VOLUME-6 | ISSUE-2 | FEBRUARY-2017 • ISSN No 2277 - 8179 | IF : 3.508 | IC Value : 78.46

SECURITY ISSUES AND SOLUTIONS IN CLOUD COMPUTING ARCHITECTURES:AN OVERVIEW

Engineering

KEYWORDS: security, cloud computing, IT, cloud services, reliability, privacy, business management

V.K.G.Kalaiselvi M.E

Assistant Professor, Department of Information Technology, Sai Ram Engineering College, West Tambaram, Chennai-600044,Tamil Nadu ,India

ABSTRACT

Cloud computing has become one of the hottest topics in the IT world today. Its model of computing as a resource has changed the landscape of computing as we know it, and its promises of increased flexibility, greater reliability, massive scalability, and decreased costs have enchanted businesses and individuals alike. However, many potential cloud users are reluctant to move to cloud computing on a large scale due to the unaddressed security issues present in cloud computing.. The cloud Services must be highly secured so that it increases the adoption of cloud for enterprise business management. Security and privacy are the main issues which decrease the growth of cloud computing and which cause question in clients This review paper aims to elaborate and analyze the numerous unresolved issues threatening the Cloud computing adoption and diffusion affecting the various stake-holders linked to it.

1.INTRODUCTION

Cloud computing has become as a popular and worldwide paradigm due to enable customers to use computational resources such as software, storage, and processing capabilities related to other companies. Cloud computing is often likened to many like technologies namely: grid computing,utility computing and autonomic computing. Cloud computing, as defined by NIST, is a model for enabling always-on, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., storage, applications, services, etc.) that can be rapidly provisioned and released with minimal management effort or service provider interaction [1]. It is a new model of providing computing resources that utilizes existing technologies. At the core of cloud computing is a data center that uses virtualization to isolate instances of applications or services being hosted on the "cloud". The data center provides cloud users the ability to rent computing resources at a rate dependent on the data center services being requested by the cloud user. Refer to the NIST definition of cloud computing, [1], for the core tenets of cloud computing. In a nut shell, cloud computing implements virtualization technology to attain the goal of providing computing resources as a utility [2]. This permits organizing pay-per-use commercial model, meaning that customers can get to exactly choose whatever resources (CPU, memory, bandwidth, security policies, platforms, and hardware load) that are they need, reducing costs by paying only for what is subscribed to [3]. Cloud computing does not realize the dream of computing as a utility only, but offers opportunity for its adoption[2]. But there are challenges faced this new technology. Security and privacy issues are considered the major challenges in cloud computing. In fact, major clients might grip back, choosing to keep infrastructures on-premises rather than moving them to outsourced locations. As the sensitive applications and data are moved into the cloud data centers, run on virtual computing resources in the form of virtual machine. This unique attributes, however, poses many novel tangible and intangible security and privacy challenges. It might be difficult to track the security issue in cloud computing environments [4].

The rest of this paper is arranged as follows: The section 2 presents cloud computing service models. The section 3 presents security issues of cloud computing. The section 4 presents current cloud security solutions. The section 5 presents Data Outsourcing Security As A Service (DOSAAS) . The final section 6 is discussed the conclusion.

2. CLOUD COMPUTING SERVICE MODELS.

According to NIST definition which is "Cloud computing is a model for enabling convenient, ondemand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction." Cloud computing model is as shown in Figure-1.

2.1 Software As A Service (SAAS)

The cloud service provider provides their end users with the capability to deploy their applications on cloud infrastructure. The cloud service provider licenses the applications to its end users based on pay as you use model or at no charge. SAAS was deployed for sales service force automation and customer relationship management. In addition to this SAAS is also extended for many business anagement such as human resource management, billing, financial management solutions[1].

2.2 Platform As A Service (PAAS)

Cloud Service Provider (CSP) rents hardware, operating system, storage, network capacity over the internet to the end users to build their application on top of platform. PAAS provides a development and deployment middleware layer[1]. The virtualized servers can be used to test the new application. With the PAAS OS features can be changed and upgraded frequently. Industries instead of maintaining multiple hardware facilities that often suffer from incompatible issues, can adapt PAAS that would provide a better solution to get rid of incompatible issues.

2.3 Infrastructure As A Service (IAAS)

The hardware resources such as servers, network and storage are virtualized and provisioned to the customers based on their application. Gartner's Cloud IAAS research guides on sourcing, infrastructure, best practices, hybrid cloud, security and risk management, and regional market evolution. The customers can use API (Application Program Interface) to start a service, to communicate with network elements (such as hosts, switches and routers) and add new devices. The user does not have control of the underlying hardware in the cloud instead they can only manage the OS, storage and delivered applications [1].

3. SECURITY ISUUES OF CLOUD COMPUTING.

Clouds are everywhere these days. They are often cheaper, more powerful, compatible with single sign-on (SSO) and often accessible via a Web browser. Of course, cloud computing is very different than physical or virtual servers, which translates into a different cyber security model as well. And these differences lead to a variety of security challenges. Using SaaS offerings in the cloud means that

there is much less need for software development. For example, using a web-based customer relationship management (CRM) offering eliminates the necessity to write code and "customize" a vendor's application. If you plan to use internally developed code in the cloud, it is even more important to have a formal secure software development life cycle (SDLC). The immature use of mashup technology (combinations of web services), which is fundamental to cloud applications, is inevitably going to cause unwitting security vulnerabilities in those applications. The development tool of choice should have a security model embedded in it to guide developers during the development phase and restrict users only to their authorized data when the system is deployed into production.[5]. Security issues have been the control barrier of the growth and extensive use of cloud computing.

3.1 Security issues in SaaS

3.1.1 Network security

In SaaS service model, different kind of data is flowing from client to cloud provider and also stored at the provider side. So, the data flowing over the internet needs to be secured to prevent the data hacking. Some strong encryption techniques are used to control using Transport layer Security (TLS) and Secure socket Layer (SSL) [6]. There are different types of attacks in network layer such as packet scanning, IP spoofing, Man in the Middle attacks (MITM) etc. There are strong risks that malicious attackers can exploit network security loopholes to sniff IP data packets.

3.1.2Data Accessibility

Application or data accessing over the network makes the life easier for cloud users. But, it also opens a gateway for security issues. The specific policies must be defined by the organization to access the data to avoid any intrusion within the network. Multi-tenant deployment can expose the issue on the managing data access within the single cloud environment [6]. So, the provider must adhere with the policies set for such scenario

3.1.3Multi-tenancy:

In SaaS service model, multi-tenants share a same database. The tenant information can be at risk if any misconfigured software application source code or data leakage takes place. Based on specific security policies, the authentication should be given to the users so that only data will be modified oraccessed into or from database for the particular tenant. The data of one client should be isolated from another client

3.2 Security Issues in PaaS:

3.2.1 Application development life cycle:

It is also a big challenge to secure a software application development because software developers face quite difficult to secure the application taking place in cloud environment. The application need to be upgraded by applying new patches or versions to keep them up-to-date and secure [8]. Developer should also aware of the legal issues of the data storage or the source code storage so that it could not be compromised [7].

3.2.2 Underlying Infrastructure security:

Cloud providers are responsible for underlying infrastructure security and the services running for applications [9]. So, the application developers have no privilege to access underlying infrastructure. SaaS and PaaS user can share the same applications because the software developed are delivered and used in SaaS while in PaaS, the development tool is used to develop and test the same application to be used by the SaaS users. So, there can be security concern about the user data and its storage [7].

3.2.3 Third-party Relationship:

Third-party also plays a important role in PaaS as the some third-party components are required in web services like Mashups which helps in integrating more than one source component into a single unit [10]. PaaS users and developers also need to depend on the services provided by third-party and the web-based development tool

3.3 Security Issues in IaaS

3.3.1 Impact of Cloud deployment model:

The IaaS layer is also vulnerable due to network and internet connectivity associated with it. It is more prone in public cloud compared to private cloud. Physical security of infrastructure is also required for any disaster happening. The data transmission path is also needed to secure as the intruders can easily attack the data communicating between sources to destination [12]. The data flowing over the internet is a major concern as the client and service providers are placed at two different locations which are connected through internet only. Therefore, it needs high encryption techniques and strong secure protocols to safeguard data transmission.

3.3.2 Virtualization:

Virtualization provides many features to the users to create, share, migrate, copy, rollback virtual machines which helps in running many applications on them [13],[14]. But, it also becomes prone to get attacked because it opens more entry for the attackers and interconnected virtual machines complexity [15]. Virtual machines should also be considered as important as any other physical device security

4. CURRENT CLOUD SECURITY SOLUTIONS

A research on cloud security is constantly going all over the world. Major cloud providers are also involved in working on the security solutions. Cloud security Alliance (CSA) is actively involving all the cloud providers and other individual people to participate and come up with some sound solutions. Tsai et al. brings a fourth-tier framework specifically for webbased development environment, provides some security at some extent [16]. In [17], Ristenpart et al. suggested that risks could be the attacks, so the cloud service providers should implement web-based co-residence check to control the attackers. Krugel et al. suggested the amount of packetsnifering output filtering for specific application services is a good approach to control security issues for specific services and network ports [18]. Kong et al. also suggested a good solution stated as "Partition-locked cache (PLcache) and random permutation cache (RPcache) to defeat cache-based side channel attacks" [19]. Raj et al. also suggested data security during processing using resource isolation method, by isolating the processor cache within the VMs and then isolating virtual cache from VMM cache [20]. The cloud security can also be enhanced by providing proper safeguard to operating systems and the virtual machines used for cloud network [21]. An cloud security has been introduced by the association with trusted third-party to ensure the security in terms of communication, integrity and confidentiality [22]. Milne et al. point out a simple solution to just use private cloud [23]. Jyoti et al. suggest that the virtualization would be the best option to shield with the security which provides less investment on hardware and multiple machines are managed centrally with high-end security [24]

5.DATA OUTSOURCING SECURITY AS A SERVICE (DOSAAS)

5.1 Out Sourcing.

It means that users physically lose control on their data and tasks. One of the root causes of cloud insecurity is the loss of control problem. To solve outsourcing security issues, it should be the cloud provider shall be trustworthy by offering trust and secure computing and data storage and the outsourced data and computation shall be confirmable to clienteles in terms of confidentiality, integrity, and other security services. Nowadays, Cloud customer negotiates their data control to the cloud provider, so there is a risk when the data is another compound. This research work introduces a new service called Data Outsourcing Security as a service to achieve robust technical security solution. We have mentioned following important aspects which helps to understand the flow of the DOSaaS and resolve this issue:

VOLUME-6 | ISSUE-2 | FEBRUARY-2017 • ISSN No 2277 - 8179 | IF : 3.508 | IC Value : 78.46

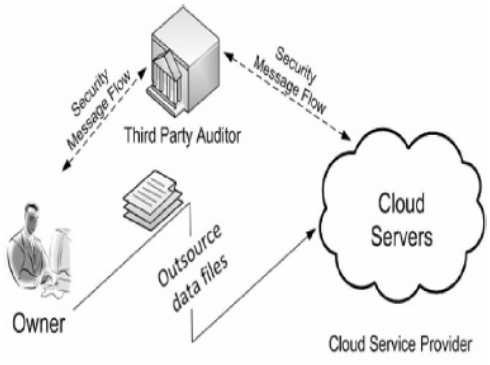

Figure-2 Data out sourcing

5.2 Confidentiality

It prevents confidential data accessed by wrong people, making sure that the right person can only reach it. There are various methods through which we can apply confidentiality like Data encryption is a common method used widely in industries, User IDs and passwords are also one of the common ways of ensuring confidentiality. Captcha is also one of the current used techniques avoiding from non-human access.

5.3 High Availability

High availability is also one of the important aspects of cloud computing security. There can be different reasons of nonavailability like network vulnerability, data storage failure etc. But the main thing which is bigger loophole is IP failover. Alternate IP addresses can be assigned to the virtual machines to avoid IP failures.

5.4 Integrity

Integrity helps to maintain the accuracy and trustworthiness of information of the entire product life cycle. There are risks that the data can be manipulated in transit by unprivileged people, and we need to make sure the user's stored data won't be corrupted. The outsourcing data needs to be kept protected by keeping the backups of data if any unexpected error occurs. The client needs to make clear and maintain the records what data is hosted on the cloud, the origin and control of data must be maintained to prevent data tampering or access of confidential data beyond the agreed territories.

5.5 Encrypted Key Management

There can be data compromised if the poor key management and insecure data storage happens, especially when any company having cloud infrastructure access managed by third-party company. At that time, the encryption keys security becomes a big issue. There can be many reasons behind the key access like key storage, weak key generation etc. Strong password also plays a vital role in securing key access. An unauthorized user or corrupt employee can come to know about your key or they can access machines where confidential data can be accessed. Data backup also highlights another problem as data archiving managed by cloud data storage provider. So, It can be better encrypted first and then send it back to cloud storage provider to avoid any risk. Crypto-shredding is also an important method of reducing risks.

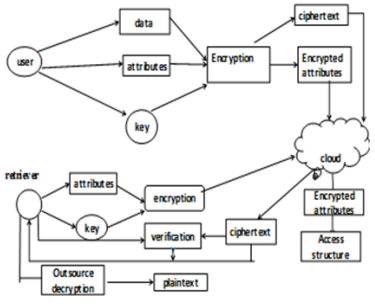

Figure-3 Cryptography during Data Sharing

5.6 Access Control

Cloud service provider needs to follow many accessing levels for the cloud computing by applying various access control lists. Encryption also helps in enabling access control to the cloud data. There could be a different level of access to the user data of the cloud. To prevent the unauthorized access of the cloud, the cloud provider creates access list. Microsoft uses Rule based Authorization for access control, Amazon web services provides SSL encrypted endpoints using secure HTTP web protocol [25].

5.7 Privacy Maintenance

The confidential information used to travel through the whole cloud network. So, there are strong chances of data being an easy prey by the attackers. They can misuse the services provided to the specific user or the data can also be manipulated. Security of private data needs to be taken care by protecting confidential information. Companies need to implement defined data privacy policy, on demand encrypted data transformation and data masking services [11]

5.8 Identity Management

Specific user only need to allow to access the application; the client should be given privilege to create, update and delete the new or existing users in order to keep the user access transparent and under client's control. There should be an add-ins or tool for password maintenance.

5.9 Service level agreements (SLAs)

SLA is a kind of contract blueprint between the customer and provider. Cloud data provider has the legal responsibility to prevent of data loss. If data is breached or lost, the blaming often goes to service providers. As with many legal documents, Cloud SLAs are more often written to the benefit of the cloud service provider, not to the cloud customer. Cloud service providers used to offer various levels of data protection, but it's still difficult to provide proper liability of customer data. Cloud SLA is documented that contains statements protecting the cloud service provider if data is lost or scrambled. In fact this agreement also helps to suggest that a cloud customer make "frequent archives" of their data and "encrypt" while transmission. The responsibility for managing the integrity of data, whether in a private cloud, hybrid cloud or public cloud or in a data centre, always goes to the company that owns data.

6. CONCLUSIONS

There are lots of advantages associated with the use of cloudcomputing. But, it also has some security concerns which slow down the open acceptance of this technology. Cloud providers need to ensure the customer about the confidential data security. This paper hasdiscussed on different security issues on services model level: IaaS, PaaS and SaaS. Network, shared resources, storage and virtualization are the main issues which are still immature and need to be looked ahead. This research work has introduced DOSaaS to illustrate the specific implications of this service model and the solutions. This research paper has also discussed current available solutions to overcome some common and major issues. There is need to have better encryption techniques and integrated cloud security framework to make it more dynamic with scalability.

ACKNOWLEDGMENT

I would like to thank Prof. Dr. T. Sheela Dean(NW) , Sairam Engineering college, West Tambaram , Prof .G.Ilanchezhiapandian, Mr.S.Kumarasamy Technical Architect, ZOHO corporation Chennai, and Dr.D.Geetha who continuously encouraged me during this study.

REFERENCES:

1. National Institute of Standards and Technology, NIST Definition of Cloud Computing, Sept 2011
2. Shahzad, F. (2014). State-of-the-art Survey on Cloud Computing Security Challenges, Approaches and Solutions. ProcediaComputer Science, 37, 357–2.doi:10.1016/j.procs.2014.08.053
3. Fernandes, D. a. B., Soares, L. F. B., Gomes, J.V., Freire, M. M., & Inacio, P. R. M. (2013). Security issues in cloud environments: asurvey. International Journal of Information

4. Security, 3(2), 113–170.doi:10.1007/s10207-013-0208-7
Williams, M. I. (n.d.). New Tool for s Busi ness A Quick Start Guide to Cloud ComputinG.
5. http://www.infosectoday.com/Articles/Cloud_Security_Challenges.htm
6. S. Subashini, V.Kavitha, "A survey on security issues in service delivery models of cloud computing", Journal of Network and Computer Applications (2010), doi:10.1016/j.jnca.2010.07.006
7. An analysis of security issues for cloud computing, Keiko Hashizume, David G Rosado, Eduardo FernándezMedina and Eduardo B Fernandez, Journal of Internet Services and Applications 2013, 4:5.
8. Ertaul L, Singhal S, Gökay S (2010) Security challenges in Cloud Computing. In: Proceedings of the 2010 International conference on Security and Management SAM'10. CSREA Press, Las Vegas, US, pp 36–42.
9. Chandramouli R, Mell P (2010) State of Security readiness. Crossroads 16 (3):23–25.
10. Keene C (2009) The Keene View on Cloud Computing. Online available: http://www.keeneview.com/2009/03/what-is-platformas-service-paas.html. Accessed: 16-Jul-2011
11. Protect Data Privacy, http://www- 01.ibm.com/software/data/optim/protect-data-privacy/.
12. Ristenpart T, Tromer E, Shacham H, Savage S. Computer Science and Artificial Intelligence Laboratory, Massachusetts Institute of Technology, Cambridge, US (2009). Hey, you, get off of my cloud: exploring information leakage in third- party compute clouds. In: Proceedings of the CCS 2009, ACM Press, 2009, p. 270– 4.
13. Jasti A, Shah P, Nagaraj R, Pendse R (2010) Security in multi-tenancy cloud. In: IEEE International Carnahan Conference on Security Technology (ICCST), KS, USA. IEEE Computer Society, Washington, DC, USA, pp 35– 41.
14. Garfinkel T, Rosenblum M (2005) When virtual is harder than real: Security challenges in virtual machine based computing environments. In: Proceedings of the 10th conference on Hot Topics in Operating Systems, Santa.
15. Reuben JS (2007) A survey on virtual machine Security Seminar on Network Security http://www.tml.tkk.fi/Publications/C/25/papers/Reuben_f inal..pdf. Technical report, Helsinki University of Technology October 2007.
16. Tsai W, Jin Z, Bai X. Internetware computing: issues and perspective. In: Proceedings of the first Asia-Pacific symposium on Internetware. Beijing, China: ACM; 2009. p. 1–10.
17. Ristenpart T, Tromer E, Shacham H, Savage S. Computer Science and Artificial Intelligence Laboratory, Massachusetts Institute of Technology, Cambridge, US (2009). Hey, you, get off of my cloud: exploring information leakage in third- party compute clouds. In: Proceedings of the CCS 2009, ACM Press, 2009, p. 270– 4.
18. Krugel C, Toth T, Kirda E. Service specific anomaly detection for network intrusion detection. In: Proceedings of the 2002 ACM symposium on applied computing, 2002, p. 201–8.
19. Kong J, O. Aciicmez, J.P. Siefert and H. Zhou, Deconstructing new cache designs for thwarting softwarecache-based side channel attacks, Proceedings of the 2nd ACM workshop on Computer security architectures, ACM, New York, USA, 2008, pp 25-34.
20. Raj H, Nathuji R, Singh A, England P. Resource management for isolation enhanced cloud services. In: Proceedings of the 2009 ACM workshop on cloud computing security, Chicago, Illinois, USA, 2009, p. 77– 84.
21. Santos N., K.P. Gummadi and R. Rodrigues, Towards trusted cloud computing. Proceeding of the conference on hot topics in cloud computing, (Hot Cloud'09), Berkeley, CA, USA.
22. Zissis D. and D. Lekkas, Addressing cloud computing security issues, Future Gener. Comput. Syst.,2012, 28:583-592.
23. J.Privatecloudprojectsdwarfpublicinitiatives,2010 http://www.cbronline.com /news/private_cloud_projects_dwarf_public_initiatives_281009S .
24. Jyoti S., S. manish and G. Rupali, Virtualization as an engine to drive cloud computing security. Proceeding of the High Performance Architecture and Grid Computing, July 19-20, 2011, Chandigarh, India, pp: 62-66
25. Dr. Arockiam L, Parthasarathy G and Monikandan S, Privacy in Cloud Computing: A Survey, CS & IT-CSCP 2012, pp. 321–330.