ENTERPRISE ADOPTION OF CLOUD COMPUTING: DATA SECURITY ACROSS NETWORKS

Y Lihan Kumar[1*], D V Krishna[2*], Dr. P Raja Prakash Rao[3*], K Sivarama Krishna[4*]

1. *M.Tech - CSE,TRREC*
2. *M.Tech - CSE,TRREC*
3. *Professor - CSE,TRREC*
4. *Assoc.Prof - CSE,TRREC*

Keywords:
Cloud computing, information security, Internet hacking, Server as a Server, long term evolution.

Abstract: *Abstract cloud computing has become one of the most significant issues in recent years. Those associative applications and services based on could computing are dramatically emerging. However, in order to enjoy the widely utilization of cloud computing through wired/wireless networking, providing sufficient assurance of information security such as confidentiality, authentication, non-repudiation, and integrity is the critical factor of success promotion. In this paper, a dynamic intrusion detection system for strengthening the proposed mechanism, numbers of intrusion detectors are dispatched on the whole topology of the networking system through multi-layers and multi-stages deployment. Those information security issues related with the application and service of cloud computing will be experimented and discussed. The experiments include the equipment security of the client side termination, the threats of web site and webpage, the detection and diagnosis and surveillance of intrusion, the access and security of database in the could side, the detection of system leakage and the monitor of real-time repairing process, the management of server system, the management of mobile e-commerce processing, and the integrated analysis of associated security information and issues. The goal of the proposed mechanism is not only focused on fined out some solutions, but also focused on develop some feasible information security techniques or products for the application demonstrate that the proposed mechanism does provide good performance for intrusion detection.*

1. INTRODUCTION

There are three common architecture for establishing the application of clouding computing such as server as a service (SaaS), platform as a service (paaS), and infrastructure as a service (IaaS) (5) (6) (7), In order toimplement the above application based on cloud computing, the assurance of information security, authentication, and integrity is the most critical foundation (8) (9) (10) (11).

*** Y Lihan Kumar**
M.Tech - CSE, TRREC

Although the proposal of IPv6 has improved the shortcoming of IPv4 and remedy a lot of security leakage. However, wireless networking around the city in anytime and anywhere will generate more information security problem than before. Therefore, enhance the techniques of information security is the key to control the marketing of IT business without any doubts and with no hesitate.

Based on these foundations, as the OS or application programs of an enterprises or personnel is initiated (requested) from the user side and operated through cloud computing on the remote service provider's side, there is explicit risks existed. Once if the remote side cannot offer regular operation, the operating schedule on the user side will thus cannot performed until the remote side normally operated.

As regarding the information security of cloud computing, those issues related with the application and service of cloud computing must be deeply concerned such as the equipment security of the client side, the threats of web site and webpage, the detection and diagnosis and surveillance of intrusion, the access and security of database on the cloud side, the detection of system leakage and the monitor of real-time repairing process, the management of server system, the management of mobile e-commerce processing, and the integrated analysis of associated security information and issues.

The goal of this paper is not only focused on find out some solutions, but also focused on develop some feasible information security techniques or products for the application and service of cloud computing.

II. INFORMATION SECURITY ISSUE OF CLOUD COMPUTING

A. SYSTEM SECURITY OF SERVER AND DATABASE

To adopt the service or application of cloud computing, firstly the necessary condition that both of the server and database on the front end must be trusted has to be satisfied. After then, an enterprise will be favor to utilize the corresponding service of cloud computing that provided by the corresponding service of cloud computing that provided by the server side. And thus, achieves the goal of reducing the needed budget and cost of storage and manipulation requirement for an enterprise or personal. The enterprise/personal that adopts the service of cloud computing then could store their data on the storage that provided by internet service provider (ISP) on the remote side via internet and utilize the computing service to sharply cut down the cost. That is the reason that achieve the assurance of confidential, integrity and authentication is very important for those information transaction, data manipulation, and service provided by cloud computing on the remote side through networking.

In order to monitor and process the internet hacking, thoroughly comprehend the source, technique, and intension of networking attack and analyze their attacking behavior is a must for information protection. In the paper, a honey-net has been deployed on the intranet of a simulated enterprise. Within the honey net, there are some honey-pots that store important data such as personnel, wage, salary, research and development project, military intelligence, or important news are installed on the server and database systems. Inside the intranet, some folders or directories are open intended for monitoring and tracks that have been accessed by the hackers. After analyzing and comprehending all of the hacking information, the corresponding derivation is quiet useful for enhancing the design of IDS and IPS. Some leakages or vulnerabilities are thus fixed.

B. NETWORKING SECURITY

Regarding the utilization of cloud computing, some possible communicating scenario including wired and wireless networking has been discussed in the following subsection.

Model of utilizing dedicated or leased line as for large size enterprises or business corporations, in order to assure the use of the application of cloud computing, the service providers of cloud computing had better construct a model that utilizing the dedicated or leased channel for communication with the enterprise. In addition, the encryption system and authenticating mechanism must be compulsive to maintain the information security in the process of communication. Therefore, the anxiety of information security can be decreased to the least unless the dedicated lines suffering physical damage. The proposed model for large size enterprises or business corporations using cloud computing via dedicated channel is shown figure1.

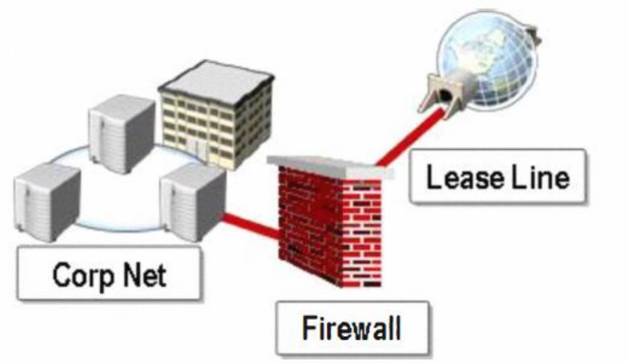


Figure 1: Dedicated channel for large size enterprises adopt the service of cloud computing.

In addition, an enterprise that adopts the application of cloud computing not only has to concerning the threats initiated from the internet, but also those implicit threats existed inside the service providers of cloud computing. For example, an enterprise might suspect that will the certificate or data be stole, forged, and misused by the employee? Nevertheless, if an enterprise is just under evaluation process and not yet make the final decision to

Adopt the application of cloud computing, the assurance of information security provided by the service provider will become very significance to come to the decision. In order to provide the guarantee of information security and quality of service, both of the enterprise and the service provider have to reach the service level agreement (SLA).

Moreover, including the service quality and assurance of information and service security have to be clearly and exactly defined in the SLA to protect the confidential business information will not be access, distributed, spoofed, and leakage without any authorization and authentication verification of the client side, enterprise. Thus, and enterprise had better negotiate with the service provider of cloud computing to reach an agreement in the following items before physical implementation and application.

1. Make sure the service requirement and scope of cloud computing.
2. The cost, price, and service content for cloud computing should be transparent and easily accessed.
3. Request the list of detail physical architecture in order to assure the physical security of devices/ equipments, system security, and operating environment security.
4. Evaluate the capability of problem management and solving information security events. As an enterprise/user negotiates with the service provider of cloud computing about the installation and the performance of software hardware and service security must be satisfied and sufficient. Therefore after then as the enterprise utilizes the application of cloud computing, the guarantee of information security has been enhanced and promoted

- Model of using Internet and vpn

  In order to provide the service of cloud computing for medium and small size enterprises, the suitable model that adopt by the service providers to implement the secure application had better constructed based on virtual private network(VPN)

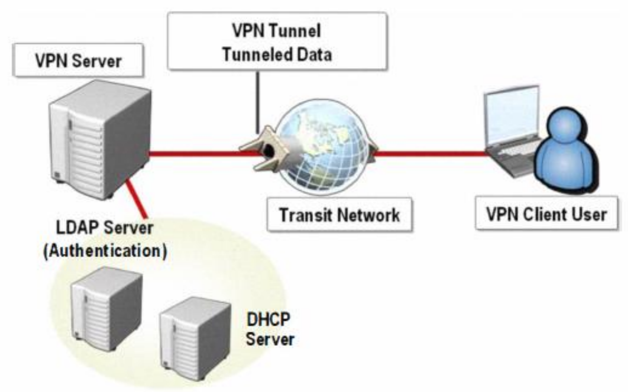


Figure 2 : Diagram for medium and small size enterprise access the service of cloud computing via Internet or VPN

As to those information transmission with confidential, via Internet for communication would be the best selection however this kind of service is not secure

- Model of utilizing wireless or mobile communication

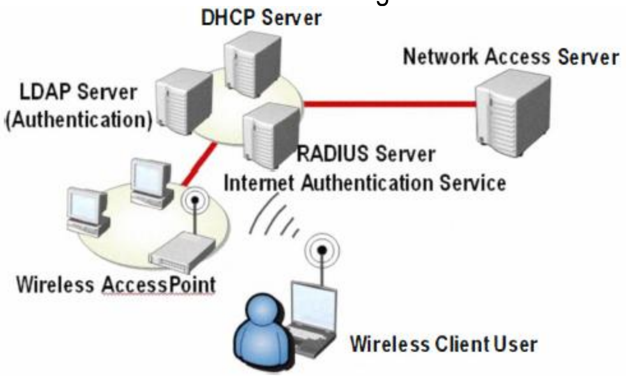
  According to emerging application of wireless communication, the information security issue increased. Their corresponding information security policy and management also are dramatically emerged and become more significant and popular. The communicating media are also not restricted to be wired such as pair wise, coaxial, cable, and etc. Due to the reason that wireless networking possesses the advantages such as lower cost lower power consumption, higher extension and more flexibility, wireless system are highly favorite and adopt to deployed for automatic control and networking monitoring. However, among the mounted wireless system, the information transmitted via wireless are easily intercepted, spoofed, cracked, and etc. Thus the information security problem of wireless system is more serious than wired system.

  As the developed networking products become more feasible diversity, and versatile such as the band width sharing equipment possesses a lot of functions the consideration of information security in much more important than the necessity of convenience for general users. Moreover, the data rate of 802. 1 in wireless communication could largely promote to

300Mbps. The data rate of 802.11n not only exceeds the data rate of802.11g wireless system, but also more than 5 times of the data rate 802.11g. Those access points 9AP) with memory could be utilized as the server of wireless networking therefore sharing the outside file service is not necessary to start the computer and thus might force to be confronted with some unpredicted information security disaster. This kind of networking policy might attract the attention of intelligentsia and hackers to access the enterprise resources and attack it without any notice Regarding the applications techniques, and products of 802.16 WIMAX wireless communication system are gradually matured and dramatically emerged , the employee of an enterprise or the customer of any possible cooperation and partners could easily access the desired server through networking in anywhere at any time to download their needed file.

Since the signal emitted by wireless communication system is broadcasted on the air, it is quiet easily and inevitably to be intercepted, sniffed, and even spoofed. As an enterprise utilizes the wireless networking, the authentication and class of security with communication might be suspected. Therefore, focus on those mobile networking devices, sniff their transmitted packets, and try to crack is a must. It is one of the best ways to well understand the vulnerability of wireless networking and could be provided for mapping out the policy of information protection.

The proposed architecture for mobile communication is shown in figure 3.



C. USER AUTHENTICATION

For all the enterprises, the management of user’s account and their corresponding authorized access privilege is very important and must be strictly defined. A lot of enterprises usually confront the problem of user account such as the adoption of single sign on (SSO) or each employee will be dispatched some different accounts to access different systems. Thus multi authentication for each employee might be every often to be confronted in an a enterprise. Those accounts that come along with each individuals might be the same or different Therefore , how could the administrator well manage those users identifications accounts and the corresponding passwords or achieve the state of SSO is an another important issue . Nevertheless the application of SSO for identification and authentication does have serious information security risk In addition, the management of authorized access privilege is also critical key point . How can the administrator define the appropriately access privilege for each employee to utilize the resources very satisfy and to achieve the goal maintaining information security without leakage or the loss of confidential / sensitive information through misuse in the mean while is kind of achieving the state of art

Through the implement of identity and access management (IAM), every enterprise could easily establish a managing mechanism to achieve the goal of user identification, authentication, and authorization simultaneously. The implementation of IAM is focused on the availability and security. Thus, it is benefit for an enterprise to obtain the advantages of promoting the productivity, reducing the IT cost, and decreasing the complexity of process of user identification, authentication and access control. Moreover, an enterprise and information asset based on the consolidate foundation of user authentication. Especially for the authentication of those mobile and wireless communication devices that belonging to the enterprise had better be accomplished through registration and hashing to assure the non-repudiation and achieve data integrity beyond the communication environment of all IP- based or mobile IPV6 are matured.

Through the implementation of open authorization (OAuth) protocol, every user could easily login on the networking system offered by previous or or9iginal service provider (SP) without revealing the information of user account and password. The OAuth scheme does have advantages for the enterprises to provide the authorization for the third party or consumer to utilize their networking service. For instance, an enterprise or individual user could authorize their own graphics or pictures to the printing service web server via networking. Thus, the process of printing out the authorized graphics is no longer needed the authentication information. Mechanism could provide reasonable application for the service of current cloud computing.

D. Data security on the cloud side

Form the iaas on the bottom foundation layer to the paas on the middle layer and the SaaS on the top layer, cloud storage is always an important key factor for implement the application of cloud computing. Especially, the storage resource of the IaaS on the bottom foundation layer is the most important factor for supporting the regular operation of networking service. A proposal possesses more flexibility to offer the application of cloud computing is to provide some services such as offering on-line storage and access data via web-based application interface (API) for all of the users of cloud computing in anytime at anywhere through wired or wireless networking devices. Moreover, a medium or large size service provider of cloud computing must possess the capability of supporting dynamical requirements and accomplish new added functions that requested by the enterprise to achieve their goals and satisfaction in timely. The above service could directly provide by the service providers of cloud computing for any user or enterprise that adopted the application or service of cloud computing. For example, the application can be applied for very popular micro-blogging (microlog) such as twitter, plurk, buboo and etc. in recently to allow millions of the user of microlog to store their personal

Information or pictures on the on-line storage that provided by the microlog or such as the simple storage service (S3) provided by the amazon to instead of storing those data on self established system.

For general user, it is quite easy to find the possible storage on the side that offers the service of could computing. To achieve the service of cloud computing, the most common utilized communication protocol is hypertext transfer protocol (HTTP). In order to assure the information security and data integrity, hypertext transfer protocol secure (HTTPS) and secure shell (SSH) are the most common adoption. However, data security on the cloud side is not only focused on the process of data transmission, but also the system security and data protection for those data stored on the storages of the cloud side. Moreover, if there are a lot of users on the client side of the cloud computing accessing the same files on the cloud side, the service provider must pay attention to find out the possible occurred problems and possess the capability of perfect database and file management to avoid data hazard.

In the following, some consideration regarding the security issue for device and equipment must be focused.

1. Storage and system protection: the service provider on the cloud side must provide the assurance of storage and system protection for those users that adopt the service of cloud computing to avoid the occurrence of storage damage and system failure that might probably induce the problem of data loss and generate the unnecessary arguments.
2. Data protection: for those data stored on the service provider of the cloud side must not be accessed or spoofed by unauthorized user or intruders and even the employee of the service provider without the authorization and authentication of request that presented by the user of the client side. In addition, the service provider must present the assurance of data integrity for the user of client side.

   Therefore, an enterprise shall evaluate the risk of storage damage, data loss, and networking security on the cloud side as they plan to adopt the application of cloud computing. As to the process defined in the specification of physical security, the service provider of cloud computing must present the necessary documents such as the purchase procedure, abolishment procedure, and management of storage for the third party that plays the role of supervisory for auditing. The enterprise, i.e. the user of cloud computing should also adopt the specification of physical security to watch over the physical retrieval procedure of the storage on the cloud side. Record the whole abolishing process including the abolishing location, verification procedure, and the process of demagnetization and recycling at the resource recycling station by video-taping as a reference or evidence. In the following, an enterprise of the user of cloud computing should also pay attention to the data security on the storage, i.e. the protection of data-at-rest. The rationale of adopting data-at-rest is the process of data encryption, authorization and authentication for the storing environment. An enterprise shall

Encrypt those confidential file or sensitive data before uploading. After then, those encrypted data could be uploading to the storage designated and provided by service provider of the cloud computing through secure channel. The demonstrated operating process is shown as figure 4.

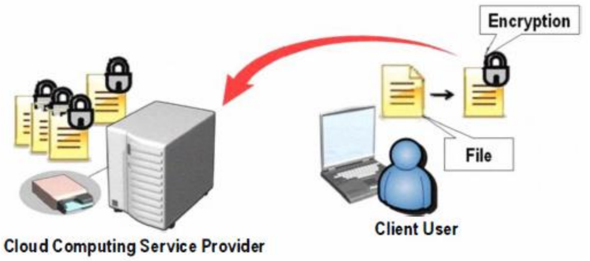


Figure 4:Diagram of data encryption scheme before uploading.

Currently, regarding the architecture of SaaS, IaaS, and paas, there is only IaaS offering this kind of information protection and data encryption. If the t5ransmitted data is categorized to high confidential for any enterprise, the cloud computing service based on IaaS architecture will be the most suitable solution for secure data process or management for those data belonged to the enterprises but stored on the service provider's side must be authorized by the user side (enterprises) to instead of the service providers.

III EXPERIMENTS

In order to verify the information security of the application of cloud computing, a small model is simulated and established. In the model, there are routers, switches, and some terminals. The server and database partition is merged based on VM ware techniques in addition, an authentication procedure for remote login is applied. In the cloud computing system, an intrusion prevention system (IPS) combined with user and data authentication to achieve user identification and data integrity has been constructed.

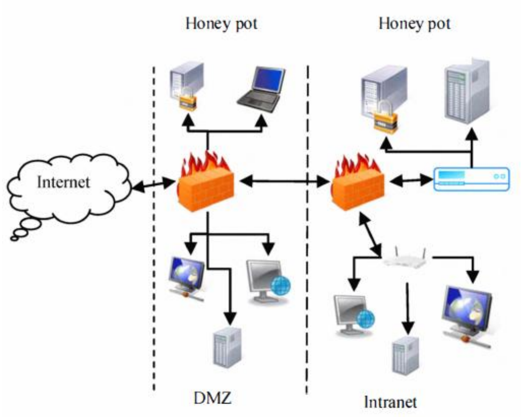


Figure 5: The simulated model of a honeynet with some honeypots.

Moreover, for the purpose of tracing the behavior and model the scenario of network attacking, a dynamic intrusion detection system (IDS) combined with honey net which is shown as figure 5 are also dispatched to verify the system's robustness.

Finally, some internet hacking such as distributed denial of service (DDoS), web-application hacking, and SQL injection are initiated to demonstrate the feasibility of IDS and IPS and verify the strength of networking security, system security, and database security of the simulated cloud computing. The simulated results could be applied for the improvement of developing a real system for cloud computing.

IV. CONCLUSIONS

In this paper, some information security issues that regarding the service and application of cloud computing are analyzed. Some possible solution for remedy the shortcoming or the security problem of cloud computing are also presented such as user authentication, device authentication and the establishment of secure communication channel. The proposed suggestions not only focus on the cloud side to present the assurance for the client side, but also the verification and authentication on both sides. Moreover, those requirements of data confidentiality, non-repudiation, and integrity are also addressed and discussed to avoid the occurrence of those unnecessary illegal problems that issued in the viewpoint of information security.

VI REFERENCES

[1] Gartner incorporation, http://www.gartner.com/.accessed on sep 2009 and April2010.

[2] Balachandra Reddy Kandukuri , Ramakrishna paturi v and Atanu Rakshit .”cloud security issues”, proceedings of 2009 IEEE international Conference on service Computing

[3] Developer perspective , http:/blog.smashedapples.com/cloud service/

[4] GregBoss , Padma Malladi,Denis Quan ,Linda Legreni Haroldhall, “Cloud computing http://www.ibm.com/developers work/eb site /Zones/hipods /library html,ppl1-4, October2009

[5] Mikekekavis, “Real time transactions in the cloud “http://www.kavistechnology.com/blog/?p=789,accessed on April 12,2009

[6] Service level Agreement Definition and contents ,http://www.service level agreement .net, accessed on march 10,2009

[7] Service level Agreement and Master Service Agreement, http:// www.softlayer. Com/sla., html, accessed on april 05,2009

[8] Server intellect service level agreement, http//www serverintellect com/legal/aspx, accessed on April 09, 2009.

[9] http://www.cloudsecurity. Org, accessed on april 10,2009

[10] Sampling issues we are addressing, http://cloudsecurityalliance. Org/issues. Html#15, accessed on april 09, 2009

[11] Secure group addresses cloud computing risks, http://www.secpoint.Com/security-group-addresses-cloudcomputing-risks.html, april 25, 2009

[12] Tim mather, “cloud security and privacy” 2009