Understanding Vulnerabilities and Data Security in Cloud Computing

Dr.WINSTON DUNN
Asst. Professor in Computer Science and Engineering
Christu Jyothi Institute of Technology & Science
Jangaon, Telangana-506167
mamatha7k@gmail.com

Dr.ARVIND PRASAD
Asst. Professor in Computer Science and Engineering
Christu Jyothi Institute of Technology & Science
Jangaon, Telangana-506167
pritikandewar09@gmail.com

Abstract-**Clouds provide a powerful computing platform that enables individuals and organizations to perform variety levels of tasks such as: use of online storage space, adoption of business applications, development of customized computer software, and creation of a "realistic" network environment. Previously, the number of people using cloud services has dramatically increased and lots of data has been stored in cloud computing environments. In the meantime, data breaches to cloud services are also increasing every year due to hackers who are always trying to exploit the security vulnerabilities of the architecture of cloud. In this paper, three cloud service models were compared; cloud security risks and threats were investigated based on the nature of the cloud service models. Cloud computing has pros and cons such as flexibility, availability, scalability and security issues respectively. We discuss here, to find vulnerabilities in system and related threats found in the literature in cloud computing as well identifying possible solutions for vulnerability and threats. In addition, countermeasures to cloud security breaches are presented.**

I. INTRODUCTION

Cloud Computing is a computing model that enables sharing of resources on-demand with cost effectiveness and location independent. In Cloud systems the customers need not to buy any resources in their own instead they can use the resources from the cloud and they can pay for the resource as per the usage. Cloud computing is a technology that offers many advantages, in that the main drivers of cloud computing is the following:

- Cost saving
- Improved Flexibility
- Better Scalability

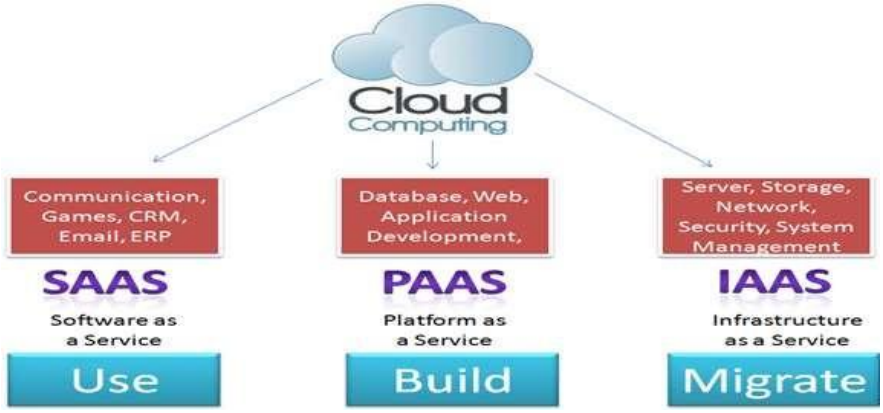

Figure1. Cloudservice models

A. Infrastructure as a Service (IaaS)

IaaS is the foundation of cloud services. This type of service provides storage space, processing power and managing the organizations Database On-Demand of the particular company.

B. Platform as a Service (PaaS)

Here the platforms or environment needed to develop the applications are provided as a service. The organizations that need a particular environment can buy it from the cloud infrastructure for developing their applications which will run on the provider's infrastructure and release the environment when the work completed.

C. Software as a Service (SaaS)

In SaaS the software applications such as CRM, ERP and some other online applications to manage the organizations are offered as a service. The additional hardware and software's that are required to support the pre made application can be offered by the cloud provider itself. It clears the idea that on customer side there is no need of investment for the extra things either the service we occupy.

Cloud computing is a domain of using a network where remote servers are hosted to store, manage, and process data at very large scale. It is used for services to provide improved reliability, availability and scalability. The main goal of cloud computing from supplier's point is combination of hardware & software connected to reduce interruption on devices over network without changing user's context. It has a layering mechanism between software, networking and storage, such that every portion can be easily designed, executed, verified and run independently from consequent layers.

Advantages:

- It has ability to scale up on demand IT capacity
- It has ability for managing large data sets
- It aligns IT resources directly with cost
- It helps in improving IT effectiveness by reducing operational cost
- It places business volatility into single domain

Drawbacks:

- Due to nature and level of security threats involved in cloud environment
- It may cause lock-in due to proprietary technology
- It may cause network latency by using internet to use some cloud applications
- In some cases cloud provider may cost more than on-premises systems
- It may be problematic while integrating on-premise system and cloud based system

However cloud computing must provide better utilization of resources by making use of virtualization. Also, it could help to take as much work load from clients even though it is having security related issue. The underlying technology that is used by cloud computing itself provides foremost security risk. This paper describe various security threats along with countermeasures in cloud computing environment.The need of cloud computing is increased and substantial growth in the scientific and business organizations. According to a study by Garner [10] recognized cloud computing as top most in utilizing technology and has seven major risks to be considered before implementing or transforming into cloud model[3]. Even though many reasonsare existing for adopted cloud computing , there are also some restrictions in adopting, The major roles for not adopting is security , privacy and legal matters,Since for cloud computing new design and models are represented,there exists how far security can be provided in each levels (i.e. network devices , application host and data level).

High security should provide to external data storage dependency on public internet, multi-tenancy and privacy in internal security. Traditional security systems are not enough for cloud to huddle like distributed, heterogeneous and virtualization [2]. Its difficulty for an organization to move its application and sensitivity data into cloud, as it maintained by third-party, which overall customer require the same security and control over their application and sensitivity data and they can meet their service - level agreement.[4]

II. CLOUD SECURITY AND PRIVACY

A. Identity management

Every enterprise will have its own identity management system to control access to information and computing resources. Cloud providers either integrate the customer's identity management system into their own infrastructure, using federation or SSO technology, or a biometric-based identification system, or provide an identity management system of their own.CloudID,for instance, provides privacy-preserving cloud-based and cross-enterprise biometric identification. It links the confidential information of the users to their biometrics and stores it in an encrypted fashion. Making use of a searchable encryption technique, biometric identification is performed in encrypted domain to make sure that the cloud provider or potential attackers do not gain access to any sensitive data or even the contents of the individual queries[9].

B. Physical security

Cloud service providers physically secure the IT hardware (servers, routers, cables etc.) against unauthorized access, interference, theft, fires, floods etc. and ensure that essential supplies (such as electricity) are sufficiently robust to minimize the possibility of disruption. This is normally achieved by serving cloud applications from 'world-class' (i.e. professionally specified, designed, constructed, managed, monitored and maintained) data centers.

C. Personnel security

Various information security concerns relating to the IT and other professionals associated with cloud services are typically handled through pre-, para- and post-employment activities such as security screening potential recruits, security awareness and training programs, proactive.

D. Privacy

Providers ensure that all critical data (credit card numbers, for example) are masked or encrypted and that only authorized users have access to data in its entirety[8]. Moreover, digital identities and credentials must be protected as should any data that the provider collects or produces about customer activity in the cloud[1].

E. Cloud Vulnerability and Penetration Testing

Scanning could from outside and inside using free or commercial products are very important because without a hardened environment your service is considered as a soft target. Virtual servers should be hardened like a physical server against data leakage, malware, and exploited vulnerabilities.

Scanning and penetration testing from inside or outside the cloud require to be authorized by the cloud provider. Since the cloud is a shared environment with other tenants following penetration testing rules of engagement step-by-step is a mandatory requirement. Violating the acceptable use of policy, this can lead to termination of the service.

III. CLOUD COMPUTING THREATS AND VULNERABILITIES WITH ITS COUNTERMEASURES

A. Data Breaches

When a virtual machine is able to access the data from another virtual machine or organization's sensitive internal data falls into the hands of their competitors, a data breach occurs. The side-channel attacks are valid attack vectors they attack timing information to extract private cryptographic keys being used in other virtual machines on the same physical server. In multitenant cloud service database is not properly designed, a flaw in one client's application could allow an attacker access not only to that client's data, but every other client's data as well. *Countermeasure*: while data loss and data leakage are both serious threats to cloud computing, the measures you put in place to mitigate one of these threats can exacerbate the other. You may be able to encrypt your data to reduce the impact of a data breach, but if you lose your encryption key, you'll lose your data as well.

B. Data Loss

Data loss can be happened in the cloud when data gets into wrong hands while transferring or be lost due to the hard drive failure. A CSP could accidentally delete the data; an attacker might

modify the data. Any accidental such as a fire or earthquake, could lead to the permanent loss of customer's data.

Countermeasure: Many new compliance policies require organizations to retain audit records, FRC techniques, digital signatures, encryption, and homographic encryption [5] .The provider must takes adequate measures to backup data.

C. Account Hijacking

Credentials and passwords are often reused to access our account in the cloud by which an attacker gaining access to our account can manipulate and change the data. An attacker having access to the cloud virtual machine hosting our business website can induce a malicious code into the web page to attack users visiting our web page – this is known as the watering hole attack. An attacker can also disrupt the service by turning down the web server serving our website, rendering it inaccessible.

Countermeasures: Organizations should look to prohibit the sharing of account credentials between users and services, and leverage strong two-factor authentication techniques where possible.

D. Insecure APIs

Various cloud services on the Internet are exposed to a set of software interfaces or APIs that customers use to manage and interact with cloud services .Organizations and third parties often build upon these interfaces to offer value-added services to their customers. An attacker gaining a token used by a customer to access the service through service API can use the same token to manipulate the customer's data[6]. Therefore it's imperative that cloud services provide a secure API, rendering such attacks worthless.

Countermeasure: Analyze the security models of cloud provider interface and understanding strong authentication and access controls are implemented in concrete transmission with encryption.

E. Denial of Service

Denial-of-service attacks are attacks meant to prevent users of a cloud service from being able to access their data or their applications. By forcing the victim cloud service to consume inordinate amounts of finite system resources such as processor power, memory, disk space or network bandwidth, the attacker (or attackers, as is the case in distributed denial-of service (DDoS) attacks) causes an intolerable system slowdown and leaves all of the legitimate service users confused and angry as to why the service isn't responding[7].

Counter measure: cloud providers can force policies to offer limited computational resources.

F. *Malicious Insiders*

Malicious insider threat to an organization is a current or former employee, contractor, or other business partner working at cloud service provider , who has or had authorized access to an

organization's network, system, or data and intentionally exceeded or misused that access in a manner that negatively affected the confidentiality, integrity, or availability of the organization's information or information systems. Since cloud service provides often don't follow the best security guidelines and don't implement a security policy, employees can gather confidential information from arbitrary customers without being detected. An attacker can create a valid account can create a virtual image containing malicious code such as Trojan horse.
Countermeasure: Access control framework, image filtering.

IV. CONCLUSION

Cloud computing provides many benefits like storage capacity, cost reduction and processing power etc. However it has its own security related issues that threaten the organizations to adopt the cloud technology. Many researches are going at present to identify the security threats and the possible solutions to those threats. This paper describes the survey of the available countermeasures for the threats which are noted as notorious threats by CSA. The main solution obtained to these security threats based on many research papers is that the SLA(Service Level Agreement) between the vendor and the customer, good degree of encryption standards provided by the vendor which protects the data security. Much vulnerability in clouds still exists and hackers continue to exploit these security holes. In order to provide better quality of service to cloud users, security flaws must be identified. In this paper, we examined the security vulnerabilities in clouds, and introduced countermeasures to those security breaches.

V. REFERENCES

[1] Xiao S, Gong W (2010) Mobility Can help: protect user identity with dynamic credential. In: Eleventh International conference on Mobile data Management (MDM). IEEE Computer Society, Washington, DC, USA, pp 378–380.
[2] Li W, Ping L (2009) Trust model to enhance Security and interoperability of Cloud environment. In: Proceedings of the 1st International conference on Cloud Computing. Springer Berlin Heidelberg, Beijing, China, pp 69–79.
[3] J. Brodkin, "Gartner: Seven Cloud-Computing Security Risks," InfoWorld, 2008. http://www.infoworld.com/d/security-central/gartner- seven-cloud-computing-security-risks-853
[4] Rittinghouse JW, Ransome JF (2009) Security in the Cloud. In: Cloud Computing. Implementation, Management, and Security, CRC Press.
[5] Wylie J, Bakkaloglu M, Pandurangan V, Bigrigg M, Oguz S, Tew K, Williams C, Ganger G, Khosla P (2001) Selecting the right data distribution scheme for a survivable Storage system. CMU-CS-01-120, Pittsburgh, PA.
[6] Somani U, Lakhani K, Mundra M (2010) Implementing digital signature with RSA encryption algorithm to enhance the data Security of Cloud in Cloud Computing. In: 1st International conference on parallel distributed and grid Computing (PDGC). IEEE Computer Society Washington, DC, USA, pp 211–216.
[7] Harnik D, Pinkas B, Shulman-Peleg A (2010) Side channels in Cloud services: deduplication in Cloud Storage. IEEE Security Privacy 8(6):40–47.
[8] Tebaa M, El Hajji S, El Ghazi A (2012) Homomorphic encryption method applied to Cloud Computing. In: *National Days of Network Security and Systems (JNS2)*. IEEE Computer Society, Washington, DC, USA, pp 86–89
[9] Wei J, Zhang X, Ammons G, Bala V, Ning P (2009) Managing Security of virtual machine images in a Cloud environment. In: Proceedings of the 2009 ACM workshop on Cloud Computing Security. ACM New York, NY, USA, pp 91–96.
[10] Gartner Inc Gartner identifies the Top 10 strategic technologies for 2011. Online. Available: http://www.gartner.com/it/page.jsp?id=1454221. Accessed: 15-Jul-2011