International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 05 Issue: 02 | Feb-2018 www.irjet.net p-ISSN: 2395-0072

Cloud Computing Security: Survey on Issues and Challenges

S. Hendry Leo Kanickam[1], Dr.L.Jayasimman[2], J.Iswarya[3]

[1]Research Scholar, Srimad Andavan Arts & Science College, Trichy, Tamilnadu, India
[2]Asst.Professor, Dept of CS, Srimad Andavan Arts & Science College, Trichy, Tamilandu, India
[3]II.M.Sc Computer Science,Dept of IT, St.Joseph's College, Trichy, Tamilnadu, India

---

Abstract - *It is providing a meaning of access the applications and its utilities over the internet. It is allow being Modify the applications online. Cloud referred as network or internet. We need not to install a piece of software on a local PC and this is how the cloud computing overcomes platform dependency issues. Hence, the Cloud Computing is making our business application mobile and collaborative. Security in cloud is a major concern. Data is to be stored in a form of cloud. A security is a Biggest concern in cloud computing. A data management infrastructure management and cloud is provided by a third party. It is to be having more secure password protected accounts. Mega data center is securely architected and the control node, entry point mega data is also to be secure. In this paper, we take a holistic view of cloud computing security spanning across the possible issues.*

KEYWORDS*: Cloud Computing, Security, Trusted Computing, and data privacy*

1. INTRODUCTION

Security is a major concern of cloud computing. Data is to be stored in encrypted form. Selecting resources is Going to move cloud and analyze its sensitivity to risk. Cloud service models are IaaS (infrastructure as a service), PaaS (platform as a service), and SaaS (software as a service). Cloud types are public, private, community or hybrid. Considering cloud service provider's how data is transferred, where it is stored and how to move data into and out of cloud. Cloud computing faces a lot of different challenges. Security is one of the key challenges, and has become the key of popularization cloud computing and restrictive factor. The enterprise and the organization accept cloud computing services, it is necessary to solve the security problems. Many companies developing and offering cloud computing products and services but have not properly considered the implications of processing, storing and accessing data in a shared and virtualized environment. In fact, many developers of cloud-based applications struggle to include security. Cloud computing is sharing of resources on a larger scale which is cost effective and location independent. Resources on the cloud can be used by the client and deployed by the vendor such as amazon, google, ibm,Microsoft. Cloud is not only for Multinational companies but it's also being used by Small and medium enterprises. The remainder of this paper deals with Cloud service model, characteristics, issues and challenges of cloud Computing. At the end we discuss about the future scope of Cloud.

II. LITERATURE REVIEW

S.S. Yeo, J.H. Park(2013) he explained Cloud Computing Open Architecture (CCOA) concept is discussed for clouds in virtual environments. The role and functions of the architecture are discussed according to different infrastructures for IT and business systems. Different types of architectures complicate security management for cloud systems. This architecture provides a solution for different security aspects regarding virtual environments. Authorized users based on the role-based access control can access the sensitive data on platforms. To pre-vent intrusion attacks, cloud service provider blocks the malicious and un-trusted codes enabling digital forensic applications. The application softwares at SaaS are provided with a specific license based subscription, pay-as-go . P. Arora, R.C. Wadhawan, E.S.P. Ahuja(2012) he given Platform as a Service (PaaS) caters services for operating system, network capacity, storage and multi-tenancy via the Internet. Infrastructure as a service (IaaS) provides utility computing, automation of administrative tasks, dynamic scaling, desktop virtualization, policy-based services, and Internet connectivity. IaaS provides virtual servers with unique IP address and storage pool as required by customers. Dikaiakos, M.D., Katsaros, D., Mehra, P (2009) he proposed Still, several outstanding issues exist, particularly related to SLAs, security and privacy, and power efficiency. Other open issues include ownership, data transfer bottlenecks, performance unpredictability, reliability, and software licensing issues. Finally, hosted applications' business models must show a clear pathway to monetizing cloud computing. Catteddu, D(2010) he explained Cloud computing are currently having many security problems and also become block to the development and popularization of cloud computing so there need to be build a cloud computing security framework and actively carry out its cloud security key technology research. S.Hendry leo kanickam , L. Jayasimman (2016) he proposed this paper deeply analyses the Cloud Computing security hazards in layer wise such as Service layer (IaaS, SaaS, PaaS) network layer, storage layer and deployment models such as Public, Private and Hybrid cloud environments.Fig.1 represents the schematic diagram showing the layers of the cloud computing, with security challenges. In the past decade the review of cloud computing issues were focused overall cloud problems but not in depth as layer wise. Because authors in previous history were focused their security views on the data storage and data transactions. but not in the networks, operating systems and its related issues. Moreover the issues identified and security provided for the service users not for providers. In cloud environment the providers also having risks when compare to users.

III. CLOUD SERVICE MODEL

Software as a Service (SaaS)

- The provider apps.
- User doesn't manage or control the network, servers, OS, storage or applications.

Platform as a Service (PaaS)

- User deploys their apps on the cloud.
- Controls their apps.
- User doesn't manage servers, IS, storage.

Infrastructure as a Service (IaaS)

- Consumer gets access to the infrastructure to deploy their stuff.
- Doesn't manage or control the infrastructure.
- Does manage or control the OS, storage, apps, selected network components.

IV. CHARACTERISTICS OF CLOUD COMPUTING

In this section we describe the characteristics that a cloud must possess. Any cloud is expected to have these five characteristics that are being described below.

A. On-demand self-service

A Cloud Computing Environment customer provision computing capabilities, which is server time and network storage, as needed automatically without requiring human interaction with each service's provider.

B. Broad network access

Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, laptops, and personal digital assistants (PDAs)).

C. Resource pooling

The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the subscriber generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or data centre). Examples of resources include storage, processing, memory, network bandwidth, and virtual machines.

D. Rapid elasticity

Capabilities can be rapidly and elastically provisioned, in some cases automatically, to quickly scale out and rapidly released to quickly scale in. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be purchased in any quantity at any time.

E. Measured Service

Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported providing transparency for both the provider and consumer of the utilized service.

V. SECURITY ISSUES IN CLOUD COMPUTING

The cloud service provider makes sure that the customer does not face any problem, so loss of data or data theft. There is also a possibility where a malicious user can penetrate the cloud by impersonating a legitimate user, there by infecting the entire cloud. This leads to affects many customers who are sharing the infected cloud.

There are four types of issues are:

- Data Issues
- Privacy issues
- Infected Application
- Security issues

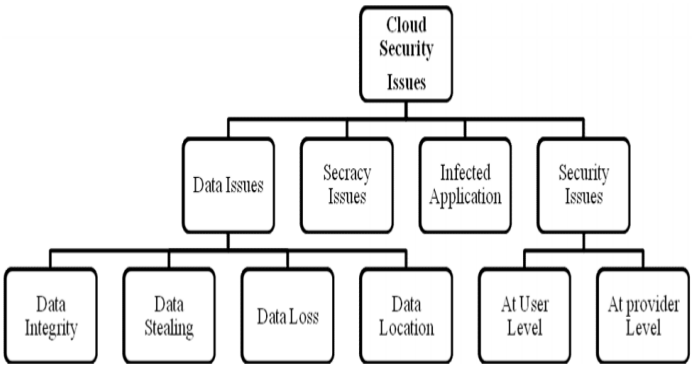

Fig 1: security issues classification in cloud

Data Issues:

Sensitive data are stored in cloud computing environment it is a major issues with regard to security in a cloud based system. First a data is on a cloud, anyone from anywhere anytime can access data from the cloud since data may be common, private data are also in a cloud. So at the same time, many cloud computing service consumer and provider accesses and modify data. Thus there is a need of some data integrity method in cloud computing. Second one is a data stealing is a one of serious issue in a cloud computing

environment. Many cloud service provider do not provide their own server instead they acquire server from other service providers due to it is cost affective and flexible for operation and cloud provider. So there is a much probability of data can be stolen from the external server. Third one is a Data loss is a common problem in cloud computing. If the cloud computing service provider shut down his services due some financial or legal problem then there will be a loss of data for the user. Moreover, data can be lost or damage or corrupted due to miss happening, natural disaster, and fire. Due to above condition, data may not be accesses able to users. Fourth one is a data location it is also one of the issues what requires focus in a cloud computing environment. Physical location of data storage is very important it should be transparent to user and customer.

Secrecy Issues:

Service provider must make sure that the customer personal information is well secured from other providers, customer and user. As most of the servers are external, the cloud service provider should make sure who is accessing the data and who is maintaining the server so that it enable the provider to protect the customer's personal information.

Infected Application:

Cloud computing service provider should have the complete access to the server with all rights for the purpose of monitoring and maintenance of server. So this is well preventing any user from uploading any infected application onto the cloud which will severely affect the customer and cloud computing service.

Security issues:

Cloud computing security has on two levels. One is on provider level and another is on user level. service provider should make sure that the server is well secured from all the external threats it may come across. Even the cloud computing service provider has provided a good security layer for the customer and user, the user should make sure that there should not be any loss of data or stealing or tampering of data for other users who are using the same cloud due to its action. A cloud is good only when there is a good security provided by the service provider to the user.

VI.CONCLUTION AND FUTURE WORK

Cloud service provider and the customer should make sure that the cloud is safe enough from all the external threats, so there will be a strong and mutual understanding between the customer and the cloud service provider. The largest gaps between cloud security practice and cloud-security research theory lies in the fact that the assumptions in the research leave out some very important differences between actual cloud security and virtual machine security. Research should be center on these gaps and differences and its removal. One of the pieces of the framework might be developing a way to monitor the cloud's management software, and another might be development of isolated processing for specific clients' applications. People's behavior can be tracked and monitored for instance whether people allow the automated patching software to run, or updating anti-virus software definitions, or whether people understand how to harden their virtual machines in the cloud. Additionally we have presented few high-level steps towards a security assessment framework. We made several observations in current cloud security landscape. Cloud computing as a platform for outsourcing and remote processing of application and data is gaining rapid momentum. Security concerns, especially those around platform, data and access it will be discussed all the issues.

REFERENCES

[1] S.S. Yeo, J.H. Park, Security considerations in cloud computingvirtualization environment, Grid Pervasive Comput. LectureNotesComput. Sci. 7861 (2013) 208–215.

[2] H. Yu, N. Powell, D. Stembridge, X. Yuan, Cloud computingand security challenges, in: Proc of the 50th Annual SoutheastRegional Conference (ACM-SE12), ACM, New York, USA,2013, pp. 298–302.

[3] P. Arora, R.C. Wadhawan, E.S.P. Ahuja, Cloud computingsecurity issues in infrastructure as a service, Int. J. Adv. Res.Comput. Sci. Softw. Eng. 2 (1) (2012) 1–7
Dikaiakos, M.D., Katsaros, D., Mehra, P., et al.: Cloud Computing: Distributed Internet Computing for IT and Scientific Research 13, 10–13 (2009)

[4] Catteddu, D.: Cloud Computing: Benefits, Risks and Recommendations for Information Security. CCIS, vol. 72, pp. 50–56 (2010)

[5] S.Hendry Leo Kanickam, L.Jayasimman ,A Layer wise Issues and Challenges in Cloud Security , IEEE Xplore,978 -1-5090-5573-9, pp 168-171 (2016)

[6] Carpenter, M., Liston, t., and Skoudis, E, Hiding Virtualization from Attackers and Malware. IEEE Security and Privacy Magazine, 2007

[7] Ristenport, T., Tromer, E., Shacham, H., and Savage, S., Hey, You, Get Off of My Cloud: Exploring Information Leakage in Third-Party Compute Clouds. Proceedings of the 16th ACM conference on Computer and Communication Security, 2009

[8] M. Jensen, N. Gruschka, and R. Herkenh¨oner, A survey of attacks on web services, ComputerScience Research and Development (CSRD), Springer Berlin/Heidelberg. 2009.

[9] King, N.J. and Raja, V.T. (2012).Protecting the privacy and security of sensitive customer data in the cloud. Computer Law and Security Reviews, 28, 308-319.

[10] Joint, A. and Baker, E. (2011). Knowing the past to understand the present 1 e issues in the contracting for

cloud based services. Computer Law & Security Review, 27, 407 - 415. doi:10.1016/j.clsr.2011.05.002.

BIOGRAPHIES

Mr.S.Hendry Leo Kanickam working as a Assistant Professor in Department of Information Technology ,St. Joseph's College (autonomous) Trichy, India.
He received his M.Phil Degree in Bharathidasan University in 2008 and also He is pursuing Ph.D (Computer Science) in Bharathidasan University.

Dr. L. Jayasimman working as a Assistant Professor, with Department of Computer Science, Srimad Andavan Arts & Science College, Trichy, India.
He received his M.Tech Degree in Bharathidasan University, Trichy, India in 2008 and completed his PhD (Computer Science) in Bharathidasan University in 2014.

Ms. Iswarya is studying II M.Sc Computer Science in Department of Information Technology, St. Joseph's College, Trichy , India.