International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2014): 5.611

# Mutual Authentication Cloud Computing Platform based on TPM

**Lei Peng[1], Yanli Xiao[2]**

[1]College of Information Engineering, Taishan Medical University, Taian Shandong, China

[2]Department of Graduate, Taishan Medical University, Taian Shandong, China

**Abstract:** ***As cloud computing services appeared on the network in large numbers. The data and calculation of users are stored in the data center of cloud service provider, and of all kinds of resources are available for multiple users to share. Security gradually become an important issue in cloud computing. In order to ensure the security of cloud computing system and protect the users' data security and privacy, the identity authentication mechanism between users and cloud computing server must be established. Currently, the technology of trusted computing has become the hotspot in the field of information security. The core of trusted computing is embedded in the terminal platform trusted platform module (TPM). In this paper, the trusted computing technology is applied in cloud computing services. Mutual authentication scheme based on TPM cloud computing platform is proposed. In this scheme it realizes the identity authentication between the users and the cloud computing server. The session key are negotiated to be generated, at the same time the trusted status of the cloud computing server platform is verified.***

**Keywords:** cloud computing, trusted computing, trusted platform module, authentication

## 1. Introduction

Once the concept of cloud computing is put forward and get the extensive concern of the industry and the academia [1]. At the same time the security problem of cloud computing has become hotspot in the field of security, which is the biggest concern about cloud computing of the current domestic and international users. For cloud computing services, users' information is stored and processed in the cloud computing service center. If key information or privacy information lost or leaked, it will seriously affect the safety of the whole system [2]. Meanwhile to transmit information between the users and the server, it also needs to provide a reliable security measures to ensure safety. Then the identity authentication, which is the foundation of the whole security system, is one of the important mechanisms ensure the security of the cloud computing system [3,4].

Currently the trusted computing technology has become a new trend in the field of network information security. Based on trusted cloud computing platform, a kind of smart card password authentication scheme between users and cloud server has been proposed. On the one hand, under the cloud computing service environment, it provides security guarantee to the truth of cloud server and user identities, and helps the legitimate users to verify the trusted status of the cloud server. On the one hand, it protects the information interaction between the users and the cloud service platform through consultation to produce the final session key. Therefore, it can effectively solve the problem of identity authentication and information transmission between the users and the cloud server in the cloud computing.

In order to deal with the security problems in the process of identity authentication and data transmission, the trusted computing technology was applied to cloud computing services, and the cloud computing service platform model was constructed based on trusted platform module (TPM). Then in view of the present complicated situation of the cloud computing system, the trusted computing technology and the smart card password authentication method combined with the application in the cloud computing platform. In this paper, a mutual authentication scheme based on TPM cloud computing platform is proposed. It effectively solved the problem of identity authentication of both sides of the users and the cloud computing server in the cloud computing system.

## 2. Related works

### 2.1 Cloud computing

Cloud computing is the development of parallel computing, distributed computing, and grid computing. Popular, cloud computing is a kind of computing model which uses the Internet to access shared resource pool, such as computing facilities, storage devices, applications, etc., anytime, anywhere, and on demand [5]. The characteristics of cloud computing are as follows.

- On-demand service: to provide users with all kinds of resources in the form of services, and according to the resource usage to bill.
- Widely to access: users can use a variety of terminal equipment, such as personal computers, smart phones, etc., to access the cloud computing services through the Internet.
- Resource virtualization: virtualization technology is used to provide storage, computing and network resources to users.
- Scale elasticity: cloud computing has the attribute of high scalability. It can have tens of thousands of computer equipment, and provide to users with unprecedented computing power.
- High reliability and availability: automatically detects the failure nodes. Through the redundancy of data, it can provide high quality service, and ensures that the user can

access to the needed services anytime and anywhere [6].

Cloud computing has made great convenience for users and enterprises to use storage resources, software resources and computing resources. One of the biggest challenges or the biggest problems for cloud computing is security. There are various potential risks and security problems for cloud computing. The basic concept or define of cloud security is blurred [6]. Cloud computing security white paper lists the security measures, such as supplier management, technical standards, data portability, data confidentiality and privacy, access control, compliance, and security service level, etc. [7], and summarizes the three types of cloud computing security elements: infrastructure, identity, and information. For cloud computing security risks, users most concerned for data security and privacy issues. In the cloud computing model, the users' data and calculation is stored and operated on the cloud service provider's data center. All kinds of resources in the data center are shared to multiple users. For the purpose of the safety of system and response to the hacker's attack, the cloud computing service provider seldom discloses the internal information of the cloud. The cloud computing users do not have the data control and are lack of necessary right to know the internal data information of the cloud. The trust issues between the cloud computing service provider and the users become a huge obstacle of the development of cloud computing. Therefore, in order to ensure the safety of cloud computing system, strong authentication mechanism between the users and the cloud server must be established. At present, the research of fusion of cloud security and trusted computing technology will become the important direction in the cloud security domain to solve the problem of identity authentication [8].

The whole system structure of cloud computing can be seen as a series of services. It includes infrastructure as a service (IaaS), platform as a service (PaaS), and platform as a service (SaaS) [9].

- IaaS: the entire infrastructure as a service is provided to users. IaaS provides not only including the virtualized computing resources and storage resources, also includes the network bandwidth and other resources while the users access the service. This layer services typically have the Amazon elastic cloud (Amazon EC2) and Apache Hadoop open source project.
- PaaS: platform as a service layer is built on infrastructure as service. It can be thought of as the core layer of the cloud computing system to provide the service, and mainly includes the parallel program design and development environment, the structured huge amounts of data distributed storage management system, huge amounts of data distributed file system, and other system management tools, such as deployment, allocation, monitoring management, security management, distributed concurrency control of the cloud computing system resources. For this layer the representative platforms are Google App Engine and Microsoft Azure.
- SaaS: it is based on the cloud computing platform developed by the application. It provides a simple software application service for users. SaaS makes the desktop application to be embodied in the Internet and realizes the application of ubiquitous access.

### 2.2 Trusted computing technology

The basic idea of trusted computing is first to establish a trusted root in the computer system, and build a trust chain, each level measurement certification for themselves, each level trust for themselves. The trust relationship is expanded to the whole computer system to ensure the trusted computer system [10-12]. The so-called trust means that the services provided by a computer system are reliable, available, and information and behavior are safe. Correspondingly, the trusted computing platform is able to provide a trusted computing service computer software and hardware of the entity. It can provide system reliability, availability, security of information and behavior [13].

The core of trusted computing technology is embedded in the terminal platform trusted platform module. TPM provides password support and certain protect storage capabilities. It can provide different trusted mechanism and securities features with hardware protection, and also provide the foundation for measurement and verification platform trusted attributes, namely the integrity. TPM is the trusted root of the trusted computing platform [14]. The TPM architecture includes I/O control, stable storage, platform configuration register, certification identity key, the program code, engineering, random number generator, SHA-1 engine, RSA engine, key generation, and optional input.

The Storage Root Key (SRK) is locates in the root of TPM. One trusted platform module owner only has one SRK. The Endorsement Key (EK), unreadable for outside, is written in the TPM chip by the manufacturer. SRK and EK are on behalf of the initial level of TPM trust. Generally, EK not in key layer, and the Attestation Identity Key (AIK) is used to instead of EK, so that EK can be better protected.

Storage Root Key (SRK) is a common basis to create key. It can produce two types of user level key: Migratable Storage Key (MSK) and Non-Migratable Storage Key (NMSK). The first key is created on one platform, but can be used normally on other platforms. The second key is created on a platform, and can only be used on this platform, that can be seen as the key is the only binding together with the hardware. MSK can derive and manage another kind of migration key named signature key (RSA key type, the length is not more than 2048 bit), which is used for the data needed signature. The MSK can also provide storage for the migration storage keys encapsulated by it. For NMSK, in addition to being able to generate the corresponding migration storage keys, signature key, it also can produce transferable storage or signing keys. Therefore the latter is relatively more flexible to use. Identity Authentication Key (AIK) belongs to the migration types, and it can be used to other key's signature [15].

TPM has the ability to prove local platform configuration information for remote authenticator, i.e. Remote Attestation (RA). The main process is proved the platform credibility through the integrity verification. TPM internal has a set of Platform Configuration Register (PCR), which stores all of the

integrity measurement information of the platform. When the system is power on, the PCR is initialized; TPM measures the hardware and the software components of the platform; the corresponding hash value is written into the platform configuration register PCR. In the process of measuring platform hardware and software components, events are created and recorded in Stored Measurement Log (SML). The values of PCR and SML are together to prove the status of the platform to the remote authenticator. In terms of guarantee measurements of trusted, using the identity key (private EK) to sign the platform integrity measurement result. If the verifier has the public EK of the trusted computing platform, he can get the result of the integrity measurement, and determine the status of the trusted computing platform.

## 3. Mutual authentication based on TPM cloud computing platform

### 3.1 TPM cloud computing platform

The core of trusted computing technology is embedded in the terminal trusted platform module. TPM provides trust root for all kinds of computing platform, and provides hardware security for various trusted mechanism and security features. TPM is foundation of measuring and verifying the trusted attributes of platform. The trusted computing technology is a hotspot in the field of network information security. The trusted computing technology is introduced into IaaS of cloud computing system. Combining the trusted platform module with cloud computing nodes, a cloud computing service platform is built based on TPM, and a trusted execution environment is formed [16-19].

Identity authentication is the important mechanism for realizing cloud services platform security system, and is the foundation of the whole security system. It provides security guarantee to the truth of the user identity of cloud service platform. Compared with traditional security mechanism, it has better security and privacy using the TPM authentication. TPM seals the primary key, which is unique, in a non-invasive hardware. A trusted platform module has only one storage key, which lies in the root of the TPM key management. Server can take advantage of the hardware architecture of trusted platform model to create a public-private key instance (PK, SK). Such keys are the derived keys of the root storage key, and are specific on the platform hardware and server itself. From the system powers up to the execution environment is built, the integrity measurement information, such as the corresponding hash values of TPM measurement platform hardware and software components, stores in a set of platform configuration register of TPM. At the same time, Events are built and recorded in the stored measurement log. Stored and recorded in the measurement at the same time create event Log. The values of PCR and SML are used together to prove the state of the platform to the remote authentication.

As shown in Fig. 1, The TPM cloud computing platform architecture is based on the IaaS model. It includes Cloud Management (CM), Trusted Node (TN), and trusted coordinator (TC). CM provides and manages cloud services. TN prevents internal intruders to spy out or tamper with the internal data. TC manages trusted nodes list. In the TPM cloud computing platform model, we assume that an external trust entity carrying the TC, and safely updated and provide to TC the node set information, which is in the scope of IaaS, and trusted facilities configuration. The system administrators of IaaS have not permission to tamper with the internal information of TC.

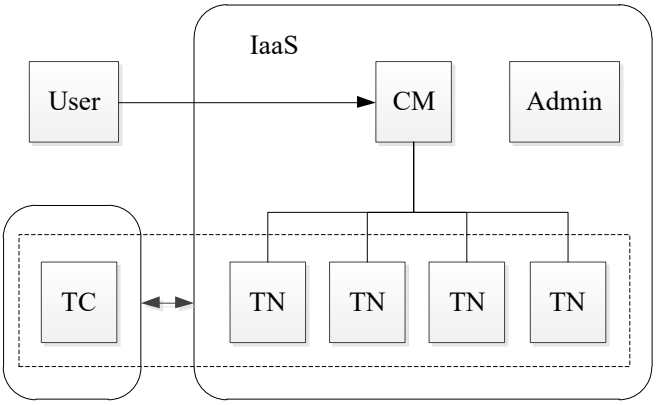


**Figure 1:** The TPM cloud computing platform architecture

The main function of TC is to manage the TPM trusted computing nodes. TC manages trusted nodes of Virtual Machine (VM) dynamically. For each compute node within the scope of security, the trusted service nodes contained TPM verify their identity to TC through endorsement key and Measurement List (ML). The public key $PK_N$ denotes the TPM computing node, and $ML_N$ denotes the expected measurement list. Some attributes of TC such as $PK_{TC}$ and $ML_{TC}$ open to the public safely. $ML_N$ and $ML_{TC}$ made clear that the authenticators should check the specification of the configuration, when verifying on the compute nodes TN and TC running on the platform. $SK_N$ and $SK_{TC}$ are the private keys respectively.

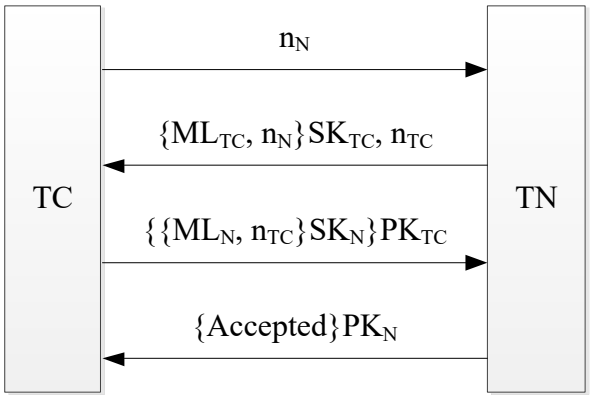


**Figure 2:** Registration of the trusted nodes

In order to gain trust, the computing nodes must register as shown in Fig. 2. First, TN asks TC for validation, to avoid the fake. TN sends a random number $n_N$ to TC, and TC responses the boot list $ML_{TC}$ After $PK_{TC}$ encrypted and the received value of $n_N$. If $ML_{TC}$ consistent with the expected structure, it shows that the TC can be trusted. Accordingly, the TC returns a random number $n_{TC}$ to validate whether the TN nodes can be trusted and conform to the expected configuration. If both validate successful, send a message to confirm trust the node.

If both are successful verification, send a message to confirm that the nodes can be trusted. If verification is passed, the TC will add the computing nodes to the trusted list. When the cloud users have related tasks and requirements, TC makes sure that the computing nodes are in the trusted list. Finally, the TPM cloud computing platform as a whole provides various kinds of cloud computing services through cloud management.

### 3.2 The basic flow of authentication

Authentication protocol is essential to the remote user login system. In the early， dynamic password authentication protocol is indispensable for the remote user login system, and is widely used in various kinds of remote login system. With the development of authentication protocol, now the remote user login system is generally divided into four stages.

- Registration stage: the user provides identity information and password to the server for login, and registers as a legitimate user of the system. The system set related secret parameters or generate the key.
- Login stage: the user inputs password, and submits the login request and login information.
- Validation stage: server authenticates the user legitimacy. After verification, the users get the bidirectional authentication information, and confirm the server status.
- Password change stage: subsequently in the interaction process, user can apply to change the login password.

With the development of identity authentication protocol, the corresponding target about the safety of authentication protocol gradually perfect, also get more and more of the attack. Generally, authentication protocol attack includes offline password guessing attacks, fake attacks, theft proof attacks, denial of service attacks, replay attacks and so on.

Desired mutual authentication scheme should satisfy certain safety design goals, so as to meet the needs of the application and effective resistance against the attack of smart card password authentication scheme. In cloud computing network environment, the identity authentication scheme faces many security threats, common type of attack is as follows: denial of service attack, replay attack, camouflage attack, smart card lost attack, password guessing attack, internal attack, verification value theft attack, and parallel session attack. Therefore, under the cloud computing network environment, the identity authentication scheme should provide users and cloud server platform mutual authentication, and when the scheme is performed, legitimate users and the cloud server can mutual authentication of each other's identity.

### 3.3 Trusted mutual authentication

In this paper, the solution scenario model is shown in Fig. 3. The users, cloud server platform (TPM), and Certificate Authority (CA) can access to each other in the Internet. At first the users registered in the cloud server platform. After login through the client, they get the smart card and send access request to the cloud server. The cloud server and the users have finished mutual authentication. CA is responsible for strengthening the identity of cloud server platform (TPM) and the public key management, and realizes the binding of cloud server platform identity and public key. The users who owned the smart card can query request to CA, and verify whether the received public key and the identity of the cloud server platform are consistent.

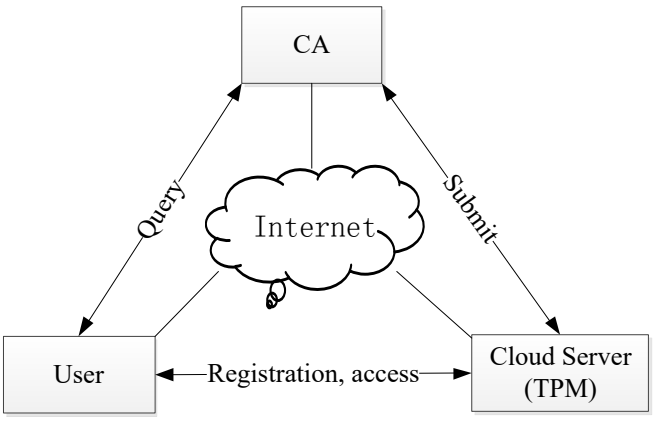


**Figure 3:** Trusted mutual authentication model

The basic idea of the schema is as follows:

- User applies for registration to the cloud server. Then the cloud server issued by a smart card to the user security, and some necessary information is stored in the smart card.
- User inserts the smart card, and enters his ID and password, so the smart card authenticates the user ID.
- User ID is verified through the smart card, and the smart card sends some operation results, which running through the stored information for certain operations, to the cloud server.
- Through the information in the smart card issued as the user registered, the cloud server judges the message user send and authenticates user ID. Then the cloud server takes advantage of the characteristics of TPM for certain operations, and sends them back to the user.
- According to the received information and the message in the smart card, user verifies the identity of the cloud server, and further completes the cloud server platform integrity verification.
- In the interaction process, both sides talks things over to generate the session key $K_{US}$.

Users who hold smart card request access to the cloud server. The implementation process of the plan includes three stages, such as registration, login authentication, and password change. Assume that the user terminal platform is trusted, and in the stage of registration the behaviors of the users and cloud service providers are honesty and kindness.

## 4. Conclusion

This paper presented cloud computing and trusted computing technology, and analyzed the characteristics of the trusted platform module. We puts forward that the TPM is applied to cloud computing services security system. For the security problem of authentication for cloud computing, build a trusted cloud computing platform based on TPM. It effectively solved

the problem of identity authentication of both sides of the users and the cloud computing server in the cloud computing system.

## References

[1] Armbrust, Michael, et al. "A view of cloud computing." Communications of the ACM 53.4 (2010): 50-58.
[2] Feng, Deng-Guo, et al. "Study on cloud computing security." Journal of software 22.1 (2011): 71-83.
[3] Zissis, Dimitrios, and Dimitrios Lekkas. "Addressing cloud computing security issues." Future Generation computer systems 28.3 (2012): 583-592.
[4] Santos, Nuno, Krishna P. Gummadi, and Rodrigo Rodrigues. "Towards trusted cloud computing." Proceedings of the 2009 conference on Hot topics in cloud computing. 2009.
[5] Mell, Peter, and Tim Grance. "The NIST definition of cloud computing." National Institute of Standards and Technology 53.6 (2009): 50.
[6] Subashini, Subashini, and V. Kavitha. "A survey on security issues in service delivery models of cloud computing." Journal of network and computer applications 34.1 (2011): 1-11.
[7] Grobauer, Bernd, Tobias Walloschek, and Elmar Stöcker. "Understanding cloud computing vulnerabilities." Security & privacy, IEEE 9.2 (2011): 50-57.
[8] Subashini, Subashini, and V. Kavitha. "A survey on security issues in service delivery models of cloud computing." Journal of network and computer applications 34.1 (2011): 1-11.
[9] Jadeja, Yaju, and Kavan Modi. "Cloud computing-concepts, architecture and challenges." Computing, Electronics and Electrical Technologies (ICCEET), 2012 International Conference on. IEEE, 2012.
[10] Dengguo, Feng, et al. "Research on trusted computing technology." Journal of Computer Research and Development 48.8 (2011): 1332-1349.
[11] Huang, Tao, et al. "A Method for Trusted Usage Control over Digital Contents Based on Cloud Computing." International Journal of Digital Content Technology & Its Applications 7.4 (2013): 795-802.
[12] Santos, Nuno, et al. "Policy-Sealed Data: A New Abstraction for Building Trusted Cloud Services." USENIX Security Symposium. 2012.
[13] Pearson, Siani. "Trusted identities on a trusted computing platform." U.S. Patent No. 8,370,631. 5 Feb. 2013.
[14] Mao, Wenbo, et al. "Software trusted computing base." U.S. Patent No. 8,176,336. 8 May 2012.
[15] Guidry, David, et al. "A Trusted Computing Architecture for Secure Substation Automation." Critical Information Infrastructures Security. Springer Berlin Heidelberg, 2013. 130-142.
[16] Yang, Li, Jian-Feng Ma, and Qi Jiang. "Mutual Authentication Scheme with Smart Cards and Password under Trusted Computing." IJ Network Security 14.3 (2012): 156-163.
[17] Patidar, Kailash, et al. "Integrating the trusted computing platform into the security of cloud computing system." International Journal of Advanced Research in Computer Science and Software Engineering, ISSN 2277 (2012).
[18] Ryan, Mark D. "Cloud computing security: The scientific challenge, and a survey of solutions." Journal of Systems and Software 86.9 (2013): 2263-2268.
[19] Bugiel, Sven, et al. "Twin clouds: An architecture for secure cloud computing." Workshop on Cryptography and Security in Clouds (WCSC 2011). 2011.

## Author Profile

**Lei Peng** received the M.S. degree in Software Engineering from Beijing Institute of Technology in 2004. Now he is an associate professor in the College of Information Engineering, Taishan Medical University. His current research interests include cloud computing and trusted computing.

**Yanli Xiao** received the M.S. degrees in Shandong University in 2010. Now she is a lecturer in the Department of Graduate, Taishan Medical University. Her current research interest is cloud computing.

**Foundation Items:** Shandong Provincial Science and Technology Development Program, China (No. 2014GGX101020); Safe Production Major Accident Prevention Key Technology Program, China (No. shandong-0021-2015AQ)