International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 04 Issue: 07 | July -2020 ISSN: 2582-3930

An Analysis of cyber threat and their Impact

Priya Ghosh
ARKA JAIN University, Jamshedpur-831014, India

Abstract *– Cloud computing is an domain and security of data must be protected over the network .Cloud computing is used by many of the organization for storing huge amount of data on the cloud. Therefore there is need to secure data which may be in form of text,audio,video,etc,.as the continuous amalgamation of technology in everyday facets of life havealso led to cyber crimes and cyber security solution is of utmost is of utmost importance in cloud platform.*

Keyword: - Cloud computing data protection, encryption, digital signature, security issues.

I. INTRODUCTION

Cloud Computing (Cloud) provides network which access to resourses which are shared and can be configured.It is basically based on shared services and infrastructure. It emerged from evolution and adoption of many prevalent technologies. It inherits many of its characteristics from client-server model, grid computing, mainframe computing, utility computing, and peer-to-peer architecture. Virtualization is the key technique behind Cloud Computing. It uses Services oriented Architecture(SOA) which helps clients to transform the problems of requirement into services and hence they derive benefit of the solution provided by Cloud. Key advantages of cloud include agility, reduced costs, device independence, location independence, easy maintenance, high performance, extremely scalable and flexible, increase productivity, privacy, and security. Cloud computing paradigm is considered as eminently useful and most feasible computing model for the distribution of data, information and resources in a flexible manner. This new computing paradigm accoutres various IT services like storage, computing, security, identity, machine learning and analytics with the help of internet. The nucleus of the research paper is on the assimilation to theoretical concepts with practical implementations of security and privacy strategies that create a secure environment for the service provider and user. This secure environment is beneficial to enhance the level of trust in the end user regarding the cloud services or applications and contrarily for cloud service providers to ensure better and secure services to the users. To achieve sustainable growth and specific goals, cloud service providers have performed the following operations. Cloud computing is the on demand delivery of compute power, database storage, applications, and other IT resources through a cloud services platform via the internet with pay-as-you-go pricing.

Whether you are running applications that share photos to millions of mobile users or you're supporting the critical operations of your business, a cloud services platform provides rapid access to flexible and low cost IT resources. With cloud computing, you don't need to make large upfront investments in hardware and spend a lot of time on the heavy lifting of managing that hardware. Instead, you can provision exactly the right type and size of computing resources you need to power your newest bright idea or operate your IT department. You can access as many resources as you need, almost instantly, and only pay for what you use.

Cloud computing provides a simple way to access servers, storage, databases and a broad set of application services over the Internet. A Cloud services platform such as Amazon Web Services owns and maintains the network-connected hardware required for these application services, while you provision and use what you need via a web application. Cloud computing security or, more simply, cloud security refers to a broad set of policies, technologies, applications, and controls utilized to protect virtualized IP, data, applications, services, and the associated infrastructure of cloud computing. It is a sub-domain of computer security, network security, and, more broadly, information security.

A. Secure Connection -Ensuring the integrity and privacy of user data is of ultimate importance ,as the data can be subject of surveillance and attack. So, custom hardware integration of operating system with hardware.

B. Cyber security and Cyber crime- Cyber security and cyber crime cannot be separated in an interconnected environment. Cyber security plays an important role in ongoing development of information technology. Cyber crime is an integral component of national security and critical for aspects of protection of data and infrastructure.

C. Advantages and risks- The growth of the information society is accompanies by some serious threats. Online fraud and hacking attacks are just some of the computer related crimes committed on the day to day basis, hence industrial IT infrastructure has a lots of opportunity to evolve and progress with the introduction of components

such as interface controllers that provide effective defence in the response to cyber attack.

D. Broad Network Access: - Services are accessible over the network, which are retrieved through some standardized mechanism, which promotes the usage of heterogeneous platforms (workstations tablets, laptops, mobile phones).

E. Resource Pooling: - The providers computing resources are pooled to serve multiple consumers and usually consumers are not aware of the accurate location of the resources provided except at the abstraction level like state, country or data centre.

F. Rapid Elasticity: - Services can be effortlessly released which appears as unlimited but can be sealed in quantity anytime.

G. Measured Services:- Cloud system are so designed in a way that they can monitor the resources usage; for example, processing, bandwidth and active user accounts, storage to deliver transparency to provider transparency to the both the provider and consumer. At some level of abstraction, they can optimize the resource usage by keeping a check through metering capability

Cloud Service Models:-

- Infrastructure as a Service (IaaS)
- Software as a Service (SaaS)
- Platform as a Service (PaaS)

Infrastructure as a Service (IaaS): Iaas is all about providing the virtual machine, operating system or networks to the end users. Some other computing resources are also provides assistance in IaaS, customer or client can run discretionary operating system on virtual machine software which he is running but he loses his control on the infrastructure which is providing him all these services.

Software as a Service (SaaS): In this kind of scenario, user is only using the applications which are being provided by the vendor and those applications run on the cloud services. Same application is accessible by many other clients as well through some common mechanism, for example by using web browser, or email. Again, the clients or users have no control over the application or underlying infrastructures, network server or operating system upon which these applications run.

Platform as a Service (PaaS): In PaaS, the client is able to create their own desired application by using some programming language, linked libraries. The vendor supports these languages or libraries. After creating the user desired application , it is established on the server provided by the vendor. User also has the access and power to configure its application.

II. LITERATURE REVIEW

S.no	Title	Author	Findings	Remarks
1	Failure Management for Reliable Cloud Computing: A Taxonomy, Model and Future Directions.	Sukhpal Singh and Inderveer Chana etal 2010	Electronic Health Record(EHR) software runs on the web instead of the computer meaning no hardware or software installation Most cloud based EHR's encrypt the data so hackers cant use the data even if they gain access to it, since the data is stored off site with bank level security Since cloud based servers are maintained off site there are instant reduction in IT cost associated with maintainig the EHR database. The real time data is accessible from multiple location	Failure of cloud computing as tested by the author are software failure which includes complex design,planned/unplanned Reboot, cyber attacks.Hardware failure includes complex circuit design, system breakdown,power outage and other reasons leaving human errors,heat issue etc.
2.	Attribute based Encryption for secure access to cloud based EHR System	Maithilee joshi etal 2008	Its Digital Policy Management where machine specific languages can be used in system in an automated one semi-automated	Patients data can be compromised if mixed with other clients Not a good option for rural with limited internet connectivity

			manner. Audit Management is for monitoring of behaviour services and adequate analysis and reporting of current and past situation. Identify Management providing service access across multiple external application through single sign on.	For long time usage , it may prove to be more expensive A medical practice may lose data if the vendor closes business operation
3.	Security Management areas in the inter cloud	Michael Kretzschmar etal 2011	Back up data locally Avoid sharing sensitive information Use cloud services that encrypt data	Few practical steps or practises fir a secure cloud experience (could have been included by Author Back up data locally Avoid sharing sensitive information Use cloud services that encrypt data Test he security measures in public Make password storage using special characters
4.	Addressing Cloud Computing	Jaypee University Anoopshahr,A	Data Location: When use cloud computing services,	The responsibility of securing the network is shared
	Security Issues and its Solutions	noopshahr,Uttar Pradesh ,India 2016.	customers don't know where the data are placed on the servers, even don't know which country these servers are placedin When these countries need to investigate these data, due to the different law, providers may be forced to submit data and be unable to guarantee the security of user data. Data backup: To the important and confidential data, if cloud services dose not backup the data, when data lost by the server problems, or users accidentally delete data, important data can't be restored.	between the cloud service provider (CSP) and the enterprise. Depending on which server model an enterprise uses, the enterprise may have little to almost no control over the cloud security. Infrastructure-as-a-Service (IaaS) allows the enterprise to have the most control as the CSP only provides the infrastructure. It falls under the enterprise's jurisdiction to build the remainder of the stack and maintain its security.
5.	Security Issues and their Solution in Cloud Computing	Prince Jain teal. 2017	Whenever a discussion about cloud security is taken place there will be very much to do for it. The cloud service provider for cloud makes sure that the customer does not face any	Encryption, authentication and authorization are important components of any security infrastructure, the cloud being no exception. However, since the

			problem such as loss of data or data theft. There is also a possibility where a malicious user can penetrate the cloud by impersonating a legitimate user, there by infecting the entire cloud. This leads to affects many customers who are sharing the infected cloud.There are four types of issues raise while discussing security of a cloud. 1. Data Issues 2. Privacy issues 3. Infected Application 4. Security issues	cloud service provider applies and enforces these security measures, clients feel insecure not knowing which other client also has the same measures in place. One solution is to use different encryption keys for each individual client; however it is wholly dependent on the service provider.

III. RELATED WORK

Ayush Agarwal et al. (2016) highlight the emergence of cloud computing along with its security concerns like data loss, data breaches, insecure API's, account hijacking, denial of service [4]. Prachi Garg et al. (2017) have worked on different cloud security aspects like basic security which includes Cross site scripting attacks, Sql injection attacks, Man in the middle attacks [5]. Pradeep Kumar Sharma et al. (2017) security concerns for cloud like cost model charge model [6], service level agreements and issue of migration should be dealt. Naseer Amara et al. (2017) highlighted the security threats, architectural principles and cloud security attacks with their techniques that can minimize the effects of malicious attacks (mitigation techniques) [7]. Sh. Ajoudanian et al, (2012) said that following four parameters were the most crucial. (a) Data Confidentiality, used to avoid leakage of information to any unauthorized individual or system [8].

IV. METHODOLOGY

The mentioned steps draws an easy and informative strategy for collecting information. However, the steps can be rearraged depending on the familiarity with the library.

Step 1: Identify and Develop Your Topic- State your topic idea as a question. For example, if you are interested in finding out about use of alcoholic beverages by college students, you might pose the question, "What effect does use of alcoholic beverages have on the health of college students?" Identify the main concepts or keywords in your question. In this case they are alcoholic beverages, health, and college students. Test the main concepts or keywords in your topic by looking them up in the appropriate background sources or by using them as search terms in the Coastal Bend College Library catalog and in online databases such as Literati or CINAHL. If you are finding too much information and too many sources, narrow your topic by using the AND operator: beer AND health AND college students, for example.

Step 2: Find Background Information- Once you have identified the main topic and keywords for your research, find one or more sources of background information to read. These sources will help you understand the broader context of your research and tell you in general terms what is known about your topic. The most common background sources are books and review articles.

Step 3: Use Catalogs to Find Books and Media- Use keyword searching for a narrow or complex search topic. Use subject searching for a broad subject. Print or write down the citation (author, title, etc.) and the location information (call number and library). Note the circulation status. When you pull the book from the shelf, scan the bibliography for additional sources. Watch for book-length bibliographies and annual reviews on your subject; they list citations to hundreds of books and articles in one subject area.

Step 4: Use Databases to Find Journal Articles- Use online databases to find citations to articles. Choose the database that best suits your particular topic; for example, search Literature Online for literary criticism topics, CINAHL for nursing topics, and Academic Search Complete for psychology topics. These databases and more are located on the library's website under Online Resources. If the full text is not linked in the database you are using, write down the citation from the database and search for the title of the journal in the Library Catalog. The catalog lists the print and electronic versions of journals.

Step 5: Find Internet Resources- Use search engines and subject directories to locate materials on the Web. As information on the Internet varies in its reliability, it is suggested that you use directories such as the Library's Delicious Links [organized by subject] or Google Scholar, which contains links to the library's resources when available.

Step 6: Evaluate What You Find- You may be asked to utilize peer reviewed articles in your assignments. Many journals are peer reviewed, meaning that submitted articles are scrutinized by one or more experts in the field before they are published in

the journal. Not all items in a peer reviewed journal have gone through this process, however. These items may include letters, editorials, news, and book reviews. Generally, only the primary articles, such as studies or review articles are peer reviewed.

V. CONCLUSION AND FUTURE SCOPE

In recent times as there has been an exponential increase in cyber crime cases like inaccurate use of personal data, unauthorized disclousure, unlawfull collection of information etc the risk of cyber crime are very real to be ignored. Every individual, licensor, franchisor, bussines owner should conduct professional analysis of their cyber security and cyber risk and plan to minimalize the liability and operate in a secure environment.

VI. REFERENCES

[1] Luo, J. Z., Jin J., Song A., Dong F.,"Cloud computing: architecture and key technologies", Journal of China Institute
of Communications 32, No. 7, pp. 3-21, 2011.

[2] Chou T.,"Security threats on cloud computing vulnerabilities",
International Journal of Computer Science & Information
Technology 5, No. 3, pp. 79, 2013.

[3] Gong C., Liu J., Zhang Q., Chen H., Gong, Z.,"The characteristics of cloud computing", In Parallel Processing
Workshops (ICPPW), 2010 39th International Conference

[4] H. Erdogmus. Cloud computing: Does Nirvana hide behind the Nebula? IEEE Software, 26(2):4–6, 2009.

[5] B. C. Kaufman and R. Venkatapathy, "Windows Azure TM Security Overview."

[6]J. Srinivas, K. Reddy, and A. Qyser, "Cloud Computing Basics," *Build. Infrastruct. Cloud Secur.*, vol. 1, no. September 2011, pp. 3–22, 2014.

[7] M. A. Vouk, "Cloud computing - Issues, research and implementations," *Proc. Int. Conf. Inf. Technol. Interfaces, ITI*, pp. 31–40, 2008.

[8] P. S. Wooley, "Identifying Cloud Computing Security Risks," *Contin. Educ.*, vol. 1277, no. February, 2011.

[9] A. Alharthi, F. Yahya, R. J. Walters, and G. B. Wills, "An Overview of Cloud Services Adoption Challenges in Higher Education Institutions," 2015.

[10]Abbadi, I.M. and Martin, A. (2011). Trust in the Cloud. Information Security Technical Report, 16, 108-114. doi:10.1016/j.istr.2011.08.006

[11] 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.

[12] Arshad, J, Townsend, P. and Xu, J. (2013).A novel intrusion severity analysis approach for Clouds. Future Generation Computer Systems, 29, 416–428. doi:10.1016/j.future.2011.08.009

[13] Atayero, A.A. and Feyisetan, O. (2011). Security Issues in Cloud Computing: The Potentials of Homomorphic Encryption. Journal of Emerging Trends in Computing and Information Sciences, 2(10), 546-552.

[14] Bisong, A. and Rahman, S.S.M. (2011). An Overview of the Security Concerns in Enterprise Cloud Computing. International Journal of Network Security & Its Applications, 3(1), 30-45.