NOVATEUR PUBLICATIONS
INTERNATIONAL JOURNAL OF INNOVATIONS IN ENGINEERING RESEARCH AND TECHNOLOGY [IJIERT]
ISSN: 2394-3696
VOLUME 7, ISSUE 6, June-2020

CLOUD COMPUTING SECURITY CHALLENGES

NARENDRA RAO TADAPANENI
Sr. Software Engineer

ABSTRACT

This paper explores security challenges faced by cloud computing. It discusses the prevailing protection tactics to secure the cloud infrastructure, programs and drawbacks. Cloud computing started in the mid 90's and one of its earlier users are Amazon and Ali Baba. It is growing really fast in the field of computer science. People nowadays are using cloud computing at a very vast level. Cloud computing is basically based on the Internet and has the most powerful architecture of computation. After a particular has deployed his/her cloud based platform, the biggest fear is its security. A cloud as mentioned earlier is all web-based which means that retrieving data from a particular cloud isn't something impossible. As the use of cloud computing is growing, so are the security challenges. More people are getting aware of the technology which is making it easier for them to break into different clouds and retrieve their desired information. Many organizations have started offering cloud based solutions to their customers which has made security a major aim in their projects. On the other hand, many security experts are working on finding better security solutions. Even though security is getting better day by day but still hackers are finding ways to exploit a particular cloud. The Cloud security concern becomes more complex below the cloud model as many other fields continuously enter the Cloud computing industry.

INTRODUCTION

The basic definition of Cloud computing is "A solution for providing a less complicated and reliable access to resources of IT". Cloud computing is an emerging technology [2] similar like Artificial Intelligent both have security challenges [11]. The amount of data that is generated now a days is huge so it's better to access the technical services like storage or computing power rather than maintaining the data servers. Various organizations of different type, size and industry use the cloud in many different data processing cases like data backup, disaster recovery, virtual desktops, software development and testing and web-based customer service. The industries use cloud computing for various purposes. The cloud is used by health care companies to develop personalized Health treatments. Whereas Financial services companies use cloud for fraud detection and real time blocking. Basically, Cloud computing is not an application oriented perhaps it is service oriented.

The security and privacy of data is one of the major concerns in cloud computing. The cloud service providers must insure the protection of contents from various malware and for that there are different policies and mechanisms of Cloud service providers. Data shared between different organizations is one of the major advantages or cloud computing but this advantage also imposes a risk as data can be misused by other users. Perhaps it must be the first priority to protect data depositories. This paper is basically about data security techniques and challenges and how you can protect the cloud. This paper also discusses different risks and threats associated with Cloud.

The remaining part of the paper is organized as. Section 2 and Section 3 is about the different deployment and service models in cloud computing. Section 4 is about the security risks to data in cloud. Section 5 is about the different security challenges to cloud computing. The last section that is section 6 is the conclusion.

Deployment Models

This part of the paper refers to applications, services or resources that are made accessible to users when needed through the Internet from the server of cloud computing provider [12].

Public Cloud Model

The systems and services that are readily made available to general public. Examples are Google, Amazon and Microsoft.

Private Cloud Model
The systems and services that are only available inside an organization. Private Cloud allows infrastructure to be accessed only by the members of organization. Examples are Vmware and Elastra-private cloud.

Hybrid Cloud Model
It is basically a blend of both Private and Public Cloud. The Private Cloud is responsible for performing all important activities and the Public Cloud is responsible for performing all the activities that are less important. Examples are IBM, EMC and Rack space.

Community Cloud Model
It permits systems and services to be made available by group of organizations. E.g. Open Cirrus.

Service Models
This part of the paper is about diverse delivery models of cloud computing. Basically, Cloud computing allows access to the network to share computing resources when needed. Cloud computing is based on Service models that are basically the reference models [4].

Software as A Service (SAAS):
It offers user with payment on demand on each use of applications. This service is platform independent and you don't have to install software on your device which means it's not like licensed bought programs. The cloud has single instance storage in its software which is accessible to numerous end users. A vendor manages all the resources of computing accountable for delivering SaaS. There are a lot of end customers who are recurrent users of SaaS. E.g. SaaS's products and services is the Google ecosystem like Gmail, Google docs and Google drive.
Security Measure of SaaS: SaaS providers guarantees the security of program and components. The major role of SaaS is to provide user authentication and password verification.

Platform as a Service (PAAS):
The PaaS service is for development and comprises of a programming language execution environment, an OS +a web server as well as database. You can even manage data and the resources of the application in this model where the vendor manages all the resources. Following PaaS products and services are provided by Cloud providers: Amazon web services elastic Windows Azure, Google App engine, Beanstalk, Heroku and force.com.
Security Measure of PaaS: It is for the defending of SSL attack and to prevent common HTTPS attacks.

Infrastructure as a Service (IAAS):
Architecture and infrastructure for computing is offered by this service i.e. for the accessibility of multiple users, in the virtual environment, it offers computing resources. The resources are Data Storage, Virtualization, Networking and Servers. Vendors manage most of these resources. You will be given the responsibility of taking care of other resources such as application, data, runtime and middleware if you use these resources. IaaS is used by SysAdmin. E.g. Amazon EC2, GoGrrid and Rackspace.com.

Data as a Service (DAAS):
It is a customer software as a service, it build on the concept that the user can be provided with the data. DaaS is basically taking data and turning in to a product its turning it into something that the everyday layman can go into access learn from. Example of DaaS includes Urban Mapping, Xiginite and D&B Hoovers.

Security Risks
Every emerging technology faces various challenges, same is with cloud Computing as it is an emerging technology so there are various risks and challenges faced by Cloud Computing. As cloud computing is handling everything related to different organizations. Everything is dependent on cloud, like the storing and

accessing of data so there are different risks associated with the storing and accessing of data [1]. This part of the paper is about what different risks in cloud are computing.

Virtualization
There is a potential concern to compromise the virtualization software, it is a hypothetical concern but it does exist. The basic work of the virtualization is to alter any relation between OS and hardware. So the Cloud Service Providers should properly manage and secure the additional layer. The another risk with virtualization is compromising a hypervisor itself. Which results in compromising the whole system. So you need to upgrade your plan to use the virtualization.

Storage
Storing information in a public cloud is a protection issue in cloud computing. Your data is exposed to hackers because of centralized storage facilities. So for these types of risk it is best to have a private cloud when the data is sensitive.

Multitenancy
Shared access to another user is the major risk in cloud computing. As the chance is always there for other users to access your private data. The mistake of other user can also lead to hacker accessing your data

Security Challenges
Cloud computing is open to different security challenges [7] that opens a wide area to research for the researchers. Every technology has two faces one face leads to prosperity and the other face rises to challenges. Same is with Cloud computing, there are different security challenges faced by Cloud Computing [3]. So this part of the paper is to discuss about the different challenges faced by cloud computing.

Third Party Handling Data
As we know that data in the cloud is handled and managed by third party, so the biggest problem is which security measures are used by the party and what is the guarantee that the data is secured because no third party can give you 100% person security of the data. So there is no proper guarantee of data security.

Cyber Attack
The most important security concern in Cloud computing is Cyber Attack. There are different attacks conducted on the data everything from malware and ransomware types of attacks to basic misconfigurations or poorly constructed infrastructures [6]. There is a lot of different challenges and when it comes to malware, we are seeing that malware is nowadays very polymorphic it attacks multiple different vectors simultaneously. It's designed to spread itself so rapidly, getting a handle on it means that there is a need to look on the security of the cloud little bit differently.

Insider Attack
Suppose if the cloud company to which you have stored the data the users of the company can easily access the data that means there will be no privacy of the data.

Government Intrusion
In a Government, there are different surveillance and supervision types of programs to monitor the data. So you can never say that your data can only be accessed by you. Your data is accessed by different agencies so again there is no privacy of the data.

Lack of Support
There is no proper support from companies to its users, as there is a great competition in market so because of the competition, companies lower there pricing of data storage which leads to the lack of support to the customers.

Lack of Standardization
Different Cloud suppliers are not always following the same standards. That means there is no proper standards used in different mechanisms like encryption or authentication mechanism or access control mechanism.

Data Integrity
There is always a chance of data being changed by a user that is not authorized. Basically It is the duty of Cloud Service Provider to make sure that data must not be modified by an unauthorized user [13]. The second concept of integrity is when the data is transferred from one cloud to another cloud. So at that stage the Cloud Service Provider must insure that data will not be modified by an unauthorized user.

Lack of Transparency
If a particular organization buys from a cloud service provider as either a public, private or hybrid cloud offering, they aren't issued with the exact details on how their data will be secured. This is a lack of service transparency which makes it difficult for organizations to figure out whether the stored and processed data is completely secured [14]. People aren't even completely sure whether their data is actually secured or not.

Insecure APIs
When a cloud is being rented to a particular client, the client doesn't actually know what range of APIs their cloud service provider is using. Even if security is fully guaranteed, the APIs that are embedded or used in the cloud service provider's system might not be secure. This problem if bigger when the applications layers are built up on top of these APIs by client company. This security threat is then automatically passed to the client's application.

OTHER THREATS
There are various issues that can be caused by Externa threats like:

Middle Man Attacks
The communication between two parties is not secured. Where third party manages to interfere between a source and destination. This middle man can easily alter the data once he achieves to interfere between them [15]. The hacker can easily listen the communication between the client and the cloud.

Denial of Service Attack:
The hacker tries to bring the server down by disturbing a cloud by flooding it with loads of traffic.

Network Sniffing:
It is basically monitoring of all the network between different clouds or between the cloud and the user. By that the hacker will learn a lot of things like which authentication mechanism is used.

Port Scanning:
In this the hacker tries to understand the ports which are being used by the cloud server. The ports are very crucial as by the information of ports the hacker can easily access to the information stored.

SQL Injection Attack:
It is the direct attack on the database by that the hacker gets the special information like username and passwords. The attack is launched by a SQL Query.

Cross-Site Scripting Attack:
It is the embedding of harmful links or Script. Hacker leaves a link on the website so if the user will open the link, he may unintentionally share the control or access to the hacker.

Account Traffic Hijacking

This kind of attach can provide an exploiter with passwords and other primary information which can easily allow them to access all the data.

CONCLUSION

The users of Cloud computing are increasing daily so the security concerns and risks of data in the cloud is also increasing. There is a need to look at the cloud security a bit differently, we have to look it from a holistic point of view in terms of what endpoints are interacting with it and what is the user community doing with it and how is our infrastructure constructed like what kind of security grips do we have and in what different ways the infrastructure can be segmented. What is allowed to communicate with what and why and how these applications are are really supposed to behave so we can put the right policies. But more important is to extend the right security capabilities to where the customer data, user, and endpoints are all going. We really need to address the generation five or generation six attacks which is a very highly automated approach. So there is a need of a clear and more centralized standpoint, to be able to do the right things to secure our networks. The security technology is just one component, security is about people, processes and technology all three which have to be in unison, all three have to be in harmony because if any one of these areas is affected , then the security posture breaks down. So Without any doubt, cloud computing is a valuable technology for almost every business that is using it. This paper provided an overview of the major security and privacy challenges faced by the cloud and the paper also discussed the risks and threats associated with the data stored on the cloud.

REFERENCES

1) Shen, Z., Tong, Q. (2010): The security of cloud computing system enabled by trusted computing technology. In: 2nd International Conference on Signal Processing Systems (ICSPS 2010), vol. 2, pp. 2–11.
2) Tadapaneni, N. R. (2020). Cloud Computing - An Emerging Technology. International Journal of Innovative Science and Research Technology. 5.
3) Jamil, D., Zaki, H. (2011) Cloud Computing Security. International Journal of Engineering Science and Technology 3(4), 3478–3483.
4) Tadapaneni, N. R. (2017). Different Types of Cloud Service Models. Available at SSRN 3614630.
5) Bikram, B. (2009) Safe on the Cloud. A Perspective into the Security Concerns of Cloud Computing 4, 34–35.
6) Dikaiakos, M.D., Katsaros, D., Mehra, P. (2009) Cloud Computing: Distributed Internet Computing for IT and Scientific Research 13, 10–13.
7) Tadapaneni, N. R. (2018). Cloud Computing: Opportunities and Challenges. SSRN Electronic Journal. 10.2139/ssrn.3563342.
8) Srinivas, Reddy, Qyser, J. (2014), Cloud Computing Basics, Build. Infrastructure. Cloud Security., vol. 1, pp. 3–22,
9) Ion, I., Sachdeva, Kumaraguru, P., & Čapkun, S. (2011). Home is safer than the cloud: privacy concerns for consumer cloud storage. In Proceedings of the Seventh Symposium on Usable Privacy and Security (p. 13).
10) Puthal, Sahoo, Mishra, Swain, P.(2015) cloud computing features,Issues and Challenges:A big picture", International Conference on Computational Intelligence & Networks, pp. 116-123.
11) Tadapaneni, N. R. (2020). Artificial Intelligence Security and Its Countermeasures. International Journal of Advanced Research in Computer Science & Technology, Vol. 8.
12) Tadapaneni, N. R. (2020). A Survey Of Various Load Balancing Algorithms In Cloud Computing. International Journal for Science and Advance Research in Technology, 6.
13) Selviandro, Suryani, A. Hasibuan, S.(2015), Open learning optimization based on cloud technology: case study implementation in personalization E-learning, February 16~19, pp. 541-546.
14) Winkler, V.(2011) Securing the Cloud, Cloud Comput. Secur. Tech. tactics. Elsevier.
15) Sabahi, F.(2011). Virtualization-level security in cloud computing, 2011 IEEE 3rd Int. Conf. Communication. Software. Networks, pp. 250–254