Volume 5, Issue 5, May 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Security Issues in Various Clouds

Preeti Sondhi*, Anuradha Panjeta
CSE & Kurushetra University
Haryana, India

Abstract—"Cloud Computing is the next step in the evolution of on-demand network access to a shared pool of configurable resources that can be rapidly provisioned and released with minimal management effort or service-provider interaction. Cloud Computing provides benefits in terms of low cost and accessibility of data, but its unique aspect is its security. This paper puts forward a basic taxonomy of Different types of clouds architecture and the security issues which affect the performance of Cloud Computing"

Keywords— Cloud Computing; Security; Resources; Scalability; Virtualization; Service Level Agreement (SLA)

I. INTRODUCTION

Throughout Numerous attempts have been made in computer science history, to disengage users from computer hardware needs, from time sharing utilities envisioned in the 1960s, to the commercial grid computing emerged in the early 1990s, as high performance computers were interconnected via fast data communication links, with the aim of supporting complex calculations and data intensive applications . Cloud Computing has resulted from the convergence of Grid Computing, Utility Computing and Saas, and essentially represent the increasing trends towards the external deployment of IT resources. From the past few years, there has been a rapid progress in Cloud Computing. Cloud Computing is a model for convenient and on-demand network access to a shared pool of configurable resources that can be rapidly released with minimal management effort [1]. It simply means "Internet Computing" generally the internet is seen as collection of clouds; thus the word cloud computing can be defined as utilizing the internet to provide technology enabled services to the people and organizations. It enables consumers to access resources online through the internet, from anywhere at any time without worrying about technical/physical management and maintenance issues of the original resources. Cloud computing is also known as utility computing or 'IT on demand'. Scalability is the key attribute of cloud computing and is achieved through server virtualization. This fresh, web based generation of computing uses remote servers placed in extremely safe and secure data centres for storage of data and management, so organizations do not need to pay for and look after the internal IT solutions . It enables consumers to access resources online through the internet, from anywhere at any time without worrying about technical/physical management and maintenance issues of the original resources Besides, Resources of cloud computing are dynamic and scalable. Google Apps is the paramount example of cloud computing, it enables to access services via the browser and deployed on millions of machines over the internet. Resources are accessible from the cloud at any time and from any place across the globe using the internet. Cloud computing is cheaper than other computing models; zero maintenance cost is involved since the service provider is responsible for the availability of services and client are free from maintenance and management problems of the resources machines. Some examples of Cloud Computing Services are Amazon's Elastic Compute Cloud (EC2) [10] and IBM's Blue Cloud [11]

The beauty of cloud computing, as shown in Fig. 1 below, is that another company hosts your application. This means that they handle the costs of servers, they manage the software updates. By having someone else host the applications, you need not buy the servers nor pay for the electricity to power and cool them. It's also convenient for telecommuters and traveling remote workers, who can simply log in and use their applications wherever they are

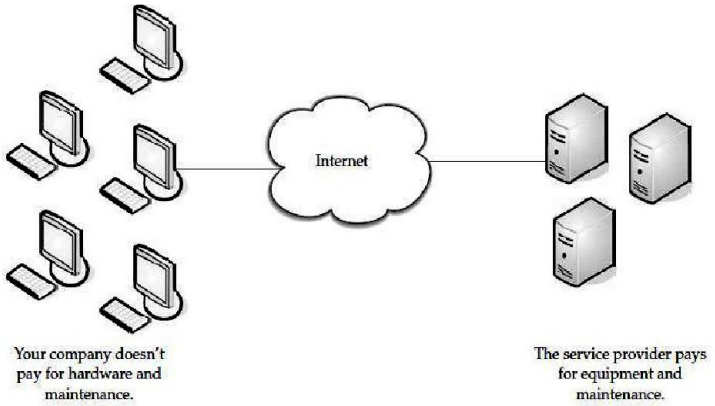

Fig. 1 Example of Cloud Computing Architecture

Although Cloud computing offers an innovative business model for organizations to adopt IT services without investment. Despite the potential gains achieved from the cloud computing, the organizations are slow in accepting it due to security issues and challenges associated with it. Security is one of the major issues which hamper the growth of cloud. The idea of handing over important data to another company is worrisome; such that the consumers needs to understand the risks of data breaches in this environment. Cloud computing is a way to increase the capacity or add capabilities dynamically without investing in new infrastructure, training new personnel, or licensing new software. It extends Information Technology's (IT) existing capabilities. In the last few years, cloud computing has grown from being a promising business concept to one of the fast growing segments of the IT industry. But as more and more information on individuals and companies are placed in the cloud, concerns are beginning to grow about just how safe an environment it is. Despite of all the hype surrounding the cloud, customers are still reluctant to deploy their business in the cloud. Security issues in cloud computing has played a major role in slowing down its acceptance, in fact security ranked first as the greatest challenge issue of cloud computing.

II. LITERATURE REVIEW

[1] Cloud Computing – Issues, Research and Implementations

Mladen A. Vouk: This Paper discusses the concept of "cloud" computing, Service-oriented Architecture and its components and tries to address the related research topics and a "cloud" implementation based on VCL technology. Their experience with VCL technology is excellent and working on additional feature that will make it more suitable for cloud framework construction.

[2] Cloud Computing Security: From Single to Multi-Clouds

Mohammed A. AlZain, Eric Pardede , Ben Soh , James A. Thom: This paper surveys recent research related to single and multi-cloud security and addresses possible solutions. It is found that the research into the use of multi-cloud providers to maintain security has received less attention from the research community than has the use of single clouds. This work aims to promote the use of multi-clouds due to its ability to reduce security risks that affect the cloud computing user. The main purpose of this paper is to showcase the recent researches on single and multi- clouds and to address the security risks and solutions. At the end they support the migration to multi-clouds due to its ability to decrease security risks that affect the cloud computing user.

[3] Security Issues in Cloud Computing -A Review

Anitha Y : This paper focussed on the security issues of cloud computing Firstly it discusses the definition of cloud computing ; components that affect the security of the cloud then it explores the cloud security issues and problems faced by the cloud service provider. It discussed solution, First solution they gave is Service Level Agreement (SLA) between the customer and service provider. Second solution they gave is the Data Splitting over multiple hosts that cannot communicate with each other; only the owner can collect data from multiple hosts. Third solution they gave is the Data Access Control with rights so that cloud service provider can verify that data is always used by the cloud service consumer. Fourth solution is the Data Access Monitoring can assure when and what data is being accessed for what purpose.

[4]A Trust Computing Mechanism for Cloud Computing

Mohamed Firdhous, Osman Ghazali, Suhaidi Hassan : In this paper, the authors propose a trust formulation and evolution mechanism that can be used to measure the performance of cloud systems. The proposed mechanism formulates trust scores for different service level requirements, hence is suitable for managing multiple service levels against single trust score. Also the proposed mechanism is an adaptive one that takes the dynamics of performance variation along with cloud attributes such as number of virtual servers into computations. Finally the proposed mechanism has been tested under a simulated environment and the results have been presented. Trust system would help users to select service providers based on the quality requirements. The trust system provides a trust score between 0 and 1 for different levels of services and continues to improve these values based on the performance of the system. Hence the proposed system would be more useful for providing differentiated services at different quality levels. The proposed mechanism has been evaluated using a simulation environment setup with Octave the open source Mat lab clone. The simulation results show that the proposed system works satisfactorily under constrained simulated environment. The proposed mechanism must be tested rigorously under a more open environment and in the face of adversaries in order to evaluate the ruggedness and resilience of the mechanism. The authors propose to carry out this in a future research.

[5] Service-Oriented Cloud Computing Architecture

Wei-Tek Tsai, Xin Sun, Janaka Balasooriya: This paper gives an overview of current cloud computing architectures and also discusses the issues that current cloud computing implementation have and proposes a Service-Oriented Cloud Computing Architecture (SOCCA) so that clouds can interoperate with each other. The SOCCA architecture is a 4-layer architecture that supports both SOA and cloud computing. It Support easy application migration from one cloud to another and service redeployment to different clouds by separating the roles of service logic provider and service cloud providers. It promotes an open platform on which oopen platforms and ontology are embraced. The SOCCA architecture also Proposes high level design to better support multi-tenancy feature of cloud computing. This Paper also introduced related topics for future research, such as service demand prediction and SLA negotiation and service request dispatching.

[6] Addressing Cloud Computing security issues

Dimitrios Zissis, Dimitrios Lekkas: In this Paper; first they evaluate cloud security by identifying unique security requirements and second attempt is to present a viable solution that eliminates these potential threats. They Proposes a Trusted Third Party, tasked with assuring specific security characteristics within a cloud environment. They Proposed a solution which calls upon cryptography, specifically Public Key Infrastructure operating in concert with SSO and LDAP, to ensure the authentication, integrity and confidentiality of involved data communication and can address most of the identified threats in cloud computing. They adopted software engineering and information design approaches. The Solution presents a horizontal level of service, available to all implicated entities, that realizes a security mesh, within which essential trust is maintained.

[7] A Survey on Security Issues in Services Delivery Models of Cloud Computing

S. Subashini, V. Kavitha: In this paper different security risks that pose a threat to cloud is presented. Research is more specific to the different security issues that has emanated due to the nature of the service delivery models of cloud computing system. They centre their research on application and data security over the cloud, and intend to develop a framework by which the security varies dynamically varies from transaction to another. This is more like storing related data in different locations based on meta data information. Another piece of framework would be providing 'Security as a Service' by providing security as a single-tier or multi-tier based on the applications requirement and addition to it, the tiers are enabled to change dynamically making the security system less predictable. They based their research on the conceptualization of the cloud security based on real world security system wherein security depends on the requirement and asset value of an individual or organization.

III. A SURVEY ON COULD COMPUTING ARCHITECTURE

The cloud computing model consists of five characteristics, three delivery models, and four deployment models [2]. The five key characteristics of cloud computing are: location-independent resource pooling, on-demand self-service, rapid elasticity, broad network access, and measured service [9]. These five characteristics represent the first layer in the cloud environment architecture

A. Three Delivery Models of Cloud Computing are:

1. Infrastructure as a Service (IaaS) : This Layer is on top of data centres layer, the service provider owns the equipment and is responsible for housing, running and maintaining it. The client typically pays on a per-use basis. IaaS [3] offers users elastic on demand access to resources (networking, servers and storage), which could be accessed via a service API. Typical examples are Flexiscale, AWS: EC2 (Amazon Web Services).
2. Platform as a Service (PaaS) : It is often referred as cloudware , this gives a developer the flexibility to develop applications on the provider's platform. It usually requires no software download or installation. Entirely virtualized platform that includes one or more servers, operating systems and specific applications. Main services provided are storage, database, and scalability. Typical examples are Google App Engine, Mosso, AWS: S3.
3. Software as a Service (SaaS): Software as a Service consists of software running on the provider's cloud infrastructure, delivered to (multiple) clients (on demand) via a thin client (e.g. browser) over the Internet. It saves the users from the troubles of software deployment and maintenance. Software can be requested on demand, and are rolled out more frequently. Typical examples are Google Docs and Salesforce.com.

B. Four Deployment Models of cloud Computing are

1. Public Cloud: Public cloud describes cloud computing in the traditional mainstream sense, whereby resources are dynamically provisioned on a fine-grained, self-service basis over the Internet, via web applications/web services, from an off-site third-party provider who shares resources and bills on a fine-grained utility computing basis. It is typically based on a pay-per-use model, similar to a prepaid electricity metering system which is flexible enough to cater for spikes in demand for cloud optimization [12]. Public clouds are less secure than the other cloud models because it places an additional burden of ensuring all applications and data accessed on the public cloud are not subjected to malicious attacks.
2. Private Cloud: In Private cloud, scalable resources and virtual applications provided by the cloud vendor are pooled together and available for cloud users to share and use. It differs from the public cloud in that all the cloud resources and applications are managed by the organization itself, similar to Intranet functionality. Utilization on the private cloud can be much more secure than that of the public cloud because of its specified internal exposure. Only the organization and designated stakeholders may have access to operate on a specific Private cloud [12]. The Private cloud is more suited to organisations which are involved in mission and safety organisations
3. Hybrid Cloud: Hybrid cloud provides solutions through a mix of public and private clouds. It is an integrated cloud service utilising both private and public clouds to perform distinct functions within the same organisation, Hybrid clouds are more secure in terms of data control, information and allow access of information to different organisations over the internet. Organisations can maximise their efficiencies by employing public cloud services for all non-sensitive operations, only relying on a private cloud where they require it and ensuring that all of their platforms are seamlessly integrated.

4. Community Cloud: A community cloud is well suited to a multi-tenant infrastructure that is shared among several organizations from a specific group with common computing concerns. The main goal of a community cloud is to have participating organizations realize the benefits of a public cloud -- such as multi-tenancy and a pay-as-you-go billing structure -- but with the added level of privacy, security and policy compliance usually associated with a private cloud. The community cloud can be either on-premises or off-premises, and can be governed by the participating organizations or by a third-party managed service provider (MSP) [13]

IV. SECURITY ISSUES

There are numerous security issues for cloud computing as it encompasses many technologies including networks, databases, operating systems, virtualization, resource scheduling, transaction management, load balancing, concurrency control and memory management. Therefore, security issues for many of these systems and technologies are applicable to cloud computing.

1. Trust: Trust management systems play an important role in distributed systems such as peer to peer systems, grid computing, cluster computing and sensor networks . Trust management systems help nodes to select the right peer to interact with. Trust basically represents a node's competence, benevolence, integrity or predictability and any mathematical model [4] defined to represent trust must be capable of representing all these aspects. A mechanism is necessary for clients to select the right service provider who could meet their requirements. A trust system built based on the QoS of different service providers will be useful in matching the capability and requirements of both service provider and clients.
2. Confidentiality and privacy: Confidentiality [6] refers to only authorized parties or systems having the ability to access protected data. The threat of data compromise increases in the cloud, due to the increased number of parties, devices and applications involved, that leads to an Increase in the number of points of access. Delegating data control to the cloud, inversely leads to an increase in the risk of data compromise, as the data becomes accessible to an augmented number of parties. A number of concerns emerge regarding the issues of multitenancy, data remanence, application security and privacy.
3. Integrity: It is a key aspect of information security. Integrity means that assets can be modified only by authorized parties or in authorized ways and refers to data, software and hardware. Data Integrity refers to protecting data from unauthorized deletion, modification or fabrication. Due to the increased number of entities and access points in a cloud environment, authorization is crucial in assuring that only authorized entities can interact with data.
4. Data Intrusion: According to Garfinkel [14], another security risk that may occur with a cloud provider, such as the Amazon cloud service, is a hacked password or data intrusion. If someone gains access to an Amazon account password, they will be able to access all of the account's instances and resources. Thus the stolen password allows the hacker to erase all the information inside any virtual machine instance for the stolen user account, modify it, or even disable its services. Furthermore, there is a possibility for the user's email(Amazon user name) to be hacked , and since Amazon allows a lost password to be reset by email, the hacker may still be able to log in to the account after receiving the new reset password.
5. Availability: Availability ensures that data processing resources are not made unavailable by malicious action. It is the simple idea that when a user tries to access something, it is available to be accessed. This is vital for mission critical systems. Availability for these systems is critical that companies have business continuity plans (BCP‟s) in order for their systems to have redundancy.
6. Data Theft: Cloud computing uses external data server for cost affective and flexible for operation. So there is a chance of data can be stolen from the external server.
7. Data Location: Consumers do not always know the location of their data.The Vendor does not reveal where all the data's are stored. Cloud Computing offers a high degree of data mobility. The Data's won't even be in the same country of the Customer, it might be located anywhere in the world.They may also wish to specify a preferred location (e.g. data to be kept in the USA) then requires a contractual agreement between the Cloud service provider and the consumer that data should stay in a particular location or reside on a given known server [8].
8. Security issues in provider level: A Cloud is good only when there is a good security provided by the vendor to the customers. Provider should make a good security layer for the customer and user .And should make sure that the server is well secured from all the external threats it may come across. The cloud computing service provider has.
9. User level Issues: User should make sure that because of its own action, there shouldn't be any loss of data or tampering of data for other users who are using the same Cloud.
10. Infected Application: Service provider should have the full access to the server with all rights for the purpose of monitoring and maintenance of server. So this will prevent any malicious user from uploading any infected application onto the cloud which will severely affect the customer and cloud computing service.

V. CONCLUSION

From the above studies, we familiarize with cloud computing. Cloud is a type of parallel and distributed system consisting of a collection of interconnected and virtualized computers that can be rapidly provisioned and released with minimal management effort. It is different from conventional computing as its empowered with virtualization technology,

supports ubiquitous computing, convenient, on-demand network access to a shared pool of configurable resources. As this technology is achieving popularity, security issues are being introduced due to the adoption of this new model. In this paper unique security challenges are being presented in different cloud computing architecture.

REFERENCES

[1] Mladen A. Vouk, Cloud Computing – Issues, Research and Implementations, Journal of Computing and Information Technology– CIT 16, 2008

[2] Mohammed A. AlZain, Eric Pardede, Ben Soh, James A. Thom, Cloud Computing Security: From Single to Multi-Clouds, 45th Hawaii International Conference on System Sciences – 2012

[3] Anitha Y , Security Issues in Cloud Computing, International Journal of Thesis Projects and Dissertatins vol 1, issue 1, 2013.

[4] Mohamed Firdhous, Osman Ghazali, Suhaidi Hassan, A Trust Computing Mechanism for Cloud Computing, Inter Net Works Research Group, Universiti Utara Malaysia, Sintok, Kedah Darul Aman, Malaysia

[5] Wei-Tek Tsai, Xin Sun, Janaka Balasooriya, Service-Oriented Cloud Computing Architecture, Seventh International Conference on Information Technology – 2010

[6] Dimitrios Zissis, Dimitrios Lekkas, Addressing Cloud Computing Security Issues, Future Generation Computer System 28 (2012), 2010.

[7] S. Subashini, V. Kavitha, A Survey on Security Issues in Service Delivery models of Cloud Computing, Journal of Network and Computer Architecture – 11 July 2010.

[8] Zaigham Mahmood, Data Location and Security Issues in Cloud Computing, International Conference on Emerging Intelligent Data and Web Technologies, 2011

[9] H. Takabi, J.B.D. Joshi and G.-J. Ahn, Security and Privacy Challenges in Cloud Computing Environments, IEEE Security & Privacy, 8(6), pp. 24-31, 2010

[10] Amazon Elastic Compute Cloud [URL]. http://aws.amazon.com/ec2, access on Oct. 2009

[11] IBM Blue Cloud project [URL]. http://www-03.ibm.com/press/us/en/pressrelease/22613.wss/, access on October 2009.

[12] Enterprise Cloud Computing: Transforming IT , A Platform Computing Whitepaper. Platform Computing, pp6, 2010.

[13] Techtarget.com, Search CloudComputing,http://searchcloudcomputing.techtarget.com/definition/hybrid.

[14] S.L. Garfinkel, An evaluation of amazon's grid computing services: EC2, S3, and SQS, Technical Report TR-08-07, pp. 1-15, 2007.

[15] Zohreh Sanaei, Saeid Abolfazli, Abdullah Gani, Rajkumar Buyya, Heterogeneity in Mobile Cloud Computing: Taxonomy and Open Challanges, IEEE Communication surveys & Tutorials, Vol. 16,No. , 2014

[16] B. Rochwerger, D. Breitgand, ELevy, A. Galis, K. Nagin, I. M. Llorente, R. Montero, Y. Wolfsthal, E. Elmroth, J. Caceres, M. Ben-Yehuda, W. Emmerich, F. Galan, The reservoir Model and Architecture for Open Federated Cloud Computing, IBM journal of Research and Development- 2009

[17] Engr: Farhan Bashir Shaikh and Sajjad Haider, Security threats in Cloud Computing**,** 6th International Conference on Internet Technology and Secured Transactions, 11-14, D2011.

[18] Zhidong Shen, Li Li and Fei Yan, Xiaoping Wu, Cloud Computing System Based on Trusted Computing Platform, International Conference on Intelligent Computation Technology and Automation, 2010

[19] Siani Pearson and Azzedine Benameur, Privacy, Security and Trust Issues Arising from Cloud Computing, 2nd IEEE International Conference on Cloud Computing Technology and Science

[20] Hussain Al-Aqrabi, Lu Liu, Jie Xu, Richard Hill, Nick Antonopoulos, Yongzhao Zhan, Investigation of IT Security and Compliance Challenges in Security-as-a-Service for Cloud Computing, IEEE 15th International Symposium on Object/Component/Service-Oriented Real-Time Distributed Computing Workshops, 2012

