Volume 4, No. 4, March-April 2013

ISSN No. 0976-5697

International Journal of Advanced Research in Computer Science

REVIEW ARTICLE

Available Online at www.ijarcs.info

Security Concerns In the World of Cloud Computing

Kashish Goyal*
M.Tech Research Scholar
Department of Computer Science and Engineering.
Sri Guru Granth Sahib World University.
Fatehgarh Sahib, Punjab, India.
er.aggarwalkashish@gmail.com

Supriya
Assistant Professor
Department of Computer Science and Engineering.
Sri Guru Granth Sahib World University.
Fatehgarh Sahib, Punjab, India.
supriya@sggswu.org

Abstract: Cloud Computing is one of the today's most exciting technology. it is base on pay-as-you-go approach . Cloud Computing is an Internet-based computing, where shared resources, software and information, are provided to computers and devices on-demand. Cloud Computing is a promising technology to facilitate development of large-scale, on-demand, flexible computing infrastructures. . It is a construct that allows user to access applications that actually reside at location other than user's own computer or other Internet-connected devices. Security is the biggest challenge for Cloud Computing currently. Trust has proved to be one of the most important and effective alternative means to construct security in distributed systems. Obviously putting everything into a single box i.e. into the Cloud will only make it easier for hacker. This paper presents an overview and the study of the Cloud Computing. Also include the several security and challenging issues

Keywords: Cloud Storage, Security, Privacy, Data Availability, Control, Attack.

I. INTRODUCTION

Cloud Computing is an emerging paradigm in the computer industry where the computing is moved to a Cloud of computers. Cloud Computing is becoming a well-known buzzword for the industry. Many companies, such as Amazon, Google, and Microsoft and so on, accelerate their paces in developing Cloud Computing systems and enhancing their services to provide for a larger amount of users [1]. Cloud Computing services can also grow and shrink according to need. Cloud Computing is particularly valuable to small and medium businesses. It is numerous. But still there are some security concerns that are to be redressed. Especially because Cloud Computing users have no choice but to rely on the service provider [2] . We closely watch Cloud Computing security on a very technical level, focusing primarily on attacks and hacking attempts related to Cloud Computing providers and systems [3]. Figure 1 discusses various functionalities provided by a Cloud system.

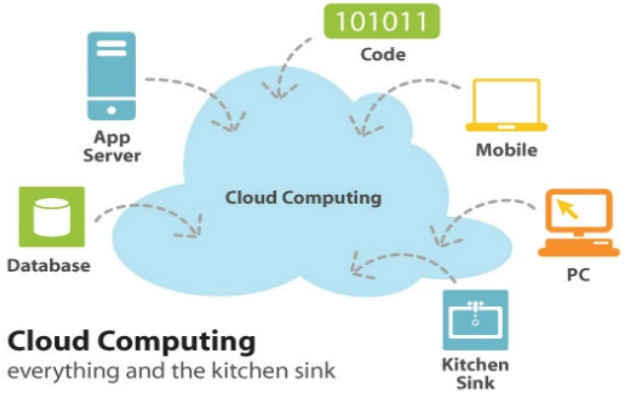

Figure 1. Cloud Computing functionalities.

II. CLOUD COMPUTING

Cloud Computing has been defined by NIST as a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction[4] . The Cloud Computing model NIST defined has three service models and four deployment models. The three service models, also called SPI model [5]. A set of pooled computing resources deliver over the internet an internet based computing environment where you pay only for resources that you use. In Cloud we have three parties (i.e., Cloud service user, Cloud service provider/Cloud user, Cloud provider) [6].

A. Cloud Software as a Service:

Cloud Software as a Service SaaS ensures that complete applications are hosted on the internet and users use them. The payment is made on a payper use model. It eliminates the need to install and run the application on the customer's local computer, thus alleviating the customer's burden for software maintenance. In SaaS, there is the Divided Cloud and Convergence coherence mechanism whereby every data item has either the "Read Lock" or "Write Lock Two types of servers are used by SaaS: the Main Consistence Server (MCS) and Domain Consistence Server (DCS). Cache coherence is achieved by the cooperation between MCS and DCS . In SaaS, if the MCS is damaged, or compromised, the control over the Cloud environment is lost. Hence securing the MCS is of great importance.[7]

B. Cloud Platform as a Service:

Cloud Platform as a Service In this Paas model of Cloud Computing, the Cloud provider provides a platform for use. Services provided by this model include all phases of the System Development Life Cycle (SDLC) and can use

Application Program Interfaces (APIs), website portals, or gateway software. Buyers do need to look closely at specific solutions, because some providers do not allow software created by their customers to be moved off the provider's platform [9]. According to NIST the capability provided to the consumer is to deploy onto the Cloud infrastructure consumer-created or acquired applications created using programming. Languages, libraries, services, and tools supported by the provider [6]. The consumer does not manage or control the underlying Cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment. Buyers do need to look closely at specific solutions, because some providers do not allow software created by their customers to be moved off the provider's platform.[8]

C. Cloud infrastructure as a service:

Cloud infrastructure as a service This is the base layer of the Cloud stack. It serves as a foundation for the other two layers, for their execution. The keyword behind this stack is Virtualization. Usually platform-independent; infrastructure costs are shared and thus reduced; service level agreements (SLAs); pay by usage; self-scaling. Avoid capital expenditure on hardware and human resources; reduced ROI risk; low barriers to entry; streamlined and automated scaling but disadvantages are Business efficiency and productivity largely depends on the vendor's capabilities; potentially greater long-term cost; centralization requires new/different security measures. With , a company can rent fundamental computing resources for deploying and running applications or storing data. IaaS enables fast deployment of applications, and improves the agility of IT services by instantly adding computing processing power and storage capacity when needed [9]

III. DEPLOYMENT MODELS

A. Private Cloud:

Private Cloud is a new term that some vendors have recently used to describe offerings that emulate Cloud Computing on private networks. It is set up within an organization's internal enterprise datacenter. In the 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]

B. 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.[13] 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.

C. Hybrid Cloud:

Hybrid Cloud is a private Cloud linked to one or more external Cloud services, centrally managed, provisioned as a single unit, and circumscribed by a secure network [14]. It provides virtual IT solutions through a mix of both public and private Clouds. Hybrid Cloud provides more secure control of the data and applications and allows various parties to access information over the Internet. It also has an open architecture that allows interfaces with other management systems. Hybrid Cloud can describe configuration combining a local device, such as a Plug computer with Cloud services. It can also describe configurations combining virtual and physical, collocated assets -for example, a mostly virtualized environment that requires physical servers, routers, or other hardware such as a network appliance acting as a firewall or spam filter.[10]

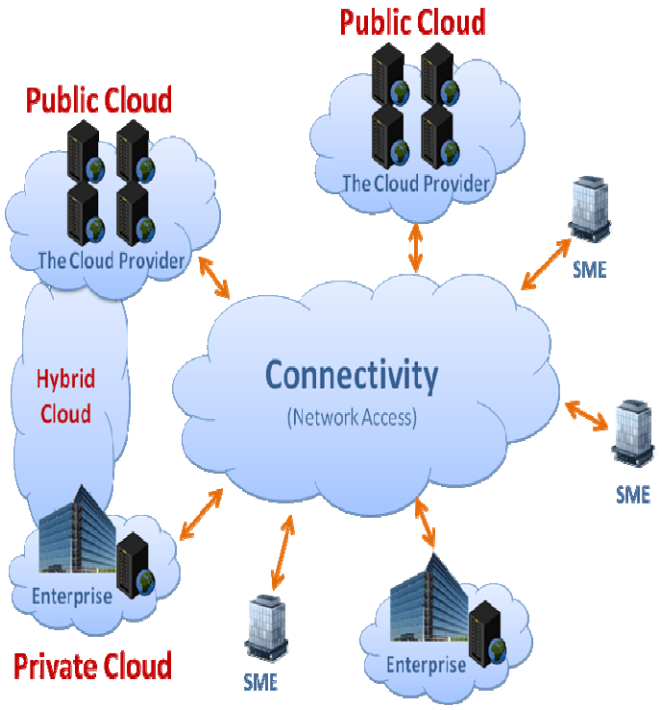

Figure 2. Cloud Computing Deployment Models.

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.

A. Legal Issues:

Cloud Computing systems (including applications and services hosted on them) has significant implications for the privacy of personal information as well as for the confidentiality of business and governmental information. That's because any information is shifted from local computers to the Cloud Computing systems at the Cloud Computing era, including email, word processing documents, spreadsheets, videos, health records, photographs, tax or other financial information, Audio Business plans, PowerPoint presentations, accounting information, advertising campaigns, sales numbers, appointment calendars, address books, and more. Furthermore, the entire contents of a user's originally stored on local device may be shifted to a single Cloud provider or even to many Cloud providers. Whenever an individual, a business, a government agency, or other entity shares information in the Cloud, privacy or confidentiality questions may arise [14]. 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.

B. Control:

A major goal of hackers is to have control over as system by which hackers will have the ability to monitor, intercept, and modify system events and activities. Control of a system is determined by which side occupies the lower layers in the software stack, [17]. Where lower layers control upper layers because lower layers implement the abstractions upon which upper layers depend. Controlling the system allows malware to remain invisible by obviating or disabling the security software. Virtualization -aware security software should be installed in the lowest layer of the software stack of the whole Cloud platform, not only the software stack of the VM (VM's OS is not the lowest layer in the virtualized environments).

C. Confidentiality:

Confidentiality means keeping user's data secret in the Cloud systems [15]. The confidentiality in Cloud systems is a big obstacle for users to step into it, as many users said "My sensitive corporate data will never be in the Cloud" in the article named "Above the Cloud".

D. Recovery:

Even if we don't know where our data is in a Cloud, Cloud provider should tell you what will happen to your data and service in case of a disaster". Any offering that does not replicate the data and application infrastructure across multiple sites is vulnerable to a total failure", Gartner says [16]. Provider must be asked if it has "the ability to do a complete restoration, and how long it will take".

E. Availability:

The goal of availability for Cloud Computing systems (including applications and its infrastructures) is to ensure its users can use them at any time, at any place. As its web-native nature, Cloud Computing system enables its users to access the system (e.g., applications, services) from anywhere. This is true for all the Cloud Computing systems (e.g., DaaS, SaaS, PaaS, IaaS, and etc.). Required to be accessed at any time, the Cloud Computing system should be severing all the time for all the users (say it is scalable for any number of users) [15]. Two strategies, say hardening and redundancy, are mainly used to enhance the availability of the Cloud system or applications hosted on it.

F. Security Breach:

If a security incident occurs, what support will we receive from the Cloud provider? While many providers promote their services as being unhackable, Cloud based services are an attractive target to hackers [13].

G. Storage of Data:

Cloud Computing is about storing their files with third party. For individuals, they might feel uneasy about sharing their files with another party especially the sensitive issues [19]. Furthermore, as Cloud Computing allows the files to be accessed from any computer through internet connection, therefore viral infection and malware could occur.

H. Data Protection:

In Cloud, on-premise application deployment model, the sensitive data of each enterprise continues to reside within the enterprise boundary and is subject to its physical, logical and personnel security and access control policies. However, in some Cloud model such as public Cloud, the enterprise data is stored outside the enterprise boundary, by the CSP [22]. Consequently, the CSP must adopt additional security checks to ensure data security and prevent breaches due to security vulnerabilities in the application or through malicious employees. This involves the use of strong encryption techniques for the protection of data.

I. Web Security:

With over 75% of attacks happening through Web applications, this becomes a critical piece in the overall Cloud decision making process [21]. 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.

J. 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 [20]. 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 that flows over the network need to be secured in order to prevent leakage of sensitive information. Virtual Segmentation of physical servers exhibits the limited visibility of inter-VM traffic. The deployment and the use of Non-standard API's provide an opportunity for intruder to spoof through network. Management of many virtual networks / VLAN in a complex environment – reliant on providers policies and procedures This involves the use of strong network traffic encryption techniques such as Secure Socket Layer (SSL) and the Transport Layer Security (TLS) for security.

K. 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. The methods of 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 [19]. 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. Also there is much less tools which may be used to develop the secure API's at the beginning level of the Cloud intrusion management.

L. Cookie Poisoning:

It involves changing or modifying the contents of cookie to have an unauthorized access to an application or to a webpage. Cookies basically contain the user's identity related credentials and once these cookies are accessible, the content of these cookies can be forged to impersonate an authorized user [8]. This can be avoided either by performing regular cookie cleanup or implementing an encryption scheme for the cookie data.

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 [8]. 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.

N. Email Security:

Today's era is the era of internet technology, global presence is important for all. Emails are the medium to stay connected, transferring the important information and so many uses. The portability of having the hackers to hack the account arise as we move on Cloud [22] . On other hand if we are using SaaS then storage is at the location which is unknown to consumer, which leads to data insecurity. Also the use of unauthorized webmail for business purposes may also raise insecurity. I got a mail form the Bmw's official site about the recruitment, and I informed the Bmw's officials about the issue and immediately took the action over it and suspended the concern account. The management of logs and access to logs which may ensuring no access to emails by Cloud provider staff should be implemented in perspective of trust. Figure 3 demonstrates Security as the Major Issue in Cloud Computing.

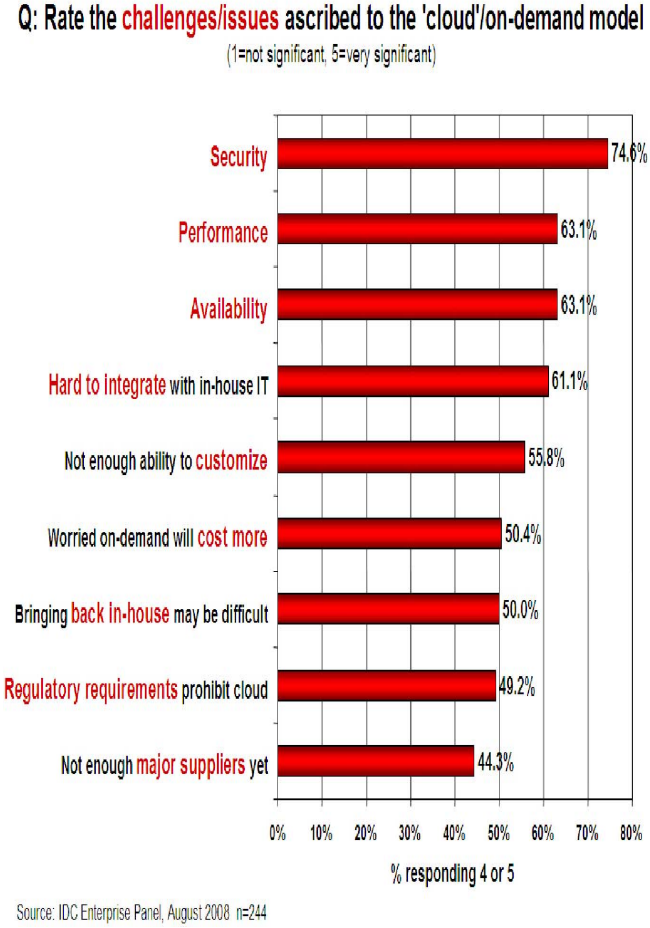

Figure 3. Security Issues in Cloud Computing.

V. CONCLUSION

Cloud Computing is the ultimate IT solution that takes secure data storage to a different level and allows both individual end users and enterprises to use their resources much more efficiently. Cloud benefits are endless. The Cloud Computing is associated with a lot of areas of information Technology, information management and services. But in order to achieve the best while spending less, have some

security issues which are unresolved. This paper discussed various aspects of Clouds and its security. 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. But the consumers never want that their data be shared or disclosed to anybody on Cloud. So, security is a very big issue in Cloud Computing. As such, building trust applications from untrusted components will be a major aspect with respect to Cloud security; we believe that security in Cloud Computing is an area full of challenges.

VI. REFERENCES

[1] Aishwarya C.S and Revathy.S, "Insight into Cloud Security issues", UACEE International Journal of Computer Science and its Applications, pp. 30-33, 2011.

[2] Amanjot Kaur and Manisha Bhardwaj, "Hybrid Encryption for Cloud Database Security", International Journal of Engineering Science & Advanced Technology, Vol.2, Issue 3, pp. 737 – 741, 2012.

[3] Rajesh Piplode and Umesh Kumar Singh, "An Overview and Study of Security Issues & Challenges in Cloud Computing," International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 2, Issue 9, pp. 115-120, 2012.

[4] Wayne A. Jansen, "Cloud Hooks: Security and Privacy Issues in Cloud Computing," in 44th Hawaii International Conference on System Sciences, Hawaii, 2011, pp.1-10.

[5] Deyan Chen and Hong Zhao, "Data Security and Privacy Protection Issues in Cloud Computing," International Conference on Computer Science and Electronics Engineering, pp. 23-25, 2012.

[6] Cloud Computing," http://nist.org csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf.

[7] CloudSecurity,Available: http://en.wikipedia.org/wiki/Cloud.

[8] Rohit Bhadauria and Sugata Sanyal, "Survey on Security Issues in Cloud Computing and Associated Mitigation Techniques", International Journal of Computer Applications, pp. 47-66, 2012.

[9] B.Meena and Krishnaveer Abhishek Challa, "Cloud Computing Security Issues with Possible Solutions," International Journal on Computer Science and Technology, Vol. 3, Issue 1, pp. 340-344, 2012.

[10] Anjum Asma1 et al., "Cloud Computing security Issues," International Journal of Application or Innovation in Engineering & Management, Vol. 1, Issue 2, pp. 141-147, 2012.

[11] Peeyush Mathur, "Cloud Computing New challenge to the entire computer industry," 1st International Conference on Parallel, Distributed and Grid Computing, 2010.

[12] Jianfeng Yang, Zhibin Chen, "Cloud Computing Research and Security Issues," IEEE, pp. 10-12, 2010.

[13] K.S.Suresh and Prof K.V.Prasad, "Security Issues and Security Algorithms in Cloud Computing," International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 2, Issue 10, pp. 110-114, 2012.

[14] Minqi Zhou et al., "Security and Privacy in Cloud Computing: A Survey," Sixth International Conference on Semantics, Knowledge and Grids, pp. 105-112, 2010.

[15] Jay Heiser and Mark Nicolette, "Assessing the Security Risks of Cloud Computing," Jay Heiser, Mark Nicolette Publication, pp. 2-6, 2008.

[16] Amani S. Ibrahim and James Hamlyn- Harris and John Grundy, "Emerging Security Challenges of Cloud Virtual Infrastructure," APSEC, 2010.

[17] Anthony Bisong and M. Rahman, "An Overview of the Security Concerns In Enterprise Cloud Computing," International Journal of Network Security & Its Applications, Vol. 3, pp. 30-45, 2011.

[18] Heru Susanto et al., "Toward Cloud Computing Evolution: Efficiency vs. Trendy vs. Security," Computer Science Journal, pp. 135-142, 2012.

[19] Young-Gi Min et al., "Cloud Computing Security Issues and Access Control Solutions," Journal of Security Engineering South Korea ,Vol. 9, pp. 135-142, 2012

[20] Soeung-Kon et al., "Mobile Cloud Computing Security Considerations," Journal of Security Engineering, pp. 143-150, 2012.

[21] Yashpal Kadam, "Security Issues in Cloud Computing A Transparent View," International Journal Comp Sci. Emerging Tech, Vol. 2, pp. 316-322, 2011.

[22] Open Security Architecture Available: http://www.opensecurityarchitecture.org.

[23] http://www.csrc.nist.gov/groups/SNS/Cloud-Computing/Cloud-Computing-v26.ppt.