Cloud Computing and the Essentials of Security Management

Zhong Hua, Xin Wang

School of Electronic Information Engineering, Tianjin University, Tianjin, China
Email: pyhiloveyou@126.com

Received 10 April 2016; accepted 27 May 2016; published 30 May 2016

Abstract

Cloud Computing has made software more attractive as a service and transformed a large part of IT industry. At present, cloud computing is a popular topic for conferences and magazines. The unique attribute of cloud computing poses a lot of security risks in the cloud environment. In this paper, we present the essentials of Security Management of the cloud computing. The management contains a distributed authentication method and device based on the cloud platform. The speed of user authentication of this method is fast. At the same time, this method and device has resolved the security problem of the cloud computing platform commendably.

Keywords

Cloud Computing, Distributed Authentication, Security, Cloud Platform

Subject Areas: **Information and Communication, Security, Privacy, and Trust**

1. Introduction

The world we live in produces huge amount of data continuously every day. This can lead to the data resource storage of the data center. Cloud computing adds capabilities dynamically without investing new infrastructure and increases the computing capacity [1]. Cloud computing offers many benefits such as lower cost, rapid provisioning, fast deployment, rapid re-constitution of services, etc. The application software and database has been moved to the large data centers. Unfortunately, the management of services and data is not reliable. At the meanwhile, the target of cloud computing is to provide better utilization of software and data using virtualization technology [2]. The unique attribute poses a lot of security risks in the cloud environment.

In order to enhance the security and save the resource of the cloud platform, in this paper, we present the essentials of Security Management of the cloud computing. The management contains a distributed authentication method and device based on the cloud platform. The management is based on the Embedded Cloud Branch Server which has multiple cloud server as the node branch. The Embedded Cloud Branch Server is connected

How to cite this paper: Hua, Z. and Wang, X. (2016) Cloud Computing and the Essentials of Security Management. *Open Access Library Journal*, **3**: e2618. http://dx.doi.org/10.4236/oalib.1102618

with the central server through the network.

2. The Characteristic of Cloud Computing Platform

The cloud computing platform refers to hardware and software which in the data centers and the applications transmitted as services through the Internet [3]. The cloud computing platform has been referred to as SaaS (Software as a Service), IaaS (Infrastructure as a Service) and PaaS (Platform as a Service) as shown in **Figure 1**.

The cloud computing is the combination of utility computing and SaaS. The public cloud refer to the cloud is made obtainable to the general public [4]. The service being sold is called utility computing. The private cloud refers to the internal data center of a business and cannot be available to the general public. The individuals can be providers or users of utility computing and SaaS.

There are three new fields in cloud computing from pricing point and hardware provisioning of views.

1) The ability to pay for use of computing resources and release them on a short-term basis as needed.

2) The ability to get infinite computing resources available quickly enough to start load surges.

3) The ability to let company to start small and increase hardware resource when needed.

The cloud computing platform uses SaaS, PaaS angulad IaaS as the transmission models to delivery different types of services to the end users. The IaaS is the base of the cloud services and PaaS and SaaS build on it. The service model places a varied level of security necessity in the cloud surroundings.

A recent survey by Cloud Security Alliance (CSA) & IEEE indicates that enterprises across sectors are eager to adopt cloud computing but that security are needed both to accelerate cloud adoption on a wide scale and to respond to regulatory drivers [5].

SaaS is a software arrangement model where application can be hosted remotely by the service provider or the application and made obtainable to the client through the internet.

IaaS transforms the method developer arrange their applications. IaaS abstracts the hardware below it and permit user to spend infrastructure like a services [6].

PaaS is the layer which is live above IaaS on the abstract and stacks away everything upper to the middleware and OS [7]. This provides a combine set of developers circumstance which the developers could develop their applications without mention what is going on below the services.

In this paper, we introduce a Cloud platform which structure is the integration of SaaS, IaaS and PaaS. In today's cloud computing environment, IaaS, is mainstream, not only Amazon EC2 but also Linode and Joyent both have a place. With the emerge of Google App Engine, sales force force.com and Microsoft Windows azure, the

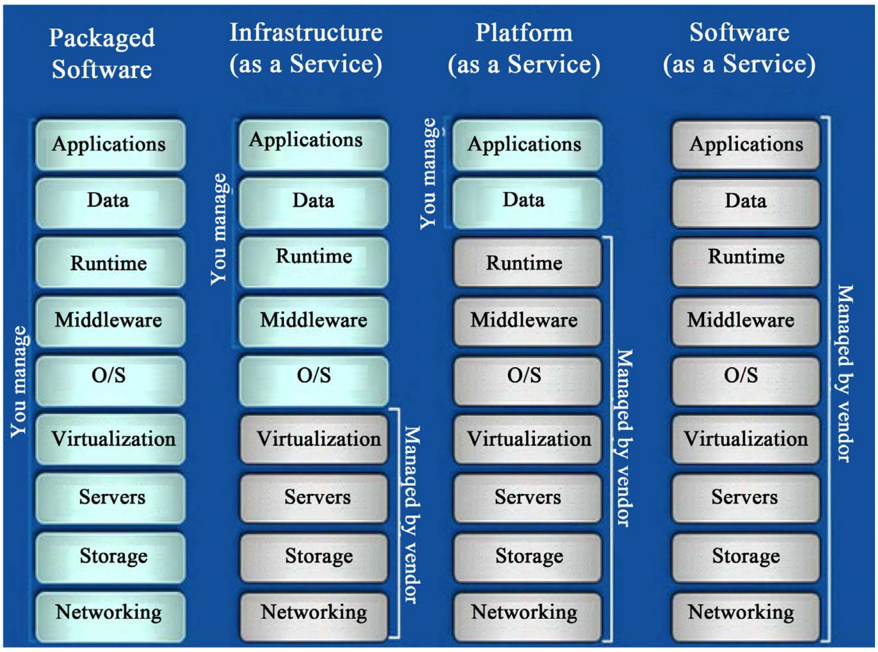

Figure 1. Cloud structure.

PAAS platform begin to play an important role in the cloud platforms [8]. The Micro Cloud has high integration rate which can bring economy to developers and can solve challenges such as general and support to the application, we think the Micro Cloud can make benefits for the developer of cloud platform.

3. A Distributed Security Authentication Method Based on the MICRO Cloud

The advantages of the distributed security authentication method based on the Micro Cloud have are listed as below:

1) The user's authentication speed is fast. Using the signature and authentication to solve the problem of security, it can also register to the Embedded Cloud Branch Server in case the Internet failure.

2) The user's database is stored in the central server not in the Embedded Cloud Branch Server. Reduce the amount of Micro cloud platform, improving the processing efficiency of Micro cloud platform.

3) The methods of the user's registration are flexible. The user register can not only through the Embedded Cloud Branch Server but also through the Internet.

a) *Set up*

Our Cloud platform is based on the cloud branch server and taking multiple cloud branch servers as nodes. The cloud branch server is connected to the central server through the network.

b) *Register and Login in to the Embedded Cloud Branch Server*

The users register and login in to the Embedded Cloud Branch Server by the cloud branch server, and the cloud branch server receives the user's registration information in real time. The Embedded Cloud Branch Server receives the user's name and password etc. After verifying the registration information, the Embedded Cloud Branch Server generates the encrypted database file which contains the user's information. At mean time the Embedded Cloud Branch Server removes all the unencrypted user's information.

c) *Encrypt*

The Embedded Cloud Branch Server generates the encrypted registration file on the base of the user's register and login in information and uploads to the central server.

d) *Generate a HASH Signature File*

The central server receives the user's register's information from the Embedded Cloud Branch Server and store the information to the database, at the same time generating a HASH signature file containing all the user's information.

e) *Download Information to the Embedded Cloud Branch Server*

The central server download the HASH signature file which containing all user's information to the cloud branch server.

f) *Signature and Authentication to the Embedded Cloud Branch Server*

The user authenticates and login in to the Embedded Cloud Branch Server, Embedded Cloud Branch Server using HASH algorithm to signature and authenticate.

1) Signature

Let the data to be signature is equal to m, its digital abstract is H.

$$h = Hash(m)$$

Among them, Hash is the one-way hash algorithms, such as MD5, SHA-1.

Let p, q, d are the private data of signer, they all included in the private key SK; n, e are the public data of the signer, they are all included in the signer's public key PK, these data meet the following requirements:

$n = pq$, where $p \neq q$, q, p are the big prime number.

e, d $\in$ R Zn, and $e = d - 1$, $ed \equiv 1 \bmod(n)$, here

$$(n) = (p-1)(q-1)$$

Then use the signer's private key to encrypt h can get the signature value s.

$$s = E(x) = hd \bmod n$$

2) Authentication

Let the application to be authenticated is m', its digital abstract is h'

$$h' = Hash(m')$$

Assuming that has obtained the real public key of the signer, then using the open data *e* of the PK to decrypt and calculate, obtaining the restored digital abstract h''. Here, h'' is equivalent to *h*.

$$h'' = D(s) = se \bmod n$$

Comparing h'' with h'. If they are not same, then the authentication is failure.

a distributed SECURITY authentication DEVICE based on the cloud platform

The characters of the distributed security authentication devices based on the cloud platform contain central server and Embedded Cloud Branch Server.

The central server is used to receive the user's register's information from the Embedded Cloud Branch Server and store the information to the database, at the same time generating a HASH signature file containing all user's information. It contains database module, file generating module and network module.

The database module is used to receive the user's register's information from the Embedded Cloud Branch Server and store the information to the database.

The file generating module is used to generate a HASH signature file which containing all the user's information.

The network module is used to receive the new user's register's information from the Embedded Cloud Branch Server and send out a HASH signature file to the Embedded Cloud Branch Server.

The Embedded Cloud Branch Server is used for the users to login in, authentication and registration.

The user authentication module is used for login and authentication.

The user registration module is used to receive new user's register's information from the Embedded Cloud Branch Server.

The network module is used to upload new user's register's information to the central server and receive a HASH signature file from the central server.

The verification module is used to sign and verify take advantage of the HASH algorithm.

4. Conclusion

In this paper, we present the essentials of Security Management of the cloud computing. The management contains a distributed authentication method and device based on the cloud platform. The speed of user authentication of this method is fast. At the same time, this method and device has resolved the security problem of the cloud computing platform commendably.

References

[1] Subashini, S. and Kavitha, V. (2015) A survey on Security Issues in Service Delivery Models of Cloud Computing. *Journal of Network and Computer Applications*.

[2] Rohrer, F., Feleke, N., Zhang, Y.T., Nimley, K., Chitkushev, L. and Zlateva, T. Android Security Analysis and Protection in Finance and Healthcare. Boston University MET, Boston.

[3] Chen, D.L., Li, Z., Wang, Y., Zhao, L.F. and Zhang, D.J. (2013) The Main Technical Characteristics and Software Architecture of NGB SMARTTVOS. Radio and Television Information, National Academy of Broadcasting Science.

[4] NGB SMARTTVOS1.0 Version of Cooperation and Development. The Next Generation of Radio and Television (NGB) Intelligent Technology TV Operating System v1.0.0. The State Press and Publication Administration.

[5] GY/T267-2012. NGB Technical Specification of Terminal Middleware. The State Press and Publication Administration.

[6] Wang, M.M. and Zhu, Y.B. (2012) To Explore the Implementation Model and Techniques of Intelligent Television Terminal Security under NGB Environment. Radio and TV Technology. http://www.cqvip.com/qk/98109X/201310/

[7] Ning, H., Li, W., Wang, K. and Lei, M.Y. (2012) Research on Intelligent Terminal Security System. *Modern Telecommunication Technology*.

[8] National Academy of Broadcasting Science (2013) The Security Framework of NGB SMARTTVOS1.0 V1.2.20131224.