords: Cloud Computing; Trust Computing; Negotiating Trust; Property-based Attestation

1 Introduction

With the rapid development in Web-Service and SOA architecture, the cloud computing has became a popular computing and storage platform for application service. As a prediction from IDC (International Data Company) [1, 2], the increasing rate of industry about cloud computing is six times more than traditional IT industry, and the average rate of cloud service will be 26% in next 5 years. By 2012, the industry value supported by the cloud computing will reach 42 billions, which account for 25% of the gross of expenses growth in IT industry. Compared with the traditional IT technology, the cloud computing, with the character of elasticity, efficiency and low-energy, makes it easy for using the IT service in cloud computing. User can require the computing or storage service just like other secondary energy. Furthermore, the governments around the world advocate this new technology for promoting and motivating the concept of energy-saving and environmental protection. By service migration and cluster application, cloud computing can relieves the problems about the energy distribution, low computing capability and reduces the energy consumption. As the SOA architecture being mature gradually, the IT industry has been developing quickly. Cloud computing is bringing an industrial revolution in IT fields.

*Project supported by the National Key Technology R&D Program in the 11th Five year Plan of China (No. 2006BAF01A00).

*Corresponding author.

Email address: ysymagnet@gmail.com (Shaoyu YANG).
However, as everyone known, the security, which is the core problem in cloud computing, has been still puzzled the cloud services’ user and developer. Compared with the security problem before, the distributing storage and parallel computing model in cloud computing take the new challenge in the security about data access and storage. How to establish the trust relationship between the two stranger nodes? And how to define and evaluate the trust in cloud computing? The issues influencing resources’ performance have been proposed in practical application.

In this article, we propose a framework, which built by the 3-layer structure, for evaluating the trust relationship. By the property exchanging, the two stranger and heterogeneous cloud resources are gradually connected with each other. The outline of article is as follow. In section 1, we shows the research condition about trust evaluation and measurement in recent years. And section 2 proposes a trust evaluation framework for cloud computing, and defines the four properties about cloud service’s security. In Section 3, underpinned by this formwork, a model for evaluating platform trust is designed. At last, we give the security analysis about this model.

2 Relate Work

The issues, for evaluating and measuring in trust relationship between resources, have been the hot topic for researching in security. The article [3] designed an Extensible Trust Evaluation model for Cloud computing environments. This model evaluated the trust relationship directly and recommended in the two variables, time variable and spatial variable. Then the paper gave the algorithm for calculating the direct trust, recommended trust and dynamic trust. This model can provide the fault-tolerant and robustness for resources in cloud computing. The article [4] analyzed dynamic and adaptation of nodes in the Ad Hoc Networks, and established a trust evaluating model. The trust relationship in this model was described by a weighed directed graph, and measured by the theory of semirings. The nodes’ robustness and defense were proved by this theory. The article [5] proposed a job scheduling model based on the trust mechanism. By the Bayesian Cognitive Approach, the reliability of nodes in cloud computing was evaluated. Underpinned by reliability, it designed the job scheduling algorithm in cloud computing, and proved its security and capability. The article [6] designed a recommended system prototype FuzzyTrust based on reputation evaluating in the P2P environment. The prototypes adopt the fuzzy logic reasoning for calculating the local trust rating and global reputation. It can solve some problems in the Peer’s trust measurement, such as uncertainty, fuzziness and imperfection. The article [7] gave the definition of dynamic trust with entities in distrusted environment, and analyzed some classical models for evaluating trust. The model included three submodel. The dynamic evaluating model can provide positive and negative feedback. The vector-based trust evaluating model contained the time factor, history factor and trust factor. And the entropy-based dynamic trust evaluating model measured uncertainty. This paper concluded these algorithms and models about dynamic trust evaluating and estimated the performance with 17 indicators, such as the capability for dynamic evaluating, the adaptation in the context, the capability for risk evaluating.

The research about trust evaluation and measurement has been spread from the traditional and static trust evaluating to the dynamic trust evaluating, and from the centralized context to the distributed context. For the combined and flexible cloud computing, how to estimate the trust relationship with resources and reduce the leakage risk of resources’ sensitive information is our main content for researching.
3 Trusted-based Cloud Computing

The definition for trust in cloud computing is a difficult work, since the complex framework of cloud services. In this section, by analysis the trust issues in cloud computing, we propose a 3-layer trust framework for evaluating cloud services.

3.1 Trusted computing

The Trusted Computing (TC) was proposed by the Trusted Computing Group (TCG) for optimizing the concept and standard about information security in heterogeneous network computing environment [8, 9]. The TCG provided the uniform security depict for the hardware and software manufactures, designed the product technical and evaluating standard in trust computing gradually, and impelled the development of trusted computing. Enforcing the trust management underpinned by the hardware products and operating system, the trusted computing extends the scope of the trust, and provides a ‘clean’ environment for the devices and applications. The Trusted Platform Module (TPM) is the core module in trusted computing. It is solidified in the ships, which have some Platform Configuration Registers (PCRs) for storing the configuration in system form boot to running. The PCRs can execute the two operations: reset and extend. The operation reset will occur at system offline, and extend can be done as follow:

\[ PCR_{new} = Hash(PCR_{old}||IntegrityMeasurement) \]

In the integrity attestation, the platform can decide current status to be trusted or not by comparing the system configuration in PCR register. However, the configuration in PCRs is stored as the binary information. The information has the risk to be leaked. For solving this problem, the researcher provides a trust attestation approach based on the security property [10, 11]. This approach has some advantages for protecting system security. Firstly, it reduced the exposing risk of sensitive information. Secondly, it can depict the privacy level by layered property. Thirdly, it kept the system status consistency in the updating and maintaining. In the end, the property-based attestation can underpin the policy design in access control system.

3.2 Security in trusted cloud computing

In the cloud computing, there are multi-layer structures for providing different security levels’ services. According to the depict for traditional security issue, we considered the property about cloud service’s security as follow.

Confidentiality

The most concerning focus for cloud service’s user is how to trust with the service’s provider. The data stored in the cloud and managed by the different administrators. The data’s confidentiality and context is weak for user. It needs the guarantee for protecting against unauthorized service’s access.

Integrity

The services provide verification for request from user correctly and integrally. The user can verify their data stored in the cloud whether the integrity has been changed or not.

Availability
It should leverage the balance between security and availability. The jobs’ efficiency is the main indicator for evaluating service’s availability. The proper cloud security model can minimize the system overhead in advisable security level.

**Privacy**

The sensitive data form users probably to be submitted to the data center. Meanwhile, the data will face to the complex context in data center without user’s concerning. It is crucial for protecting these data by hiding, distorting and encrypting.

The evaluation of trust relationship in cloud computing is effected largely by the subjective factor. We can define a group of trusted property for measuring the security of system or software. The property can attest the trust relationship with unknown subjects. In the other word, the subject can decide trust relationship with the unknown object by the result of property-based attestation.

### 3.3 Trusted cloud computing model

For evaluating trust relationship conveniently between resources in cloud computing, we propose a suitable trust evaluating model. Show as Fig. 1. In cloud computing, the resources provide services to application in the form of SPI (SaaS, PaaS & IaaS) layered model. As the similarly thinking, we construct the layered trust framework, which composed of platform trust, identity trust and behavior trust. The platform trust is the hardware’s satisfaction for security (include physical devices, visual machine monitor, visual machine and TPM). The identity trust verifies the access requests by resources’ access authorized relationship, and establishes the trust relation by this verification. The behavior trust is a dynamic trust measurement by evaluating of services’ behavior. Such a layered trust model obeys the natural law when we get trust relationship with a stranger. At first, we must make sure of the strange entity are located or grew in the verified environment. And then, according to the entity’s identity information, the authority right can be estimated. At last, while the entity is exciting in cloud computing, it should check the operation or action for building the trust relation. As the foundation of the layered trust framework, platform is the basic security guarantee in cloud computing. For measuring the platform trust effectively, Property-based attestation is proposed for evaluating trust relation.

### 4 Property-based Negotiation Platform Trust

In the trusted computing, property-based trust attestation can avoid the leakage of system configuration, enforce the expandability for system security verifying, and reduce the complexity of trust attestation in heterogeneous context. In this section, we design a platform attestation model by automated trust negotiation mechanism, and analysis the security property.

#### 4.1 Property-based attestation

Property-based platform trust attestation is based on the binary integrity attestation. The component property instead of the binary configuration to measure the trust relation.
Definition 1 Trust measurement $TRUST_i = SIGN_{AIK}(PCR_i, c)$, $c$ is the trust evaluating request, $PCR$ is the register of platform status in TPM, $AIK$ is for identifying the TPM.

Definition 2 The components’ set $C = \{c_1, c_2, c_3, \ldots, c_i, \ldots, c_m\}, m \in \mathbb{Z}^+.$

Definition 3 The property set $SP = \{SP_1, SP_2, SP_3, \ldots, SP_i, \ldots, SP_n\}, n \in \mathbb{Z}^+$, and $SP_k = \emptyset | \{sp_1, sp_2, \ldots, sp_j\}, n, j \in \mathbb{Z}^+, k \in [1, n].$

Definition 4 The property matching $SPMR = (SP, TRUST), SP \subseteq C^m \times S^m$ and $TRUST \subseteq \bigcup_{TRST, m, n} \mathbb{Z}^+.$

The property-based attestation needs the third part verify proxy to construct the safety verification channel between challenger and verifier. The process of verify shows as Fig. 2.

The verify process is started by challenger. Firstly, the verify proxy receives the request and the TPM’s information from challenger. It chooses the proper platform to verify by the component and property parameter. Secondly, the platform chooses the PCRs in TPM by the attestation request from verify proxy. Then it sends the PCRs’ value and the log files SML back to the proxy. Thirdly, the proxy reconstructs the binary configuration by SML. In the end, by comparing $SP^*$ which generate by the reconstruction with the require $SP$, the trust relationship can be decided.

4.2 Trust negotiation model

The core component in the property-based attestation is the verify proxy. The main job of this proxy is attestation process, such as property analysis, PCR verify. In cloud computing, the
resource’s nodes are highly independent. It is difficult for distributing such a verify proxy in the global scope. Meanwhile, the centralized security service will be a bottleneck affected quality of service. Automates trust negotiation (ATN) mechanism [12, 13] is purposed by Winsborough etc. It can establish the relationship by certificates’ exchanging and policy negotiation. Moreover, this approach exchanges the certificate and policy under the other negotiated part’s security level, but without participation of the third part. This character makes this approach suitable for the distributed P2P environment.

Definition 5 Automated negotiation trust is composed by a five-tuple array.

\[ \text{ATN}_{\text{cloud}} = \{c, SP, SPMR(SP, \text{TRUST}), \text{Unlock}(SP_2, SP_1), \text{NegotiaType}\}, \text{includes two system variables, two operated functions and one controlled parameter.} \]

\( c \) and \( SP \) is the negotiating request and property set for building trust relation. The property set contains free unprotected property and sensitive locked property. \( SPMR(SP, \text{TRUST}) \) represents the satisfaction from request \( c \) to \( SP \). \( \text{Unlock}(SP_2, SP_1) \) means that property set \( SP_1 \) can be unlocked by property set \( SP_2 \). The locked property in \( SP_1 \) changed to be free unprotected. \( \text{NegotiaType} \) is the capability constrained parameter of ATN. It can adjust the capability by effective request of service’s user, which is from positive model to negative model.

The process for establishing the trust by property-based negotiation is shown as Fig. 3. It can be depicted as 6 steps as follow.

STEP 1. Verify platform \( A \) sends the trust request to platform \( B \) by security channel (assume that the communication channel is safe). The trust request includes the free unprotected properties \( SP_1 \) of platform \( A \).

STEP 2. Verify platform \( B \) generates trust computing attestation request \( c \) according to the property set \( SP_1 \).

STEP 3. The process of attestation evaluates PCRs’ value by \( c \), and returns results \( \text{TRUST}_i \) back to the property verify module.

STEP 4. The evaluating result \( \text{TRUST}_i \) is converted to the property set \( SP_2(SP_2 \subseteq SP_1) \) by property verifying. \( SP_2 \) will represent platform \( B \)’s negotiating certificates.

STEP 5. In negotiation policy module, \( \text{Unlock} \) operation will unlock the sensitive protected property in platform \( B \), which is activated by satisfying the \( SP_2 \) negotiating policy. Unlocked
property set is returned back to property verify module.

STEP 6. *SPMR* operation decides whether the trust between platform \( A \) and \( B \) can be established. If the current property can satisfy trust request \( c \), then it returns the success flag to platform \( A \), or returns to STEP 1 in platform \( A \) and continues negotiating process.

### 4.3 Security analysis

The approach for building trust relation by ATN mechanism is fit for evaluating and measuring the entities in cloud computing. By exposing security property gradually, the leakage risk of sensitive system configuration is mitigated. This section analysis the model’s security representation by cloud service’s security property mentioned at previous section.

**Confidentiality**

The user in cloud computing don’t sends the service’s request only, but should also provides the platform security property where they lived in by themselves. The security properties in one side in negotiating process are provided to the others. It can guarantee the platform where data will store or computing can be trusted by the data owner.

**Integrity**

When the platform’s configuration has been tampered, the trust measurement result \( TRUST_i \) and the log file SML should matched inconsistent, and then informs the user that the platform configuration changed. The platform trust relationship should discards and reconstructs the trust relationship of the two platforms.

**Availability**

Comparing the previous property-based attestation, the problem of security and capability bottleneck is solved by this model. Without the third part participating, entities can be communicated directly by their security properties.

**Privacy**

The bi-property can be locked by their privacy protection level. The locked property can be
unlocked only when they can be satisfied by the properties of the other negotiating part. This model provides a protected mechanism to system sensitive information.

5 Conclusion

For the distributed and elastic characters, the trust relationship between resources in cloud computing is hard to define. According to analysis the cloud service’s layered framework, a regulation of trust building in the two strange entities is disclosed. And along with this regulation, we propose a layered trust framework which is composed by platform trust, identity trust and behavior trust. By the ATN mechanism, we design a property-based platform trust verifying model. In the future work, we plan to extend the layered trust framework, and design the trust verifying model for identity trust layer and behavior trust layer. It will make the resources’ evaluation in cloud computing more accuracy and conveniently.

References