Security Issues in Cloud Computing a Review:

Er.Kashish Goyal[1]
[1]Student of M. Tech
[1]Department of Computer Science & Engineering
[1]Sri Guru Granth Sahib World University, Fatehgarh Sahib, Punjab, India

Abstract— As the use of computers in our day-to-day life increases, the computing resources that we need also go up. For companies like Google and Microsoft, harnessing the resources as and when they need it is not a problem. But when it comes to smaller enterprises, affordability becomes a huge factor. With the huge infrastructure come problems like machines failure, hard drive crashes, software bugs, etc. This might be a big headache for such a community. Cloud Computing offers a solution to this situation. Google, Microsoft, Yahoo, IBM and Amazon have started providing cloud computing services. In this paper, a survey of the different security risks that pose a threat to the cloud is presented. This paper is a survey more specific to the different security issues in cloud computing system.

Key words: Cloud Computing, Access Control, Authentication, security, SaaS, PaaS, Iaas, Security Challenges

I. INTRODUCTION

Cloud computing" is the next natural step in the evolution of on-demand information technology services and products [1]. Many of today's Information Technology (IT) applications rely on access to state-of-the-art computing facilities. For instance, as business decisions are increasingly driven by (data) analytics, the practice of operations research and business analytics becomes inherently intertwined with the management of IT resources. According to NIST "Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (for example, networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service-provider interaction" [2]. The basis of cloud computing is to create a set of virtual servers on the available vast resource pool and give it to the clients. Based on the computing needs of the client, the infrastructure allotted to the client can be scaled up or down. One of the key concepts of cloud computing is that processing of 1000 times the data need not be 1000 times harder. As and when the amount of data increases, the cloud computing services can be used to manage the load effectively and make the processing tasks easier. in cloud computing services, the users are charged based on the number of cycles of execution performed or the number of bytes transferred. The hardware or the machines on which the applications run are hidden from the user.

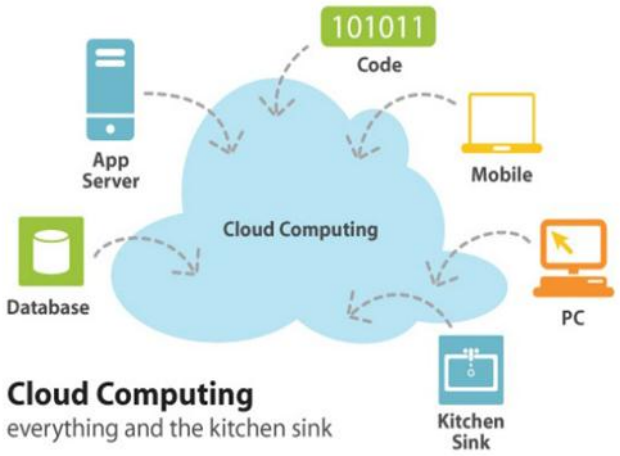

Fig. 1: Cloud computing functionalities

II. CLOUD COMPUTING SERVICES

The cloud computing services are broadly divided into three categories:

1) Infrastructure-as-a-Service (IaaS)
2) Platform-as-a-Service (PaaS)
3) Software-as a-Service (SaaS).

A. Infrastructure-As-A-Service:

Infrastructure-as-a-Service provides virtual server instances with unique IP addresses and blocks of storage on demand. Customers use the provider's application program interface to start, stop, access and configure their virtual servers and storage. In the enterprise, cloud computing allows a company to pay for only as much capacity as is needed, and bring more online as soon as required [3].

B. Platform-As-A-Service:

In the cloud is defined as a set of software and product development tools hosted on the provider's infrastructure. Developers create applications on the provider's platform over the Internet [4].

C. Software-As-A Service:

Cloud model, the vendor supplies the hardware infrastructure, the software product and interacts with the user through a front-end portal. Cloud computing is a pretty new technology, there are many companies offering the above mentioned cloud computing services. Different companies like Amazon, Google, Yahoo, IBM and Microsoft are all players in the cloud computing services industry. But Amazon is the pioneer in the cloud computing industry with services like EC2 (Elastic Compute Cloud) and S3 (Simple Storage Service) dominating the industry. Amazon has an expertise in this industry and has a small advantage over the others because of this. Microsoft has good knowledge of the fundamentals of cloud science and is building massive data centers [5]. IBM, the king of business

computing and traditional supercomputers, teams up with Google to get a foothold in the clouds. Google is far and away the leader in cloud computing with the company itself built from the ground up on hardware.

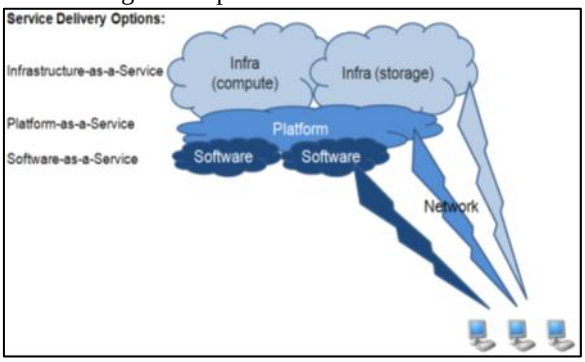

Fig. 2: Cloud Service Delivery Options

III. TYPES OF CLOUDS

There are different types of clouds that you can subscribe to depending on your needs. As a home user or small business owner, you will most likely use public cloud services.

A. Public Cloud:

A public cloud can be accessed by any subscriber with an internet connection and access to the cloud space.

B. Private Cloud:

A private cloud is established for a specific group or organization and limits access to just that group.

C. Community Cloud:

A community cloud is shared among two or more organizations that have similar cloud requirements.

D. Hybrid Cloud:

A hybrid cloud is essentially a combination of at least two clouds, where the clouds included are a mixture of public, private, or community [6].

IV. SECURITY ISSUES

There are numerous security issues associated with Cloud Computing. And these issues fall into two broad categories: Security issues faced by Cloud providers and security issues faced by their customers. In most cases, the provider must ensure that their infrastructure is secure and that their clients' personal data and applications are protected while the customer must ensure that the Cloud provider has taken the proper security measures to protect their information. Data in the hands of third-party companies and users relegates control of their data in the hands of others. The Cloud acts as a big black box, nothing inside the Cloud is inside the Cloud is visible to the clients. clients have no idea or control over what happens inside a Cloud. a lot of security issues exist which are becoming more important to be tackled with the increase in IT services. Some of the issues are discussed below [7].

A. Intrusion Detection:

Intrusion detection is the process of using pattern recognition to detect and react to the abnormal events. This may include reconfiguring system components in real time to stop / prevent an intrusion. Intrusion detection, prevention, and response in physical environments are mature; however, the growth of virtualization and massive multi tenancy is creating new targets for intrusion and raises many questions about the implementation of the same protection in Cloud environments. The security challenge which involves intrusion detection is the Proliferation of Secure Socket Layer (SSL) required by deployment in public Cloud's adds complexity or blocks visibility to network-based IDS/IPS. To configure and manage the API's as to meet the need of the current Cloud Computing scenario [8, 2].

B. Unencrypted Data:

Data encryption is a process that helps to address various external and malicious threats. Unencrypted data is vulnerable for susceptible data, as it does not provide any security mechanism. These unencrypted data can easily be accessed by unauthorized users. Unencrypted data risks the user data leading cloud server to escape various data information to unauthorized users. For example, the famous file sharing service Drop box was accused for using a single encryption key for all user data the company stored [9].

C. Backup and Storage:

The cloud vendor must ensure that regular backup of data is implemented that even ensure security with all measures. But this backup data is generally found in unencrypted form leading to misuse of the data by unauthorized parties. Thus data backups lead to various security threats. As per the study carried by Intel IT center, more the server virtualization increases, a very difficult problem with backup and storage is created. Data de-duplication is listed as one of the solution to reduce backup and offline storage volumes [10].

D. SQL Injection Attack:

SQL injection attacks are malicious act on the cloud computing in which a spiteful code is inserted into a model SQL code. This allows the invader to gain unauthorized access to a database and eventually to other confidential information. Further, SQL injection attacks uses the special characters to return the data for example in SQL scripting the query usually ends up with where clause which again may be modified by adding more rows and information in it. The information entered by the hacker is misread by the website as that of the user's data and this will then allow the hacker to access the SQL server leading the invader to easily access and modify the functioning of a website. cloud computing and have also shown the SQL injection attack as the top intrusion detection [11].

E. Locks in:

Locks in is a small tender in the manner of tools, standard data format or procedures, services edge that could embark on data, application and service portability, not leading to facilitate the customer in transferring from one cloud provider to another or transferring the services back to home IT location [12].

F. Vulnerability in Virtualization:

Virtualization is one of the main components of a cloud. But this poses major security risks. Ensuring that different instances running on the same physical machine are isolated

from each other is a major task of virtualization which is not met completely in today's scenario. Current VMMs (Virtual Machine Monitor) do not offer perfect isolation. Many bugs have been found in all popular VMMs that allow escaping from VM. Some vulnerability has been found in all virtualization software which can be exploited by malicious, local users to bypass certain security restrictions or gain privileges. For example, the vulnerability of Microsoft Virtual PC and Microsoft Virtual Server could allow a guest operating system user to run code on the host or another guest operating system. Vulnerability in Virtual PC and Virtual Server could allow elevation of privilege. A perfection of properties like isolation, inspection and interposition is yet to be completely achieved in VMMs [13].

G. Data Locality:

In a SaaS model of a cloud environment, the consumers use the applications provided by the SaaS and process their business data. But in this scenario, the customer does not know where the data is getting stored. In many a cases, this can be an issue. Due to compliance and data privacy laws in various countries, locality of data is of utmost importance in many enterprise architecture (Softlayer, 2009). For example, in many EU and South America countries, certain types of data cannot leave the country because of potentially sensitive information. In addition to the issue of local laws, there's also the question of whose jurisdiction the data falls under, when an investigation occurs. A secure SaaS model must be capable of providing reliability to the customer on the location of the data of the consumer [14].

H. SLA/QOS:

Service Level Agreements between a CSP and CSC decides the nature of the service. Here nature of service reflects to the understanding between the both CSP and CSC about to be the expectation of the service that should be delivered, and in case if the provider fails to deliver that service, then the compensation will be given to CSC. SLA decides the terms of service, licensing, suspension and termination, privacy security and policies that have to be implemented.
There are two types of SLAs predefined are negotiable agreements and non-negotiable agreements. Non-negotiable agreements are much enjoyed by the CSP as with having some offerings, which can be modified by provider to terms without giving any prior direct notification to the customer On other hand the negotiable agreements are just like today's IT outsourcing contracts. They address about the privacy and security policies along with the control over the employee, data owner, software isolation, data encryption and the use of products meeting international/national standards. The non- negotiable SLAs make a rough move towards the CSP, as the CSP has all right to change the agreements without any notifications, which arise a type of insecurity to the CSC as he has no control over his/her own assets. So to increase a trustable security negotiable agreements should be done between both CSC and CSP. More over to it the SLA only decide what type of quality should be delivered to the consumer. Quality of service which should be provided to consumer is defined by C-QoSMS which is QOS management strategy, is proposed to add in resource [14].

I. Network security:

In cloud deployment models instead of traditional clearly defined network boundaries the borders between tenant networks can be dynamic and potentially blurred in a large scale virtual/cloud environment. In a cloud deployment model, sensitive data is obtained from the enterprises, processed by the SaaS application and stored at the SaaS vendor end. All data flow over the network needs to be secured in order to prevent leakage of sensitive information. Virtual Segmentation of physical servers exhibits the limited visibility of inter-VM traffic [15].

J. Authentication and Authorization:

Many a times user credentials are stored in the SaaS providers' databases and not as part of the corporate IT infrastructure. This means SaaS customers must remember to remove/disable accounts as employees leave the company and create/enable accounts as come onboard. In essence, having multiple SaaS products will increase IT management overhead. For example, SaaS providers can provide delegate the authentication process to the customer's internal LDAP/AD server, so that companies can retain control over the management of users [16].

K. Monitor the Data Access:

Cloud service providers have to assure about whom, when and what data is being accessed for what purpose. For example many website or server had a security complaint regarding snooping activities by many people such as listening to voice calls, reading emails and personal data etc [17].

L. Web Security:

With over 75% of attacks happening through Web applications, this becomes a critical piece in the overall cloud decision making process. The key concern issues with web security is that whether the security ownership transfer to the infrastructure provider, means if the web securities are implanted then the access to it would provided to owner or not. Another issue is the impact of the implantation of the security on SDLC and the surety after the security to protection against key vulnerabilities like XSS, SQL Injection, CSRF, Session Management etc. These are the some major issues in concerned with cloud web security [18].

M. Sniffer Attacks:

These types of attacks are launched by applications which can capture packets flowing in a network and if the data that is being transferred through these packets is not encrypted, it can be read. There are chances that vital information flowing across the network can be traced or captured. A sniffer program, through the NIC (Network Interface Card) ensures that the data/traffic linked to other systems on the network also gets recorded. It can be achieved by placing the NIC in promiscuous mode and in promiscuous mode it can track all data, flowing on the same network. A malicious sniffing detection platform based on ARP (address resolution protocol) and RTT (round trip time) can be used to detect a sniffing system running on a network [19].

N. Distributed Denial of Service Attacks:

DDoS may be called an advanced version of DoS in terms of denying the important services running on a server by flooding the destination sever with large numbers of packets such that the target server is not able to handle it. In DDoS the attack is relayed from different dynamic networks which have already been compromised unlike the DoS attack. The attackers have the power to control the flow of information by allowing some information available at certain times. Thus the amount and type of information available for public usage is clearly under the control of the attacker [20].

O. Data separation:

A particular cloud computing service provider not only handles your organization's data, but also at the same time manages data for various other companies. Insecurity concern, risk is also an area that the user thought about cloud computing; we show a table of the security guide was concentrated to some of the most common risks of cloud computing [21].

P. Governance:

Governance means keeping control and oversight over policies, procedures and standards for application development. Basic issues of governance in cloud computing is related to identification and implementation of appropriate organizational structures ,process and controls to maintain effective information security governance, risk management compliance This problem can be solved by including security metrics and standards in Service Level Agreements (SLA) and contracts. While a SLA is going to establish, security department should be engaged to ensure that security [22].

Q. Legal Issues:

Geographical locations are not fixed for any resources in the clouds. They may migrate between the physical locations due to the different factors and reasons. Because of the migration they may come under multiple legal jurisdictions and these jurisdictions may have conflicting rules about security issues such as intrusion and data protection [16]. Make sure that the migration rules, country location restrictions are defined and enforced or mentioned in SLA or contract. SLA is the only legal agreement between the service provider and the client. Providers should assure customer that their data is safe, authentic. They should have mutual understandings between them. Rules should be mentioned in SLA regarding expected or unexpected transmission of contract. Legal intercepts are not classical attacks but they might violate security goals [1].

V. Conclusion

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, it has grown from being a promising business concept to one of the fast growing segments of the IT industry. The use of internet and network is growing rapidly. So there are more requirements to secure the data transmitted over different networks using different services. This paper discussed the various security concerns of cloud and security issues of cloud computing. Though this paper has covered almost all security issues in the Cloud environment, but maybe there are some areas which are untouched. Cloud is the cheapest and the easiest way to use the resources. security is a very big issue in Cloud Computing and also this field is full of challenges.

References

[1] Mladen A. Vouk, Cloud Computing – Issues, Research and Implementations. Journal of Computing and Information Technology - CIT 2008. 16(4): p. 235–246.
[2] NIST Definition of Cloud Computing v15, csrc.nist.gov/groups/SNS/cloud-computing/cloud-def-v15.doc
[3] http://en.wikipedia.org/wiki/Cloud_computing.
[4] http://searchcloudcomputing.techtarget.com.
[5] http://salesforce.com/cloudcomputing
[6] http://csrc.nist.gov/publications/drafts/800-145/Draft-SP-800-145_cloud-definition.pdf.
[7] Kashish Goyal, Supriya, Security Concerns In the World of Cloud Computing. IJARCS International Journal of Advanced Research in Computer Science, 2013. 4 (4), p. 230-234.
[8] Young-Gi Min et al., Cloud Computing Security Issues and Access Control Solutions. Journal of Security Engineering ,Vol.(9), p. 135-142.
[9] K. Owens, Securing Virtual Computer Infrastructure in the Cloud. white paper, Savvis Communications Corp., 2009.
[10] Krishnan Subramanian, Private, Public and Hybrid Clouds. whitepaper: Trend Micro, 2011.
[11] Sara Qaisar, Kausar Fiaz Khawaja, Cloud Computing: Network/Security Threats and counter measures. Interdisciplinary Journal of Contemporary Research in Business, ijcrb.webs.com, January 2012, Vol 3, N0 9, p: 1323 – 1329.
[12] Jamil, D., Zaki, H. Security issues in cloud computing and counter measures. International Journal of Engineering Science and Technology (IJEST) , Vol. 3 No. (4), p: 2672-2676.
[13] S. Subashini, V. Kavitha. A survey on security issues in service delivery models of cloud computing .Journal of Network and Computer Applications (34) p. 1–11
[14] Wayne A Jansen, Cloud hooks: security and privacy issue in cloud computing. Proceeding of 44th Hawaii international conference on system science-2011 p. 1605-2011.
[15] Wayne Jansen, Timothy Grance, Guidelines for security and privacy in pubic cloud. Draft Special Publication 800-144
[16] Michael glas and paul Andres, An Oracle white paper in enterprise architecture achieving.
[17] The cloud computing vision", CA-U.S.A, Oct 2010.
[18] Wayne Jansen, Timothy Grance, Guidelines for security and privacy in pubic cloud. Draft Special Publication. p. 800-144
[19] http://docs.ismgcorp.com/files/external/Draft-SP-800-145_cloud-definition.pdf

[20] http://www.usenix.org/event/hotcloud09/tech/full_papers/wood.pdf
[21] A. Weiss, BComputing in the clouds, netWorker, vol. 11, no. 4, p. 16–25.
[22] N. Provos, M.A. Rajab, P. Mavrommatis, Cybercrime 2.0: When the cloud turns dark. Queue (2), P. 46–47

