An Insight In to Cloud Security: Techniques, Challenges & Solutions

Kanika Sharma[1], Anushka Singh[2]
[1,2] B.Tech (CS) Student,
School of Engineering & Technology,
Apeejay Stya University, Gurgaon

Deepti Juneja Thakral[3],
[3] Assistant Professor,
School of Engineering & Technology,
Apeejay Stya University, Gurgaon

Animesh Yadav[4]
[4] Research Engineer,
Espertosys Private limited,
Bangalore

***Abstract*: Cloud computing is an internet based computing where we store, manage, access and protect our data on a network of remote servers hosted on the internet. The security of the data stored on cloud is always been one of the major issues. In this paper, we will discuss about the available security techniques for cloud and the challenges the world is facing for security and privacy of data on cloud. We have also conducted a survey to see the outlook of the people over the cloud storage. The results will be discussed and some of the solutions to avoid the possible attacks on the data over cloud are proposed.**

Keywords: Cloud computing, security, techniques, challenges

I. INTRODUCTION

Cloud computing [5] is stated us as an umbrella term which shapes different connotation in different circumstances to different individuals. The notion of computing was taken into actuality to avoid of capital expenditure on infrastructure, operating system, deployment and storage.The explanation of "cloud computing" from the National Institute of Standards and Technology (NIST) is that cloud computing enables ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

Cloud computing can be demarcated in simple verses as UTILITY COMPUTING. It essentially means that we can use as many resources as needed without paying for each of them separately. It helps us in cutting the cost of hardware and software and work with the shared pool of resources.It also offers various computing services to us like Iaas, Paas, Saas, and Naas etc. The cloud computing majorly works on the principle of virtualization and parallel computing. The cloud can be majorly categorized into 4 major categories as public cloud, private cloud, hybrid cloud and community cloud.

- **Public cloud** - Public cloud is a model which is easily accessible on the internet from a minor party**.** It is something which can be owned and managed by the cloud provider. Customers are only charged for the resources they use. The Examples of a public cloud includes Microsoft Azure, Google App Engine.
- **Private cloud**- It is a cloud model that is owned and managed by a third party or an organization. For the benefit of the client, there is optimized control of infrastructure with improved security as the everyone is not allowed to access it. Eucalyptus Systems is one of the best examples of private cloud.
- **Hybrid Cloud** - This deployment model of the cloud is the composition of two or more cloud models that is public, private or community clouds. The construction and governing of model is difficult but it is managed by splitting the responsibility between enterprise and the cloud provider. It is very useful in providing services that are very secured which includes both the primary and secondary business. Few examples of hybrid cloud includes Amazon Web services.
- **Community Cloud-** It is a unique model in which infrastructure is shared by many organizations which are either managed by themselves or a third party service provider is formed.
  The existence of this cloud model depends on operating environment. Facebook is an example of this model.

II. WORKING ON CLOUD

Cloud computing can be used in various aspects like deployment of applications, making soft wares, for storing data and accessing it whenever and wherever required.

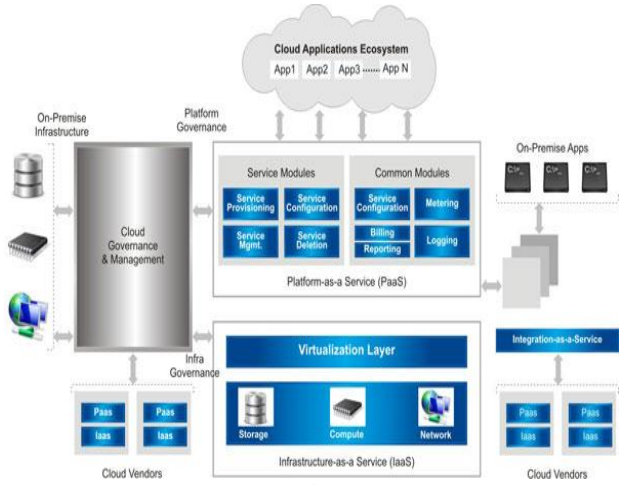


Fig. 1 : Deployment of applications

The procedure to deploy can vary for each CSP. One of the method is stated as follows.[9]

Step 1: Prepare to Deploy.

Step 2: Know Your Credentials and Target.

Step 3: (Optional) Configure Domains.

Step 4: Determine Deployment Options. Define Deployment Options. ...

Step 5: Push the App.

Step 6: (Optional) Configure Service Connections.

Step 7: Troubleshoot Deployment Problems.

III. SECURITY ON CLOUD

Security[6] on internet is all about data. Data security is a major concern nowadays. It deals with unauthorized access by intruders or leakage of data by any means. It is a supposition by many people that saving data online is similar to making the data publicly accessible. Internet is considered to be public platform and uploading private data is a fear for everyone.

Many of the computer infrastructures are increasingly vulnerable to attacks, since intrusion detection is necessary but unfortunately insufficient. So we need to design and implement an effective detection and response techniques to circumvent intrusions when they are detected. This intrusion and detection technique is based on different types of counter-measures. The main idea is to design and develop a decision support tool to help the administrator to choose the appropriate counter-measure when an intrusion is detected. Cloud Computing is a new emerging technique in computer oriented services. This system have some similar distributed system, according to these similarities of cloud computing also uses the features of virtual networking environment. Therefore the security is the biggest concern of cloud computing system, because these services of cloud computing are based on resource sharing.

A. Security Techniques on Cloud

Cloud computing deals with two major concepts of security and privacy. It includes various domains as security is a concern everywhere. It contracts with maintaining a balance into each domain. These domains are the control nodes, network, virtualization, databases, load balancing, concurrency control, operating system, and resource scheduling and memory management.

- Authentication: - This is the first step security which checks the user identity i.e. username and password.
- Authorization:- this is the second security measure which deals with verifying your access to various resources
- Encryption: - This is also an important measure for security which encrypts the data in the form that can only be decoded by the key of the receiver.
- SMS or OTP: - This is a measure taken at the last step of nay major action like transaction and so it confirms by using reference from another device by sending sms or one time passwords for confirmations.

DDos as a problem for cloud security

For understanding the distributed denial of service (DDos) attack we have to first understand the denial of service(Dos) attack. These two concepts are interrelated but the only major difference is the level of destructiveness DDos causes.

Cloud Servers against Flooding Based DDoS Attacks

A Denial of Service (DoS) attack is a type of attack focused on disrupting availability. Such an attack can take many shapes, ranging from an attack on the physical IT environment to the overloading of network connection capacity, or through exploiting application's weaknesses. A DoS attack involves, using one computer or internet connection to flood a server with packets (TCP/UDP). The objective of this attack is to 'overload' the server's bandwidth, and other resources, so that anyone who may be trying to get access to the server is not served, hence the term "denial of service". A DDoS (Distributed Denial of Service) attack is almost the same as a DoS attack, but the results of the DDoS attacks are massively destructive. As the name suggests, the DDoS attack is executed using a distributed computing method.

We can take an example to understand this.

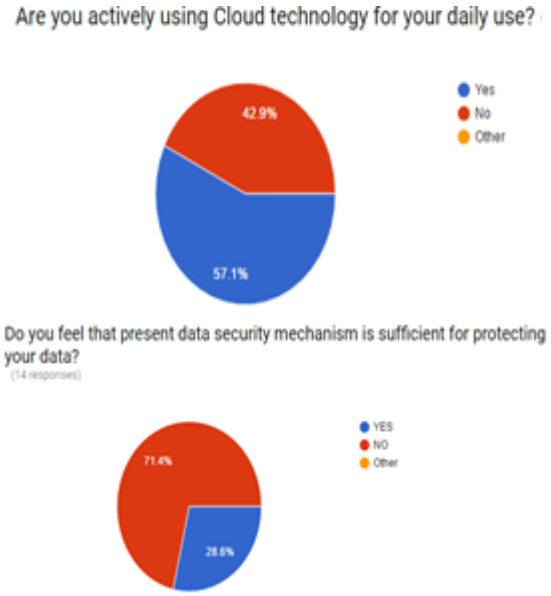
A person comes home and has a long weekend and so he decides to spend time playing online games. And when u tried to connect to the network , the browser denied access your network. This is called as denial of service(Dos). This is only when one computer is involved. But later he found that it was Distributed Denial of access. The attacker flooded the gaming server and prevented anyone from gaining access.

This is a method in which the attacker takes control over user's computer and use it to attack 1000 other computers. Then those 1000 computers will work like zombies as they

are infected. They generate millions of data packet and overload server. It is considered as distributed attacks

IV. RESEARCH SURVEY

Since past years many types of research and works have been carried for cloud security. There are many issues related to cloud computing and for this paper, we have taken into consideration the most evolving topic i.e., "Security in cloud computing". We conducted a survey on security issues. From this survey, we could draw out a conclusion that people resist storing their data on a cloud for the fear of losing it and unauthorized access of their data by others. The conclusions drawn by the survey is presented in the form of pie chart below:



According to the survey, there are more than half of the totals using cloud technology and among them, they use cloud basically for data storage. Among the people who are surveyed, most of them feel that the present security mechanism is not sufficient. There is a need of updating and introducing the new mechanism for security. From the above, we conclude that with the emerging technology people are using cloud environment but they have a fear about the security issues for their data storage. So, security issues in the cloud have become one of the most discussed topics among the people.

Till date, many works are being carried out to improve and update the security mechanism of cloud computing. Some of the important works have been mentioned in this paper.

Among them, two authors Navia Jose and Clara Kanmani [1] has proposed a new model on cloud security. This model is based on a system structure consisting of three-layers, in which each layer performs its specific task to ensure security. The three-layer perform functions for cloud user authentication, user's data encryption by using AES algorithm and the faster user data recovery by using Byzantine fault tolerance algorithm respectively. With this there are least chances of data being tampered. This is one of the most efficient techniques used for cloud security mechanism.

The authors Ashwini Bansode and Megha Singh [2] proposed a model of implementing cloud storage security by the use of Digital signature. This model works by generating private and public keys by cloud server for client admin which is done by the process of encryption and decryption. While performing this experiment, they also came up with a conclusion that despite the attacks by several malicious users , the privacy of client remained intact. According to this model, the efficiency of this model is calculated by both file distribution preparation and verification of token.

The authors Vinothkumar Muthurajan and Balaji Narayanasamy [3] proposed a model to investigate how can the integrity and security of data transfer can be improved which is based on the Elliptic Curve based Schnarr scheme. In this model, they have proposed a cloud model using virtual machine with Hybrid Cloud Security Algorithm (HCSA) which is highly used for removing the expired content. This improves the malicious activity that occurs during the data transfer. The duplicate degrades the performances. Thus, there is an improvement in the security performance which is achieved by combination of EC-Schnorr and blooming filtration.

V. PROPOSED IDEAS

There can be some methods which can be used to avoid the DDos. So the possible solutions for such attacks that were introduced in this paper earlier are listed below:-

1) Increasing Queue Length

To prevent the DDoS attack early techniques have focused on increasing the length of the queues and reducing a timeout value. The timeout value controls how long an entry waits in the queue until an acknowledgement is received. The problem with simply making the queue longer is that there are actually many queues (one for each TCP server on the system--HTTP, FTP, SMTP, etc.), and lengthening the queues to very large values, for example, eight kilobytes, results in an operating system requiring enormous amount of memory (over 100 megabytes for a system with 25 server applications).

Commonly used DDoS detection techniques fall into either IP Attributes-based DDoS Detection or Traffic Volume based DDoS Detection. The first ones use such as IP protocol-type and packet-size, source IP prefix and TTL values, as well as server port number and protocol-type, etc. to determine the anomalous behavior. However the other one uses a multi-level tree that keeps packet rate statistics for subnet prefixes at different aggregate levels. Normal traffic usually has a proportional rate to or from hosts and subnets. Therefore, an attack will be detected when a disproportional rate of traffic is observed. Most of the techniques in these categories suffer either through large dependence on the attribute used for the computation of the entropy or too long time delay due to complex computation or weak connection between selected

attributes and DDoS attacks, making the detection scheme ineffective.

2) Intrusion Detection System (IDS) and firewall

Intrusion Detection System (IDS) is a device that monitors all the activities and works as a firewall when it detects an attack. It is very flexible .There are various types and configurations where each one records information. Notifies security administrators of unusual activities. Some IDS actually responds to and prevent attempted attacks. They use two common techniques, they are signatures and anomaly baselines. It keeps a list of malware signatures and so it compares incoming threats to the list designed and blocks the attacks on the list. It uses anomaly baselines as to locate abnormalities and compare it with the system baseline and considers at all variations from that baseline. It makes a normal range baseline for comparision of any threats.

Some configurations are

In host based network IDS are placed between firewall and network.

In host based with network based together, we put a switch between a firewall and your network which allows you to install a dedicated IDS. Eg SNORT (capable of real time traffic analysis and packet logging) It also functions as a sensor. However, the false alarms and the large volume of raw alerts from IDS are two major problems for any IDS implementations.

IDS software offers two types of protection: active and passive.

Active IDS software tries to prevent a hacker from gaining access to your system. If it founds a malfunction web address coming through the wire, it actively blocks the originating IP address.

Passive IDS software logs and reports potential attacks, but it doesn't actively responds to threats. It makes the user take the final decision of how to act.

Many attack graph-based alert correlation techniques have been planned recently. One of which is called queue graph (QG). It is used to trace alerts matching each exploit in the attack graph.. Another technique is modified attack-graph-based correlation algorithm to generate explicit correlations merely by matching alerts to specific exploitation nodes in the attack graph with multiple mapping functions, and devised an alert dependencies graph (DG) to group related alerts with multiple correlation criteria. Each path in DG represents a subset of alerts that might be part of an attack scenario

3) Security and Privacy Challenges in Cloud Computing

Cloud computing is an sprouting paradigm with tremendous motion, but its unique aspects worsen security and privacy challenges.

4) Unique Security and Privacy Insinuations in Cloud Computing

Understanding the security and privacy risks in cloud computing are critical. Clouds allow customers to evade start-up costs, cut operating costs and upsurge their agility by immediately acquiring services and infrastructural resources when necessary, their unique architectural topographies also raise security and privacy concerns. Multi-tenancy is one more unique feature to clouds, especially in public clouds. Fundamentally, it allows cloud providers to manage resource utilization more proficiently by partitioning a virtualized, pooled infrastructure among various customers. From a customer's perspective, the notion of using a shared infrastructure could be a enormous concern.

5) Virtualization and Hypervisors

Virtualization is an important permitting technology that helps intellectual infrastructure and resources to be made available to clients as isolated VMs. A hypervisor or VM monitor is a piece of platform-virtualization software that lets numerous operating systems run on a host PC concurrently. This offers a means to generate virtualized resources for distribution, such technology's presence also increases the outbreak surface. For some applications, it might be important to associate process outputs to exact hardware components because of the need to ensure authenticity of data generated or to establish the usage of authentic hardware components. In networked environments, hardware association might be used to establish suggestion back. However, virtualization might make such association hard to establish.

VI. CONCLUSION

In today's world of internet, cloud computing technology is one of those technologies which is widely used all around the globe. The following survey focused basically on the security mechanism used in the cloud for storing databases and its issues to overcome the issues in privacy and untrusted authorization. And the proposed ideas can be used and implemented to make the cloud more secure and the best place for everyone to store data on.

REFERENCES

[1] Jose N, & Kanmani C. (2013, April). Data Security Model Enhancement in Cloud Environment Retrived April 9, 2017, from http://www.iosrjournals.org/iosr-jce/papers/Vol10-issue2/A01020106.pdf

[2] Bansoda, A., & Singh, M. (2015, January 01). Implementation of Cloud storage Security Echanism using Digital Signature .Retrieved ,April 5, 2017, from https://www.ijarcsse.com/docs/papers/Volume_5/1_January2015/V5I1-0365.pdf

[3] Muthuranjan,V.,&Narayanasamy,B.(2015,December). An Elliptic Curve Based Schnorr Cloud Security Model in Disributed Environment Retrived April 3, 2017, from https://www.hindawi.com/journals/tswj/2016/4913015/

[4] Srinivasamurhty, S,. & Liu, D. Q. (n.d.). Survey on Cloud Computing Security. Retrieved from http://salsahpc.indiana.edu/CloudCom2010/Poster/cloudcom2010_submission_67.pdf

[5] Bhadauria, R., & Sanyal, S. (n.d.). Survey on Security Issues in Cloud Computing and Associated Mitigation Techniques . Retrieved from https://arxiv.org/ftp/arxiv/papers/1204/1204.0764.pdf

[6] Kaur, M., & Singh, H. (2015.June.). A Review Of Cloud Computing Security Issues. Retrieved from http://www.ijaet.org/media/17I27-IJAET0827796-v8-iss3-397-403.pdf

[7] Singh, J., & Sharma, S. (n.d.). Review on Cloud Computing Security Issues and Encryption Techniques. Retrieved from https://www.ijedr.org/papers/IJEDR1502181.pdf
[8] Pal, G., Barala, K. K., & Kumar, M. (2014, September). A Review Paper on Cloud Computing. Retrieved from http://www.ijraset.com/fileserve.php?FID=963
[9] https://docs.cloudfoundry.org/devguide/deploy-apps/deploy-app.html