International Journal of Current Engineering and Technology
E-ISSN 2277 – 4106, P-ISSN 2347 - 5161

Available at http://inpressco.com/category/ijcet

General Article

Intelligent Data Security in Cloud Computing

Pachipala Yellamma[Å*], N arasimham Challa[Å] and V Sreenivas[Å]

[Å]Bharathiar University, Coimbatore, India

Accepted 30 January 2014, Available online 01 February 2014, **Vol.4, No.1 (February 2014)**

Abstract

Cloud computing can be defined as management and provision of different resources, such as, software, applications and information as services over the cloud (internet) on demand. Cloud computing provides people a way to share large mount of distributed resources belonging to different organizations. That is a good way to share many kinds of distributed resources, but it also makes security problems more complicate and more important for users than before. In this paper, we analyze some security requirements in cloud computing environment. .Data Security and Access Control is an exigent work in the environment of Cloud Computing. This paper gives the architecture and characteristics of the intelligence security control platform based on cloud computing .The achievement of the paper has significant meaning to the automation of information and popularization of national economic information network, and has very high reference value to the research of network security technology.

Keywords: *Data security, intelligent, Network security*

1. Introduction

Cloud computing is the next generation in computation. People can have everything they need on the cloud. Cloud computing is the next natural step in the evolution of on-demand information technology services and products. The cloud is a metaphor for the Internet, based on how it is depicted in computer network diagrams, and is an Abstraction for the complex Infrastructure. With the rapid development of Collaborative Management, cloud computing has been the tool for human-human interaction to support the group communication and collaboration as well as for design computation, intelligence reasoning and graphics manipulation. Cloud Computing is Internet-based computing, whereby shared resources, software. Cloud computing describes a new supplement, consumption, and delivery model for IT services based on the Internet, and it typically .Involves Internet provision of dynamically scalable and often virtualized resources. The platform is based on trustworthy computing technology. Through strengthening the end security, the control workflow and the network security management, it builds the new administrative security system. The end security mainly uses terminals credible security solutions to achieve credible access terminals. The network security and the safety and security will follow the intelligence information security management system so as to support and ensure internet and inter-communicating, resources-sharing and commanding and decision-making among various information systems. Most cloud computing infrastructures consist of services delivered through common centers and built on servers. Clouds often appear as single points of access for all consumers' computing needs. Complete cloud computing is a dynamic computing system (Tharam Dillon, Chen Wu and Elizabeth Chang *et al*,2010).It provides the management applications and dynamic environment which can be dynamically allocated or assigned to the computational resources, real-time monitoring, the security identification and feature protection. According to the security configuration and administration, computers can work in accordance with security strategies, coordination and sustainable management. In the intelligence information security control platform, the computer replaces the management activities and achieves the machine management and overall information security. However there still exist many problems in cloud computing today, a recent survey shows that data security and privacy risks have become the primary concern for people to shift to cloud computing.

2. Related concepts about cloud

The earlier version of the Cloud Security Alliance's guidance featured definitions that were written prior to the published work of the scientists at the U.S. National Institute of Standards and Technology (NIST) and their efforts around defining cloud computing .NIST defines cloud computing by describing five essential characteristics, three cloud service models, and four cloud deployment models.

2.1. Deployment cloud models

2.1.1. Public cloud: the cloud infrastructure is made avail-

*Corresponding author: **Pachipala Yellamma** is a Research Scholar

-able to the general public people or a large industry group and provided by single service provider selling cloud services.
2.1.2. Private cloud: the cloud infrastructure is operated solely for an organization. The main advantage of this model is the security, compliance and QoS.
2.1.3. Community cloud: the cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns like security requirements, policy, and compliance considerations.
2.1.4. Hybrid cloud: the cloud infrastructure is a combination of two or more clouds. It enables data application portability through load balancing between clouds. In following figure 1 shows different types of clouds.(prof Kai Hwang *et al* , 2010).

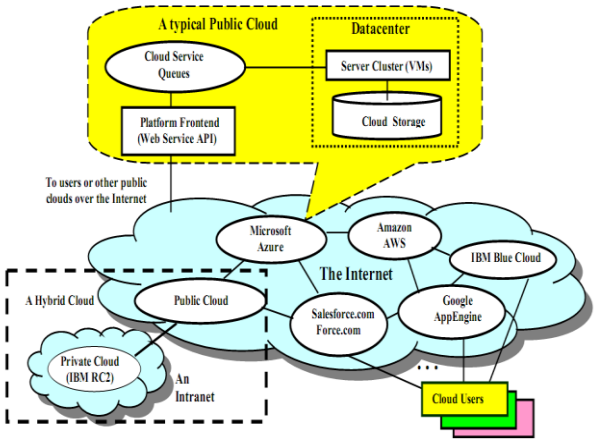

Figure1 Public, Private and Hybrid Clouds

2.2. Cloud characteristics

2.2.1. On demand service: cloud is large resource and service pool that you can get service or resource whenever you need by paying amount that you used.
2.2.2. Ubiquitous network access: cloud provides services everywhere though standard terminal like mobile phones, laptops and personal digital assistants.
2.2.3. Easy use: The most cloud provider's offers internet based interfaces which are simpler than application program interfaces so user can easily use cloud services.
2.2.4..Business model: cloud is a business model because it is pay per use of service or resource.
2.2.5. Location independent resource poling: the providers computing resources are pooled to serve multiple customers using multitenant model with different physical and virtual resources dynamically assigned and reassigned according to demand.

2.3. Cloud Computing as a Service

Services in cloud computing is the concept of being able to use reusable and fine grained component across a vendor's network.

This is widely known as "as a service". Offering with as services as a suffix include traits like Following:
1. Low barriers to entry, making them available to small businesses.
2. Large scalability.
3. Multi-tenancy, which allow resources to be shared by many users.
4. Device independence, which allows user to access the systems on different hardware
.
2.3.1. Infrastructure as a service: it delivers a platform virtualization environment as a service rather than purchasing servers, software, data centers.
2.3.2. Software as a service: it is software that is deployed over internet and or is deployed to run behind a firewall in your LAN or PC.
2.3.3. Platform as a service: this kind of cloud computing provide development environment as a service. You can use the middleman's equipment to develop your own program and deliver it to the users through internet and servers.
2.3.4. Storage as a service: this is database like services billed on a utility computing basis, e.g., gigabyte per month.
2.3.5. Desktop as a service: this is the provisioning of the desktop environment either within a browser or as a terminal server. In following figure2 shows different kinds of cloud computing services.(prof Kai Hwang *et al* , 2010)

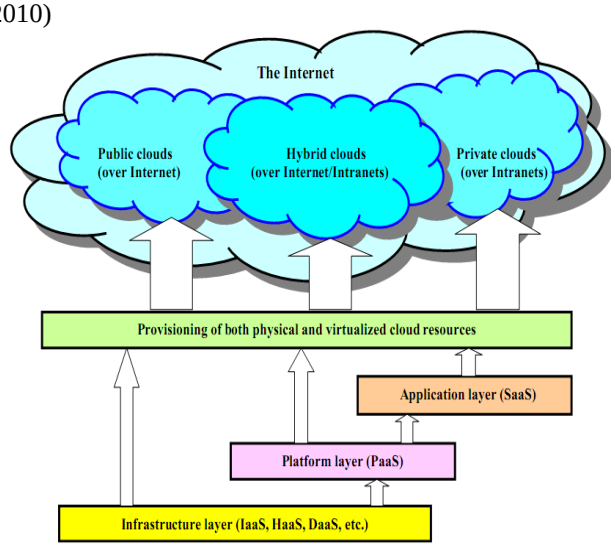

Figure 2.Cloud Computing as A Service

3. Cloud security issues

In the cloud computing the client stores its data to the location about which he does not know anything, and There fore some sort of security mechanism is needed to ensure the client for not being worried about its data. A recent survey by Cloud Security Alliance (CSA) & IEEE indicates that many organizations are wont to implement cloud computing but they need the security solution. Security in the cloud computing environment can be identifies as following:
1. Security in SaaS.
2. Security in PaaS.
3. Security in HaaS.
In this paper we are representing network security; therefore we are going to have brief look on security in

SaaS. Although SaaS offer great advantages to the clients but there are some security issues are related to it. In SaaS, the client has to depend on the provider for proper security measures. The Cloud Service Provider (CSP) has to ensure the client about security. The following key security issues should be considered as Integral part of SaaS implementation.

1. Data Security.
2. Network Security.
3. Data locality.
4. Authentication and Authorization.

In following figure 3 shows cloud storage environment.

3.1 Data Security

Data security is the means of ensuring that data is kept safe from corruption and that access to it is suitably controlled. Thus data security helps to ensure privacy. It also helps in protecting personal data. In a traditional application deployment model, the important data of each organization continues to reside within the organization boundary and is subject to its physical, logical and personnel security and access control policies. However, in the SaaS model, the organization data is stored outside the organization boundary, at the SaaS service provider end. Therefore the service provider has to use techniques such as encryption, strong user authentication and back up for providing data security.

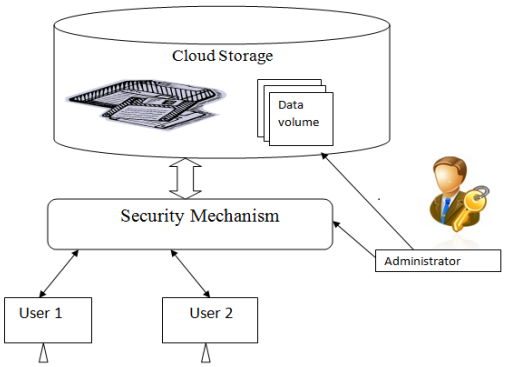

Figure 3 Cloud Storage Environment

3.2 Network Security

In the cloud computing environment all the data flows through the internet that is subjected to influence by various type of attacks. Therefore the service provider has to use some network security mechanism. In the next section of the paper we will have detail look on network security.

3.3 Data locality

In a cloud environment, the consumers use the applications provided by the SaaS and process their business data. But the customer does not know where the data is getting stored. In many a cases, this can be an issue. Due to compliance and data privacy laws in various countries, locality of data is of importance in many organizations architecture. For example, in many EU and South America countries, certain types of data can not leave the country because of potentially sensitive information. In addition to the issue of local laws, there's also the question of whose jurisdiction the data falls under, when an investigation occurs. A secure SaaS model must be capable of providing reliability to the customer on the location of the data of the consumer.

3.4 Authentication and Authorization

Because in the application and data is hosted outside of the organization in the cloud computing environment, the cloud service provider has to use Authentication and Authorization mechanism. Authentication is the mechanism whereby systems may securely identify their users. Authorization is the mechanism by which a system determines what level of access a particular authenticated user should have to secure resources controlled by the system.

4. Related Work

In the intelligent information security management control platform, a unified security platform based on trusted computing technology considers the aspects including the credibility of the terminal access, reliable network infrastructure, reliable network access control, intelligent security management, network security and operational security management. The credibility of information management, control bus, other trusted business services, effective integration and electronic government business tightly are coupled to form a complete security organic system. Considering the overall solution scalability and security requirements based on the above model and unified security management protocol standards(Lejiang Guo1, XiangPing Chen1, Chao Gao2, DaiPing Wang2 *et al*, 2012)

5. Securities during transmission

Using Cloud reduce the cost, greater flexibility and dynamic allocation of the resources provide greater advantages for the users but despite these advantages there are also challenges when transmit data from cloud to user and one cloud to other cloud. So there are mechanisms to provide security during transmission that are as under

5.1 Provide Authentication

In cloud computing environment, different users from different origin can appeal to join the Cloud. Then the first step is to prove their identities to the cloud computing system. Administration Because in cloud computing different users demand different resources and other applications, so the authentication is important and it is difficult process. It should be ensuring that administrator has different access mechanism and users have different access mechanism. If access is granted to the administrator, it does not necessarily mean access is granted to other users. Our main goal is to maintaining security without any loss of information. So we can

achieve this, firstly when any user sends request to server then user has to first register himself and after that login with its username and password that was provided to him. If the user is valid then server creates its log file that contains the information regarding its login and role of information accessed. After this process there should be encryption scheme with keys that the server creates unique key and send to client for the decryption. Then the client decrypts data with this key. It is very important in this type of shared environment to properly and securely authenticate system users and administrators, and provide them with access to only the resources they need to do their jobs or the resources that they own within the system.

5.2 Network Security

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 network 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

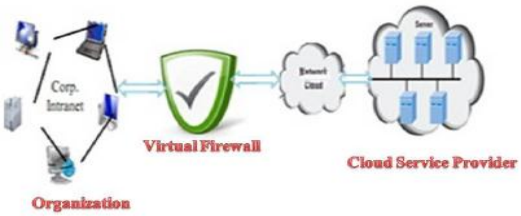

Figure 4 Virtual firewall

Figure 4.virtual Firewall that supports filtering of packets, traffic management and access control. In this way, it can mitigate the risks of viruses, worms, Trojans, and inappropriate use in a virtual environment in the same way that a physical firewall could mitigate those risks if every physical server was directly connect to a physical firewall. A virtual Firewall provides multiple logical firewalls for multiple networks on a single system. Using Virtual Firewall you can control bandwidth utilization of each virtual machine in your infrastructure, preventing over utilization and denial of service to critical applications.

6. Security intelligence can defend the entire cloud

Integrated security intelligence is a critical tool for detecting external and internal threats, predicting business risks, overcoming vulnerabilities, and addressing regulatory mandates.(IBM Software white paper *et al*, 2013). By consolidating and enriching data from across IT silos, and performing near real-time analytics on that data, security intelligence is crucial to providing visibility across the cloud environment. Effective security intelligence will provide core capabilities across the cloud, such as:

- providing a consolidated view of the entire cloud to defend against advanced attacks
- Correlating different events from across the infrastructure for actionable insight
- utilizing a single dashboard to display security events across security domains A key requirement is the ability to protect and track user activities on the virtual infrastructure, providing effective administrative access control. The security team needs to track suspicious role changes, unauthorized user actions and failed (and potentially harmful) login attempts. It must monitor user activities on physical servers or virtual machines such as Create, Delete or Move VMs and create an audit trail. The team needs the ability to correlate events from virtual machine components, storage, routers, firewalls, switches and more, and to track this data as virtual machines are migrated or moved. They must be able to follow and report on issues such as duplicate IPs and virtual machine connectivity. For complete visibility, the security team also needs operational intelligence for the virtual infrastructure. It should be able to browse and alert on errors occurring in logs, as well as to track changes to software and hardware resources and configuration changes in the cloud. To complete the team's management function, it will also need information to help investigate application response times and performance, and aid in capacity management. In delivering visibility, an advanced security intelligence solution should span organizational silos and functions, utilizing centralized controls and capabilities such as granular management of log and flow data, advanced threat visualization and impact analysis, attack path visualization, and device or interface mapping.

7. Protects Data in the Cloud

With SafeNet's security offerings, organizations can fully leverage the business benefits of cloud Environments while ensuring trust, compliance, and privacy. SafeNet offers intelligent, data-centric Solutions that persistently protect data throughout the information lifecycle and evolve to support changing cloud delivery models from today's SaaS and private clouds, to the evolving demands of hybrid and public clouds. SafeNet offers a broad set of solutions that enable both enterprises and cloud providers to protect data in the cloud (Russ Dietz *et al* ,2012).

SafeNet solutions offer an unparalleled combination of features including central key and policy management, robust encryption support, flexible integration, and more that make cryptography as a service practical, efficient, and secure.

7.1. Cloud Security Solutions

To identify indicators of attacks before breaches occur, security intelligence integrates information and uses advanced analytics across the security domains of people, data, applications and infrastructure.

7.1.1. Secure access to cloud resources with intelligent authentication tokens

Ensuring that only authorized users gain access to cloud-based resources is critical for cloud providers and enterprises. Providers need to ensure proper access controls for users at client sites, and for administrators

within the service provider's organization. SafeNet's wide range of multi-factor strong authentication solutions ensure that only authorized individuals access your organization's sensitive information enabling business, protecting your data, lowering IT costs, and boosting user productivity.

7.1.2. Secure cryptographic key storage

Any cryptographic system and trust in the protected data is only as strong as the underlying protection of the keys used to encrypt data. A centralized, hardened security appliance manages cryptographic keys, access control, and other security policies. In addition, a virtualized instance of this appliance is deployed in the cloud to replicate policies and security enforcement on the data. Security administrators can dictate policy based on business content, documents, and folders in order to ensure only authorized users and groups access sensitive data. SafeNet hardware security modules offer centralized, FIPS- and Common Criteria-certified storage of cryptographic keys.

7.1.3. Secure storage in the cloud across file, application, and database systems

Driven by a need to use the cloud's elastic storage, enterprises can securely store data in the cloud, effectively using the cloud for the backup, disaster recovery, and archival of data. SafeNet provides protection of stored data through a hardened appliance that centralizes encryption processing, keys, logging, auditing, and policy administration across file, application, and database systems.

7.1.4. Secure infrastructure within public and hybrid clouds

Clouds are a target rich environment for cyber attacks on the interconnected critical fabric that weaves together the elastic computing, storage and connectivity in the back-end of the cloud data centers. SafeNet provides strong Layer 3 and Layer 2 link encryption solutions to harden this critical network infrastructure while maintaining low-latency high throughput data exchanges to keep the cloud operating at peak efficiency. Together, these solutions deliver the critical capabilities required for a robust, cost-effective, and secure cloud security implementation.

Conclusion

In this paper, we investigated the problem of data security in cloud data storage and data transmission. Recognized as an industry leader in security, this paper provides best-of-breed solutions for security intelligence based on innovative solutions such as Security Intelligence Platform, intelligent authentication tokens, Secure infrastructure within public and hybrid clouds, Secure cryptographic key storage insights and security alerts for customers provided by SafeNet's research and development, and ongoing investments in developing security technology. This paper provides security intelligence solutions deliver integrated, automated and comprehensive capabilities that provide visibility into the entire cloud environment to support regulatory compliance and enable a proactive security posture that helps stop attacks before breaches can occur.

References

Lejiang Guo, XiangPing Chen, Chao Gao, DaiPing Wang2 (2012) The Intelligence Security Control Platform Based on Cloud and Trusted Computing Technology, *International Conference on Electrical and Computer Engineering Advances in Biomedical Engineering*, Vol.11

Russ Dietz (2012) .securing data in the cloud *SafeNet cloud security solutions*

Prof. Kai Hwang(2010) Security, Privacy, and Data Protection for Trusted Cloud Computing *International Conference on Parallel and Distributed Computing and Systems, University of Southern California*

Tharam Dillon, Chen Wu and Elizabeth Chang (2010), Cloud Computing: Issues and Challenges, *24th IEEE International Conference on Advanced Information Networking and Applications.*

IBM Software white paper (2013), Security intelligence is the smart way to keep the cloud safe.