National Conference on “Advanced Technologies in Computing and Networking”-ATCON-2015
Special Issue of International Journal of Electronics, Communication & Soft Computing Science and Engineering, ISSN: 2277-9477

# Study of Security Platform Framework in Cloud Computing

**Anuradha R. Deshmukh** **Radhika M. Kharode**

*Abstract* — **Cloud computing is the rapidly evolved technology with new aspects and capabilities. It has highly virtualized and standardized infrastructures and can give more efficient and application management. The data can be stored in the cloud system and the user can use the data in any time and in any here. The cloud computing can guarantee the data security and the user do not protect the data by himself again. So the cloud computing must ensure the security of data stored in the cloud system. In this paper explains the security platform framework in cloud computing. This paper also explains, future of security in cloud computing.**

*Key Words* — **Cloud computing, Security platform framework in cloud computing, Future of security in cloud computing.**

## I. INTRODUCTION

Highlight a section that you want to designate with a certain Cloud computing has a very fast pace of development and shows good prospects and great potential. Cloud computing is based on five attributes, multitendancy(shared resources),massive scalability, elasticity, pay as you go and self providing resources. And IT environment requires a specific set of characteristics to enable the remote provisioning of scalable and measured IT resources in an effective manner. These characteristics need to exist to a meaningful extent for the IT environment to be considered an effective cloud. Cloud providers and cloud consumers can assess these characteristics individually and collectively to measure the value offering of a given cloud platform. Although cloud-based services and IT resources will inherit and exhibit individual characteristics to varying extents, usually the greater the degree to which they are supported and utilized, the greater the resulting value proposition. It is based on the network and has the format of service for the consumer. The cloud computing system provides the service for the user and has the character of high scalability and reliability. The resource in the cloud system is transparent for the application and the user do not know the place of the resource. The cloud computing is on-demand service and it gives computing capabilities as needed automatically. The cloud computing is related to many areas of information management and services. The data security becomes more prominent than the traditional network because the data in the cloud computing environment is greatly dependent on the network and server. Hence Security is the important factor when using cloud computing at all levels i.e. in Infrastructure as a service(Iaas),Platform as a service( Paas), Software as a service(Saas).Security is the significant task with a lot of complexity and it is just important for customer to evaluate thoroughly as the traditional aspect of infrastructure security. Cloud computing security is the set of control-based technologies and policies designed to adhere to regulatory compliance rules and protect information, data applications and infrastructure associated with cloud computing use. Cloud computing security is the set of control-based technologies and policies designed to adhere to regulatory compliance rules and protect information, data applications and infrastructure associated with cloud computing use. Cloud Computing is a paradigm that focuses on sharing data and computations over a scalable network of nodes. Cloud Computing is a paradigm that focuses on sharing data and computations over a scalable network of nodes.

## II. THE SECURITY FRAMEWORK OF CLOUD PLATFORM

### A. *Security framework of cloud computing platform*

The security framework of cloud computing platform should guarantee the confidentiality, integrity, no repudiation, availability and reliability of the data.

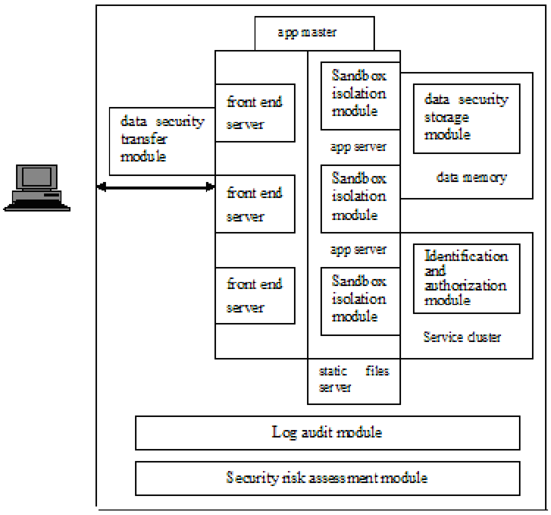

Fig 1. Security framework of cloud computing platform

The security framework of cloud computing platform is mainly comprised of the following modules: data security transfer module, identification and authorization module, sandbox isolation module, data security storage module, log audit module and security risk assessment module.

### *B. The operation process of security framework*

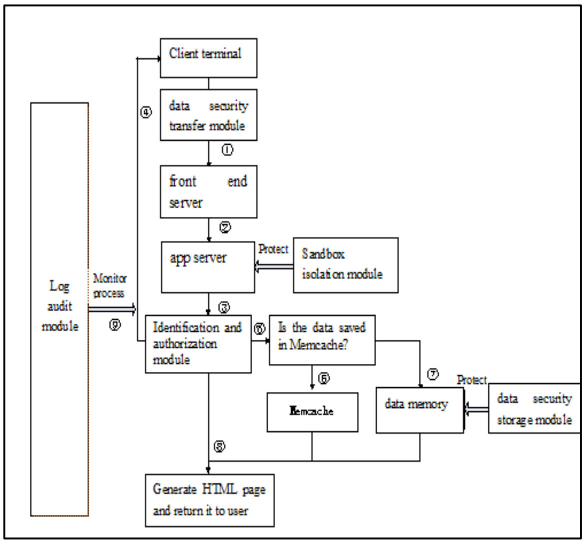
Client terminal
data security transfer module
①
front end server
②
app server
Protect
Sandbox isolation module
③
Log audit module
Monitor process
⑨
④
Identification and authorization module
⑤
Is the data saved in Memcache?
⑥
Memcache
⑦
Protect
data memory
data security storage module
⑧
Generate HTML page and return it to user

Fig 2. Cloud platform security framework operation process

See the operation process of the whole security framework in fig 2.

• Before the client issues an access request through client terminal to the platform, the client terminal and the front end server in platform establish a safe connection with the support of data security transfer module.

• The client access request is transferred to the front end server in platform by the safe connection so that the front end server can take charge of the load information collected by the app master and transfer the request to the void app server.

• The app server receives the client access request, and then the identification and authorization module identify and authorize the user profile that send the request.

• Once failed the user profile identification or authorization, the app server stops the request process and response an invalid identification message to the user.

• Once passed the user profile identification or authorization, the app server uses the relevant application program, processes the request under the restriction of sandbox isolation module, and consults if the data required by the processed request is stored in the Memcache of service cluster.

• If the data is stored in the Memcache of service cluster, the app server uses the data directly to make the process.

• If the data isn't stored in the Memcache of service cluster, the data security storage module obtains the data from the data memory.

• The app server processes the collected data, generates the relevant HTML response page, and returns it to the user.

• The log audit module monitors the whole process, sends alert message and executes the relevant preventive measures in case of abnormal situation.

Moreover, the security risk assessment module validates the security of the platform to avoid or reduce platform risk.

As consumers transition their applications and data to use cloud computing, it is critically important that the level of security provided in the cloud environment be equal to or better than the security provided by their traditional IT environment. Failure to ensure appropriate security protection could ultimately result in higher costs and potential loss of business thus eliminating any of the potential benefits of cloud computing. Internal network security differs from external network security in that we postulate that any attackers have already made it through the external defenses, either via an attack or, more commonly, because the attackers are legitimately authorized for a different part of the network. After a user is allowed access to a portion of the cloud service provider's network, the provider has a number of additional responsibilities with respect to internal network security.

## III. SECURITY PROBLEMS

The main security problems include data security, user data privacy protection, cloud computing platform stability and cloud computing administration. Cloud computing is a technology evolution of the widespread adoption of virtualization, service oriented architecture and utility computing. Over the Internet and it includes the applications, platform and services. The data resource storage and operation and network transform also deals with the cloud system. The key data resource and privacy data are very import for the user. The cloud must provide data control system for the user. The data security audit also can be deployed in the cloud system. Data moving to any authorized place you need it, in a form that any authorized application can use it, by any authorized user, on any authorized device.

In the cloud computing, the cloud provider system has many users in a dynamic response to changing service needs. Cloud computing storage security is primarily related to data storage isolation, storage place, data recovery and data long term survivability. Once the data is stored in the cloud, the control of the data is transferred to the hands of cloud computing providers. Some unscrupulous businesses can get the customer privacy information by unfair means which is easier from the customer. The web service has many security mechanisms such as WS-Security, WS-Reliability, WS-Trust, WS-Authorization, and WS-Secure Conversation.

## IV.THE FUTURE OF SECURITY IN CLOUD COMPUTING

1) Infrastructure security-In future identity management should be doped to address the interrelationships between systems, services and people. As inter cloud means cloud-to-cloud

communications come into existence and this is only on customers’ demands these relationships will take on even greater urgency.

2) Data security and storage- As cloud computing have nature of multitenancy and volume of data likely to be put in the cloud, data security capabilities are important for the future of cloud computing. Because of that predicate encryption are underway to limit the amount of data that can be decrypted for processing in the cloud.

3) Identity and access management-In the era of business consolidation where mergers and acquisitions are the norm, identity and access management solutions will become dynamic and flexible to meet the needs of merged corporate entity or divested entities. The cloud based identity and access process anchored on trusted relationships between domains will obviate the need for any major architectural or costly implementations to reflect the changed access landscape and support new entitlement requirements.

4) Security management-In the future the standard organizations such as ISO,World Wide Web Consortium(W3C),Internet Engineering Task Force(IETF) initiate new efforts to standardize management protocols that interoperate with many clouds. To accelerate enterprise cloud adoption, it is imperative that cloud management standards are created that will supported by cloud service provider (CPS) and facilitate seamless interoperability’s across disparate clouds. Also these standards will help to create an ecosystem and service providers that provide customers with choice, flexibility and greater agility by the way of automation.

5) Privacy- It is essential for the CPS to understand international privacy laws to comprehend how data can be transferred from one part of the word to the other. This was challenge during the globalization of the world economy, for security purpose it will beneficial to create a global privacy standard that will provide consistency across jurisdictions. Such standards will help define the way business grows cloud computing.

## Conclusion

A greater transparency alone will not be sufficient for improving the levels of security that are needed in cloud computing. The cloud computing platform still has many problems to be solved, among which the security is the hardest obstruction to come over. This paper studies security platform framework, problem associated with security and future of security in cloud computing. The platform security framework is significant for establishing the standard of security strategy which is beneficial to maintain security and privacy in cloud computing very well.

## References

[1] Xu Xiaoping, Yan Junhu, Research on Cloud Computing Security Platform, Fourth International Conference on Computational and Information Sciences 2012

[2] Wentao Liu, Research on Cloud Computing Security Problem and Strategy,

[3] Cloud Security Alliance:http://www.cloudsecurityalliance.org/

[4] Refference book of cloud security and privacy by Tim Mather, Subra kumaraswamy and shahed latif.

[5] http://searchdatamanagement.techtarget.com/definition/compliance.

[6] Google App Engine, http://appengine.google.com

[7] Tim Mather, Cloud security and Privacy, Subra Kumaraswamy, Shahed Latif, 2011, pp.260