RESEARCH ARTICLE OPEN ACCESS

Cloud Computing and Security Issues: A Survey

Barinder Kaur
CSE, GNDU, Amritsar
Punjab - India

ABSTRACT
Cloud computing has been a revolution in the field of IT industry. It has changed the way people think about accessing and storing resources over the internet. Furthermore the reduced cost, scalability and flexibility have made it a top notch technology in present scenario. But with advantages comes the disadvantages and security is one of the critical aspect. In this paper cloud computing, its delivery models, deployment models and security issues concerning it are surveyed.
Keywords:- Cloud Computing; Service Models; Deployment Models; Security Issues

I. INTRODUCTION

Cloud computing is becoming prominent topic whenever the information technology is discussed. It creates the large scale virtual resource pool connecting storage resources, computing resources and software resources which remote users can utilize at anytime and anywhere. Virtualization technology allows multiple operation systems and applications to be run on shared system. And when the server is heavily loaded it can migrate an instance of operating system and applications from a heavily loaded server to lightly loaded one in the cloud resource pool. User need not to know the actual location of data it is accessing. The local computing and storage resources are moved into the cloud in the cloud computing model. In this way user need to pay only for the data it is accessing, hence saving him the cost of buying the entire software. For the small scale enterprises, it is undoubtedly beneficial as they need not to buy expensive servers and need not to employ professionals to deploy IT infrastructure.

So to quote the most widely used definition of cloud computing made by NIST is as. " Cloud Computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management efforts or service provider interaction. This cloud model promotes availability and is composed of five essential characteristics. Three service models, and four deployment models." The cloud computing model NIST defined has three service models, and four deployment models. The three service models, also called SPI model, are: Cloud Software as a Service (Saas), Cloud Platform as a Service (PaaS) and Cloud Infrastructure as a Service (IaaS). The four deployment models are: Private cloud, Community cloud, and Public cloud and Hybrid cloud. Besides having the potential benefits, on the other hand there are many problems in the cloud computing with security the major one. As we have discussed that cloud computing is still the new technology in the field of IT, the traditional security policies are not able to respond to the emergence of new cloud computing security issues.[1][2][3]

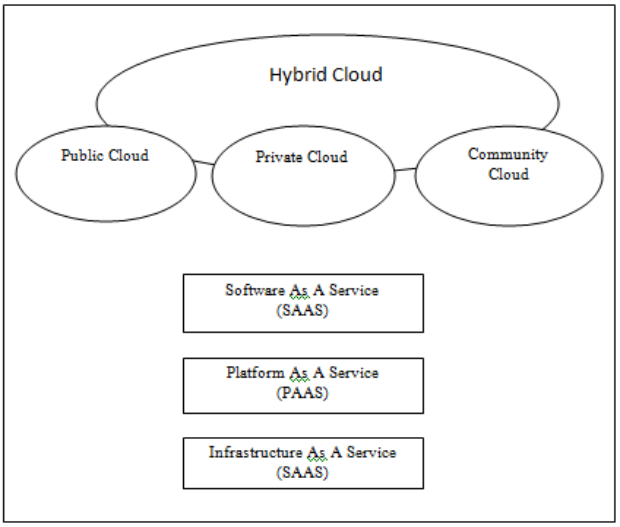

Fig.1 Cloud Computing Service Models and Deployment Models

Fig.1 shows layered architecture of Cloud Computing Security Models comprising of SaaS, PaaS and Saas and Cloud Computing Deployment Models.

II. CLOUD SERVICE MODELS

Cloud service delivery is divided among three architectural models and various derivative combinations. Three fundamental classifications are often referred to as the "SPI Model", where 'SPI' refers to Software, Platform or Infrastructure (as a Service), respectively-defined.

- Infrastructure as a Service (IaaS): Here computing resources are acquired by the user such as processing power, memory and storage from an IaaS provider and the resources are used to deploy and run their applications. IaaS has low level of abstraction as compared to PaaS that allows users to access the underlying infrastructure through the use of virtual machines. IaaS gives users more flexibility than PaaS as it allows the user to deploy any software stack on top of the operating system. However, flexibility comes with a cost and users are responsible for updating and patching the operating system at the IaaS level. Amazon Web Services' EC2 and S37 are popular IaaS examples.
- Platform as a Service (PaaS): In here applications are developed using a set of programming languages and tools that are supported by the PaaS provider. High level of abstraction is provided by PaaS that allows them to focus on developing their applications and not worry about the underlying infrastructure. Just like the SaaS model, users do not have control or access to the underlying infrastructure being used to host their applications at the PaaS level. Google App Engine5 and Microsoft Azure6 are popular PaaS examples
- Software as a Service (SaaS): In SaaS, users simply make use of a web-browser to access software that others have developed and offer as a service over the web. At the SaaS level, users do not have control or access to the underlying infrastructure being used to host the software. Salesforce's Customer Relationship Management software3 and Google Docs4 are popular examples that use the SaaS model of cloud computing.[4]

III. CLOUD DEPLOYMENT MODELS

The four deployment models of Cloud Computing are: Private cloud, Community cloud, and Public cloud and Hybrid cloud.

- **Private cloud**: Private Cloud is a cloud that is used exclusively by one organisation. The cloud may be operated by the organisation itself or a third party. The St Andrews Cloud Computing Co-laboratory8 and Concur Technologies are example organisations that have private clouds.
- **Public cloud**: It is a cloud that can be used by the general public. Public clouds require significant investment and are usually owned by large corporations such as Microsoft, Google or Amazon.
- **Community cloud**: It is shared by several organisations and is usually setup for their specific requirements. The Open Cirrus cloud testbed could be regarded as a community cloud that aims to support research in cloud computing.
- **Hybrid cloud**: It is a cloud that is setup using a mixture of the above three deployment models. Each cloud in a hybrid cloud could be independently managed but applications and data would be allowed to move across the hybrid cloud. Hybrid clouds allow cloud bursting to take place, which is where a private cloud can burst-out to a public cloud when it requires more resources.[4][12]

TABLE1. DIFFERENCES IN CLOUD COMPUTING DEPLOYMENT MODELS

Parameters	Public	Private	Community	Hybrid
Ownership	Large Corporations	One Organisation	Several Organisation	Several Organisation
Security	Low	High	Medium	Medium
Access	Open	Closed	Partially Closed	Partially Closed
Confidentiality	Low	High	Medium	Medium
Malicious Attackers	High	Low	Medium	Medium

IV. CLOUD COMPUTING SECURITY ISSUES

Wikipedia [5] defines Cloud computing security as "Cloud Computing security (sometimes referred to simply as cloud security) is an evolving sub-domain of computer security, network security, and, more broadly, information security. It refers to a broad set of policies, technologies, and controls deployed to protect data, applications, and the associated infrastructure of cloud computing [6].

The cloud system is running on internet and the security problems in the internet also can be found in the cloud system. The cloud system is not different than the traditional system in the PC and it can meet other special and new security problems. The biggest concerns about cloud computing are security and privacy.

A. Gartner's Seven Security Issues of Cloud Computing

Well-known Gartner's seven security issues which cloud clients should avert are mentioned below [7]:

- **Privileged user access**: An inherent level of risk is brought along when sensitive data processed outside the enterprise as outsourced services bypass the physical, logical and personnel controls IT shops exert over in house programs.
- **Regulatory compliance**: Even when the data is held by a service provider, customers are held responsible for the security and integrity of their own data [8]. Rational service providers are subjected to external audits and security certifications
- **Data location**: Users don't know exactly where their data is hosted while using the cloud. Distributed data storage is a usual manner of cloud providers that can cause lack of control and this is not good for customers who have their data in local machine before moving from local to cloud.
- **Data segregation**: Data in the cloud is typically in the shared environment alongside data from other customers. Encryption is effective but isn't an effective cure. Encryption and decryption is a classic
  way to cover security issues but it couldn't ensure to provide perfect solution for it.
- **Recovery**: Various questions such as if a cloud provider broke or some problems cause failure in cloud server what will happen to users' data? Can cloud provider restore data completely? Moreover clients prefer don't get permission to third- party companies to control their data. This issue can cause an impasse in security.
- **Investigate support**: Due to logging and data for multiple customers may be co-located and may also be spread across an ever changing set of hosts and data centres, Cloud services becomes especially difficult to investigate.
- **Long-term viability**: The clients must be sure their data will remain available if by any chance cloud computing provider go broke or get acquired by a larger company with may be new policies. [9][10]

B. Three Parties' Security Issues of Cloud Computing

The analysis of the security risks of cloud computing from the perspective of customer, service provider and government is as follows.

- The security risks confronted by customers The security risks that customers need to confront in cloud computing environment includes the downtime of cloud computing environment that brings great depress to the confidence of customers cannot be avoided totally; the leak of commercial secrets that means a nightmare for customer cannot be avoided totally and how to face the privilege status of cloud service provider and the security concerns such as fault elimination, damage compensation and business migration etc.
- The security risks confronted by service providers The security risks that service providers need to confront in cloud computing environment includes how to

  assure the long-term secure operation of the cloud data centre and isolate the fault to reduce its influence to a smallest extent are the security risks that service providers have to face with; how to fight against the numerous and aggressive network hackers is a disturbing security problem and for customers with various demands, how to effectively and securely manage these customers and identify and block the malicious customers is another unavoidable task.
- The security risks confronted by government The security risks that government administrators need to confront in cloud computing environment includes how to enhance the security protection of a mass-scale data centre is one important concern; how to securely manage the numerous and various scale cloud service providers and how to evaluate and rank the security level of cloud service providers and the security credit of cloud customers, and publish the proactive alarm of malicious programs.[11]

V. CONCLUSION

Cloud computing is a boon for the IT industry. But inspite of several services it provides it remain vulnerable to security and protection issues. Data and user's privacy has to be maintained at all levels. Various Clod computing security models has been designed to minimise the risks. Hope so in the near future the cloud service provider takes variety of measures to protect the security in order to effectively solve these problems.

REFERENCES

[1] Su Qinggang; Wang Fu; Hang Qiangwei, "Study of Cloud Computing Security Service Model," Engineering and Technology (S-CET), 2012 Spring Congress on , vol., no., pp.1,4, 27-30 May 2012.

[2] Xue Jing; Zhang Jian-jun, "A Brief Survey on the Security Model of Cloud Computing," Distributed Computing and Applications to Business Engineering and Science (DCABES), 2010 Ninth International Symposium on , vol., no., pp.475,478, 10-12 Aug. 2010.

[3] Deyan Chen; Hong Zhao, "Data Security and Privacy Protection Issues in Cloud Computing," Computer Science and Electronics Engineering (ICCSEE), 2012 International Conference on , vol.1, no., pp.647,651, 23-25 March 2012.

[4] Ilango Sriram; Ali Khajeh-Hosseini, "Research Agenda in Cloud Technologies," http://arxiv.org/ftp/arxiv/papers/1001/1001.3259.pdf

[5] Cloud computing secutity, http://en.wikipedia.org/wiki/cloud_computing_security.

[6] Wentao Liu, "Research on cloud computing security problem and strategy," Consumer Electronics, Communications and Networks (CECNet), 2012 2nd International Conference on , vol., no., pp.1216,1219, 21-23 April 2012 .

[7] J.Brodkin.(2008). Gartner: Seven cloud- computing security risks. Available; http://www.networkworld.com/news/2008/070208-cloud.html

[8] D.L.Ponemon,"Security of cloud computing users,"2010.

[9] Sabahi, F., "Cloud computing security threats and responses," Communication Software and Networks (ICCSN), 2011 IEEE 3rd International Conference on , vol., no., pp.245,249, 27-29 May 2011.

[10] Patidar, S.; Rane, D.; Jain, P., "A Survey Paper on Cloud Computing," Advanced Computing & Communication Technologies (ACCT), 2012 Second International Conference on , vol., no., pp.394,398, 7-8 Jan. 2012.

[11] Jianhua Che, Yamin Duan, Tao Zhang, Jie Fan, Study on the Security Models and Strategies of Cloud Computing, Procedia Engineering, Volume 23, 2011, Pages 586-593, ISSN 1877-7058.

[12] Ramgovind, S.; Eloff, M.M.; Smith, E., "The management of security in Cloud computing," *Information Security for South Africa (ISSA), 2010* , vol., no., pp.1,7, 2-4 Aug. 2010.