International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2018 IJSRCSEIT | Volume 3 | Issue 1 | ISSN : 2456-3307

Network Security Issues In Cloud Computing

Rajarathinam*[1], Marrynal S Eastaff[2]
*[1]PG Scholar, PG Department of IT, Hindusthan College of Arts and Science (Autonomous), Avinashi Road, Coimbatorem, TamilNadu, India
[2]Assistant Professor, PG Department of IT, Hindusthan College of Arts and Science (Autonomous), Coimbatorem, TamilNadu, India

ABSTRACT

Today, cloud computing is a rising way of computing in computer knowledge. Cloud computing is a set of possessions and services that are on hand by the network or internet. Cloud computing extend a variety of computing techniques like grid compute, distributed computing. Today cloud computing is used in both industrial pasture and educational field. As the meadow of cloud computing is scattering the new technique are increasing. This amplifies in cloud computing location also increases security challenges for cloud developers. Users of confuse save their data in the shade hence the lack of security in cloud can lose the user's trust. In this paper we will discuss some of the cloud security issue in a mixture of aspects like multi-tenancy, stretch, accessibility etc. the paper also argue existing security technique and approaches for a protected cloud.

Keywords : Security issues for clouds, Cloud Computing Challenges, and Security Problem Space

I. INTRODUCTION

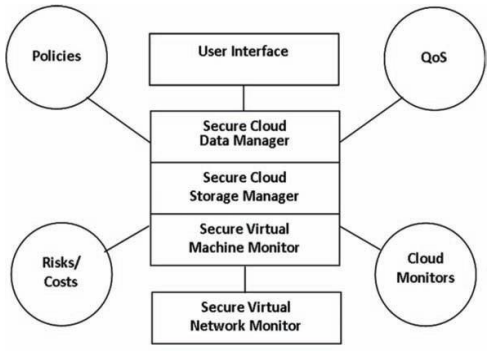
Cloud computing is another Christian name for Internet computing. The description of cloud computing provided by countrywide Institute of values and Technology (NIST) says that: "Cloud computing is a model for enabling on-demand and convenient network access to a shared pool of configurable computing resources (e.g., networks, servers, storage applications and services) that can be speedily provisioned and unconfined with minimal management effort or service provider communication. For some a paradigm provides computing resources and storage while for others it is just a way to access software and data from the cloud. Cloud computing is popular in organization and academic today because it provides its user scalability, litheness and ease of use of data. Also cloud computing reduces the cost by enable the sharing of data to the organization. Organization can port their data on the cloud so that their shareholders can use their statistics. Google apps is an example of cloud compute However Cloud provides various capability and benefits but still it has some issues concerning safe admission and storage space of data.

SaaS (Software as a Service): Complete applications, customizable within limits, solving specific business needs, with focus on end-users requirements
PaaS (Platform as a Services): No need to directly manage OS, databases, etc. API's for building higher level applications. Pre-built applications components.
IaaS (Infrastructure as a service): No need to purchase or manage physical data center equipment(servers, storage, networking, etc.

II. SECURITY ISSUES FOR CLOUDS

There are frequent refuge issues for cloud computing as it encompass many equipment- gives as well as network, record, operating system, virtualization, resource scheduling, business function, load balancing, connotes run with recollection in a row. Therefore, sanctuary issue for many of these systems

and technologies are applicable to cloud compute. Finally, data mining technique may be applicable to malware detection in clouds. We have completed the technology and concepts we have urbanized for secure grid to a secure cloud. We have distinct a coated construction for assured cloud compute consisting of the locked virtual appliance layer, safe and sound cloud luggage compartment layer, secure cloud data layer, along with the protected virtual network monitor coating . Cross cutting services are provided by the policy layer, the cloud monitor layer, the reliability layer and the risk analysis layer. For protected Cloud account- age supervision, we are developing a storage infrastructure, which integrates funds from multiple providers to form a colossal virtual storeroom system. When a storage bump hosts the data from multiple spheres of influence, a VM will be created for each sphere of influence to isolate the information and corresponding data processing.



The problem of security in cloud computing has been analyzed. All the Security issues of cloud computing are tinted in this paper, because of the density which users found in the cloud, it will be difficult to achieve end-to-end security. New security techniques need to be developed and older security techniques needed to be changed or better. In this study, we reviewed the literature for security challenges in cloud computing and proposed a security model and framework to make cloud computing environment safe. Consumer Based seclusion superintendent This technique helps to reduce the loss of private data and threat of data escape that processed in the cloud, as well as provides additional privacy related benefits Transparent Cloud Protection System (TCPS) This provides protection system for clouds designed at clearly monitoring the reliability of cloud components. Secure and Efficient Access to Outsourced Data This make available protected and regimented access to Outsourced data is an middle factor of cloud computing and forms the foundation for information organization and other operation In this paper, security in cloud computing was discussed in a manner that covers security issues and challenge, security principles and security management models.

III. CLOUD COMPUTING CHALLENGES

The current adoption of cloud computing is associated with numerous challenges because users are still unconvinced about its dependability. Based on a survey conducted by IDC in 2008, the major challenges that prevent Cloud Computing from being adopted are recognized by organizations are as follows:

A. Security

It is understandable that the safety issue has played the most imperative role in hinder Cloud computing receipt. Well-known security issues such as data loss, phishing (running remotely on a collection of machines) pose serious threats to organization's data and software. What is more, the multi-tenancy representation and the joint computing resources in cloud computing has introduced new safekeeping challenged that need novel technique to undertake with.

B. Charging Model

The stretchy reserve puddle have complete the cost investigation a lot more complex than ordinary data centres, which often calculate their cost based on consumptions of stationary computing. In addition, an instantiated virtual machine has become the unit of cost psychiatry rather than the original physical server. These contain: re-design and re- development

of the software that was at first used for single-tenancy, cost of providing new features that allow for intensive customization, performance and security enhancement for simultaneous user access, and dealing with complexities induced by the above changes. as a consequence, SaaS supplier require to consider up the trade-off flanked by the state of multi- tenancy and the cost-savings give way by multi-tenancy such as strong overhead all the way through paying back, condensed number of on-site software licenses, etc.

C. Service Level Agreement (SLA)

Although cloud clients do not contain manage over the primary computing capital, they do require to make sure the excellence, accessibility, consistency, and presentation of these possessions when consumers have core business functions onto their entrust cloud. In other words, it is vital for patrons to obtain guarantee from providers on service release. The extremely primary copy is the explanation of SLA circumstance in such a way that has an opposite level of granularity, namely the tradeoffs between expressiveness and complicatedness, so that they can coat most of the user potential and is quite simple to be slanted, unproven, evaluate, and enforced by the resource allocation mechanism on the cloud.

D. Cloud Interoperability Issue

As the hype over cloud computing evolves into a more substantive discussion, one thing has become clear -- customers do not want to be locked into a single cloud provider. They would like the freedom to move among the clouds -- ideally from public to private and back again. This would give customers the freedom to switch providers as their computing needs grow or shrink, and the ability to move applications and workloads around as their business requirements change. The primary goal of interoperability is to realize the seamless fluid data across clouds and between cloud and local applications. Present are a numeral of level that interoperability is indispensable for cloud compute. First, to optimize the IT advantage and computing possessions, an association often requirements to maintain in-house IT assets and capability connected with their core competencies while outsourcing insignificant function and actions on to the obscure. Second, more often than not, for the principle of optimization, an association may need to subcontract a figure of trivial function to cloud services obtainable by dissimilar vendor.

E. Security Problem Space

It is anticipated that security is one of the major factor influencing the a rejection for cloud computing in realistic purpose domain, especially when receptive information shall be bring into the cloud or IT governance require an elaborated control concerning the (legal) accountability of computing in vapours. From a users' perspective the security topics differentiate infrastructure safekeeping, platform and application safety, the safekeeping of the administration processes and Nelly compliance and governance. The solutions that address these topics can be distinguished by the extent to which security objectives are met (authentication & authorisation), how are system components and content protested (availability, confidentiality & integrity), how can the security properties be validated and checked (auditing), how can the cloud provider avert others from doing forbidden things (misuse protection). Cloud networking adds new defence challenges to the cloud computing security issues, arising from additional networking capability. On the other hand, there are indication that cloud networking can potentially get better control over the cloud computing consumption model, thus solving the security challenges that impact acceptance of this know-how.

F. Information Security in Clouds

Information security relies on the conventional three pillars, confidentiality (information should not be disclosed to unauthorised third parties), integrity (information should not be altered without evidence of the transformation), and accessibility (information should not be withheld from rightful access). The cloud scope adds a significant dimension in the integration of code and data. Cloud users will need to

ship code for implementation on their data to cloud provider.

G. Trust in an Adversarial Environment Cloud environment

Cloud providers balance the needs their multiple user, and attempt to monetize by-product of their movement. Cloud users strive to obtain the cheapest possible armed forces, while request services of towering excellence, and in respect of their time alone. Attackers, who have become very skilled at operating huge botnets (which can be seen as the first large scale clouds), will attempt to either right of entry the in rank obtainable in blur, or avail themselves to this processing power free of charge. All actors thus have their own trust objectives, implemented in their safekeeping policies.

H. Confidentiality of Information and Processes

One of the most effective ways to maintain truthfulness and confidentiality of in turn is encryption. While encryption in its current form is sufficient for data luggage screened-off area and trans- port, it necessarily prevents data processing. Thus, sending encrypted data to cloud providers for handing out is useless. Homomorphism cryptography ensures that operations performed on an encrypted text essentially still allow retrieving by decryption the procedure text in plain text.

IV. CONCLUSION

There are many new technologies budding at a rapid speed each with technological advancements and with the potential of production human's lives easier. However, solitary must be very careful to recognize the safekeeping risks and challenges posed in utilizing these technologies. Cloud computing is no immunity. In this paper key security consideration and challenges, which are presently face in the Cloud computing are discussed.

V. REFERENCES

[1] Akhil Behl (2011), Emerging Security Challenges in Cloud Computing (An insight to Cloud security challenges and their mitigation).

[2] Bertino, E. (2002). Access Control for XML Docu- ments. Data & Knowledge Engineering, 43(3).

[3] Bertino, E. (2004). Selective and Authentic Third Party Distribution of XML Documents. IEEE Transactions on Knowledge and Data Engineering, 16(10). doi:10.1109/TKDE.2004.63

[4] DeVries, B. W., Gupta, G., Hamlen, K. W., Moore, S., & Sridhar, M. (2009). ActionScript Bytecode Verifi- cation with Co-Logic Programming. In Proceedings of the ACM SIGPLAN Workshop on Programming Languages and Analysis for Security (PLAS).

[5] Arijit Ukil, Debasish Jana and Ajanta De Sarkar" A SECURITY FRAMEWORK IN CLOUD COMPUTING INFRASTRUCTURE "International Journal of Network Security & Its Applications (IJNSA), Vol.5, No.5, September 2013 DOI: 10.5121/ijnsa.2013.550211.

[6] Rabi Prasad Padhy, Manas Ranjan Patra and Suresh Chandra Satapathy ," Cloud Computing: Security Issues and Research Challenges", IRACST - International Journal of Computer Science and Information Technology & Security (IJCSITS) Vol. 1, No. 2, December 2011.

[7] Kashif Munir and Prof Dr. Sellapan Palaniappan," FRAMEWORK FOR SECURE CLOUD COMPUTING ", International Journal on Cloud Computing: Services and Architecture (IJCCSA), Vol.3, No.2, April 2013.

[8] J. Brodkin. (2008, Jun.). "Gartner: Seven cloud-computing security risks." Infoworld , Available: <http://www.infoworld.com/d/security-

central/gartner-seven-cloudcomputing-security-risks-853?page=0,1> [Mar. 13, 2009].

[9] Arjun Kumar, Byung Gook Lee, HoonJae Lee, Anu Kumari, "Secure Storage and Access of Data in Cloud Computing", 2012 International Conference on ICT Convergence (ICTC), 15-17 Oct. 2012

[10] Uma Somani, Kanika Lakhani, Manish Mundra, "Implementing Digital Signature with RSA Encryption Algorithm to Enhance the Data Security of Cloud in Cloud Computing", 1st International Conference on Parallel, Distributed and Grid Computing (PDGC - 2010).

[11] V.Nirmala, R.K.Sivanandhan, Dr.R.Shanmuga Lakshmi, "Data Confidentiality and Integrity Verification usingUser Authenticator scheme in cloud", Proceedings of 2013 International Conference on Green High Performance Computing (ICGHPC 2013). March 14-15, 2013, India.

[12] Sultan Aldossary, William Allen, "Data Security, Privacy, Availability and Integrity in Cloud Computing: Issues and Current Solutions", in International Journal of Advanced Computer Science and Applications, Vol. 7, No. 4, 2016

[13] Kuyoro S. O., Ibikunle F. & Awodele O. International Journal of Computer Networks (IJCN), Volume (3) : Issue (5) : 2011 254

[14] Cloud Computing Use Case Discussion Group. "Cloud Computing UseCases Version 3.0," 2010.

[15] Streitberger W. Ruppel, A.: Cloud computing security - protection goals, taxon- omy, market review. Tech. rep., Institute for Secure Information Technology SIT (2010)

[16] Abi Haidar, D., Cuppens-Boulahia, N., Cuppens, F., Debar, H.: XeNA: an access negotiation framework using XACML. Annals