Proceedings of the Second International Conference on Research in Intelligent and Computing in Engineering pp. 245–250
DOI: 10.15439/2017R70
ACSIS, Vol. 10 ISSN 2300-5963

# A Review Paper on Cloud Computing and its Security Concerns

Steven Mathew
Student, B.Tech,
Computer Science & Engineering
Dronacharya College of Engineering
Gurgaon, India
Email: mathewsteven92@gmail.com

Sarita Gulia
Assistant Professor,
Computer Science & Engineering Dronacharya
College of Engineering Gurgaon, India
Email: sarita10103@gmail.com

Varinder Singh
Student, B.Tech,
Computer Science & Engineering
Dronacharya College of Engineering
Gurgaon, India
Email: vinnykhurana42@gmail.com

Vivek Dev
Student, B.Tech,
Computer Science & Engineering
Dronacharya College of Engineering
Gurgaon, India
Email: devvivek12@gmail.com

***Abstract*—Cloud computing in the present scenario is a developing and fast growing technology that is being widely used around the globe. It utilizes the power of Internet based computing and here the data, information and other resources are provided to the user via computer or device on-demand. It's a new conception that uses virtual resources for sharing data has evolved. Yahoo or Gmail are some suitable examples of cloud computing. Various industries that include health care, banking and education are drifting towards this technology, all because of the efficiency provided by the system which is powered by pay as you use model and hence it takes care of the bandwidth, data movement, transactions and storage information.**

***Index Terms*—Cloud, network, virtual, economical computing, effectiveness, pay-per-use.**

## I. Introduction

Cloud is a common representation for an Internet-accessible organization which is hidden from users. Cloud Computing can be described in simple words as a combination of technology that provides hosting and storage services over the internet. Cloud can be classified into public, private or hybrid.

With the increasing popularity of Cloud based system, the cloud operators have been targeting at its consistency, safety, privacy-preserving and cost-efficient cloud design. Requirements of Cloud applications vary based on the resources which are demanded as services. Thus, the resources may rise to heavy computation resources, large storage resources, high volume network resources and so on. Cloud computing in other words is a standard term for conveying hosted work over the Net. It offers abundant benefits for the initiative, though; there are also a number of issues, as with any new technology. And one of the major concern relates to the safety and privacy of client information in terms of its placement, accessibility and security. Cloud computing may also be referred as permitting a network of remote server hosted over the internet to store, manage and process data.

## II. Heuristic Search Method

Cloud computing allows customers and industries to utilize applications via internet on any computer

directly without any established connection and access to their private files. The user uses the information and resources and in turn they just need to pay for the service in order to save time and money without including any third party. In the process of Cloud computing the services are provided by the enterprises and accessed by the users over the internet.

## III. DEPLOYMENT OF CLOUD SERVICES

Deployment of cloud services

There are four assorted types of cloud preparation models viz.: “Private cloud”, “Public cloud”, “Hybrid cloud” and “Community cloud”. Information about theses are given below:

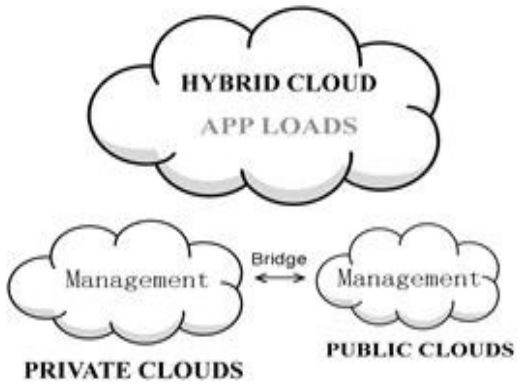


*Fig 1. Deployment Methods in Cloud*

*Private cloud:*

This cloud computing is very similar in nature to public cloud and includes “scalability” and “reliability”. But the main difference in private clouds is that, it is designed only for a single organization.

*Public cloud:*

In public cloud, the cloud seller at the vendor’s places hosts the computing model. The consumer has no perceptibility and power over where the computing model is hosted.

*Hybrid cloud:*

This is basically the joint venture of the public and private cloud system working together.

*Community cloud:*

Community cloud: a cloud that is mutually used by various organizations and is commonly framed-up for their special requirements. The framework may be closely-held and operated by the organizations or by the cloud company provider.

The nature and mode of services offered by the cloud computing providers to the cloud clients is defined into three fundamental models:

1) Software as a Service(SaaS):
   Also called as ‘On-demand software’, SaaS is a layer of cloud computing that allows the users to have access to information and application required, not locally, but, from a remote server or facility via Internet. The client can access such services on their laptops, desktops, mobiles, browser etc. on a pay-per-use basis.
   Security of data is a major concern when it comes to the user’s data being stored on the cloud.
2) Platform as a Service(PaaS):
   Even if we have a software available on-demand on the cloud sometimes the local machine is not efficient enough to deliver a high processing power required for certain applications.
   This problem is solved by the cloud providers who provide platforms, basically compilers, interpreters, webservers, assemblers, virtual environments, Processing engines , development environments operating systems, programming language specific program specific execution environments. So this allows application developers to develop applications without caring about the software and hardware layers, and the amount and complexity associated with them. This layer makes scaling the business an easy piece of job as the cloud providers scale the processing power and the requisite resources automatically, to meet the application development requirements.

3) Infrastructure as a Service
The services that support a software and platform service, are the infrastructural services. These basically include the services pertaining to the hardware resources that support and the software and platform services of the cloud providers. The cloud providers facilitate a cloud infrastructure for installing the software and the platform.

*Cloud Services:*


*Fig 2. Showing the three types of Cloud Services*

## IV. SECURITY IN CLOUDS

Gartner an American information technology research and advisory firm recently suggested that cloud computing as used for service-enabled applications still had seven years until it reached market maturity. Some of the problems it faces till now includes scalability, interoperability, shared environment and security, not to mention more business-focused topics.There is no denying the fact that Cloud resources are virtualized, different cloud service users share the same infrastructure and platform for building application and to store data. One key interest is affiliated to architecture set, asset alienation, and data segregation. Any disapproved and ferocious access to cloud service user's delicate data may accord its wholeness, secrecy and privacy.

A. Cloud Threats:

Several of the threats that were analyzed over a period of time, and it was found that a large amount of data was compromised by Thefts and Unauthorized Access. Other small percentage of security threat was due to Loss, Combination, IT incident, Improper Disposal etc.


*Fig 3. The Statistics of Various Cloud Threats*

B. Technical Issues:

- *Security*

Security can be defined as “how information can be locked safely”. The fact that the priceless enterprise information will dwell outside the firm firewall raises grave concerns.
Many high sensitive data can be exposed publicly if necessary measures are not taken. Hacking and different attacks to cloud structure would impact multiple clients even if merely one site is broken into. These risks can be impaired by using safety applications, encrypted data file scheme, data loss software, and purchasing security hardware to track out-of-the-way conduct across servers.

- *Distributed Responsibilities*

The main security issue is that the user must check before uploading the delicate data into the cloud storage. They must also take decent security measures such as using 32-bit encryption. This is a vital part because data can be secured if it is encrypted before saving it in the cloud store. Thus,

even if intrusion happens, there is a very minimum chance of the data getting stolen.
Encryption in the cloud is given in the diagram below.

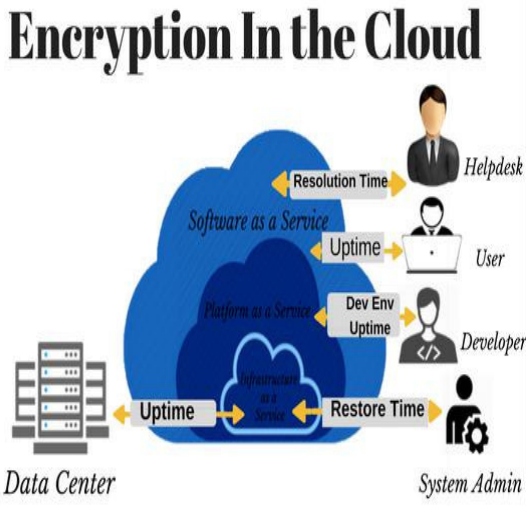


*Fig 4. Encryption in the cloud*

. .

- *Fault tolerance and failure recovery*

The data centers are merely responsible to process tremendous amount of data each day. Cloud services can face the problem of loss of data due to the failure of the system of the cloud. The shortage of power supply, low space or break down of the main system could lead to failure.

C. Challenges Faced In Cloud Computing

These are some of the challenges that are needed for security and their knowledge is necessary for mitigation purposes.

*Privileged User Access:*
Any client that accesses data outside the enterprise then the user has to take permission or buy membership for prevention of data leak.

*Data Location:*
The client shouldn't know where the data is stored or the place form where the data is being propagated (hosted).

*Availability:*
Data should be available everywhere even when the range of company is not available at that moment. This is called anywhere-anytime availability of software.

*Regulatory Compliance:*
The hosting providers should never allow external audits or allow installation of external new security certificates.

*Recovery:*
If under any condition the data is ruined by any disaster, man-made or natural, the providers should be able to deliver the backup data to the users on time.

*C. Security Risks in Cloud Computing*

Cloud Computing helps us to access data and information for particular organization. Hackers and Attackers have found out loopholes to gain access to these information.

IP Spoofing:

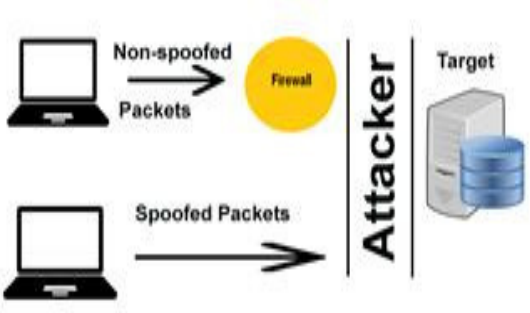


*Fig 5 Showing IP Spoofing attack by modifying packets*

IP Spoofing is known as analysis of the data that is being sent over the network. When data is sent over the network the attacker manipulates the data. The manipulation is done in a way that the IP address of the trusted system and then modifies the packet information and then sends it to the receiving system.

*DDOS attack:*

In this attack, DDOS the attacker spoofs the information and sends many requests of the data. The

server gets confused and doesn't understand what to do with all these request and finally ends up giving up authenticated data. The basic diagram of a DDOS attack is below:

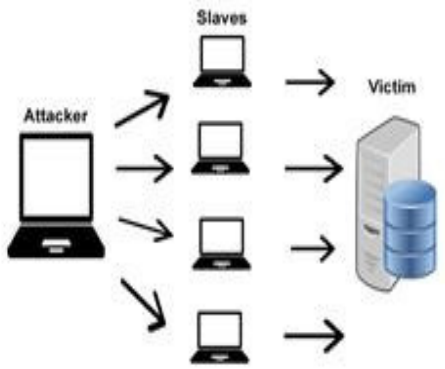


*Fig 6. Showing the multi-requests sent by the attacker*

*Insecure Interface:*

Interface is the model that helps the client to adhere to the cloud internal software. Management of data, identity management, monitor service and other functions that happen on the cloud are done through these interfaces. If interface is not secure, then data theft is very easy.

*Malicious Insider:*

The insiders such as the employees or any user can manipulate the data, such that they can even sell the information to other organizations. Any this causes severe data leaks in cloud computing.

*Data Loss or Leakage:*

There are two process taking place when data is being transmitted from host to client. First of all, data is being stored in a far of place and secondly, data transmission happens from one mode of execution to modes that are multiple in nature. Thus, if any modification happen in between, the loss or leakage of data occurs

*Malware attack on VM:*

Cloud Security can be compromised by the unwanted Vm-based virus or tool-kits that are used to cloak the information sent to the server by the user. Same process can happen when the data is being sent form the server to the client.

These viruses or malwares are also used to store the data such as registry information, system logs, and security program details. This flow charts shows us how these risks are interrelated:


*Fig 7. Showing the risks that cloud computing faces.*

But security & privacy issues caused by hackers and crackers and many security researchers have concluded that due to loss of control, invalid storage, access control and data boundary. The cloud computing is insecure and many preventive measures have been implemented over the time to reduce such risks.

## V. CONCLUSION

Cloud computing is the newest technology that is becoming very popular now-a-days. This is a developing technology due to its applications in various fields like testing & development, big data analytics, file storage etc. Cloud Computing and their services are new but many new organizations are implementing the cloud services but there is always a risk of data breaching. There are more chances for data breaching for the organizations that implements the cloud services rather than the other that don't. Malware injection is also a big problem in cloud

services due to this the attacker can easily steal the sensitive data of organization. Cloud companies offer real benefits to the companies seeking a competitive edge in today's economy.

The biggest and scariest concern about cloud computing is that privacy and security doesn't come in the package, because while companies are sharing data with each other, critical data is being exchanged, the chances of data leakage and data theft is an undeniable fact.

So every company should have a reliable security measures to implement the technology to protect the data of the client. While many clouds have firewalls and intrusion prevention, but they are not tailored to meet the clients' specific system.

## References


[1] Azura Che Soh, Mohd Khair Hassan and Li Hong Fey 2004. "Intelligent movement control for robots using fuzzy logic", Conference Artificial Intelligence in Engineering and Technology (ICAET-2004), Sabah, Malaysia.

[2] A. C. Nearchou, "Adaptive navigation of autonomous vehicles using evolutionary algorithms," Artificial Intelligence in Engineering, vol. 13, 1999, pp. 159-173.

[3] J. C. Latombe, Robot Motion Planning, Norwell, MA: Kluwer, 1991.

[4] Fuzzy Logic Reasoning to Control Mobile Robot on Pre-defined Strip Path.

[5] Satveer Kaur and Amanpreet Singh "The concept of Cloud Computing and Issues regarding its Privacy and Security" International Journal of Engineering Research & Technology (IJERT), Vol 1 Issue 3, May 2012.

[6] Farzad Sabahi "Cloud Computing Security threats and Responses", 2011 IEEE 3rd International Conference on Communication Software and Network (ICCSN), pp. 245-249, May 2011.

[7] Chen, D. and Zhao, H. (2012). Data Security and Privacy Protection Issues in Cloud Computing. International Conference on Computer Science and Electronics Engineering, 647-651. doi: 10.1109/ICCSEE.2012.193

[8] Hamlen, K., Kantarcioglu, M., Khan, L. and Thuraisingham, V. (2010). Security Issues for Cloud Computing. International Journal of Information Security and Privacy, 4(2), 39-51. doi: 10.4018/jisp.2010040103

[9] Kuyoro, S.O., Ibikunle, F. and Awodele, O. (2011). Cloud Computing Security Issues and Challenges. International Journal of Computer Networks, 3(5), 247-255.

[10] Aman Bakshi, Yogesh B. Dujodwala, "Securing cloud from DDoS Attacks using Intrusion Detection System in Virtual Machine," ICCSN '10 Proceeding of the 2010 Second International Conference on Communication Software and networks, pp. 260-264, 2010, IEEE Computer Society, USA, 2010. ISBN: 978-0-7695-3961-4.

[11] V. Krishna Reddy, B. Thirumal Rao, Dr. L.S.S. Reddy, P.Sai Kiran "Research Issues in Cloud Computing " Global Journal of Computer Science and Technology, Volume 11, Issue 11, July 2011.

[12] Lee, K. (2012). Security Threats in Cloud Computing Environments. International Journal of Security and Its Application, 6(4), 25-32.

[13] Agarwal, A. and Agarwal, A. (2011). The Security Risks Associated with Cloud Computing. International Journal of Computer Applications in Engineering Sciences, 1 (Special Issue on CNS), 257-259.

[14] Hashizume et al. (2013). An analysis of security issues for cloud computing. Journal of Internet Services and Applications, 4(5), 1-13.

[15] www.springer.com/engineering/mechanical+eng/journal/163