International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249 – 8958 (Online), Volume-9 Issue-5, June 2020

Security Threats to Cloud Services

Kapil Singh, Sanjay Verma, Md Sharib, Nitasha Soni, Krishan Kumar

Abstract: ***This research paper looks into the world of how-to of cloud services and the ways through which it is threatened by various elements that regularly disrupt the functioning of these services. We will see how different models are being implemented across different fields. These various models are adopted by different users and organizations according to their needs. As there is almost no service with its specific problems, we delve into the discussion about various threats that loom over this expanded service step by step. These problems may be related to networking or authentication problems or security breach. Then we will look into how these problems are overcome by cloud service experts.***

Keywords: cloud services, cloud models, data privacy, security, servers

I. INTRODUCTION

Cloud services have crept in our daily technological scenario and have rapidly become a key component of our life. From messaging apps to mailing services, cloud has become an indispensable feature of technology. Millions of users are actively using cloud services for variety of reasons and many others are planning to join the bandwagon. But this brings with itself both an opportunity and challenge. Opportunity for the service providers in the sense that it will help in revenue growth and in the expansion of the companies. It will also help to deliver the services to wider population. More and more people will be able to take advantage of advancements made by cloud technology. Now let us look at the challenges. First and fore-most challenge would be to set up and install the hardware and software resources for the implementation of cloud services. Next challenge would be to keep the services running virtually for 24x7 as they would be used around the globe by users. So the servers hosting data must be readily available. Lastly, it will be severely important for service providers to secure their services from a ton of malicious software, hackers, unauthorized access etc. So to securely provide many users around the globe the fruits of cloud services, there must be solutions to fix the aforementioned problems and many more. But before looking into problems and their solutions, let us take a peek into cloud services.

II. WHAT ARE CLOUD SERVICES?

Cloud services may be referred to as 'the backbone' of current Internet technology. Most of the real-time data we access and share online is hosted by powerful cloud servers. These servers are based on various architectures that are very powerful and can handle hundreds of thousands of client requests. Thus their architectures are primarily important for their performances. [1]

Why do we need Cloud Service?

We need cloud services to achieve below listed goals. [3]

- Flexibility
- For working online from anywhere without worrying about file update
- Automatic updates to various software
- Storage of important documents in an organization or for general public
- For emergency backups in case of data losses

III. CLOUD SERVICE MODELS:

Cloud services are implemented via two kinds of models:

1. Deployment
2. Delivery
3.

Deployment Model Types:

Three major types of cloud deployment models are as follows:

1. **Private Cloud –** It is basically done in in a contractually manner with organizations to provide them with an in-house cloud network. These are highly secured networks with optimal data transfer speeds and servers are very scalable. The challenges in this cloud network include management skills and steep costs of implementation. [2]

2. **Public Cloud –** This cloud model is implemented over Internet and used by websites working in public domains. These websites are powered by huge cloud services providers. It is based pay-per-use. The main challenge in this service is that the security threats are increased drastically due to the more number of connections. [2]

3. **Hybrid Cloud –** It is the combination of private and public cloud systems. Here, a private cloud is linked to external cloud services. It helps in centralizing the security and offloading other operations. The main challenge here is the complexity of the networking. Any glitch or misstep will lead to the exposure of the service. [2]

All these above discussed, the following models are briefly explained in Fig.1

Revised Manuscript Received on May 27, 2020.
* Correspondence Author
Kapil Singh*, Manav Rachna International Institute of Research and Studies, Faridabad, Haryana kapilsinghks7@gmail.com
Sanjay Verma, Manav Rachna International Institute of Research and Studies, Faridabad, Haryana sv83850@gmail.com
Md Sharib, Manav Rachna International Institute of Research and Studies, Faridabad, Haryana sharibkhan222@gmail.com
Nitasha Soni, Manav Rachna International Institute of Research and Studies, Faridabad, Haryana nitasha.fet@mriu.edu.in
Krishan Kumar, Manav Rachna International Institute of Research and Studies, Faridabad, Haryana krishan.fet@mriu.edu.in

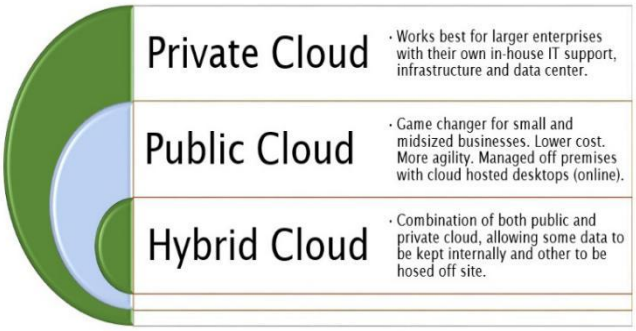

Fig-1: Three Basic Cloud Deployment Models

Delivery Models Types:

The three types of delivery models are as follows:

1. **Infrastructure as a Service (IaaS) –** It is delivery model where clients are provided with dedicated resources for a fees. Here, clients are provided with a suitable OS where they can run their software. Mainly the user are network architects. [2]
2. **Platform as a Service (PaaS) –** Here alongside the OS, development tools are also provided to the clients where they get databases and application administration. It is useful for people who are not familiar with technicalities of under-the-hood processes. Cloud service providers are more in work because they supply more resources to clients. Like IaaS, PaaS is also pay-per-use model. [2]
3. **Software as a Service (SaaS) –** It is most popular model with clients who just want complete application best suited to their needs be hosted online. All the development, networking, licensing etc. is done by cloud provider. It is suitable for end-users who just want to use the features rather than to develop and maintain them. [2]

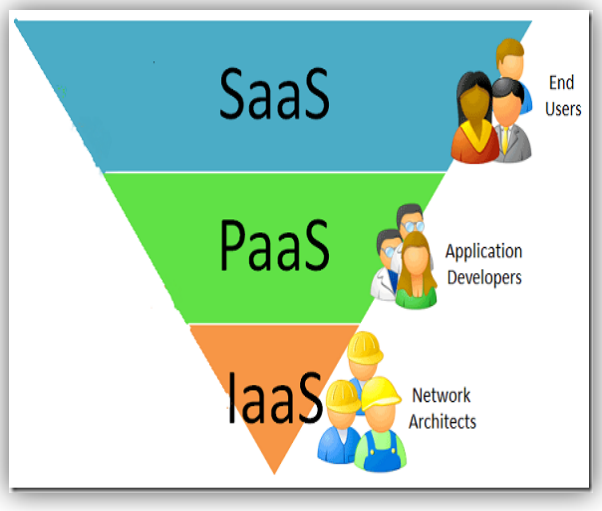

Fig-2: Three Cloud Delivery Models

IV. WHERE DOES THE PROBLEM LIE?

Cloud services are divided into separate levels/segments in which they operate. Key segments includes databases, networking, authentication, virtualization etc. A failure in either or all of these segments leads to collapse of the cloud service mechanism.

A variety of security shortcomings are responsible for failure of a service. Most of these have been identified by the developers of the various companies that provide cloud related solutions through the numerous attacks on cloud servers throughout the years. [6][7] Some of the threats that still loom over cloud services are:

1. Unchecked Access to Servers
2. Data Transmission Problems
3. Network Security
4. Data Privacy and Integrity
5. Data Availability
6. Patch Management

1. **Unchecked Access to Servers –** In traditional data centers, only the people with administrative rights had access to central server. But in cloud services, one can easily connect to the server and launch an attack. Data theft is also pretty obvious option for stealers. Many times past users have been found to access the network of organizations they worked in. This is because authentication and database management are out of scope of network administrators and they are required for immediate problems and proper functioning of cloud servers.[17]
2. **Data Transmission Problems –** Most of the data that is sent and received is encrypted. In cloud environment, many times data is not encrypted because it is needed by application in its unlocked condition. After the processing, data is transmitted through SSL/TLS protocols. They only ensure secure delivery and not changes in the transmitted data. Newer encryption methods allow to change the encrypted files without having them decrypted at all. This technology is misused by data stealers to steal and modify important data without anyone knowing. [16]
3. **Network Security –** Many problems with networks like DNS attacks, reused IP addresses are related to weak cloud security. When a user requests a particular Domain Name Server (DNS), he/she asks for their IP address and thus need for DNS server arises. But many time these servers reroute the user to dangerous and malicious websites and hosts which risks their online presence. Reused IP addresses are those which are provided by a website to some other client in place of old client. There is some time gap between the website clears its old caches and readies. During this period, new user can access old user's data. This fault can be used by hackers to take illegal control over accounts and steal credentials and even change them.[20]
4. **Data Privacy & Integrity –** As the spread and usage of cloud services becomes global for every provider, it is of out-most importance for them to have in place a strict privacy policy regarding its customers. But many providers simply neglect to follow the standards fearing it would burden their profits to engage more workforce over these matters. Data corruption is also a common problem in cloud servers where millions of files can be affected due to a single error. All the data that is created is stored on these servers and only the providers have controls to access all these files. Hence they are highly responsible for data integrity.

5. **Data Availability** – For large and small organizations alike, availability of data 24x7 is of prime importance. Due to system failures on part of providers, data becomes unavailable to users. Denial of Service is a severe problem where servers hosting data do not respond to clients' requests to access their data.[18]

6. **Patch Management** – Most of the times, users are risked because they lack sense of security. Providers update their applications with patches to bugs and problems which can be used by hackers to harm the users. But many-a-times, user refrain from updating their applications.[19]

How Can These Problems Be Solved?

We have looked at various problems which are plaguing the cloud service industry. Many of these problems are deep rooted which would require complete overhaul of the system and others are just small defects which can be corrected if given proper solutions.

Many great solutions have been provided by IT experts over the years to tackle these problems. Some of them are implemented by the cloud providers and other few can be put in action by users themselves to avoid problems in their applications later.

1. **Secure Consumer Authentication**- One of the most basic step towards a secure cloud environment consists of granting access to service only to a real user. Many hackers try to get into the accounts using bots who retry attempts. Cloud providers should put in place software that can identify real users and filter out hacking tools. [5,13]
2. **Insider Attacks** – More than often due to an internal breach at an organization, there is huge data leak that compromises all the users of the company. Thus it is very important for company to strictly implement security measures within their own network to avoid such embarrassing situations. [5, 14, 15]

3. **End-to-End Encryption** – As the latest buzzword in today's world, it roughly means that data that is being shared between users of cloud services is encrypted in such a manner that only sender and receiver have ability to decrypt and access the secured data. Not even the service providers should be able such data. Popular messaging app WhatsApp is known to use this method to store the users' messages to avoid data theft. [5, 8, 9]

4. **Maintenance of the Server Systems** – As important it is to secure the data generated, it is equally important to keep the 'machine' that processes it to work efficiently and error free. Regular maintenance of server ensures that none of its components are prone to malfunction. It also means that various software fixes should also be applied to systems so that they are secure from viruses. [10,11,12]

5. **Backups** – Many a times, data is lost even by big corporations because they simply fail to make a timely backup of their data. This can be very disastrous in case of system failure or cyberattacks on servers. To make up for the data loss, there must always be latest backed up data for easy recovery. [3]

6. **System Testing** – As we know even the best need to get better. So it is important for cloud providers to test their systems for errors. Many companies organize events where many experts try to find bugs and weakness of their systems. This gives the companies feedback and tips to improve their servers. [4]

7. **User Alertness** – There are many steps that can be taken by the users of the applications to ensure their safety. They should inform the provider about any unintended login. Regular updates should also be implemented to shrug off old errors. [4]

V. CONCLUSION & FUTURE SCOPE:

This paper conclude various essential security issues in cloud computing and their proposed promising defense solutions to avoid such security issue

Table1: Summarizes various essential security issues in cloud computing and their proposed promising defense solutions to solve security issues,

Issue Sr No:	SIGNIFICANT SECURITY ISSUES IN CLOUD COMPUTING	PROPOSED POSSIBLE PROTECTION SOLUTIONNS
I1	Unchecked Access to Servers: An invader can use the victim's account to get admittance to the target's resources	***Secure Consumer Authentication:*** Cloud providers should put in place software that can recognize genuine users and sort out hacking tools
I2	Data Transmission Problems: Newer encryption methods can change the encrypted files without having them decrypted at all. This expertise is tainted by data stealers to whip and modify many important and useful data without anyone knowing about this.	***End-to-End Encryption:*** Data that is being collective between users of cloud services is encrypted in such a way that only & only sender and receiver have capability to decrypt and entrée the secured data
I3	Network Security: Hackers take illegal and prohibited control over some accounts and can whip credentials and can even change them	***Insider Attacks***: Company should firmly apply security method within their own network to shun such problems
I 4	Data Privacy and Integrity: All the data that is formed is stored on servers and only the providers have pedals to right to use all these files. Hence they are extremely answerable for data integrity	***Maintenance of the Server Systems***: Standard maintenance of server ensures that no components are prone to malfunction. It also means that a variety of software fixes should also be practical applied to systems
I 5	Data Availability: Denial of Service is a severe trouble where servers hosting data do not answer to clients' requests to access their data.	***Backups:*** in case of system failure or cyber attacks on servers, data loss, there must always be latest back up to solved the issue of data unavailability.
I 6	Patch Management: Many-a-times, user refrain from updating their applications and issue arise on the part of security	***System Testing & User Alertness:*** Testing gives the companies feedback and tips to improve their servers and Regular updates should also be implemented to shrug off old errors.

The cloud environment will continue to grow despite the various challenges it is facing and many more that created either knowingly or unknowingly. But one thing that keeps the cloud service providers in the business is their ability to face the problems.

The businesses have never been stalled due difficulties faced by them due to technologies. As long as the IT industry continues to provide viable solutions to improve the cloud services, the cloud services will make the services of Internet based tools more efficient and friendly for a large pool of people.

ACKNOWLEDGEMENT

We would like to sincerely bring our kind gratitude to Dr. Prateek Jain, Accendere Knowledge Management Services for helping and guiding us in this paper formation.

REFERENCES:

1. Peter Mell, "The NIST Definition of Cloud", Reports on Computer Systems Technology, sept., p. 7.,2011
2. Akhil Behl, Kanika Behl, "An analysis of cloud computing security issues", World Congress on Information and Communications Technologies, IEEE,2012
3. Ni Zhang Di Liu Yun-Yong Zhang, "Research on cloud computing security", International Conference on Information Technology and Applications, IEEE, 2013
4. A. Kundu, C. D. Banerjee, P. Saha, "Introducing New Services in Cloud Computing Environment", International Journal of Digital Content Technology and its Applications, AICIT, Vol. 4, No. 5, pp. 143-152, 2010.
5. Sharma, R. & Trivedi, R. K. (2014). Literature review: Cloud Computing –Security Issues, Solution and Technologies. International Journal of Engineering Research, Vol. 3, Issue 4, pp. 221-225.
6. Rabi Prasad Padhy, Manas Ranjan Patra , Suresh Chandra Satapathy, " Cloud Computing: Security Issues and Research Challenges", IRACST - International Journal of Computer Science and Information Technology & Security (IJCSITS) Vol. 1, No. 2, December 2011
7. Osama Harfoushi, "Data Security issues and challenges in Cloud Computing: A Conceptual Analysis and Review", Communications and Network, 2014, 6, 15-21
8. Abhigna B.S, Nitasha Soni, Shilpa Dixit , "Crowdsourcing – A Step Towards Advanced Machine Learning", ICCIDS 2018, vol-132 pp-632-642, Procedia , Elsevier, 2018.
9. Deepika, Nitasha Soni, Database Security: Threats and Security Techniques, International Journal of Advanced Research in Computer Science and Software Engineering, IJARCSSE, Volume 5, Issue 5, MAY 2015, ISSN: 2277 128X
10. Dr. Krishan Kumar Shobha Tyagi, Evaluation of Static Web Vulnerability Analysis Tools, Fifth International Conference on Parallel, Distributed and Grid Computing (PDGC) IEEE, 10.1109/PDGC.2018.8745996, Dec 2018
11. Dr. Krishan Kumar Dr. Ochin Sharma, Review for Best Multidimensional Index Structure,IJCRT, SSN: 2320-2882, 2018
12. Kritika Mahajan, Shilpa Shukla, Nitasha Soni,A Review of Computerized Payroll System, International Journal of Advanced Research in Computer and Communication Engineering, IJARCCE, Vol. 4, Issue 1, ISSN (Online) : 2278-1021 ISSN (Print): 2319-5940, Jan 2015.
13. Nitasha Soni, Tapas Kumar, Cloud based Financial Market Prediction through Genetic Algorithms: A Review, International Journal of Computer Applications (ISSN: 0975 – 8887) Volume 123 – No.8, August 2015.
14. Dr. Krishan Kumar, How Hyperlan, IEEE 802.11 and Bluetooth are Responsible in Growth and Commercial Deployment of MANET, (IJNIET)International Journal of New Innovations in Engineering and Technology, ISSN: 2319-6319, 2013
15. Dr. Krishan Kumar Surya Kant, Performance Analysis Of Dynamic Source Routing Protocol In Wireless Mobile Ad Hoc Network,IJERT, SSN (Online) : 2278-0181,2012
16. Pawan Nagar, Nitasha Soni , "Optimizing program states using exception handling constructs in Java" , IJESAT ,Vol02, ISSN: 2250-3676,Iss-02 Mar-Apr, 2012.
17. Dr. Krishan Kumar, Methodology and Challenges of Mobile Adhoc Networks and Types of Attack, (IJNIET)International Journal of New Innovations in Engineering and Technology,2012
18. Pawan Nagar, Nitasha Soni, "Minimization of Time & Cost Factors with Optimized Program-States Using Exception-Handling Constructs in Java (During Analysis and Testing of Programs" ,International organization of scientific research). ISSN:2250-3021 , Vol 2(4) PP: 544-554, apr 2012.
19. Jyoti, Nitasha Soni ,"Comparative study of ADhoc routing protocol, AODV, DSR and DSDV in mobile ADhoc network", International Journal of Applied Engineering Research (IJAER). ISSN0973-4562,vol-7, (11)2012
20. Bharat Singh Krishan Kumar, Performance Evaluation for Routing Protocols of MANET in Different Mobility Speed Models, IEEE/IACSIT, ICCMS –Bombay, 2011

AUTHORS PROFILE

Kapil Singh is pre final year student of Department of Computer Engineering, in Manav Rachna International Institute of Research and Study.

Sanjay Verma is pre final year student of Department of Computer Engineering, in Manav Rachna International Institute of Research and Study.

Md Sharib is pre final year student of Department of Computer Engineering, in Manav Rachna International Institute of Research and Study.

Nitasha Soni received Ph.D in Computer Science & Engineering from Lingaya's University, Faridabad, India in 2017. She is working as Assistant Professor in Manav Rachna International Institute of Research and Study. Her research interests include Big Data, Cloud Computing.

Krishan Kumar received Ph.D in Computer Science & Engineering from Singhania's University, Rajasthan, India in 2012. He is working as Associate Professor in Manav Rachna International Institute of Research and Study. His research interests include Big Data, Cloud Computing, and Mobile Adhoc network.