Research Journal of Information Technology

ISSN 1815-7432

Academic Journals Inc.

www.academicjournals.com

Research Journal of Information Technology 5 (3): 442-448, 2013
ISSN 1815-7432 / DOI: 10.3923/rjit.2013.442.448

Elucidating the Robust and Resilient Cloud Security Solution Approaches

[1]Pethuru Raj, [2]C. Nithya, [2]A. Parvathy, [2]K. Thenmozhi, [2]J.B.B. Rayappan and [2]Rengarajan Amirtharajan
[1]Wipro Technologies, Bangalore, 560035, India
[2]School of Electrical and Electronics Engineering, SASTRA University Tamil Nadu, India

Corresponding Author: Pethuru Raj, Wipro Technologies, Bangalore, 560035, India

ABSTRACT

The cloud idea has been percolating to every tangible domain. Having understood the fact that significant savings can be availed and acquired with the assimilation and adoption of cloud concepts, business executives, entrepreneurs and engineers are working overtime in putting cloud-centric tactical as well as strategical plans and proposals in place to easily and quickly accomplish the lingering mantra of 'more with less'. Cloud infrastructures (private, public and hybrid) are erupting across the globe, cloud platforms, applications and services are being developed or assembled, deployed, managed, delivered via one or more of these cloud infrastructure providers. The popularity and pervasiveness of cloud services are quiet surging. Though cloud computing is being seen as a silver bullet for the ICT industry, there are a few shortcomings such as security, availability, data ownership, etc. In this study, we are concentrating on the perpetual and prominent security problem of the cloud paradigm. We have discussed about the possible solutions for the security issues at different layers and levels.

Key words: Cloud, data security, IaaS, SaaS, PaaS

INTRODUCTION

The Key Drivers for the Cloud technology have a need to share the hardware resources in the field of computing due to the growing number of users. To handle this task of allocating and managing resources, time sharing utilities like the networking in the 1990s and the grid computing were devised. However, today the demand for such resources is skyrocketing and thus behooves a new scheme to make available resources on a massive scale and yet efficient.

"Cloud Computing" is a large group of interconnected computers where one can virtually access the resource through the Internet (Talib *et al*., 2012), although they are in different geographic locations and pay only for the amount of resources used. This kind of migration from conventional networks to a cloud has been empowered in the recent years to maintain the data base which contains data, audio, images, video files, etc. The server is located in a remote area which can be accessed through networks (Talib *et al*., 2011). This architecture shares the resources among various IT sectors (Ding *et al*., 2012). Cloud environment was established by virtualization in the year of 1967 but it is has been offered only in mainframe structure for decades. A hypervisor is a swarm system, where all the required applications are executed. Cloud service provides infrastructures services, software, hardware services whose reliability and scalability is are high

and also the service purely relay on demand. This paper deals about the vision of cloud in this computing era in the sense it is answering for how the cloud provides profit to the business as well the security threads of it and the problem solution.

THE LEADING CLOUD DEPLOYMENT AND DELIVERY MODELS

The Leading Cloud Deployment and Delivery Models provide us with three basic services, which are software as a service (SaaS), platform as a service (PaaS) and Infrastructure as a Service (IaaS).

There is no need of conventional software to run any sort of application. Instead it is available in cloud, which can be utilized by the registered concern through the internet (Azeez *et al*., 2012). This service is called Software as a Service (SaaS), such as Saleforce.com. Many users are able to utilize the applications running on the cloud environment by using a thin client interface, like web browsers. The clients need not to maintain the cloud's infrastructure (Schwarzkopf *et al*., 2011), such as network, servers, operating systems, storage. Since cloud is a multi tenant structure the remotely located consumers can also construct and organize their own applications (Gao and Kang, 2012) in the platform available in the cloud this kind of service of the cloud is called as Platform as a Service (PaaS). Few examples of PaaS are Google App Engine Platform and Microsoft's Windows Azure platform. From the cloud basic building blocks, hardware such as storage server maintain the database and an efficient environment for computing called infrastructure, for an application can be rented by the developer. Amazon provides popular services called Elastic Compute Cloud (Amazon EC2) or Amazon Simple Storage Service (Amazon S3) which falls under Infrastructure as a Service (IaaS). The consumers need not maintain the cloud's resource but it can be controlled by them (Silas *et al*., 2012). That is, the Customer can control the cloud's infrastructure, such as operating system, storage, application and gain partial control on networking component's selection (Yuan *et al*., 2012).

The following are the four deployment models of cloud:

- **Private clouds:** It is a conventional for a particular group or organization and limit's right to use to that set. This is meant for that particular group or corporate. Operations and properties of this kind of clouds are not open to the end-users but for some extended features of the cloud can be offered. Example: eBay, Eucalyptus, Amazon VPC (Virtual Private Cloud), VMware
- **Public clouds:** In this any client can get through into cloud by an Internet. Enterprises may enter to the public cloud whose functionality and the services can be offered even outside the corporation to the clients. Providing the user capacity to make use of cloud for their function and permit other corporation also farm out their service to service provider which is cloud. The cost reduction and effort to build up their own infrastructure. Example: Amazon EC2, Google Apps, Windows Azure
- **Hybrid clouds:** Combination of private and public clouds environment makes hybrid cloud. Cost is getting reduced due to the outsourcing but security aspects must be considered. Example: VMware, vcloud
- **Community clouds:** A community cloud is shared among two or more organizations that have similar cloud requirements. Here infrastructure is shared among multiple numbers of organizations under a specific community for an universal anxiety such as safety, conformity, authority, etc., these are handled by the cloud or by trusted party and hosted internally or externally with that of the cloud

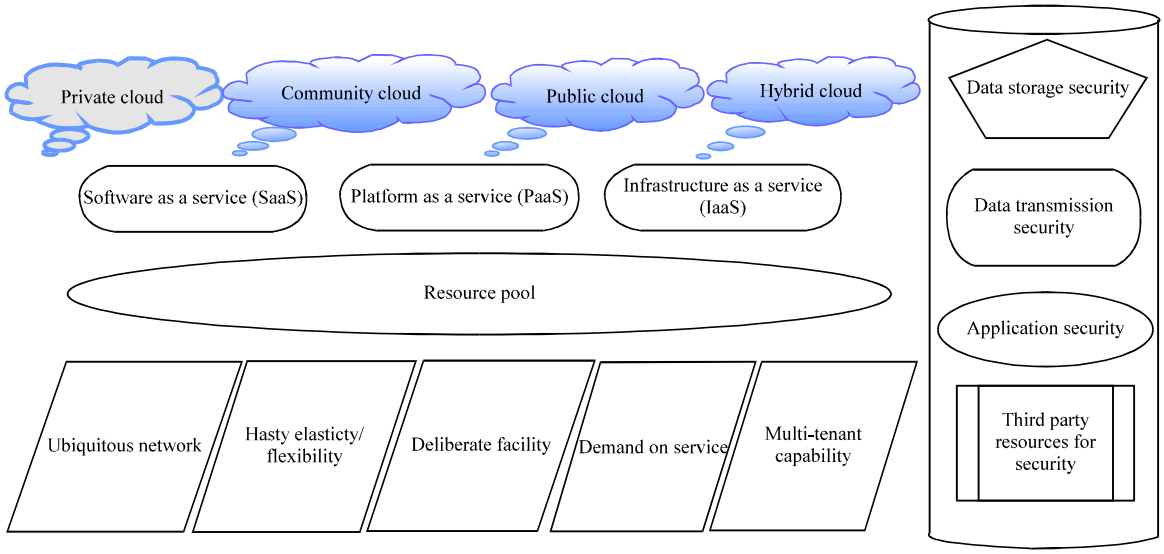

Fig. 1: Cloud environment security skeleton

Profits of cloud: It has many advantages in various aspects' namely high efficiency, on-demand availability, flexible, dynamical, scalable, security and low-cost.

Non-functional aspects include flexibility, consistency and quality of service, ease of use, agility and malleability. Economic aspects such as, cost drop, cost for usage, Return of Investment (ROI), going Green (Zhang and Fu, 2011) and the technical aspects follow virtualization, Multi- tenancy, security, privacy and compliance, data Management, APIs and /or programming enhancements.

The security conundrum: Cloud computing reduces the complexity of the end users regarding hardware requirements even a software and the Cloud Environment Security Skeleton is given in Fig. 1. However, cloud has become popular in recent years due to its nature of pay on use, which will preserve everything in it but the security becomes one of the big issues in the cloud. Since privacy is a basic need of cloud where data is stored, many new models have been adopted for highly secure environment (Rong *et al*., 2013).There are so many conventional security techniques that are available. These are once again reconsidered with the measure of its efficiency and effectiveness (Qi *et al*., 2010). This paper suggests some of the security deployment models and from that arrive at a distinct solution for security openings in cloud.

Security issues in SaaS: Security, Locality, Integrity check (Nepal *et al*., 2011), Segregation, Access, Confidentiality all above stated are the key factors of the data in the cloud, Authentication and authorization, Network security, Web application security, Virtualization vulnerability, Availability, Backup, Identity management and sign-on process are some of the important terminologies of security in SaaS application development.

Security issues in PaaS: In PaaS, client can construct their own application on the platform of cloud. Service provider should give the assurances for the in the cloud which is inaccessible between applications. With this client can ensure that there is no such vulnerability in the host or network. Since this service allows building the application at the top of platform PaaS is more extensible than

SaaS. Still the complex task is leveraging an Enterprise Service Bus (ESB) and must to be secure Web Service (WS) Security (Oracle, 2009) is the protocol to achieve the above stated (Jiang *et al.*, 2011). PaaS is struggling to slice the ESB. Consideration should be salaried to how cruel actors deal the arrival of cloud application and their incomprehensible components from their analysis. Hackers are like to attack the infrastructure and carry out widespread black box testing.

Security issues in IaaS: As we know IaaS service is for providing the basic requirements like hardware and cloud environment of an application so user can achieve virtualization. The developer can control the security. One of the important factors in this service is the privacy of data which has been stored in storage server of service providers. Customer must take care of their data, application and OS where as vendors can be only responsible for the security of environmental physically as well virtually.

THE IMPACT OF DEPLOYMENT MODEL

Degrees of security issues are varied depending on a deployment model of cloud. In general private cloud is comparatively less prone to risks than the public clouds because of the physical security i.e infrastructure of the cloud may get damaged due do the natural cause or internal cause, so it becomes most important. Information has been routed through so many third-party infrastructures in cloud, which may be an intruder's infrastructure while it is transmitted from source to destination. Even though a cloud is an advanced server, the fundamental technology remains the same. Since cloud is multi tenant network architecture, many users can be connected with the cloud through the internet. Here the problem comes in the form of security (Xia *et al.*, 2010). Due to the reasons stated above security of the cloud not only depends on the concerns but also the network. There are many security measures taken and some prominent security has also been given to the cloud. Still the normal Internet technology is being used for data transmission. Threats of the internet will also be the threats of cloud. Due to this, the risk level of cloud is being increased tremendously. The internet's security measure and the normal protocol are used by the cloud also since it follows the Internet but for cloud the need is much more. Secure protocol which robust in nature is required to safeguard the data in the mode of migration in cloud. So intrusion in the network must be considered (Dingguo *et al.*, 2011). Finally, with this security measures the cloud becomes secure, private and separated from the Internet, which will steer clear of cyber crimes in the cloud.

THE FIT-IN-PURPOSE CLOUD SECURITY SOLUTIONS

Data security solutions: One of the most prominent technique for the data security is cryptography scheme such as encryption and decryption. Basically security can be of simplest, one where it is low of cost for construction and easy for maintenance. This is relatively honest but not very secure. The high level security can also be used where it is incredibly difficult, maintenance becomes tough and limited provisions of access. In this case collections of data which is stored in the cloud are encrypted using secret keys later it can be decrypted to get back the information with the help of keys. But the question is about the key maintenance and managing it because the cloud servers are required to store the huge quantity of data as well the secret keys. To reduce the computational complexity proxy re-encryption schemes are used.

Physical security solutions: Here the security is to ensure the data center physically protected and the ability of power management, how long it will retain. Since cloud is a multi tenant network,

there is a query about the multi port configuration as well as the power distribution to those clients independently. The establishment of communication through fiber links between the users and service providers. All these problems are solved and the service providers need to get the certificate for the data center. The main issues and the remedial factor are listed below.

Port scanning: If the end user entering into the security platform through which it can get access permission from the resource to a precise destination, that particular node is susceptible for scanning. No such subscriber can stop the port scanning because it is gateway open for internet access. Clients can report suspected exploitation. So the tapping of port is avoided.

Man in the middle attack: A third person independently listening to the conversation between parties, making the parties believe that there is no such hole in their connection. But the conversation is entirely under the control of hacker. Application Programming Interface offered through SSL confined ports will grant authorization so that it can access server.

Network security solutions: Authentication is the best key to secure the cloud computing environment with TCP. Since cloud consist of various entities connected from different networks. As its first step those entities must prove their identity to the system admin of the cloud environment. An authentication process is the one which is important to the cloud because huge amount of entities, such as users and resources from different source. So authentication becomes complicated too. Authentication with TCP is depends on Trusted Platform Modules (TPM) which is a hardware defended against the attack from software as well as hardware since it is logically independent. TPM holds private master key which can also be a hardware certificate so hard to attack the key. TPM can provide conviction root for users. Key will be in the form of identities of the entities. Each site in the cloud, system admin will record the visitor's details. So user's can be traced easily in the cloud to avoid the entry of unauthenticated users.

Message security solutions: It consists of information risk management and the disaster recovery program. The stored data in a cloud should not be corrupted and also there should not be any leakage. It must be highly transparent to the access the cloud through which its ability to reduce risk of intrusion. Some rich computation is required to verify the authentication also through the signature platform or when the application code is running, as well as whether the cloud has strictly enforced their data's privacy policies. To balance the cloud when the following occupations are happening, managing disaster, bugs to find and fix, regularly updating the software, continuous usage pattern changes and user demand for high performance the developers will receive both development and maintenance support.

SERVICE AND APPLICATION SECURITY SOLUTIONS

Issue of incompatibility: Since cloud is a multi-tenant architecture many users can demand for cloud and there are so many cloud retailers are also available. The service providers are originating makes the process called "sticky services" where services of user are migrating between different cloud vendors.

Constant feature additions: Features of cloud applications are updated in a regular fashion by means of adding new features with the existing and clients will also need to keep track the improvements in cloud application. Rate and speed of change will affect both the security and Software development life cycle.

Failure in provider's security: If cloud server is getting crash due to the lack of security then there is a problem of accessing the physical resource, user's system need to be compromised. Cloud need to carry out many users, no cloud can be more secure than its weakest link. Basis of cloud environment is belief of client on service provider's security.

Infrastructure (servers, storage and network) security solutions: There is a need to safeguard data which is migrating, between client and system and between computer and computer. This kind of demanding process requires access control techniques to have a secured network which consist of servers and storage disks. Some of solutions are listed below.

Distributed denial of service (DDOS) attack: The servers and networks are getting down due to the large amount of traffic in a network and end users are left without the entrance to a convinced service like Internet (Azeez *et al*., 2011). The world's leading online retailer is Amazon Web Service (AWS) Application Programming Interface (API) are based on huge as Internet-scaling and top-notch infrastructure. It has its own Proprietary DDOS mitigation techniques.

IP spoofing: This is another big issue of security threat where some intruder who is an unauthorized person can get the access to the system by spoofing the IP address. Since information being transmitted along with the IP address by an intruder but the system identifies it as a trusted party.

Packet sniffing: Cloud is a multi tenant network so other client may try to listen (with software) the unprocessed network device for packets. If it fix in a particular criteria then it will logon to the packet. But in cloud it is impossible because of virtual machines. Different virtual requests can't be sniff. So the traffic can also be encrypted sensitively by the high end consumers.

Security incidents audit: Some habitual security auditing techniques like security log, compliance check tools are used for security audit in cloud environment to avoid situations like same security incidents occurring again. Basically audit is contributing the report based on reason analysis. But for the demand of security audit some new techniques need to be developed. In addition, as a new evidence- obtaining way, electric discovery is gradually accepted by court.

CONCLUSION

Security has been a major roadblock for the mass adoption of the powerful and pioneering cloud concepts. The concerned students, scholars and scientists are collaborating for unearthing competent, unbreakable and impenetrable security solutions. As virtual machines are being created or contracted on the fly from physical machines for provisioning compute and storage resources to subscribers on demand, the security complications go up sharply in cloud environments. In this paper, we have discussed the typical security issues and the corresponding solution approaches in the raging cloud space.

REFERENCES

Azeez, N.A., A.P. Abidoye, K.K. Agbele and A.O. Adesina, 2012. A dependable model for attaining maximum authentication security procedure in a grid based environment. Trends Appl. Sci. Res., 7: 78-86.

Azeez, N.A., I. Tiko, I.M. Venter, O.F.W. Onifade and R.A. Azeez, 2011. Grid security: Evaluation of active and passive attacks with proposed countermeasures. Res. J. Inform. Technol., 3: 181-190.

Ding, B., X.Y. Yu and L.J. Sun, 2012. A cloud-based collaborative manufacturing resource sharing services. Inform. Technol. J., 11: 1258-1264.

Dingguo, Y., C. Nan and T. Chengxiang, 2011. Research on trust cloud-based subjective trust management model under open network environment. Inform. Technol. J., 10: 759-768.

Gao, W. and F. Kang, 2012. Cloud simulation resource scheduling algorithm based on multi-dimension quality of service. Inform. Technol. J., 11: 94-101.

Jiang, Z., L. Zhu and Q. Xiao, 2011. A new rapid triangulation method of space closed point cloud. Inform. Technol. J., 10: 2476-2480.

Nepal, S., S. Chen, J. Yao and D. Thilakanathan, 2011. Data integrity as a service in the cloud. Proceedings of the IEEE 4th International Conference on Cloud Computing (CLOUD), July 4-9, 2011, Washington, DC., pp: 308-315.

Qi, K., D.F. Zhang and D. Xie, 2010. A high-capacity steganographic scheme for 3D point cloud models. Inform. Technol. J., 9: 412-421.

Rong, C., S.T. Nguyen and M.G. Jaatun, 2013. Beyond lightning: A survey on security challenges in cloud computing. Comput. Electr. Eng., 39: 47-54.

Schwarzkopf, R., M. Schmidt, C. Strack and B. Freisleben, 2011. Checking running and dormant virtual machines for the necessity of security updates in cloud environments. Proceedings of the 3rd IEEE International Conference on Cloud Computing Technology and Science, November 29-December-1, 2011, Athens, Greece, pp: 239-246.

Silas, S., E.B. Rajsingh and K. Ezra, 2012. Efficient service selection middleware using ELECTRE methodology for cloud environments. Inform. Technol. J., 11: 868-875.

Talib, A.M., R. Atan, R. Abdullah and M.A.A. Murad, 2011. Multi agent system architecture oriented prometheus methodology design to facilitate security of cloud data storage. J. Software Eng., 5: 78-90.

Talib, A.M., R. Atan, R. Abdullah and M.A.A. Murad, 2012. Security facilitation in collaborative cloud data storage implementation environment based on multi agent system architecture. J. Software Eng., 6: 49-64.

Xia, Y., L. Kuang and M. Zhu, 2010. A hierarchical access control scheme in cloud using HHECC. Inform. Technol. J., 9: 1598-1606.

Yuan, H., C. Li and M. Du, 2012. Resource scheduling of cloud computing for node of wireless sensor network based on ant colony algorithm. Inform. Technol. J., 11: 1638-1643.

Zhang, Z. and S. Fu, 2011. Characterizing power and energy usage in cloud computing systems. Proceedings of the 3rd IEEE International Conference on Cloud Computing Technology and Science, November 29-December-1, 2011, Athens, pp: 146-153.