# Cloud Computing: Analyzing Security Issues & Need of Prevention against Vulnerabilities

**Laxmi Shankar Awasthi, Himanshu Pathak, Parth Singhal**

***Abstract*—Cloud computing, is fast growing Technology having its originations from Distributed computing technology. Cloud computing is a collaboration of different computing technologies and it has many advantages in the field of data storage, high expansibility, high reliability, virtualization, and low price service. Cloud computing has massive effects how we store and access our personal and business data. It is a matter of great concern to secure personal information and data from attacks like DDos, MIMA and data theft. And therefore it is extremely important to understand the existing security issues and risks in cloud computing. This paper analyses the above mentioned existing security issues and protection against threats in cloud computing. This paper is to quantify the need of security between networks in cloud computing, therefore minimizes the vulnerabilities.***

***Index Terms*— DDos, man in the middle attack, packet sniffing.***

## I. INTRODUCTION

As cloud computing means the use of public networks and subsequently putting the transmitting data exposed to the world, like any other network cloud computing is also vulnerable to the cyber-attacks in any form. The contemporary Cloud networks suffers the security loop holes, which act as the deterrent to the cloud based services. We have to find out ways to make the cloud services secure and more user friendly. Here we will analyze such issues. This paper is further divided into 4 section:

1. Introduction
2. Cloud Privacy
3. Network Threats
4. Security Measures against Network Threats

## II. CLOUD PRIVACY

Privacy is another sensitive issue with regards to cloud computing because customer's data and business logic are kept among distrusted cloud servers, which are maintained and owned by the cloud service providers.

Therefore, there are potential risks that the confidential data (e.g., financial data, health record) or personal information (e.g., phone No., address etc.) may be disclosed to public or business competitors. Privacy has been a most important and priority one issue on the Internet. To keep private data safe and secure, confidentiality becomes unavoidable, and integrity ensures that data and or computation is not corrupted and accurate, which somehow have positive effects on privacy. Accountability, on the other hand, may undermine privacy because of the fact that the methods of attaining the two attributes usually contradict.

- The secure transmission of data and sensitive information to the cloud server,
- The dispatch of data from the cloud server to clients' computers
- The storage of clients' sensitive data in remote cloud servers which are owned by the cloud service providers.

## III. NETWORK THREATS

3.1 DOS Attack: DoS (Denial of Service or Distributed denial-of-attack) DoS attacks pose an interesting trade-off to the services hosted on cloud, independently of the facility protection guaranteed by your cloud provider. Uses of Botnets are increased, this makes it much more difficult to resolve this sort of attack.

3.2 Malware-based attacks such as worms, viruses, and DoS exploit system vulnerabilities and give intruders unauthorized access to critical information. Risky cloud platforms can cause businesses to lose billions of dollars and might disrupt public services [1] [2].

3.3 Man in The Middle Attack: This attack is carried out when an attacker places himself between the communication two users. At any given time attackers can hack the information's path, there is the possibility that they can intercept, look into and/or modify data transmission.

3.4 Packet Sniffing: This will captures network traffic at the Ethernet frame level. Then, this data can be analyzed and sensitive information can be retrieved. Such a network attack starts with the easily online available tool such as Wireshark. This toll allows us to capture and examine data that is flowing across our network. And any unencrypted data flowing through the network is vulnerable, many types of traffic on our network are passed as unencrypted data — even passwords and other sensitive data may also be transmitted in the same unencrypted manner [3].

3.5 XML Signature Element Wrapping (Wrapper Attack): A Wrapping attack is done by duplication of the user account and password in the log-in phase so that the SOAP (Simple Object Access Protocol) messages that are exchanged during the setup phase between the Web browser and server are affected by the hackers.

3.6 Cloud Malware Injection Attack: This is one of the most frequent attacks. The attack is done by Compromised FTP passwords, virus can sniff passwords and then send it back to the

Manuscript received on March, 2014.

**Dr. Laxmi Shankar Awasthi**, Computer Science, Lucknow Public College of Professional Studies, Lucknow, India.
**Himanshu Pathak**, AIIT, Amity University, Lucknow, India.
**Parth Singhal**, St. Francis College, Lucknow, India.

hacker. The hacker then uses same sniffed passwords i.e., our FTP password to access our website and can easily harm/infect our website.

Following data in Fig. 1 & Fig. 2 [4]is collected from Internet showing the top sectors by Number of data breaches and Number of identity exposed. Showing that Security is an eminent threat to the cloud base network services.

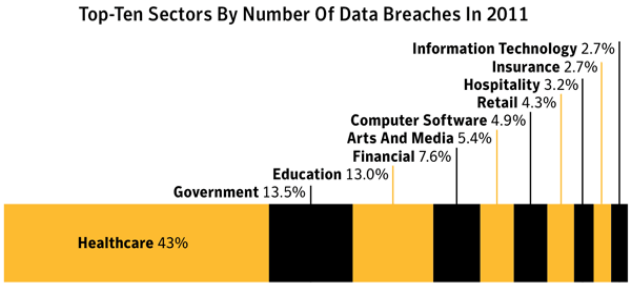


Fig. -1: Graph of Data Breaches

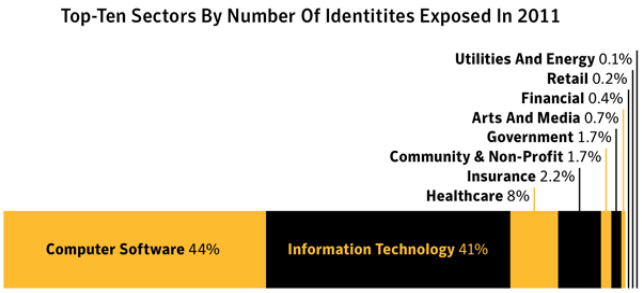


**Fig. -2: Graph of Identity Exposed after Data Breaches**

## IV. SECURITY MEASURES AGAINST NETWORK THREAT

Security for any system is an indispensable requirement for any system and cloud computing is no exception. There are various ways to protect the Cloud architecture and protect the critical data and information. Some of the most promising and widely used techniques are listed and discussed here.

### 4.1 Security-Aware Cloud Architecture

This architecture helps insulate network attacks by establishing trusted operational zones for various cloud applications. Security standards demands that CSPs will protect all data-center servers, data repositories and data storages. This architecture protects VM monitors (or hypervisors) from software-based attacks and safeguards data and information from theft, corruption, and natural disasters. It provides strong authentication and authorized access to sensitive data and on-demand services. There are several design objectives to be met for a trusted and secure cloud when creating this architecture.

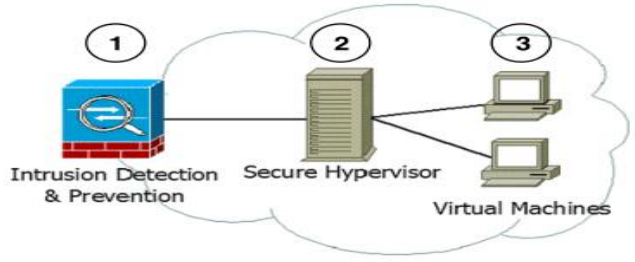


**Fig. -3: Cloud Security techniques by Intrusion detection & prevention, Secure Hypervisor and Virtual Machines [5].**

## V. CONCLUSION

Cloud computing has bright prospects and future possibilities, but the security threats in cloud computing approaches are also as magnanimous in its efficiency and advantages. Cloud computing is a lucrative opportunity and hence will be highly sought by both, the businesses and the attackers – either parties can have their own purposes and ends to meet from cloud computing **[6]**. This paper will also evaluate how data can be protected against vulnerabilities. The various possibilities and plausibility of cloud computing cannot be cornered solely for the security reason alone – the ongoing search for reliable and robust, consistent and integrated security models for cloud computing is the only solution to fully harness the power of this idea of Cloud computing.

## REFERENCES

1. Survey of network-based defence mechanisms countering the DoS and DDoS problems.
2. Trusted cloud computing with secure resources and data coloring 1080-7801/10/$26 2010 by IEEE.
3. http://www.dummies.com/how-to/content/common-network-attack-strategies-packet-sniffing.html
4. http://www.symantec.com/threatreport/topic.jsp?id=threat_activity_trends&aid=data_breaches_that_could_lead [9]. Above the Clouds: A Berkeley View of Cloud Computing"
5. Denz and Taylor Journal of Cloud Computing: Advances, Systems and Applications 2013, 2:17http://www.journalofcloudcomputing.com/content/2/1/17
6. CLOUD COMPUTING AND SECURITY ISSUES IN THE CLOUD International Journal of Network Security & Its Applications (IJNSA), Vol.6, No.1, January 2014

## AUTHOR PROFILE

**Dr. Laxmi Shankar Awasthi** is working as H.O.D in Lucknow Public College of Professional Studies in Computer Department. He has published research papers in many various national and International Journals.

**Himanshu Pathak** is pursuing M.C.A from Amity University Lucknow campus in Amity Institute of Information Technology. He has published research papers in various International Journals.

**Parth Singhal** is a student of St. Francis College Lucknow .He will strive to write more research papers on Cloud Computing.