Web and Network Security For Cloud

Nayan Shivhare
Northern Arizona University
Flagstaff,AZ,USA
ns977@nau.edu

***Abstract*—Cloud computing has a different meaning to different people. It is one of the biggest revolutions in terms of computing services and how we access them. Cloud is growing rapidly from the industrial field to the education field. With the increase in cloud usage, there is also an increase in security attacks which is one of the major issues. Many cloud providers overlooked security threats of the cloud due to the security cost associated with its prevention. This paper discusses different security issues and countermeasures to secure cloud services and cloud models. This paper is the best introduction to the cloud for a researcher or student who is new to the existing field of cloud.**

***Index Terms*—Network, Cloud, Iaas, Saas, PaaS, SA,RSA, DDoS, SQLI**

I. Introduction

What cloud computing is? Cloud computing is providing computing resources-servers, data storage, and software over the internet on-demand. Cloud is also one of the growing computing fields due to the on-demand, reliable, cheap, and flexible computing resource it provides [20]. There are many definitions proposed by the National Institute of Standards and Technology, USA. However, we define "cloud computing as a way to utilize computing resources or IT services on-demand through the Internet". With the increase in the use of the cloud, there is also an increase in its security threats [27], which creates a problem for developers and cloud providers to make the cloud more secure. Over the past decade, many types of cybercrime have been linked to security breaches. With the rapid growth of the Cloud, there comes security and privacy issue that is associated with the cloud computing. When a user is using a cloud-based service he is trusting a third-party service to protect and secure his data against cybercrimes. However, there are some web standards which cover the generic aspect of cloud security such as confidentiality, authentication, and integrity but no one address majors issues such as DDoS attacks, DoS attack or HX-DoS attack [31]. And with the rapid growth and providing resources through web services cloud becomes more vulnerable to the HTTP Denial of Service or XML-Based Denial of service. The advancement of cybersecurity plays an important role in information technology and services [28]. In this paper, we will also focus on what are the crucial security issues associated with the cloud and ways to mitigate them. We will also cover CSQD(Cloud Service Queuing Defender) to detect and mitigate XML vulnerabilities in web services. Fig 1 [13] is presenting the security report of core security issue of cloud DoS [25] attack with the expected growth.

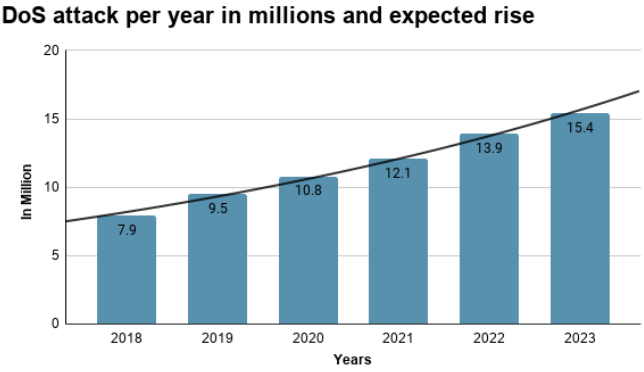

Fig. 1. Security Attacks and expected growth

II. Background

Cloud computing is a term that is being overused and applied to everything in the computational world. In the Centennial of 1961 at MIT, John McCarthy said "The computer utility could become the basis of a new and important industry" that clearly represent the basic foundation of the cloud. However, "cloud computing" used in modern days was first presented by Google CEO Eric Schmidt at the industry conference [29].Cloud computing provides different cloud and service models.

A. Types of Cloud Models:-

Cloud models are basically divided into four group according to the usage,security and utilization purpose and it can be described as follows:-

- Public Cloud
- Private Cloud
- Hybrid Cloud
- Community Cloud

1) Public Cloud: The public cloud is the cloud data center that is made for the general public or companies so that everyone can use its services on-demand via the internet. [21] Examples of top public cloud providers- Amazon, Azure, Microsoft, Google. Scalability and resource sharing was made possible by the decentralized cloud, which would not have been possible for a single company. Public clouds are less secured than other cloud models because not all data or resources available on the public clouds are subjected to be

under malicious attacks. Therefore the security of the public cloud is a major concern.

2) Private Cloud: The private cloud is the cloud model which is used within the organization or offices for their private usage- NAU Monsoon Cloud. It is a computing model that provides a unique environment for a single business unit. Similar to other types of cloud computing environments. Private clouds provide a wide range of virtualized computing resources through physical components stored in local or vendor data centers. One of the main benefits of private cloud deployments is the increased level of control provided to your computational process. Private cloud policies configured with hardware locally hosted on a company-owned site or hosted by a cloud service provider. [20] Virtual private cloud is paid on an ongoing basis, and it managed by service providers. It gives benefits to hardware management, data storage, and system configuration. It also provides a secure and exclusive network.

3) Hybrid Cloud: A hybrid cloud is a combination of public and private clouds. It provides a single environment that runs on private, public, and local clouds. In Hybrid Cloud private cloud can use resources from the public cloud whenever it needs scalability. [3] It is a cloud storage environment that orchestrates these frameworks by integrating on-premises public and private cloud services. The hybrid cloud model enables companies to implement workloads in either private or public clouds and turn back and forth according to needs and costs shift. This offers companies more flexibility and choices when it comes to data migration. Data and applications over the hybrid cloud provide more secure control of data and applications as compared to public cloud.

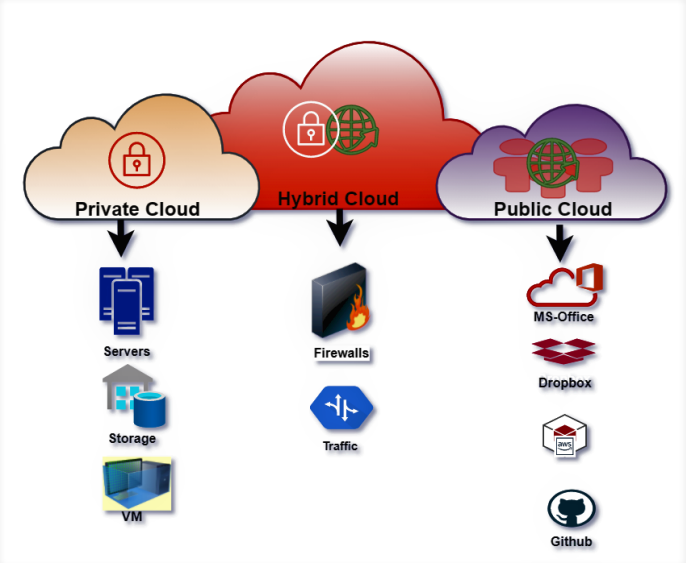

Fig. 2. Cloud models

4) Community Cloud:: A Community cloud refers to a shared computing service environment. It provides services to a small number of companies or employees (such as bank or company executives).The organization of groups varies, but group members usually have common protection, privacy, efficiency, and enforcement criteria.Members of the group handle service (rather than only dependent on the provider) to examine who wishes to join the community. A community cloud is a hybrid form of a private cloud.

B. Types of Cloud services:

Cloud services are divided into three major category according to the service they provide to the user or organization that are described as follows:-

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

1) Software as a Service(SaaS): Software as a service or software on demand is a cloud service that can provide software or applications via the Internet in a prepaid or pay-per-use manner. In SaaS, users can access the software through the Internet without installation and maintenance, thus eliminating the need for complicated software and equipment administrators. SaaS also referred to as web-based software or on-demand software. The application in SaaS runs on the environment provided by the service provider, and the service provider supervises the access of the application, including security, accessibility, and execution.

2) Platform as a Service: Paas is a cloud service that provides on-demand resources, infrastructure, and databases based on pay as you use basis which can be used over the internet. In the PaaS model, customers rent the resources needed to develop applications based on their needs. This is one of the three cloud service models of distributed computing that provides a framework. From the user's point of view, PaaS has infinitely improved the development of web applications. It provides middleware that can help with deployment and development it enables developers to easily develop, test, run and deploy web applications. In PaaS, back-end adaptability is managed by the cloud providers, end-clients don't have to stress over dealing with the framework. PaaS combines the foundation (labor, inventory, and system management) and stages (middleware, upgrade equipment, data set management framework, and business insight) that help in managing the web application progress cycle. That's just the beginning of PaaS.

3) Infrastructure as a Service (IaaS): Infrastructure as a Service (IaaS) is a cloud infrastructure service in which businesses rent or lease servers for different computing resources according to need. IaaS integrates infrastructure on the general public cloud and personal cloud rather than in an outdated on-premises data center. It's a service in which companies rent resources for processing and storage data in the cloud. Users can run operating systems or software in the environment provided by infrastructure as a service without having to think about the maintenance and operating costs of these servers. Cloud service providers are responsible for providing security and maintaining hardware. Other benefits of IaaS include providing clients with connections to servers in any regional area. IaaS automatically scales up and down based on demand

requirements from the customer and delivers a stable service-level agreement (SLA) in terms of time and efficiency. It removes the need for data centers and servers to handle it physically.
Fig. 3 represent different types of cloud services.

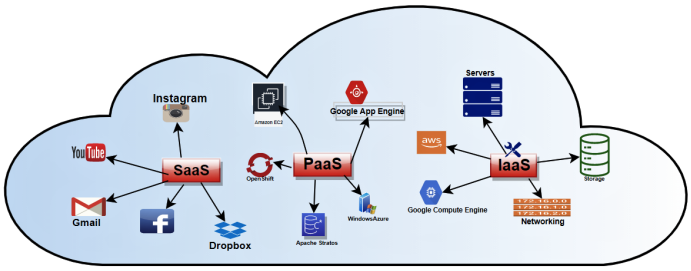

Fig. 3. Types of Cloud services

III. Major Security Issues in Cloud Computing

Cloud computing has different security issues due to SOA(Service Oriented Architecture) and resource it provide over the internet [30]. Some of the major security issues are described below:-

A. DDoS attack:

Distributed Denial of Service attack is an attack that impedes an online service by flooding it with traffic from multiple networks. They attack a wide range of essential public services, from banks to news services, which presents a severe challenge to the public and makes service unavailable for the user to access. [8] It can be mitigated using Cloud Defender System(CSQD) which we will be discussing in our next section [30]

B. Denial of Service(DoS) attack:

A DoS attack is a type of attack that makes the cloud system unavailable for the new request by flooding the cloud system so it stops responding to new requests. [30] Network bandwidth or connectivity is common targets of attackers.There are some major DoS attacks on Cloud such as:-

1) Denial of Service attacks on software as a service(SaaS): - Denial of Service attacks on applications focuses on SaaS, by exploiting loopholes in the applications and hold back users to have legal access to services.These attacks are difficult to detect and track back, existing monitoring systems are not sufficient to detect them. [25] HTTP and HTTPS protocols are being used by these attacks and they use proxy servers to complicate the attack which makes it difficult to detect the origin of cyber criminals who attacking the server.

2) DoS attacks on Infrastructure as a service(IaaS): - Energy-oriented Denial of Service Attacks is considered as an emerging big threat to cloud Infrastructures energy-oriented DOS attacks is the type of attack that make cloud infrastructure and data centers consume as much energy as possible. This attack increase of workloads on the system which keeps them running and it results in higher consumption of energy, increase cost, and penalty due to greenhouse gas that emits from the cloud data centers.

3) DoS XML based attack(X-DoS): - X-Dos or XML-based attacks flood web services with XML messages instead of packets which result's in using all the space or resources that the server has and it results in unabling the web services or system for users. [10] A generic XDoS attack sent an XML message with a large number of digital signatures, and a weak compiler scans each signature and utilizes all CPU cycles, exhausting all resources.

4) Denial of Service HX based attack(HX-DoS): - Cloud services run on HTTP and XML protocols such as Simple Object Access Protocol(SOAP). [1] HX-DoS is one of the major issues that cloud providers deal with, it runs on HTTP and XML protocol. HX-DoS attacks use HTTP and XML protocols to flood the servers of cloud providers.

5) DoS Http based attacks(H-DoS): - This attack is based on cloud networking infrastructure and it is a major threat to web-based applications. [11] With the help of attack browser software, attackers bypass network proxy restrictions and execute an H-DoS attack on the webserver. And, due to the hidden information of the attackers, the webserver is unable to detect malicious client attacks by web proxy server [2].

6) DoS SYN flood attacks: - SYN flood is the type of DoS attack in which it targets the web servers. These attacks occur when the attacker sends a stream of TCP/SYN packets to the victim's device by using a false sender's address. All request is treated as a connection request, which leaves communication server half-opened. While victims transmit TCP/SYN-ACK packets and wait for the attacker's response which never comes. [5] All the half-open connections make the TCP queue full because the server must keep the queue open for 75s and it results in rejecting the connection request because no new connection can be accepted. Fig 4 represents DoS SYN Flood attack.

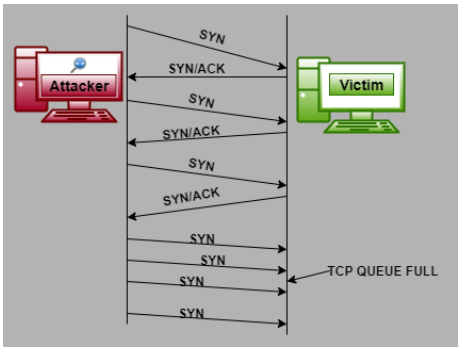

Fig. 4. DoS SYN Flood Attack

C. Man-in-the-Middle Cryptographic Attack:

The attacker intercepts messages in a public key exchange and retransmits them,substituting his own public key for the requested one, so that the two original parties seem to be communicating normally in the process. [32] However, the

TABLE I
DIFFERENT TYPES OF MITM ATTACKS

Types of MITM	Definition
ARP Communication	In standard ARP communication, the host PC sends a packet containing the source and destination IP addresses broadcasts it to all network-connected computers. The computer with the target IP address can only give the ARP the response which contains a MAC address, after which contact is made. The ARP the protocol is not a secured protocol and the ARP cache doesn't have a foolproof mechanism which results in a big problem
ARP Cache Poisoning	The attacker will sniff into the network by manipulating the network switch to track network traffic and fake the ARP packets between the host and the target PC, then execute the MIM attack.
DNS Spoofing	This is a type of online MIM attack in which the attacker has created a fake website for your bank, so that when you visit your bank's website, you are routed to the attacker's website, where the the attacker obtains all of your credentials.

message sender is unaware that the recipient is an anonymous intruder attempting to view or alter the message before retransmitting it.As a result, the intruder has complete control over the communication.Types of Man-in-the-Middle attacks- Address Resolution Protocol Communication, ARP Cache Poisoning,DNS Spoofing, and Session Hijacking. Table 1 describes all types of Man-in-the-Middle attacks.

D. Cloud Malware Injection Attack:

Cloud Malware injection attacks are carried out in order to gain access to user's sensitive information in the cloud. [12] An infected service deployment module is injected into a SaaS, PaaS, or a virtual machine instance for an IaaS service. If the cloud system is successfully exploited, it will redirect cloud users' requests to the malicious instance, resulting in the execution of malicious code. The hacker will then continue their malicious operation, such as data manipulation, theft, or eavesdropping. Cross-site scripting and SQL injection attacks are the most common types of cloud malware injection attacks.

E. SQL Injection Attacks:

SQL injection, also known as SQLI, [19] stands as Structured Query Language. Query languages are the programming languages that are being used to get the required information from databases. [17] It is a popular attack vector and it uses malicious SQL code to exploit backend databases. The attacker enters malicious commands in the login page, search bar, or URL location that result in affecting CIA (Confidentiality, Integrity and Availability) and it gives access to information that was not meant to be displayed. This information may include confidential business records, user lists, private customer information, passwords, etc. [8] A simple way an attacker can perform an SQLi attack is by changing a query and adding a condition of "OR 1=1".In fig 4 is the snippet of PHP code to create a dynamic query in response to user input. When an attacker uses a query attack in the login form he will be using OR operator to get the username and use the statement operator which will ignore the password. However different attackers can use different queries according to their motive behind the code. An example of one is presented in fig 7.

In fig 5 PHP script for login has been created.

```
//connecting to database
mysql_connect(servername,username,password);

//Collected user input from login form
$username=$_POST[username];
$password=$_POST[password];

//dynamically building the query from the user input
$query="SELECT"FROM the_users WHERE username="$username"
AND password="$password"

//execute a query $result-mysql_query($query);
If($result) return true;
else return false;
```

Fig. 5. PHP script for login form

In fig 6 sql query has been generated.

```
//Sql query result of the above code
SELECT *FROM tbl users
WHERE username='user_Name
AND PASSWORD='pwd';
```

Fig. 6. Sql query for script generated

In fig 7 we are using query attack by writing query using OR operator for the login form.

```
SELECT *FROM tbl users
WHERE username='user_Name' OR 1=1
AND password='Whatever'
```

Fig. 7. Query attack for login form

F. Cross-site scripting attack(XSS):

This is the type of attack in which malicious scripts are injected into trusted websites. [10] When a user enters the correct URL Sites and hackers redirect users to malicious attack sites. This problem is getting worse due to AJAX-(asynchronous JavaScript and XML) that improves user's experience but complicates the security part and creates loopholes. [24]. From the address URL, the attacker redirects users to a malicious URL. It results in collecting sensitive information and user credentials.

G. Side-Channel Attack:

An attacker attempts to penetrate the cloud infrastructure by initiating a side-channel attack, the attacker places a malicious virtual machine near a target cloud server system. Side-channel attacks have emerged as a type of successful security threat aimed at cryptographic algorithm implementation in systems. [4] Evaluating the durability of cryptographic systems to side-channel attacks is therefore critical for safe system architectures.Side-channel attacks are carried out in two steps:

VM CO-Residence and Placement. An attacker puts his instance on the same physical computer as a target instance; a malicious instance has the ability to use side channels to learn information about co-resident instances. Since obtaining confidential information from a computer can be very simple, protection against side-channel attacks becomes very important.

H. Multi-tenancy issue:

Virtualization + Resource Sharing = Multi-Tenancy
In multi-tenancy is a type of cloud computing in which more than one user shares a pool of resources in the same environment at the same time. [6] Multi-tenancy presents a great risk of one user or tenant getting access to neighbor's data.It can be due to computational error that the data is returning to the wrong user or it can be one user affecting other tenants in resource sharing. [14] All these security challenges can be used for attack by attackers or anyone looking for personal gain.

IV. Countermeasure and Detection Technique for Cloud Security Issues

This section will discuss about the security risk in cloud computing. There are some framework and countermeasure presented by different researcher to provide security and detection methods. [26]

A. PALM live migration framework

PALM is a live migration framework and it is based on Xen and GNU Linux. In the migration of VM, it guarantees that the security strength is not degraded during and after migration. He proposed three modules- privacy and Integrity protection of sensitive data, metadata, and migration process. [34] When using the prototype it shows the downtime in performance however it was due to encryption and decryption of data but it successfully secure the VM during migration.

B. Virtual network VNSS

For providing security for virtual network VNSS [33] proposed a framework that provides security for each virtual machine. It ensures continuous security for virtual machine live migration. They built a prototype framework using Xen hypervisors and firewall technologies, as well as user-space applications like iptables, XM commands, and conntrack-tools. The authors performed several tests to determine their framework, and the findings showed that security policies remain in effect throughout.

C. AMAD for IaaS

AMAD(Abusive Migration Attack Detection).It is a framework design to detect the existence of malicious VM migration attacks and point out the origin of the attack. It gathers resource utilization metrics at the hypervisor level and can run without any help from the running VM. [23]

D. Security of XML-based DDoS attack

XDetector is a distributed defense filter that filters and monitors DDoS threats such as HTTP and XML DDoS. It employs a service-oriented trackback mark that includes a proxy it tags incoming packets with the source message identity, resulting in the separation between true and false clients. For countering the HTTP or XML-based DDoS attack filtering tree is a solution introduces by [22]. He proposes a filtering tree approach to protect against HTTP or XML-based DDoS attacks, which acts as a service broker within an SOA model. To guard against these forms of threats, it translates the client's request to XML tree form and implements a virtual cloud protector. The cloud defender is responsible in this framework for detecting malicious messages, detecting HTTP DDoS attacks, and detecting intrusive parsing XML DDoS.

E. Cloud Service Queuing Defender System(CSQD)

In this [30] paper author developed a CSQD a defender system for detecting and mitigating XML vulnerabilities in web services. It uses a trackback solution for discovering the origin of the attack and CSQD is a self-learner system that can learn from the attack if the attack brings down the server. It uses three databases and one internal data store for architecture-

- Blacklist database:- All the IP address that needs to be blocked.
- Poison Request database:- The database used to record discovered attack
- Time-consuming parts:- In this database admin enters the details manually and it contains two names and URLs.
- Request list:- Its an internal data store which keeps track of incoming request. Every element in the data consists of five attributes IP address, content, requested URL, ID, and date.

When CSQD implemented against different types of XML attacks, a Windows Framework Communication(WCF) is being developed in c to bring up different web services. When the system is deployed it's being observed that as the number of requests increases the overhead and overhead depends on buffer size, response time, and waiting time. However,it acheived the main goal and CSQD is effective and efficient in detecting and countering most DoS attacks.

F. Advanced Encryption Standard and SSL

Encryption plays an important role in ensuring stored data is secured over the cloud. It is true that encrypted algorithms are strong and robust. A well-known encryption scheme is Advanced Encryption Standard. For transmitting the data SSL can also be used for [9] protecting the data and ensuring security. Encrypting your data can also helps in protecting against side-channel attacks.

G. Securing system against SYN flooding attack

A solution designed to protect against SYN flooding attack is based on network and end-point based solution. Network based solution can prevent the attack by forwading request

only after client side ACK is received. Network based solution are Firewall proxies. End point based solution includes SYN cookies and SYN caches that will allocate full state of memory only after client's ACK request recieved which can protect flooding of queue. In [15] author presented solution for protecting against TCP SYN flooding:-

- Changing the algorithm and data structure that is used for connection establishment and lookup, also making end-host TCP implementation robust.
- filtering out the packets using network level defence technique described in RFC 2827.
- Use of ingress filtering in which ISP deny route packets coming from end site whose IP source address do not match.
- Using firewall and proxies that can protect against SYN flooding by spoofing SYN-ACKs to the initiators.

H. MapReduce Operation

In paper [11] auhtor presented MapReduce method for HTTP GET flooding detection, in Mapreduce method suspected IP by DDoS attack is replied with challenge values, which result in filtering of IP by allowing IP who is giving normal response.MapReduce operation uses checking of large HTTP request and depletion of TCP connection.This detection method of DDoS packet use input values of MapReduce using statistical analysis and threshold.

I. Securing again MITM Attack

Using a virtual private network is one of the most effective techniques against MITM. It masks the IP address by returning the IP address through a dedicated server. Mutual authentication can also protect against MITM. However, due to a large number of clients and server implementation, the initial trust between client and server is confirmed using one-way verification. Through mutual authentication [12], the server can verify the client, and the client can verify the server to ensure that the communication through the connection is legitimate. For verification, a private key and a public key can be used.

V. OPEN CHALLENGES AND FUTURE WORK:

This section will discuss about open challenges that researcher and security expert are trying to deal with. It's not only vulnerable according to the security expert but also create a loop hole in security for Cloud computing which present a bigger challenge for cloud service providers.
Most recent and growing challenge is Multi-Tenancy that presents an unsolved security risk that can be minimized but can not be eliminated because it provides resource sharing of the same physical machine to different tenants and its security can not be mitigated through traditional security measures. [7] Both victim and attacker use the same resources provided by the cloud service provider, without knowing about the underlying resources. Most security measures are limited to the network layer and they can not secure inside server attacks. Once the attacker achieves Multi-tenancy, he can also perform a side-channel attack. So mitigating multi-tenancy becomes an open challenge for CSP(Cloud Service Provider). However, it can be mitigated to some extent by having a good resource distribution technique.
Encryption of data using a private key over a cloud is also an unsolved challenge because the encrypted file is the deterministic of the encryption key and the original file. Therefore, in order to prevent deduplication of the file it must be encrypted with a private key instead of a public key that is shared by all users of the system. However, most cloud providers do not provide private key encryption methods, because it presents cost-related and key management issues.
Next big challenge is about Account and session hijacking in cloud services that can not be solved completely even after securing cloud services. [18] Account and session hijacking are taking place in most of the cloud service models mainly due to the use of protocols such as TCP/IP or FTP. TCP delivers the packets in a sequence that they are sent and ensures that the packets are delivered in the right order, however, the connection between server and client initiates in a three-way handshake, which uses a full-duplex stream connection between two points using acknowledgment (ACK) packets and sequence number. The TCP session hijacker's aim is to make the client and server unable to share data while faking legitimate packets on both ends that imitate the real packets. It results in, giving control of the session to the attacker. However most of the cloud service provider still do uses SSL that can make this attack less likely to take place.

Well open challenges in cloud not stops at Multi-tenancy, Encryption and session hijacking.Data breaches are also one of the most concerning and growing security risk organization is focusing on because failure to deal with data through encryption. It opens cloud providers for big risk such as-penalties, fines, customer trust. So protecting customer data becomes one of the most important despite what the Service level Agreement says.

This paper provides an overview of the Cloud Computing Services for a person who is new to pre-existing cloud platform or for a researcher who needs to get an overview of cloud security. Paper explains IaaS, SaaS, and PaaS, cloud models, and their security measures. It also explains the major security attack on cloud platforms with solutions to mitigate it. However, this paper can be extended by getting hands-on experience by creating a robust Reference Architecture (RA)a [16] tool that can be used to build complex systems, which many software vendors use it for development. Security is the basic issue in the cloud, and Security Reference Architecture(SRA) is the conceptual model for cloud security systems that specifies security requirements. By considering all the cloud vulnerabilities and loopholes discussed in this paper, having a robust SRA can enhance security in an efficient, and practical way.

VI. Conclusion

Cloud computing is a growing computational field that has been introduced in the business environment where big or small businesses, organizations, and industries can rent or buy computing resources for on-demand requirements at the minimum price. Cloud provides scaling of the resources as per-use, it can be scaled up and down as required. SaaS, PaaS, and IaaS are the three most important cloud computing models which provide flexible, scalable, reliable- infrastructure and services on a pay-as-per-use basis; however various benefits of cloud computing are obvious, so the security risks. Cloud security has become one of the main key factors among cloud providers. Cloud providers are mainly concerned with the additional hardware capacity connected to the cloud, which can handle downtime in the network without effective user performance by overlooking the security aspects due to the cost involved in maintaining it. Security of cloud still remains the debatable area of research due to unanswered questions of the researcher by a cloud provider in the name of security privacy and policies. In This paper we presented major security issues such as DoS, SQLi which still remains the core issue for the cloud service providers, and with security issues paper also covers countermeasures,open challenges and frameworks such as PALM, CSQD, AMAD to mitigate security risk.

References

[1] Detecting and Mitigating HX-DoS Attacks against Cloud Web Services, author=Chonka, Ashley and Abawajy, Jemal, booktitle=2012 15th International Conference on Network-Based Information Systems, pages=429–434, year=2012, organization=IEEE, address=Melbourne, VIC, Australia.

[2] Detection of Malicious Client-Based HTTP/DoS Attack on Web Server, author=Jayan, Dhanya and Babu, Pretty, journal=International Journal of Science and Research (IJSR), volume=3, number=7, year=2014.

[3] Hybrid Cloud Computing Platform: The Next Generation IT Backbone for Smart Grid, author=Luo, Fengji and Dong, Zhao Yang and Chen, Yingying and Xu, Yan and Meng, Ke and Wong, Kit Po, booktitle=2012 IEEE Power and Energy Society General Meeting, pages=1–7, year=2012, organization=IEEE, address=San Diego, CA, USA.

[4] Security against Side Channel Attack in Cloud Computing, author=Sevak, Bhrugu, journal=International journal of engineering and advanced technology (IJEAT), volume=2, number=2, pages=183, year=2013, publisher=Citeseer,.

[5] Abdulaziz Aborujilah, Mohd Nazri Ismail, and Shahrulniza Musa. Detecting Tcp Syn Based Flooding Attacks by Analyzing Cpu and Network Resources Performance. In *2014 3rd International Conference on Advanced Computer Science Applications and Technologies*, pages 157–161, Amman, Jordan, 2014. IEEE.

[6] Mohamed Almorsy, John Grundy, and Ingo Müller. An Analysis of the Cloud Computing Security Problem. *arXiv preprint arXiv:1609.01107*, 2016.

[7] Afkham Azeez, Srinath Perera, Dimuthu Gamage, Ruwan Linton, Prabath Siriwardana, Dimuthu Leelaratne, Sanjiva Weerawarana, and Paul Fremantle. Multi-tenant SOA Middleware for Cloud Computing. In *2010 IEEE 3rd international conference on cloud computing*, pages 458–465, Miami, FL, USA, 2010. IEEE.

[8] S. Basu, A. Bardhan, K. Gupta, P. Saha, M. Pal, M. Bose, K. Basu, S. Chaudhury, and P. Sarkar. Cloud Computing Security Challenges Solutions-A Survey. In *2018 IEEE 8th Annual Computing and Communication Workshop and Conference (CCWC)*, pages 347–356, Las Vegas, NV, USA, Jan 2018.

[9] Adam Bates, Joe Pletcher, Tyler Nichols, Braden Hollembaek, Dave Tian, Kevin R.B. Butler, and Abdulrahman Alkhelaifi. Securing SSL Certificate Verification through Dynamic Linking. In *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, CCS '14, pages 394—-405, Scottsdale, Arizona, USA, November 2014. Association for Computing Machinery.

[10] Stefano Calzavara, Riccardo Focardi, Marco Squarcina, and Mauro Tempesta. Surviving the Web: A Journey into Web Session Security. *ACM Computing Surveys*, 50(1), mar 2017.

[11] Junho Choi, Chang Choi, Byeongkyu Ko, Dongjin Choi, and Pankoo Kim. Detecting Web Based DDoS Attack using MapReduce Operations in Cloud Computing Environment. *J. Internet Serv. Inf. Secur.*, 3(3/4):28–37, 2013.

[12] Priyanka Chouhan and Rajendra Singh. Security Attacks on Cloud Computing with Possible Solution. *International Journal of Advanced Research in Computer Science and Software Engineering*, 6(1), 2016.

[13] Cisco". Cisco Annual Internet Report (2018–2023) White Paper, 03 2020.

[14] Tharam Dillon, Chen Wu, and Elizabeth Chang. Cloud Computing: Issues and Challenges. In *2010 24th IEEE international conference on advanced information networking and applications*, pages 27–33, Perth, WA, Australia, 2010. Ieee.

[15] Wesley M Eddy. Defenses against tcp syn flooding attacks. *The Internet Protocol Journal*, 9(4):2–16, 2006.

[16] Eduardo B Fernandez, Raul Monge, and Keiko Hashizume. Building a Security Reference Architecture For Cloud Systems. *Requirements Engineering*, 21(2):225–249, 2016.

[17] J. Fonseca, N. Seixas, M. Vieira, and H. Madeira. Analysis of Field Data on Web Security Vulnerabilities. *IEEE Transactions on Dependable and Secure Computing*, 11(2):89–100, 2014.

[18] Bernd Grobauer, Tobias Walloschek, and Elmar Stocker. Understanding Cloud Computing Vulnerabilities. *IEEE Security Privacy*, 9(2):50–57, 2011.

[19] Md Fazlul Haque, Mohammad Badrul Alam Miah, and Fuyad Al Masud. Enhancement of Web Security Against External Attack. *European Scientific Journal May*, 2017.

[20] Ahtisham Hashmi, Aarushi Ranjan, and Abhineet Anand. Security and Compliance Management in Cloud Computing. *International Journal of Advanced Studies in Computers, Science and Engineering*, 7(1):47–54, 2018.

[21] Yashpalsinh Jadeja and Kirit Modi. Cloud Computing-Concepts, Architecture and Challenges. In *2012 International Conference on Computing, Electronics and Electrical Technologies (ICCEET)*, pages 877–880, Kherva,Gujrat,India, 2012. IEEE.

[22] Tarun Karnwal, T. Sivakumar, and G. Aghila. A Comber Approach to Protect Cloud Computing against XML DDoS and HTTP DDoS attack. In *2012 IEEE Students' Conference on Electrical, Electronics and Computer Science*, pages 1–5, Bhopal, India, 2012.

[23] Kahina Lazri, Sylvie Laniepce, Haiming Zheng, and Jalel Ben-Othman. AMAD: Resource Consumption Profile-Aware Attack Detection in IaaS Cloud. In *2014 IEEE/ACM 7th International Conference on Utility and Cloud Computing*, pages 379–386, London, UK, 2014.

[24] Xiaowei Li and Yuan Xue. A Survey on Web Application Security. *Nashville, TN USA*, 25(5):1–14, 2011.

[25] Mohammad Masdari and Marzie Jalali. A Survey and Taxonomy of DoS Attacks in Cloud Computing. *Security and Communication Networks*, 9(16):3724–3751, 2016.

[26] Derek Mohammed. Security in Cloud Computing: An Analysis of Key Drivers and Constraints. *Information Security Journal: A Global Perspective*, 20(3):123–127, 2011.

[27] Masayuki Okuhara, Tetsuo Shiozaki, and Takuya Suzuki. Security Architecture for Cloud Computing. *Fujitsu Sci. Tech. J*, 46(4):397–402, 2010.

[28] Kumar Patel and Antonina Alabisi. Cloud Computing Security Risks: Identification and Assessment. *The Journal of New Business Ideas Trends*, 17(2):11–19, 2019.

[29] V Rajaraman. Cloud computing. *Resonance*, 19(3):242–258, 2014.

[30] Reza Manouchehri Sarhadi and Vahid Ghafori. New Approach to Mitigate XML-DOS and HTTP-DOS Attacks for Cloud Computing. *International Journal of Computer Applications*, 72(16), June 2013.

[31] Shubhanjali Sharma, Garima Gupta, and PR Laxmi. A Survey on Cloud Security Issues and Techniques. *arXiv preprint arXiv:1403.5627*, 2014.

[32] A. Tripathi and A. Mishra. Cloud Computing Security Considerations. In *2011 IEEE International Conference on Signal Processing, Communications and Computing (ICSPCC)*, pages 1–5, Sep. 2011.

[33] Gao Xiaopeng, Wang Sumei, and Chen Xianqin. VNSS: A Network Security Sandbox for Virtual Computing Environment. In *2010 IEEE Youth Conference on Information, Computing and Telecommunications*, pages 395–398, Beijing, China, 2010.

[34] Fengzhe Zhang, Yijian Huang, Huihong Wang, Haibo Chen, and Binyu Zang. PALM: Security Preserving VM Live Migration for Systems with VMM-enforced Protection. In *2008 Third Asia-Pacific Trusted Infrastructure Technologies Conference*, pages 9–18, Wuhan, China, 2008.