Cloud Computing Service Modelsand Solution to their Security Concerns

Saritha K R
Lecturer,
Dept of ISE, Dr AIT

Pushpalatha S
Assoc. Prof,
Dept of ISE, Dr AIT

VidyaRani H J
Assoc. Prof,
Dept of ISE, Dr AIT

***Abstract*— Cloud computing provides a major shift in the way companies see the IT infrastructure. This technology is primarily driven by the internet and requires rapid provisioning ,high availability, high scalability and virtualized environments. The cloud computing is the result of many factors such as traditional computer technology and communication technology and business mode. 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 amount of resources provided in the cloud system for the users is increased when they need more and decrease when they need less.**

***Keywords*— Cloud computing,Service models, encryption mechanism, security, PKI technology.**

I. INTRODUCTION

This section visualizes the different cloud models with respect to services .Clouded concerns beyond generic concerns regarding the cloud approach, each of the three models has its own security concerns.

A. Software as a Service

Saas concerns users must rely heavily on their cloud providers for security.The providermust protect the underlying infrastructure from break-ins and generally has responsibility for all authentication and encryption. Also the provider must do the work to keep multiple companies or users from seeing each other's data without permission. It's not easy for the customer to get the details that ensure that the right things are being done. In the same way, it's difficult to get assurance that the application will be available when needed.

B. Platform as a Service

Paasconcerns,the provider might give some control to the people building applications atop its platform. For example, developers might be able to craft their own authentication systems and data encryption, but any security below the application level—such as host or network intrusion prevention— will still be completely in the provider's hands. Usually, the provider will offer little or no visibility into its practices. Plus, the platform provider must be able to offer strong assurances that the data remains inaccessible between applications. Large banks don't want to run a program delivered in the cloud that risks compromising their data through interaction with some other program.

C. Infrastructure as a Service

Iaasconcerns With IaaS, the developer has much better control over the security environment, primarily because applications run on virtual machines separated from other virtual machines running on the same physical machine, as long as there is no gaping security hole in the virtual machine manager. This control makes it easier to ensure that developers properly address security and compliance concerns—with the downside that building the application can be more expensive and time-consuming. Backing up data poses another concern. Even though some providers do their own backups for the customer, much can still go wrong. Maybe they increase their prices and make it difficult to get data off their network.

II. CLOUD SERVICE MODELS AND THEIR SECURITY CONCERNS

In this section, cloud service models and their security concerns are discussed. Each service has its own security issues. These models are based on different SLAs that are between providers and users.

A. Security Issues in Saas Model

In the SaaS model, the user buys a subscription to some software product, but some or all of the data and code resides remotely [1] and customers can access to this services via internet. In this model, applications could run entirely on the network, with the user interface living on a thin client. With SaaS, users must rely heavily on their cloud providers for security [2]. Degree of control by providers is high and they are responsible for confidentiality, integrity and availability of their services. Users have no responsibilities about anything.

B. Security Issues in Paas Model

This model provides the user to deploy user-built applications onto the cloud infrastructure that are built using programming languages and software tools supported by the provider (e.g., Java, python, .Net). The user does not manage the underlying cloud infrastructure

[3]. PaaS supplies all the resources required to build applications and services completely from the Internet, without having to download or install software. A downfall to PaaS is a lack of interoperability and portability among providers. That is, if you create an application with one cloud provider and decide to move to another provider, you may not be able to do so—or you'll have to pay a high price. Also, if the provider goes out of business, your applications and your data will be lost. Degree of control by providers is medium and they are only responsible for integrity and availability of their services. But users' responsibility is medium and they are responsible of confidentiality and data privacy. For example, users can use their data encryption and authentication systems in application level but security in other levels is in the provider's hands and they must be able to guarantee that the data remains secure from other applications.

C. Security Issues in Iaas Model

IaaS model lets the development organization define its own software environment [1]. Whereas SaaS and PaaS are providing applications to customers, IaaS doesn't. It simply offers the hardware so that your organization can put whatever they want onto it. This basically delivers virtual machine images to the IaaS provider, instead of programs, and the machines can contain whatever the developers want. Degree of control by providers is low and they are only responsible for availability of their services. But users' responsibility is high and they are responsible of confidentiality, data privacy and integrity. Fig. 1 shows provider and user responsibility in security of cloud service models.

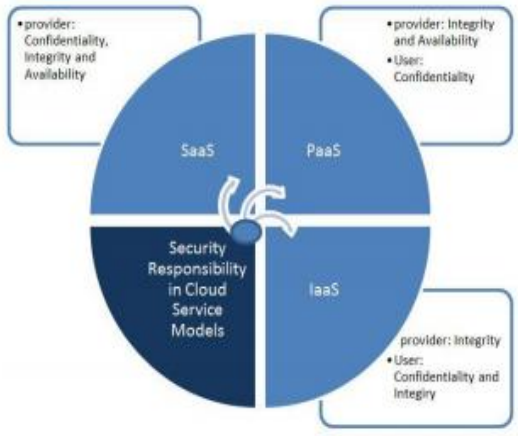

Fig1 : Responsibilities of users and providers in security of cloud service models.

III. SOLUTION FOR CLOUD SECURITY PROBLEM

The data stored in the cloud system can meet the problem of stolen and modified unlawfully. The data can be encrypted before stored in the cloud system. But if the data size is very large, it will need more time and computing resource. The confidential data will be treated outer people of company and the other people can access the data. Traditional techniques can protect user data privacy and security in cloud the environment to some extent. These technologies include encryption mechanism, security authentication mechanism and access control policy. Encryption mechanism depends on the reliability of the difficulty of decryption. Encryption methods include symmetric key encryption systems and asymmetric key encryption system. Asymmetric key can get high security but encryption and decryption is slow. Security authentication mechanism currently has a complete set of technical solutions. It uses the internationally accepted PKI technology, X.509 certificate standard and X.500 published standards of information technology standards. Access control policy is basic technology and is to ensure that network resources are not illegal use. It includes network access control and directory level security control. The user which can connect the cloud system includes the cloud provider, operation and maintenance personnel and the customer user. How to ensure customer data is not illegal to steal or utilize by other cloud computing providers is a major problem. The operation and maintenance personnel are responsible for data storage and backup and make the data classification management according to the level of data security. 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 cloud provider can transmit the customer data from the server to another server and the user can not know the data storage place. The data storage and manipulation are related to the resources of cloud center in cloud computing environment. The cloud provider is responsible for security but the monitoring and auditing for them become important problem. The cloud computing services provided for customers are difficult to achieve full transparency. Customers do not understand internal processes of cloud computing and data storage location information. The customers do not know what kind of situation data will meet if an accident occurs. Customers should have the right of the supervision and audit of cloud computing services in order to fully ensure the security of customer data. The communication of worms, virus and Trojan in cloud computing platform within the network of internal and external must be controlled. Malicious programs must be isolated promptly. Damage to the system must be repaired immediately. The data traffic in the cloud system and cloud computing system running status should be monitored in real time. The abnormal action of network and system must be detected and fixed timely. The network attack detection and defense system must be deployed in the cloud network. The service interruption and system failures because of hackers must be amended. The disaster recovery mechanism of cloud computing platform must be realized which includes important system backup and data disaster recovery. The emergency response mechanism and the emergency response

capabilities for emergency case must be established and improved. The user information availability privacy and integrity must be protected. The user system and data security isolation and protection must be considered. The network data transmission security can be protected by use of data encryption and VPN technology. The management of user data encryption and key distribution mechanism must be designed carefully. The management and maintenance of user data must be safe and effective. Data backup is very important, data security recovery mechanism is also very necessary. The user's data can be promptly restored if the abnormal behavior of the system occurs. The cloud system can be considered as service oriented architecture system which hide the underlying details and provide transparent services to customers. The cloud service can be considered as the web service and the security mechanism in the service oriented architecture can be used for reference. SOA achieves interoperability between different systems and programming languages provides the basis for integration between applications on different platforms through a communication protocol. The web service has many security mechanisms such as WS-Security, WSReliability, WS-Trust, WS-Authorization, WS-Secure Conversation [4].

IV. CONCLUSION

This paper introduces a detailed analysis of the cloud computing service models. It also focuses on security issues and challenges in cloud computing types and the service delivery types.Cloud computing providers can build large datacenters at low cost due to their expertise in organizing and provisioning computational resources. Cloud computing is a trend in IT that moves computing and data away from desktop and portable PCs into large data centers. It refers to applications delivered as services over the Internet as well as to the actual cloud infrastructure — namely, the hardware and systems software in data centers that provide these services.A data center holds information that end-users would more traditionally have stored on their computers. This raises concerns regarding user privacy protection because users must outsource their data.

These technologies include encryption mechanism, security authentication mechanism and access control policy.This paper states some of the traditionally used mechanisms for user data privacy and security. It also says about the network data transmission security by VPN technology and web service security mechanisms.

REFERENCES

[1] J. Viega and McAffee, “Cloud Computing and the Common Man,” Published by the IEEE Computer Society. 2009.
[2] Costanzo, M. Assuncao, and R. Buyya, “Harnessing Cloud Technologies for a Virtualized Distributed Computing Infrastructure,” IEEE Internet Computing, Sept. 2009.
[3] Hoffa, et al., “On the Use of Cloud Computing for Scientific Workflows,” IEEE Fourth Int’l Conf. oneScience, Dec. 2008.
[4] International Business Machines Corporation,Security in a Web Services World: A Proposed Architecture and Roadmap,http://msdn.microsoft.com/en-us/library/ms977312.aspx,2002
[5] Cong Wang, Qian Wang, and Kui Ren Department of ECE Illinois Institute of Technology" Ensuring Data Storage Security in Cloud Computing" .