CLOUD COMPUTING AND CYBER CRIMES

LL.M Student, Bharati Vidyapeeth
(Deemed to be University), New Law
College, Pune

Mr.Manohar Gawade

Dr.Sagar Shelke

Assistant Professor, Bharati Vidyapeeth (Deemed to be University), New Law College, Pune advsagarshelke@gmail.com

Abstract:

Cloud computing is a new way of delivering computing services. Cloud network of 'Cloud Computing' is formed in the same manner by collection of networks. It is an internet-based most powerful architecture of computation that is used to store, manage, and process data. This paper discusses the concept of Cloud Computing, types of Cloud Computing. Concept of Cyber Crimes regarding computing is also discussed.

Keyword: Cloud Computing, Scalability, Cyber-theft, Hybrid Clouds, Public Clouds

INTRODUTION: Word cloud in 'cloud computing' denotes networks. It symbolizes idea of the real clouds which formed from water molecules; cloud network of 'Cloud Computing' is formed in the same manner by collection of networks. It is an internet-based most powerful architecture of computation that is used to store, manage, and process data. Data managing, storing, and processing are different and more difficult in physical form. Physical form also requires a lot of resources and money. This problem is solved by cloud computing as it helps local computers to reduce load. In cloud server load is managed by the network which forms the cloud while running applications. The Trend in the present time is adopting a multi-cloud approach where businesses use more than one public cloud service. Cloud computing is useful and efficient because without cloud computing even for maintaining a simple website, one had to buy a stack of servers to host their website on. It was very expensive and requires keeping an eye on problems related to troubleshooting and idleness of servers. To avoid troubleshooting (without cloud computing /server), it was necessary to focus on peak traffic and buy more servers to avoid troubleshooting problems. The Need of buying a stack of servers ended with the coming of 'Cloud Computing' as it puts all data on the cloud. It also set free businesses from minding troubleshooting and idleness of server issues as it transferred onus of managing troubleshooting issues to cloud service providers which is less expensive in comparison to managing data in physical form. Parameters of economic scale usually enjoyed by cloud service providers are very significant as to their delivery of equivalent services to a good range of consumers¹. Earlier it was very difficult as along with managing a business, you had to keep an eye on your website server, appoint a team to look into troubleshooting problems and buy more

¹ Ranger, S. article on cloud computing.



servers to avoid troubleshooting issues. All of these problems were resolved by 'cloud computing'. The server was also ideal earlier but traffic was varying so it required monitoring and maintenance of the server. It is also resolved by cloud computing as now this responsibility shifted on cloud server provider. A very positive thing which helped businesses economically as well as technologically was 'Scalability'. 'Scalability' increases and decreases your server capacity according to the need of traffic so the server doesn't face troubleshooting issues. It is cheap as well.

TYPES OF CLOUDS: Classification of clouds in cloud computing most appropriately can be made on the basis of a cloud location. Clouds can be classified into following three broad categories:

- 1. Public Clouds
- 2. Private Clouds
- 3. Hybrid Clouds

(i). Public Clouds: Orthodox approach of implementing cloud computing is adopting Public clouds. A public cloud is accessible through a web browser². It is implemented by using offpremises shared data center infrastructure of hardware and software which are usually owned and managed by cloud providers. It is more popular and useful because it allows users to experience new things without investing in new hardware or software. It is very easy to use and access. Users can set up accounts simply by filling a web form and access data anywhere. Some Public Clouds provide access without charging anything from its users; others charge a very nominal amount (a much lesser amount from hard drives and software). While accessing Public Clouds you don't need to purchase hardware or software as it charges only for the service which you're using. Subscriber doesn't need to worry about maintenance as t is done by the service provider herself. And in case if there is any failure on the server a vast number of networks are available to protect the server. Most prominent public clouds for example are Amazon web services, Sales force's CRM system and Microsoft Azure among many others. Public clouds are mostly deployed to provide email services, storage, analyzing, preparing various in organization and out organization applications, and data storage. A Public Cloud may participate in Hybrid cloud also.

(ii). **Private Cloud:** Private cloud is exclusively used by one company/business. In a private cloud services and hardware are used only for the work of an organization and managed on a private network deployed to organizational work. It makes easy for an organization to customize cloud settings to meet their IT requirements. Data centers used to launch a private cloud can be

² Cloud Computing – Types Of Cloud – Web Hosting Blog By ESDS



on-premises as well as off-premises. It gives more flexibility (as an organization can customize its cloud settings to meet specific goals), improved security (as resources are not shared outside the organization), and high scalability³. It can also participate in hybrid cloud and mostly use by giant organizations, governmental agencies, survey companies, financial institutions, etc.

(iii). Hybrid Cloud: Both Public Cloud and Private Cloud can be part of hybrid cloud as it is a combination of clouds. It can be a private cloud, public cloud, private clouds, public clouds, and public and private clouds⁴. It is not merely a combination of multiple clouds but to satisfy its resources must be shared among the clouds. It provides the freedom to data to move among private and public clouds for greater flexibility. By adopting hybrid clouds a business can manage private infrastructure for assets which are of utmost priority and provides some more advanced resources in the public cloud. Businesses can access that public cloud when it seems to them necessary. An example of a hybrid cloud is cloud bursting.

CLOUD COMPUTING AND CYBER CRIMES: With the development of technology, patterns of crime have also changed. It is true about Cloud Computing also. Above, we analyzed how Cloud Computing is creating an important impact on the life of people in general and businesses in particular⁵. But it also contributed to the increase of omnipresent cybercrime threat⁶. Cloud Computing gives flexibility which is misused by cybercriminals. They use the cloud as a business platform either from the dark web or by accessing someone else's cloud server⁷. Ability to send messages, share files and plans make them stronger as while they share files through cloud storage, it is protected by the cloud server. Many times they have access to a large number of cloud accounts which makes a large number of users vulnerable to the risk of cyber threats and other crimes. Cybercriminals are in advantage as mostly they even don't pay for cloud services. Either cloud services are obtained by them through maladies methods as phishing, cyber attack, by using someone else card (which is also obtained through fraudulent methods) or by hijacking a server. Cyber-theft is mostly used by cybercriminals to purchase or rent services and by using the same server they attack on other users databases, computing activities and storage which leads to crimes. Services which cloud platforms provides are cheap, easily accessible and available beyond any boarder boundaries which also make cybercrimes a great threat as we don't have any common global legislation ealing with the subject in spite of having knowledge that a cybercrime can engage more than a country's citizens. Cloud storage make it easy to access and stole data related to users. Cybercriminals accesses useful data including personal details about the users, their contact lists, work, home address, etc by using

³ Cloud Computing – Types Of Cloud – Web Hosting Blog By ESDS

⁴ Different Types Of Cloud Computing Service Models.

⁵ Cyber Crime And Cloud Computing: Security Perspectives.

⁶ The 6 Major Cyber Security Risks To Cloud Computing.

⁷ Cyber Crime And Cloud Computing.



AIJRRLSJM VOLUME 6, ISSUE 6 (2021, JUNE) (ISSN-2455-6602)ONLINE Anveshana's International Journal of Research in Regional Studies, Law, Social Sciences, Journalism and Management Practices

cloud storage. Blackmailing and cyber-bullying are also new forms of cyber-crimes which are increased by the use of cloud computing as cybercriminals now have more data and information about you to bully! At the same times there are many government regulations and cloud company policies everywhere in the world which makes businesses to be more careful about cybercrimes or they may fine heavily if any consumer suffers because f them, in case they failed to prove that it was result of unauthorized use. The most important example in this regard is GDPR laws of European Union. It exposes important corporate data, personal data, outside the organization's control on an external application provider's servers or in their database⁸. If one is planning to steal files, cloud server helps them in doing this as after uploading file on server, you may have access to an individual/organization's important data such as file sizes and content.

As monitoring is critical in the cloud, we do need to have information related to usage and potential attacks. Cloud Computing provides easy, cheap, and flexible services to businesses as well as individuals without worrying them about management. It does limit our capacity to see what's going on with security management. How and where cloud server is storing or data? Data accessing became very easy through cloud computing as it allow its user to access that data from anywhere in the world, whether they are at their workplace, home or simply walking on roadside. These facilities are available to cybercriminals also.

Conclusion:

Cloud services also are vulnerable to disruptive cyber attacks, because it provides more ways to a cybercriminals to watch the data activities on shared clouds. The best two methods which businesses can opt to reduce this risk are that firstly they ensure that under no circumstances there should be password sharing among the users and they also need to ensure proper implementation of multifactor authentication. Efforts should be taken by businesses to prevent loss of account details and taking measures to ensure safety of cloud applications from the unwanted risk of phishing and other similar violations. In most of the case they even don't pay for cloud services from their own pocket as often they use someone else card which itself is a result of cyber fraud. Criminals do this to mitigate the risk of getting caught. In no way, restrictions can be put on cybercriminal from using cloud services. If anyhow you get success in doing this, they can attack you from a hijacked server. So vulnerability is increased by Cloud Computing.

Reference:

⁸ Bartholomae, F., 2017. Cybercrime and Cloud Computing.



AIJRRLSJM

VOLUME 6, ISSUE 6 (2021, JUNE)

(ISSN-2455-6602)ONLINE

Anveshana's International Journal of Research in Regional Studies, Law, Social Sciences, Journalism and Management Practices

- The Main Types of Cloud Computing available at <u>https://www.esds.co.in/blog/the-main-types-of-</u> <u>cloud-computing/</u>
- What is cloud computing? Everything you need to know about the cloud explained, <u>https://www.zdnet.com/article/what-is-cloud-computing-everything-you-need-to-know-about-the-cloud/</u>
- Different Types of Cloud Computing Service Models, <u>https://www.bluepiit.com/blog/different-types-of-cloud-computing-service-models/</u>
- Cyber crime and cloud computing: Security perspectives, <u>https://www.huntsmansecurity.com/blog/cyber-crime-and-cloud-security/</u>
- Top 6 Security Threats in Cloud Computing and How to Mitigate Them, https://blog.netwrix.com/2020/09/08/cloud-security-threats/
- Cyber crime and cloud computing: Security perspectives, <u>https://www.huntsmansecurity.com/blog/cyber-crime-and-cloud-security/</u>