Analytical Study of Security Issues in Cloud Computing

Rana Kumar Saini[1], Bhanu Sharma[2], Amlesh Roy[3,] Dr. Raman Chadha[4]
[1]Student, B.Tech, [2]Assistant Professor, [3]Student, B.Tech, [4]HoD
CSE Department, CGC Technical Campus Jhanjeri, Mohali, India

Abstract **-** Cloud computing is an emerging and powerful technology in the field of information technology due its flexible and cost reduction. But biggest challenges in clod computing e in cloud computing is the security and privacy problems caused by its multi-tenancy nature and the outsourcing of infrastructure, sensitive data and critical applications. We also address the characteristics and applications of several popular cloud computing platforms. In this paper, we aim to pinpoint the challenges and issues of cloud computing. We identified several challenges from the cloud computing adoption perspective and we also highlighted the cloud interoperability issue that deserves substantial further research and development. However, security and privacy issues present a strong barrier for users to adapt into cloud computing systems. In this paper, we investigate several cloud computing system providers about their concerns on security and privacy issues.

Keywords **-** Cloud services, Cloud Security Issues, Cloud Security Technique

I. INTRODUCTION

Today network security is very challenging task, as it is an integral part of network service. But due to rely on computer network for secret and important file, security has become very important part of it. Network security becomes much more difficult to control when the environment becomes as dynamic and demanding as cloud computing. Main aim of cloud computing is to reduce the cost of using resources such as storage, processing power, services etc. These help users to focus on their business without worry of resources. The evolution of cloud computing is from many different technologies such as virtualization, grid computing, autonomic computing, and some other technologies. Recent advances in cloud computing are pushing virtualization more than ever. In other words, cloud computing services can be considered as a significant step towards realizing the utility computing concept. In such a computing model, services can be accessed by users regardless of where they are hosted or how they are delivered. In this paper to describe the various type of security issues and various type of solution.

Cloud computing has emerged as a way for IT businesses to increase capabilities on the fly without investing much in new infrastructure, training of personals or licensing new software. It follows a simple “pay as you go” model, which allows an organization to pay for only the service they use. It eliminates the need to maintain an in-house data center by migrating enterprise data to a remote location at the Cloud provider’s site. Minimal investment, cost reduction, and rapid deployment are the main factors that drive industries to utilize Cloud services and allow them to focus on core business concerns and priorities rather than dealing with technical issues. As more and more companies are embracing the cloud computing, the security issues are escalating due to the accumulation of digital assets. Traditional security measures will not be effective in cloud computing because the cloud operating environments (multi-tenant, heterogeneity, virtualization, etc.) are totally different from traditional computing. In the traditional computing, there is a clear distinction between insiders and outsiders and the security administrator takes the sole responsibility for the security policies and protection of data and assets. In cloud computing, the gap between insiders and outsiders are very ambiguous and in certain cases, the outsiders become insiders. Many researches have been conducted on security issues in cloud computing with various aspects. A survey of security issues in service delivery models are done in wherein the former gave a special attention to Software as a Service (SaaS) model. A survey of security issues in the deployment models are done in and the authors provided mitigation techniques also. In the authors did a survey on data security and privacy issues in cloud computing.

II. CLOUD SERVICES MODEL

Cloud Computing service provide in four type model;

A. IaaS
B. PaaS
C. SaaS
D. DaaS

A. Infrastructure as a Service (IaaS) - Cloud consumers directly use IT infrastructures provided in the IaaS cloud. Virtualization is extensively used in IaaS cloud in order to integrate physical resources in an ad-hoc manner to meet growing or shrinking resource demand from cloud consumers. The basic strategy of virtualization is to set up independent virtual machines (VM) that are isolated from both the underlying hardware and other VMs. Notice that this strategy is different from the multi-tenancy model, which aims to transform the application software architecture so that multiple instances can run on a single application. An example of IaaS is Amazon's EC2.

B. Software as a Service (SaaS) - It is also called a delivery model where the software and the data which is associated with is hosted over the cloud environment by third party and that third party is called cloud service provider, like your Gmail account, you use that application on someone else's system.

C. Platform as a Service (PaaS) - In this, you can use Web-based tools to Platform as Service develop applications so they run on systems software which is provided by another company, like Google App Engine.

D. Data as a Service (DaaS) - The delivery of virtualized storage on demand becomes a separate Cloud service - data storage service. Notice that Data as a Service could be seen as a special type IaaS. The motivation is that on -premise enterprise database systems are often tied in a prohibitive upfront cost in dedicated server, software license, post-delivery services and in-house IT maintenance. Examples of this kind of Data as a Service include Amazon S3, Google Big Table, and Apache H Base, etc.

III. CLOUD DEPLOYMENT MODELS

There are Four Deployment Models and are described below.

Public Cloud: This infrastructure is available to the general public. As the name suggests, public cloud is a model in which resources are generally available to everyone or anywhere

Private Cloud: This model is developed for the private organizations like one house and an organization and they can use it for their own purpose. This kind of a service is not accessed by everyone

Hybrid Cloud: Hybrid Clouds are combination of public and private cloud in a same network. This can be done if private cloud need some important services from the public cloud like Private cloud can store some information on their private cloud and we can use that information on public cloud.

Community Cloud: A Community Cloud is similar to a public cloud except that its access is limited to a specific community of cloud consumers. The community cloud may be jointly owned by the community members or by a third-party cloud provider that provisions a public cloud with limited access. The member cloud consumers of the community typically share the responsibility for defining and evolving the community cloud. Membership in the community does not necessarily guarantee access to or control of all the cloud's IT resources. Parties outside the community are generally not granted access unless allowed by the community. Example: Facebook.

IV. PROBLEM STATEMENT

In this paper focus on the security issues of data over a cloud. We will broadly cover the aspect of multi-tenancy in cloud computing which will meet the challenges of security of data, so that the data will remain protected while being on the network.

V. LITERATURE REVIEW

In This paper, the problem of cloud security analyzed. This paper gives security architecture and necessary support techniques for making our cloud computing infrastructure secured.

All the Security issues of cloud computing are highlighted in this paper, because of the complexity 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 improved. We reviewed the literature for security challenges in cloud computing and proposed a security model and framework to make cloud computing environment secure. In this paper, security in cloud computing was discussed in a manner that covers security issues and challenges, security principles and security management models. This paper introduced technical layers and categories, with which it recognized and structured security challenges and approaches of multitenant cloud computing. In this paper the main issue with multi tenancy is that the clients use the same computer hardware to share and process information and the result is that tenants may share hardware on which their virtual machines or server runs, or they may share database tables.

VI. CLOUD SECURITY ISSUE

The based on study to cloud security issues and challenges face to new era technology. The following challenges in cloud computing in today:

Data Security: Data protection is among the biggest concerns in cloud computing. When confidential information is hosted by cloud service providers, it means that a considerable amount of the end user’s security and privacy control is transferred to the cloud vendor. It is essential to ensure the cloud provider understands the end user’s security and privacy needs, which normally presents the hugest challenge. The risk is that confidential information is shared with an outside party and thus, it’s always advisable for cloud computing users to ensure that their providers are aware of certain data security and privacy rules and regulations. Hence, data security and privacy remains one of the major worries when it comes to the risks and challenges of cloud computing.

Traffic Hijacking: Cloud account hijacking at the enterprise level can be particularly devastating, depending on what the attackers do with the information. Company integrity and reputations can be destroyed, and confidential data can be leaked or falsified causing significant cost to businesses or their customers. Legal implications are also possible for companies and organizations in highly regulated industries, such as healthcare, if clients’ or patients’ confidential data is exposed during cloud account hijacking incidents. In recent survey, 69 percent of North American IT professionals shared their belief that the risks of using cloud-based services outweighed the benefits. The main reason they cited was a concern for data security. Similarly, in a 2013 report, the identified service traffic hijacking as the third-greatest cloud computing security risk. These types of security breaches occur when attackers hijack cloud accounts by stealing security credentials and eavesdropping on activities and transactions. Attackers manipulate data, insert false information, and redirect clients to illegitimate sites.

Insider Attack: Security breaches from the inside are equally on the rise just like cyber Attacks. The shared access, as discussed earlier, heightens the risk of other employees or people accessing your cloud. The case of 2 million customer records breach at Vodafone is a wake-up call that privileged user access can result in insider attack. When a person or an employee gets access to others cloud, then everything from secret information to data and intellectual property becomes available for anyone to obtain. Hence, cloud environments are at high risk of insider attacks as other people or moles can pose as cloud administrators to gain access to the cloud and steal any virtual machine unnoticed.

Outsider Attack: In this paper to discuss outsider attack in cloud security, many witnessed a rise in security incidents and breaches, with a significant increase in documented APT (Advance Persistent Threat) type of attacks targeting top corporations or government entities. In this paper, concerns for security are rising to the top levels, with decisions taken at the board level in most organisations. We are concerned about security, not only because of the cost of a breach, but also because the reputation of their companies is at risk when customer data is lost or exposed to criminals. As real cases have shown, the bigger the media coverage a security breach receives, the greater the complexity of the malware causing it. On top of this, migrating corporate information from traditional data centers to a cloud infrastructure has significantly increased companies' attackable surface, bringing new threats and more worries to offices regarding the safety of their data.

DDoS Attack: Distributed denial of service (DDoS) attacks are more common than ever before. Verisign reported IT services, cloud and SaaS was the most frequently targeted industry during the first quarter of 2015. A DDoS attack is designed to overwhelm website servers so it can no longer respond to legitimate user requests. If a DDoS attack is successful, it renders a website useless for hours, or even days. This can result in a loss of revenue, customer trust and brand authority. Complementing cloud services with DDoS protection is no longer just good idea for the enterprise; it's a necessity. Websites and web-based applications are core components of 21st century business and require state-of-the-art security.

Data Loss: In this paper highlight the problem statement to Data Loss from the cloud, either though accidental deletion, malicious tampering or an act of nature brings down a cloud service provider, could be disastrous for an enterprise business. Often a DDoS attack is only a diversion for a greater threat, such as an attempt to steal or delete data. To face this challenge, it's imperative to ensure there is a disaster recovery process in place, as well as an integrated system to mitigate malicious attacks. In addition, protecting every network layer, including the application layer (layer 7), should be built-in to a cloud security solution

Multi Tenancy: In this paper, the fundamental security issue with multi-tenancy is clients using Cloud Computing by employing single and the same computer hardware to share and process information. This presents a number of challenges in terms of compliance, security, and privacy. The lack of user network isolation. In this technique, as the data stored by cloud applications used by tenants is on a same database but in a different partitions. So to ensure security for data of each tenant, in this paper we are proposing Data Partition Encryption Technique(DPET) in which each record in partition before stored is encrypted two times first by tenant's public key and by Cloud Service Provider (CSP), and decrypted only by tenant. Since the record 'R' to be stored at CSP is encrypted by tenant, 'R' cannot be revealed by CSP also. In this way the proposed DPET technique is secure by not revealing the record to other Tenants residing or using shared database. Several issues should be considered during the testing of multi-tenant SaaS application: resources are shared among tenants and their end-users, each variant application addresses a specific requirements set for a tenant, it is executed as if it was in a dedicated environment and can be composed of several components and a variant application is delivered to the customers through a run-time engine from cloud provider that weaves the tenant customization data and specific metadata to kernel code. Thus, each application provides different screens and logic.

VII. CLOUD SECURITY TECHNIQUE

Authentication and Identity: Authentication is the process for confirming the identity of the user. The typical authentication process allows the system to identify the user (typically via a username), and then validate their identity through user-provided evidence such as a password. There are stronger methods of authenticating the user, including x.509 certificates, one-time passwords, and device fingerprinting. These can be combined to provide a stronger combination of authentication factors. Federated identity allows a user to access an application in one domain, such as a Software-as-as-Service (SaaS) application, using the authentication that occurred in another domain, such as a corporate Identity Management (IdM) system.

Data Encryption: Data encryption in the cloud is the process of transforming or encoding data before it's moved to cloud storage. Typically cloud service providers offer encryption services ranging from an encrypted connection to limited encryption of sensitive data and provide encryption keys to decrypt the data as needed. Both inside and outside of the platform. Encryption services like these prevent unauthorized free access to your system or file data without the decryption key, making it an effective data security method. Keeping information secure in the cloud should be your top priority. Just taking a few preventative measures around data encryption can tighten security for your most sensitive information. Follow these encryption tips to lock down your information in the cloud.

Availability of Information (SLA): One of the most important areas for consumers is security, performance and availability when it comes to cloud computing. Availability refers to the uptime of a system, a network of systems, hardware and software that collectively provide a service during its usage. Traditionally the availability of these has been limited to local installations of hardware and software resources which businesses and consumers deployed and maintained. With the advent of cloud services there is a considerable shift of these resources into the cloud. While cloud computing presents some cost effective benefits for the consumers and businesses, it is also extremely important for the cloud service providers to offer environments that are highly scalable and high in availability. This will in many ways dictate the credibility of these cloud services.

Secure Information Management: Security information management (SIM) is software that automates the collection of event log data from security devices such as firewalls, proxy servers, intrusion detection systems and anti-virus software. This data is then translated into correlated and simplified formats. SIM products are software agents that communicate with a centralized server, acting as a security console and sending the server information about security-related events. The SIM displays reports, charts and graphs of this information.

In cloud computing system application run by the customer are considered with high efficiency and integrity. So to prevent cloud from malware injection attack we can combine the integrity with hardware or can use hardware for integrity purpose because for an attacker it is difficult to intrude in the IaaS level. For this we can utilize a file allocation table (FAT) system, by using it we can determine the validity and integrity of new instance by comparing the current and previous instance. For this purpose, we need to deploy a hypervisor on the provider's side. In cloud system hypervisor is considered to be the most secure and sophisticated part of it whose security cannot be broken by any means. The Hypervisor is responsible for scheduling all the instance and services so we can make hypervisor to check file allocation table to validate and integrate an instance of customer. Other approach is that we can maintain the information of the platform type version that a customer user to access the cloud in first phase when a customer open an account and can use those information to check the validity of new instance of the customer.

Image Management System: This system addresses the problems related to safe management of the virtual machine images that summarize each application of the cloud.

Client Based Privacy Manager: This technique helps to reduce the loss of private data and threat of data leakage 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. TCPS is planned to protect the integrity of distributed computing by allowing the cloud to monitor infrastructure components.

Secure and Efficient Access to Outsourced Data: This Provides secure and efficient access to Outsourced data is an important factor of cloud computing and forms the foundation for information Management and other Operations

VIII. CONCLUSION

In this paper, We give the review study of cloud security issues and its possible solution. In either case security measures are a must to ensure that tenant do not pose a risk to one another in the term of data risk. Multi-tenant protection must be offered by cloud services provider for all layers of there offering (i.e. IaaS and SaaS) cloud services provider own it to have latest and best approaches as available option. Based on this discussion we recommend that cloud computing security solutions should focus on the problem abstraction, using model-based approaches to capture different security views and link such views in a holistic cloud security model. Inherent in the cloud architecture. Where delivered mechanisms (such as elasticity engines) and APIs should provide flexible security interfaces. Support for: multi-tenancy where each user can see only his security configurations, elasticity, to scale up and down based on the current context. Support integration and coordination with other security controls at different layers to deliver integrated security. Be adaptive to meet continuous environment changes and stakeholders needs.

IX. REFERENCES

[1]. www.juniper.net/us/en/local/pdf/whitepapers/2000381-en.pdf

[2]. www.ijert.org/engineering-multi-tenant-software-as-a-service-systems

[3]. www.ksiresearchorg.ipage.com/seke/seke16paper/seke16paper_68.pdf

[4]. www.whatis.techtarget.com/definition/multi-tenancy

[5]. www.researchgate.net/publication/260305189_Multi-Tenancy_in_Cloud_Computing

[6]. www.ieeexplore.ieee.org/document/6733211

[7]. www. personal.rhul.ac.uk/vsai/149/Multi-tenancy doc 300614.pdf

[8]. www.cloudcouncil.org/CSCC_Security_for_Cloud_Computing_10_Steps_to_Ensure_Success_Webinar_Presentation_3_17_15.pdf

[9]. www.researchgate.net/publication/321637905_Exploring_Security_Issues_and_Solutions_in_Cloud_Computing_Services_-_A_Survey

[10]. www.paper.ijcsns.org/07_book/201212/20121217.pdf

[11]. www.semanticscholar.org/paper/Security-Threats%2FAttacks-Present-in-Cloud-Munir-Palaniappan/44dc8494b2bbd8aa56320de8a209d3aa6c36628b

[12]. www.arxiv.org/ftp/arxiv/papers/1512/1512.01701.pdf