A Survey of Security Issues and Attacks in Cloud and their Possible Defenses

Aaqib Iqbal Wani
M.tech, Department of Computer Science and Engineering, SMVD University, Katra, India

Zubair Ahmad Lone
M.tech, Department of Computer Science and Engineering, SMVD University, Katra, India

Abstract – Cloud computing has emerged as one of the most popular and powerful technologies over the last decade. It has laid the basis for conceptual and infrastructural computing of the future. Organizations are moving their business to the cloud and taking advantage of the power of cloud-based computing, however, security remains of core interest and because of which many organizations are avoiding migration to the cloud. With the introduction of numerous cloud services and geographically diverse service providers, sensitive information is stored at different physical locations, elevating the threat of being compromised. If the security issues are not a concern, cloud computing can become an even huger success. Continuous research is being done to make the cloud computing paradigm a safe and secure environment and expand the services to a greater number of users. In this paper, we discuss the various security and privacy concerns related to the cloud computing environment and provide the related solutions for each problem.

Index Terms – Cloud security, defense, privacy.

1. INTRODUCTION

Cloud computing is the delivery of on-demand resources like hardware, storage, networking and software from Cloud Service Providers (CSP) over the Internet to any computer or device as a metered service [1] [2]. A user or several users request one or many kinds of the services offered by the Cloud Service Provider. The only thing the user needs is an interface software which can be as simple as a web browser [2]. The CSP dynamically allocates the resources to the user based on his needs, scaling up and down as the demand increases or decreases and the users are only charged for what they use, known as pay-as-you-go model [2]. This computing solution is growing popularity in small and medium sized companies. This provides a way to increase capacity and add capability without investing in new infrastructure, training new personnel and licensing software.

1.1 Cloud Characteristics

Cloud computing has a few essential characteristics which can be described as [2] [3]:

- On Demand Service: Cloud computing resources like network and storage are provisioned automatically without human intervention when the user needs them. They are not a permanent part of IT infrastructure [2].
- Broad Network Access: All these capabilities of the cloud are available over the network and can be easily accessed using standard protocols that support a variety of devices e.g. laptops, smartphones, desktops, PDAs [2].
- Multitenancy: The resources are pooled so that multiple users can use the cloud services as per individual requirements within the same IT infrastructure [2].
- Elasticity and Scalability: The resources can be dynamically assigned based on the demand. If the demand is high the resources and be expanded and vice versa [2].
- Resiliency: The cloud isolates the failure of resources from the user and automatically migrates the work to a different physical resource in the cloud without any user intervention. The user usually has no knowledge and control over the physical location of the resources.
- Pay per Use: The resources used by the user are monitored and metered as per the usage. The user pays for only what he uses.

1.2 Cloud Deployment Models

The deployment models specify the way in which cloud services can be made available to customers depending upon the structure of the organization and the provisioning location. These deployment models can be categorized as:

- Private Cloud: The Cloud resources are deployed for exclusive use by an organization. The resources may be owned, managed and operated by the organization or by a third party or by both, and may exist on or off premises [2].
- Public Cloud: The Cloud resources are deployed for use by the public, used for B2C (Business to Customer) type interactions. The resources are owned, managed and operated by a business, academic or government organization. It exists on the premises of the Cloud provider [2].

- Community Cloud: The Cloud resources are deployed for a community consisting of several organizations sharing a common goal. The resources may be owned by the organization or a third party and may exist on or off premises [2].
- Hybrid Cloud: The Hybrid Cloud is the combination of two or more Cloud deployment models in which cloud resources are bound together by different clouds. It can be used for both types of interactions B2C and B2B [2].

1.3 Cloud Service Models

The Cloud provides three types of service models. It is also known as the Service Platform Infrastructure (SPI) model of the cloud [4] [5]. These are:

- Software as a Service (SaaS): It is a software distribution model in which software/application hosted by the cloud provider are made available to the customer as a service over the network, typically the internet [2]. The customer is able to use provider's applications running on the cloud infrastructure consisting of networks, servers, storage etc., but with the exception of some user-specific application settings. Traditionally, applications needed to be purchased and licensed and then installed on each computer in order to be used. With SaaS, the users are able to subscribe to the software on a monthly basis. The applications can be accessed through various client devices (laptops, desktops, smartphones etc.) through a web browser or a program interface from anywhere. Examples are Customer Relationship Management CRM software, Google Docs, Salesforce, Office 365 etc.
- Platform as a Service (PaaS): It provides the user usually developers with a platform and environment to build applications and services over the Internet without any downloads or installations [2]. The user is provided with the capability to deploy consumer-created or acquired applications on the cloud infrastructure using programming languages supported by the cloud provider. The user has no control over the underlying infrastructure whatsoever but over the deployed applications and configurations settings for the application-hosting environment. The PaaS vendor manages the levels of scalability and maintenance. The user pays for the services used. Examples are Google App Engine and Microsoft Azure Services.
- Infrastructure as a Service (IaaS): It provides access to computing resources in a virtualized environment over the internet. The user is provided with the capability to provision processing, network, storage and other fundamental computing resources on a pay per use model [2]. The pool of hardware resources provided are extracted from multiple servers and network and distributed across various data centers. This provides redundancy and reliability to IaaS. The user is free to run any software on the hardware resources including operating systems and other applications. The user has no control over the infrastructure but over the OS and deployed applications and partial control over networking components e.g. Firewalls, DHCP server etc. Examples are Amazon Web Services and Rackspace.

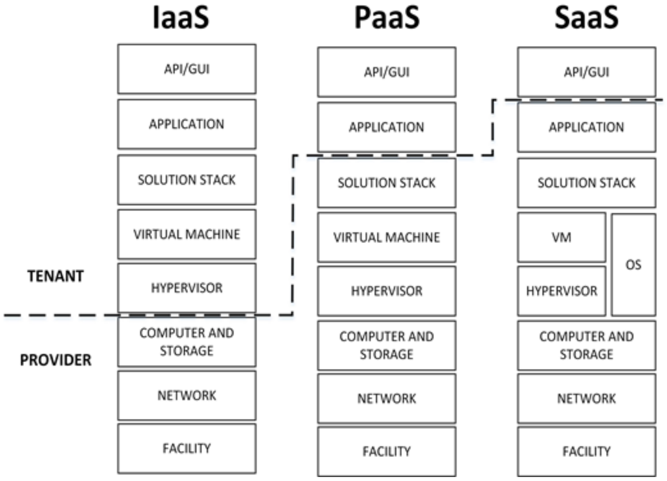

Figure 1 Service Models in Cloud

2. SECURITY ISSUES IN CLOUD

Security is the prime concern in cloud computing right now and this is the main reason that is preventing many organizations from moving their business to the cloud [6] [7]. The organizations use the cloud in a variety of different service models SaaS, PaaS, IaaS and in different deployment models Public, Private, Hybrid, and Community. There are a number of security threats to cloud computing [8] [9] and can be broadly divided into two categories. First, the security issues faced by the cloud providers and second, the issues faced by the customers [10]. Apart from the security issues in the cloud there are various attacks that are possible on the cloud [11]. In this paper, we review the various security issues and attacks in the cloud and classify them based on internal or external security issues and attacks.

3. INTERNAL ISSUES AND ATTACKS

3.1 Data Breaches:

Data breaches can result in the loss of personal and sensitive information and take place during the normal processing and storage of data. The security corresponding to hypervisor operation and virtual machine operations is still not solid.

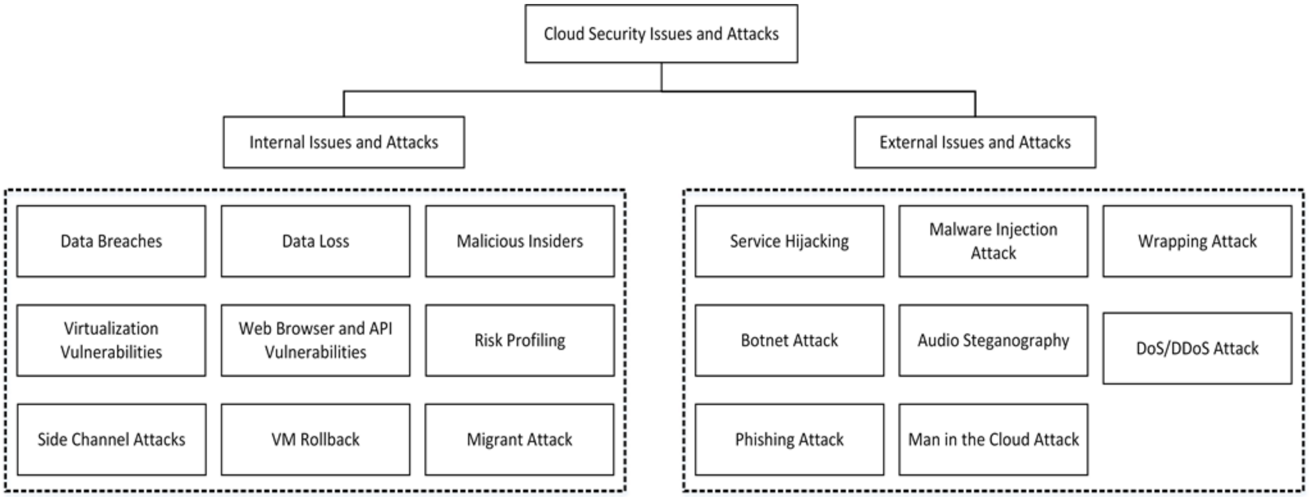

Figure 2 Classification of Security Issues and Attacks

There is a possibility that breaches through hypervisors and virtual machines can happen leaving the organization’s sensitive internal data into the hands of their competitors. Side channel timing information can be used to extract private cryptographic keys being used in other virtual machines on the same physical server [12].

In a multitenant cloud service, if the database is not properly designed, a single flaw in one of the client’s applications can allow an attacker access the client’s data and every other client’s data as well. However, any such advanced techniques have not been used so far but still acts as a hurdle to the enterprise adoption of cloud computing.

The best way to confront data breach is by encrypting the data and using key management practices to protect encryption keys. Encryption protects the data but if the encryption key is lost the whole data is lost [13]. There are three ways to protect keys for encrypted data in the cloud: Store the keys in the house, Store the keys in hosted environment or Store the keys in the cloud. The cloud regularly makes copies of data to prevent data loss due to an unexpected server crashes [14]. But the more copies, the more risk of data breaches. The User ID credentials of customers should be secured and encrypted on the cloud side, the user should also take measures to protect his credentials from falling into the wrong hands [15]. Security architectures like Remote User Multi-Factor should be used to authenticate users [16]. Only authorized personnel should be given access to data for a brief period and the access documented with reasons. The infrastructure should be audited to certifications like SOX and HIPPA.

3.2 Data Loss:

As we discussed data loss can occur as a result of data breach by malicious and intrusive actions of attackers intentionally. However, there can be many other reasons for data loss [15], the owner can encrypt the data before uploading it to the cloud but then lose the encryption key. Data loss can also occur at the cloud service provider’s side, a bug in the cloud service or an accidental deletion by the cloud service provider, or even worse, a physical catastrophe such as a fire or earthquake, can lead to the permanent loss of data unless adequate measures have been taken by the provider to back up all the data.

Data loss can be prevented by replicating data or backing up the data in different physical servers at various locations [14]. The backup can be done periodically or because of a certain event. However, as earlier said having more copies can increase the risk of data breaches. In addition, the data centers where data is to be stored should be free from environmental risks like fire, earthquake, flood etc. [17].

3.3 Malicious Insider:

A malicious insider is a current or former employee or a business partner who has or had authorized access to an organization's network, system, or data [18]. As such he/she can misuse that access to negatively affect the confidentiality, integrity, or availability of the organization's sensitive information. A malicious insider such as a system admin can bypass firewall and IDS and have access to potentially sensitive information in an improperly designed cloud scenario [15].

In the different service models, IaaS, PaaS, and SaaS, the malicious insider has increasing levels of access to more critical systems and eventually to data. A system that depends entirely on the cloud service provider (CSP) for security is at a greater risk of attack. Even if encryption is implemented [13], the keys are to be kept with the customer and should be only available at usage time or else the system can still be vulnerable to malicious insider attacks [15].

The approach to this problem is to keep the encryption keys on premises outside the cloud. The proper background check of employees should be done before hiring them and proper guidance should be given to the employees according to a moral code of conduct. Segregation of duties should be done, and only authorized users should be allowed to access data, restricting other users. The access to data by employees should be documented with reasons.

3.4 Virtualization Vulnerabilities:

Virtualization is the main component of cloud computing architecture and a major security risk. The task of virtualization is to isolate different instances on the same physical server and the control of administrator on the host and guest OS's. However, many bugs have been found in the Hypervisor or Virtual Machine Monitors (VMM) that allow escaping from a Virtual Machine [19] [20] [21]. Three types of virtualizations are used: OS level virtualization, application based virtualization and Hypervisor based virtualization. Vulnerabilities are found in all virtualization software that can be used by malicious or local users to bypass security restrictions and gain privileges. In OS level virtualization where multiple guest OS's are running on a host OS, an attacker can take control of the entire guest OS's by compromising the host OS [22] [23]. In application based virtualization where virtualization is enabled on the top layer of the host OS, each VM has its own guest OS and related applications. This type of virtualization suffers from the same vulnerability as OS based virtualization [23]. In Hypervisor based virtualization, the code is embedded to the host OS which is available at boot time to control guest OS's. The code can, however, suffer from bugs and native errors which can allow an attacker to compromise the hypervisor and consequently all the guest OS's [23].

The vulnerabilities in virtualization can allow an attacker to perform attacks like cross-VM side-channel and DoS attacks. BLUEPILL [24], SubVirt [25], and DKSM [26] are examples of attacks on the virtual layer. Through these attacks, hackers can modify the VMM and gain unauthorized access to the host. To reduce such attacks strong isolation between VMs and inter-user processes should be implemented [27] or NoHype virtualization may be used [28] [29] which removes the virtualization layer and makes the guest VMs runs directly on the hardware without an underlying active hypervisor. Once a VM has started it runs uninterrupted and has direct access to devices [28].

Another technique HyperCoffer can be used. It works by introducing a mechanism called VM-Shim that runs in between a guest VM and the hypervisor. Each VM-Shim instance for a VM runs in a separate protected context and only declassifies necessary information designated by the VM to the hypervisor and external environments [30].

Another technique C2Detector is proposed which detects the channels that leak confidential information. It includes a captor located in the hypervisor and a two-phase synthesis algorithm implemented as Markov and Bayesian detectors [31].

3.5 Web Browser and API Vulnerabilities:

Application Programming Interface (API) is a set of software interfaces (SOAP, REST, HTML) used to offer various services in the cloud through a client software (Web Browser) [32]. The API's, as well as the web browser, suffer from various vulnerabilities that an attacker can take advantage of and adversely affect the cloud system [33]. Some of the problems include weak credentials, insufficient authorization checks, and insufficient input data validation. SSL certificate spoofing attacks, browser cache attacks, SQL injection, Cross Site scripting (XSS), Cross Site Request Forgery (CSRF), Clickjacking and phishing attacks are examples of attacks that can be executed because of Web and API vulnerabilities [18].

To provide a strong layer of security, the API's should be checked for vulnerabilities and the same removed before delivering the services to the user [11]. Internetware, a four-tier framework for web-based development may be a solution [34].

3.6 Risk Profiling:

The user is not involved with the implementation of the hardware and software in the cloud system, this, however, has notable advantages but can pose another security threat for the cloud user. The inadequate awareness of the cloud providers internal security policies, protocols, patching, auditing and logging process may expose the user to serious risks [18].

To reduce this risk, the cloud providers should reveal partial infrastructure details, security software, update and patch procedures, logs and data to the user [35]. In addition, there should also be an Intrusion detection and alerting system [36] [37].

3.7 Side Channel Attacks:

A side-channel attack is an attack based on information gained from the physical implementation of a cryptosystem, rather by brute force or weaknesses in the algorithms e.g. timing information, energy/power consumption [38], electromagnetic leaks or even sound can provide an extra source of information, which can be exploited to break the system. A side channel attack consists of two phases: VM Co-Residence and Placement and VM Extraction. In the first phase, an attacker places a malicious VM in the proximity of the physical location as the target VM, a technique also known as co-location. In VM Extraction, the malicious VM can be used to extract RSA keys by observing how the user accessed information in memory [39] [39]. It is of two types: Timing side channel [40] and Energy side-channel attacks [38]. In the timing side channel attacks is based on the measuring the amount of time it requires for a job to perform whereas in energy side channel attacks energy consumption logs are used [40] [38].

Previously, side channel attacks exploited the L1 cache, however, these are private to every processor core which practically limits the attacker to co-locate multiple owners VM

on the same processor core. Conversely, a new co-location technique that exploits the last-level cache shared between all cores can be used as the new attack vector [41]. Once co-located with a target machine, PRIME+PROBE attack [41] [42], which involves filling a portion of the cache with data and then observing the response of target, can be carried out. Another attack FLUSH+RELOAD monitors access to memory line and the monitored memory line is flushed from the cache hierarchy, the attacker then waits for the victim to access memory line after which the attacker reloads the memory line measuring the time to reload it [43].

Different techniques have been proposed to prevent side-channel attacks [44], HomeAlone that uses a side-channel in the L2 memory cache as a defensive detection tool. [27] and StealthMem that manages a set of locked cache lines per core that never evict from the cache and efficiently multiplex them so that each VM can load its own sensitive data into the locked cache lines [45]. Another technique C2Detector is proposed which works by detecting channels that leak confidential information. It includes a captor located in the hypervisor and a two-phase synthesis algorithm implemented as Markov and Bayesian detectors [31].

3.8 VM Rollback Attacks:

Virtualization is the most volatile part of cloud computing environment and to no surprise can be used to compromise virtual machines by a malicious hypervisor. The hypervisor at any point of time is authorized to suspend a VM during execution, take a snapshot of current CPU states, memory and disk and resume a snapshot afterwards without the knowledge of guest VM. This characteristic of the hypervisor is used mainly for fault tolerance and maintenance, but the attackers have exploited this characteristic of the hypervisor to successfully launch VM rollback attacks [19]. The attackers take advantage of previously taken snapshots and run them without the user’s knowledge. The history is cleared to avoid getting caught and the same or different snapshot can be run again. Example, an attacker could launch a brute force attack to acquire the login password for a VM. Even if the guest OS has a restriction on the number of login attempts and blocks the user after three unsuccessful attempts or erases all the data after 10 times, the attacker can still rollback the VM to its initial state after each attempt by clearing the counter inside the VM and thus bypass restriction on the number of attempts and run the brute-force attack again.

This can be prevented by involving end users during VM booting, suspending and resuming, however it may not be feasible because it requires a lot of user interaction. A better solution to prevent VM rollback named Hyperwall works by disabling the suspend/resume functionality of the hypervisor [46]. However, this is a powerful feature of virtualization and disabling it will do no good. An improvement of the HyperWall [57], Extended-HyperWall architecture is a combination of HyperWall [46] with Rollback Sensitive Data Memory with Architecture Assistance (RSDM-A) [47]. It works by integrating the Confidentiality and Integrity Table to ensure confidentiality and integrity of data and RSDM-table to protect the system from rollback attacks [47].

Other solutions may include NoHype that works by eliminating the hypervisor attack surface by enabling the guest VMs to run directly on the underlying hardware while preserving the ability to run several VMs simultaneously [28]. In other solution, the end user audits the log of VM activities and concludes whether a rollback is malicious or not [48].

3.9 Migrant Attack:

This is a new type of DoS attack that targets the allocation scheme of the cloud to cause damage to users and the cloud. The resource usage of a malicious VM (which the attacker might have rented) are deliberately varied to trigger live migration. Even if the VM's are perfectly isolated, the attack can still affect the availability and degrade the performance of the co-located VM's. The attack can also be used to coordinate with a victim VM or service and result in a chain migration [49].

Not much research has been done on the mitigation of such attack. However, using the conventional method of resource limiting may be used to mitigate the attack or another layer of isolation may be implemented between the malicious VM’s and benign VM’s.

4. EXTERNAL ISSUES AND ATTACKS

4.1 Service Hijacking:

In Service hijacking, attacker deceits a legitimate user to an illegitimate website in order to gain unauthorized access to their accounts [18] thereby monitoring transactions/activities, returning falsified information and manipulating data. Phishing, exploitation of software vulnerabilities, fraud, and reused credentials may pose the risk of service hijacking.

Some of the defense techniques to mitigate this threat include security policies, strong authentication, and activity monitoring [50].

4.2 Malware Injection Attack:

The attack is carried out by inserting a malicious code as a genuine service in the cloud. The intention can be eavesdropping and include data modifications, creation of deadlocks and changing functionality [6]. The attacker creates a malicious service module or an instance and attaches it to the cloud. The malicious service deceits the cloud system by

Attack	Service Model	Mitigation Techniques
Data Breaches	IaaS PaaS Saas	-Use of Data Backup and Recovery Protocols -Use of SSL encryption -Data Security Protocols -Proper Decommissioning of Hardware -Data Encryption and Secure Storage of Encryption Keys -Data Access Protocols and Audit Logs
Data Loss	IaaS PaaS Saas	-Use of Data Backup and Recovery Protocols -API Security -Data Integrity -Data Access Protocols and Audit Logs
Malicious Insiders	IaaS PaaS Saas	-Proper background check of employees -Identity and Access Management -Data Encryption and Storage of Encryption keys outside of premises -Proper Decommissioning of Hardware -Data Access Protocols and Audit Logs
Virtualization Vulnerabilities	IaaS	-Use of secure Hypervisor -Isolation of Hypervisor -NoHype Virtualization -HyperCoffer -C^2Detector
Web Browser and API Vulnerabilities	SaaS	-API Security -Semantic Access Control Policy Language -CloudProtect -Internetware
Risk Profiling	Iaas PaaS Iaas	-Reveal partial infrastructure and software details, patch procedure and logs -Implement a monitoring and alerting system
Side Channel Attacks	Iaas	-HomeAlone -StealthMem -C^2Detector
VM Rollback Attack	IaaS	-HyperWall/Extended HyperWall -NoHype Virtualization

Table 1 Internal Security Attacks and Issues

pretending to be a new valid service. The attacker then redirects the request of the benign user to the malicious module and achieves access to service rights of the victim with deleteUser and sysadmin rights. The only thing checked when the instance is run is whether the service is a valid service or not, however, no integrity check is done. This attack is also called meta-data spoofing attack.

The attack can be mitigated by performing service integrity checks using File Allocation Table and implementing strong isolation between VMs and inter-user processes [27].

4.3 Wrapping Attack:

In a Wrapping attack, an adversary modifies the signed documents due to limitations in the use XML Signature in order to gain unauthorized access to protected resources [51]. When the user makes a request to the web server from his VM through a web browser, a SOAP message is generated in the web browser and this SOAP message contains the structural information that would be exchanged between a web browser and the server during message passing. The Body of the message contains the operation information and is supposedly signed by a legitimate user. For a wrapping attack, the attacker through simple validation could easily disclose the original SOAP message if the body of the message is included with a new Wrapper element inside the SOAP Header. This is done before the translation of the SOAP message in the Transport Layer. By making use of this privilege, the attacker wraps the entire message in a new header. The wrapper will then contain the original message body, which is the valid request from the user. Now when the validation session will take place, the Bogus elements and its contents will be ignored by the recipient since this header is unknown, but the signature will be acceptable because the element at reference URI equals the value in the wrapper element.

There are ways to detect and prevent an XML Wrapping attack. One of the proposed solutions is the Inline approach, which works by including a SOAP Structure information (SOAP Account) in outgoing SOAP messages and validating this information before policy driven validation in the receiving end. This allows the detection of XML rewriting attacks early in the validation process [52].

The above approach, however, does not discuss the possibility of forging the message structure information itself as such an improved solution was proposed to counter this problem and prevent the integrity of the SOAP account [53]. Another prevention measure can be strengthening the XML Schema declarations for Web services messages [54].

Another detection technique uses node counting. The frequency of each node in web service request is calculated to detect XML signature wrapping attacks [55].

4.4 Botnet Attack (Stepping Stone Attack):

The Infrastructure as a Service (IaaS) cloud provides users to rent high-performance virtual machines (VM) with abundant access to computing resources such as bandwidth, processing, and storage [1]. These abundant resources can be used as a feasible ground for attacks of high magnitude. A botnet is a network of compromised hosts or VM's called stepping stones. The attack is carried out by gaining unauthorized access to a high-performance cloud server with the help of fake/stolen credit card details. The attacker then sets up a command and control center and engages stepping stones, which can then be used to steal sensitive information, execute DoS/DDoS attacks or perform port scans to find new victims etc [56]. This is done by attacking the victim indirectly through a sequence of compromised VM's called stepping stones. Because of the use of stepping stones, the attacker also mitigates the probability of detection and traceback.

A lot of attempts have been made to detect botnets/stepping stones and defend botnet/stepping stone attacks [57] [58] [59] [60]. These defense techniques can, however, be faked by attackers using encrypted traffic and authentication forging or by introducing jitter, while other techniques are inefficient due to the huge traffic that needs to be monitored and analyzed. To further improve these techniques other solutions have been proposed [61] that detect the presence of jitter and chaff in interactive connections by using three anomaly detection algorithms [62].

A new self-protection mechanism against stepping-stone attacks for IaaS clouds called xFilter is used [63]. For pinpoint active response, xFilter runs in the VMM and uses information on sender processes in compromised VMs for packet filtering. Using VM introspection, it directly obtains the process IDs and user IDs of sender processes in the VMs. Another algorithm uses modified association rule mining to detect stepping-stones [64].

4.5 Audio Steganography Attack:

Audio Steganography attack is considered as one of the dangerous attacks on cloud storage systems. With the help of audio steganography, a user can hide his secret data within regular audio files [65] [66]. Using steganography, an attacker can transmit information secretly through media files which seem as normal audio files. Hackers can exploit this feature by hiding malicious code in sound files and sending the same to victim servers thus evading the current security mechanisms like steg-analysis. Three factors need to be considered when using steganography: file format, hiding area, and steganography scheme. The steganography tool will first analyze the file format and look for suitable areas for hiding information, then the information is split into blocks and these blocks replace the original information in the hiding areas [65] [67]. Not much research has been done on proposals to prevent Audio Steganography attacks and requires practical solutions.

A solution called StegAD (steganography Active defense) is designed and implemented to tackle the threat of data leakage by Audio Steganography attacks. StegAD includes two algorithms, the enhanced-RS algorithm, and the SADI algorithm. In the first step, the hiding place of audio files is scanned under cloud storage system through famous RS image grayscale steganalysis algorithm. If any suspicious files are acquired, SADI (Steganography Audio Dynamical Interference) technique is used to interfere in all the possible places in those suspicious files [68].

4.6 DoS (Denial of Service) Attack:

Denial of service (DoS) attack in cloud computing is aimed at bringing down a cloud system and suspending its services temporarily or indefinitely by flooding it with nonsense messages/requests. A distributed DoS (DDoS) is where the attack source is more than one compromised node or bot, often thousands of unique IP addresses. It is undoubtedly one of the most dangerous and penetrable attacks in cloud computing. The attacker uses a master program known as handler to propagate commands to the bots under its control which then start the attack on the target until the service provided by the target goes down. DDoS affects all the layers of the cloud and can occur internally or externally. An external cloud-based DDoS attack starts from outside the cloud environment and targets cloud-based services. This type of attack affects the availability of services. An internal cloud-based DDoS attack occurs within the cloud system and attacks the victim's machine internally [69].

When under attack the load increases, the cloud system starts to deliver additional computational power in the form of more virtual machines and service instances to deal with the additional load. The cloud system is actually working against the attacker by offering more computational power but in fact, assists the attacker to do more possible damage on the availability of services. As such to halt an intended service the attacker does not necessary need to flood all servers but can merely flood a single cloud-based address. There are 3 broad categories of DDoS attacks: Volume based DDoS attacks in which the target is flooded with high volume of packets or connections overwhelming networking equipment, servers or bandwidth resources. Application based DDoS attacks which target different applications such as HTTP, VoIP or DNS. Low-rate DoS attacks which take advantage of application implementation weakness and design flaws [69].

There are several types of DDoS attacks that can be performed to disrupt cloud services. Some of the specific types are:

- Flooding attacks: In these type of attacks, the attacker uses bots to flood the target with massive volumes of traffic like ICMP (ping), SYN or UDP packets to drastically saturate the target network and slow down the network infrastructure [69].
  The ICMP flood attacks work by simply sending huge volumes of ICMP echo requests to the victim. To reply to such huge volume of requests, the bandwidth of the victim will be maximized resulting in inaccessibility to benign users.
  SYN flood attack exploits the TCP three-way handshake in which the client requests a connection by sending a SYN message to the server. The server replies with the acknowledgment message SYN-ACK back to the client. The client then responds with an ACK message and the connection is established. In a SYN flood attack, the attacker does not reply to the server with the expected ACK but spoofs the source IP address or just does not reply to the SYN-ACK.
  A UDP flood attack is initiated by sending a large number of UDP packets to random ports on the target system. The system observes that no application is listening at that port and replies with an ICMP destination unreachable packet. Consequently, if a large number of UDP packets are sent, the victim is forced to reply with numerous ICMP packets. These attacks are usually achieved by spoofing the attacker's source IP address.
- Amplification attacks: This type of attack uses the broadcast address feature to send a large number of packets to a broadcast IP address which causes the nodes in the broadcast IP range to send a reply to victim servers resulting in malicious traffic [69]. Examples of this attack are DNS amplification attack, Smurf attack, and Fraggle attack.
  In a DNS amplification DDoS attack, the attacker sends small spoofed address queries to an open resolver, causing it to send much larger responses to the spoofed address target. Thus, the resolver aids in the DDoS attack on spoofed addresses.
  In Smurf attack, an attacker broadcasts a huge number of ICMP packets with the victim's spoofed source IP to a network using an IP broadcast address. This causes all the devices in the broadcast network to respond by sending an ICMP echo reply to the victims IP address.
  The Fraggle attack is a variation of Smurf attack in which UDP echo packets are sent to ports that support character generation with the victim's spoofed IP address thus creating an infinite loop. This target the port supporting character generation of all the systems reached by a broadcast address. All the systems in the range echo back to the character generator port in the victim. This process is repeated since UDP echo packets are used.
- Encrypted SSL DDoS attacks: These types of attacks allow attackers to consume more CPU resources during encryption and decryption process thus amplifying the impact on the target.
- IP spoofing attack: In this type of attack, the packet transmissions that take place between the end user and the cloud server are intercepted and their headers modified. Attackers can forge IP source field in the IP packet by a legitimate IP address or by an inaccessible IP address. Due to which the server responds to and affects the legitimate user machine, or the server is unable to complete the transaction for the inaccessible IP address affecting the server resources.
- H-DoS attack and X-DoS attack: In a H-DoS or HTML based DoS, the attacker uses the HTTP Get/Post request messages to flood the victim [69]. The HTTP GET request tries to get some information (images etc.) from the server during SSL sessions. The server gets overloaded with GET requests using the CPU and memory and as such will be unable to respond to any further requests [70]. The HTTP POST request is more complex since it involves input data from forms which need more computation from the cloud server [71].
  A X-DoS or XML based DoS attack occurs when a network is flooded with XML messages instead of packets to stop genuine users from accessing network communications [71] [72] [69]. Additionally, if the attacker floods the web server with XML requests, it affects the availability of web services [73]. There are three ways to launch an X-DoS attack namely oversized payload, external entity references and entity expansion [74].
  HX-DoS attack is a combination of HTTP and XML messages that are intentionally sent to flood and

Attack	Service Model	Mitigation Techniques
Service Hijacking	IaaS PaaS Saas	-Security Policies -Strong Authentication -Activity Monitoring
Malware Injection Attack	IaaS PaaS SaaS	-Service Integrity Checks -Strong Isolation between VMs
Wrapping Attack	SaaS PaaS	-Inline Approach -Strengthening XML schema -Node counting
Botnet Attack	IaaS PaaS SaaS	-xFilter
Audio Steganography Attack	SaaS	-StegAD
Denial of Service Attack	IaaS PaaS SaaS	-IPS/IDS/Firewall -Covariance Matrix -Hop Count Filtering -Random port Hopping
Phishing Attack	IaaS PaaS SaaS	-PhishTank -CANTINA+
Man in the Cloud Attack	SaaS	-Strong Encryption -2-factor Authentication -CASB

Table 2 External Security Attacks and Issues

destroy the communication channel of the cloud service provider [75] [76] [77].

- E-DoS attack: An Economic Denial of Sustainability or E-DoS attack is a new form of DoS attack that specifically targets the cloud environment. As the cloud services are provided in the form of Service Level Agreement (SLA) which defines the type of service required by the user. Some SLA will restrict the use of resources while others will provide an infinite amount of resources. In the former type of SLA, when the cloud is under attack, the resources (CPU, memory) will be depleted and the legitimate users will be denied of service. In the latter, the cloud will allocate more and more resources to deal with the additional load to maintain SLA. Finally, this additional use of resources will be charged to the customer. Thus, a traditional DoS can be transformed into an EDoS in a cloud environment [78] [79] [80].

Many solutions have been proposed to detect, analyse and prevent DoS/DDoS attacks in cloud e.g. using Covariance Matrix approach [81], NSA Algorithm [82], Multivariate Correlation Analysis [83], Hop Count filtering [84] [85], Confidence based filtering [86] [87], Random port hopping [88], Ingress and Engress filtering [89], Path Identification mechanism [90], etc. But before any method is used for the prevention and mitigation of DDoS attack certain precautions must be taken beforehand such as Firewalls, Filtering switches and Routers, Disabling IP Broadcasts, Audit, Security Patches, IPS, and IDS, Black holing and Sink holing.

4.7 Phishing Attack:

In this type of attack, the attacker attempts to solicit personal/sensitive information (passwords, credit card details, etc.) from the victim by employing social engineering techniques. The attack is usually carried out by creating an exact replica of a website and sending the link of the false website to the victim. If the victim enters his/her credentials, then the same would be passed on to the attacker and thereby the attacker can gain access to sensitive data. The attack may be divided into two categories: Firstly, the attacker can use the cloud services to host phishing websites. Second, the phishing attack can be used to gain unauthorized access to the cloud service. A recent type of phishing attack called Homograph attack uses Punycode which helps register domain names with foreign characters. As a result, the browser displays normal characters instead of Unicode characters, thus making the attack impossible to detect [91]. One of the ways to prevent phishing attacks is PhishTank which works by maintaining a blacklist of all known phishing web pages, nowadays these lists are implemented in all popular web browsers.

Another technique based on weighted URL tokens system works by extracting identity keywords from a web page and using the same as search terms, a search engine is invoked to pinpoint the target domain name which can be used to determine the legitimacy of the webpage [92].

Another solution, CANTINA+ works by exploiting the HTML Document Object Model, search engines and third-party services with machine learning techniques to detect phishing [93].

A new efficient and accurate solution has been proposed which uses web page noise and N-gram to detect phishing web pages [94].

4.8 Man in the Cloud Attack:

This type of attack is mainly performed on file sync services, the attacker steals the synchronization token which is used to access the cloud services without having to enter the password. The synchronization token is saved in the victim's machine after the victim successfully authenticates to the cloud service and the same token can be used to access the service across multiple devices. If the victim, however, changes the password, the token does not change. To successfully gain access to a victim cloud service, all the attacker must do is intercept and copy the token and install it on his/her machine [95].

The attack can be performed using a tool called Switcher which users can be tricked to install. The tool will install a new token of the attacker into the victim's machine, thus syncing the victim with the attacker's account. This will cause the token for the user's actual account to sync with the attacker's account. The attacker can then access to the victim's account and steal files or perform malicious code injection [95].

The attack can be undetectable and untraceable since the attacker at any time copy the users token back into his account [95]. The attack can be prevented by encrypting files in the cloud [13] and storing the encryption keys outside of the cloud. Another solution can be to use two-factor authentication [96] if the cloud service offers it or enable log-in alerts to get informed of log-in from a new device.

Another solution may be using a Cloud Access Security Broker (CASB), a tool that sits in between the cloud's infrastructure and organization's infrastructure. It functions as a proxy to monitor cloud traffic for anomalies [97].

5. CONCLUSION

Cloud computing is a powerful technology that can help organizations thrive by reducing operating costs and increase efficiency. Due to the rapid growth of cloud computing paradigm, a burst of problems related to security and privacy have emerged. These problems have significantly impeded the adoption of cloud and prevented many organizations from moving their business to the cloud. In this paper, we review the different issues and attacks on the cloud and have provided different solutions to these problems but still much research must be done to make cloud a safe and secure environment.

REFERENCES

[1] Hassan, Q.F., l.M. Riad, and A.E. Hassan, Understanding Cloud Computing, ed. H. Yang and X. Liu. Information Science Reference.
[2] Mell, P. and T. Grance, The NIST definition of cloud computing. 2011.
[3] Zhao, G., et al. Deployment models: Towards eliminating security concerns from cloud computing. in High Performance Computing and Simulation (HPCS), 2010 International Conference on. 2010. IEEE.
[4] Gibson, J., et al. Benefits and challenges of three cloud computing service models. in Computational Aspects of Social Networks (CASoN), 2012 Fourth International Conference on. 2012. IEEE.
[5] Fehling, C., et al., A collection of patterns for cloud types, cloud service models, and cloud-based application architectures. University of Stuttgart, Faculty of Computer Science, Electrical Engineering, and Information Technology, Germany, University of Stuttgart, Institute of Architecture of Application Systems, Technical Report Computer Science, 2011. 5.
[6] Dillon, T., C. Wu, and E. Chang. Cloud computing: issues and challenges. in Advanced Information Networking and Applications (AINA), 2010 24th IEEE International Conference on. 2010. Ieee.
[7] Moghaddam, F.F., et al. Cloud computing challenges and opportunities: A survey. in Telematics and Future Generation Networks (TAFGEN), 2015 1st International Conference on. 2015. IEEE.
[8] Subashini, S. and V. Kavitha, A survey on security issues in service delivery models of cloud computing. Journal of network and computer applications, 2011. 34(1): p. 1-11.
[9] Fernandes, D.A., et al., Security issues in cloud environments: a survey. International Journal of Information Security, 2014. 13(2): p. 113-170.
[10] Jula, A., E. Sundararajan, and Z. Othman, Cloud computing service composition: A systematic literature review. Expert Systems with Applications, 2014. 41(8): p. 3809-3824.
[11] Sharma, S. and Y. Gigras, A Survey: Threats and Vulnerabilities in Cloud, in Detecting and Mitigating Robotic Cyber Security Risks. 2017, IGI Global. p. 87-97.
[12] Chen, S., et al. Side-channel leaks in web applications: A reality today, a challenge tomorrow. in Security and Privacy (SP), 2010 IEEE Symposium on. 2010. IEEE.
[13] Prakash, G., M. Prateek, and I. Singh. Data encryption and decryption algorithms using key rotations for data security in cloud system. in Signal Propagation and Computer Technology (ICSPCT), 2014 International Conference on. 2014. IEEE.
[14] Stanek, J., et al. A secure data deduplication scheme for cloud storage. in International Conference on Financial Cryptography and Data Security. 2014. Springer.
[15] Duncan, A., S. Creese, and M. Goldsmith, An overview of insider attacks in cloud computing. Concurrency and Computation: Practice and Experience, 2015. 27(12): p. 2964-2981.

[16] Banyal, R.K., P. Jain, and V.K. Jain. Multi-factor authentication framework for cloud computing. in Computational Intelligence, Modelling and Simulation (CIMSim), 2013 Fifth International Conference on. 2013. IEEE.

[17] Yeboah-Boateng, E.O. and K.A. Essandoh, Factors influencing the adoption of cloud computing by small and medium enterprises in developing economies. International Journal of Emerging Science and Engineering, 2014. 2(4): p. 13-20.

[18] Top 7 threats to cloud computing HELP NET SECURITY https://www.helpnetsecurity.com/2010/03/01/top-7-threats-to-cloud-computing/, 2010.

[19] Riddle, A.R. and S.M. Chung. A survey on the security of hypervisors in cloud computing. in Distributed Computing Systems Workshops (ICDCSW), 2015 IEEE 35th International Conference on. 2015. IEEE.

[20] Thongthua, A. and S. Ngamsuriyaroj. Assessment of Hypervisor Vulnerabilities. in Cloud Computing Research and Innovations (ICCCRI), 2016 International Conference on. 2016. IEEE.

[21] Kulikov, R. and S. Kolesnikova, Evaluation of Hypervisor Stability towards Insider Attacks. 2016.

[22] Reshetova, E., et al. Security of OS-level virtualization technologies. in Nordic Conference on Secure IT Systems. 2014. Springer.

[23] García-Valls, M., T. Cucinotta, and C. Lu, Challenges in real-time virtualization and predictable cloud computing. Journal of Systems Architecture, 2014. 60(9): p. 726-740.

[24] Rutkowska, J., Subverting VistaTM kernel for fun and profit. Black Hat Briefings, 2006.

[25] King, S. and P. Chen. SubVirt: Implementing malware with virtual machines. InSecurity and Privacy. in 2006 IEEE Symposium on. May. 2006.

[26] Bahram, S., et al. Dksm: Subverting virtual machine introspection for fun and profit. in Reliable Distributed Systems, 2010 29th IEEE Symposium on. 2010. IEEE.

[27] Zhang, Y., et al. Homealone: Co-residency detection in the cloud via side-channel analysis. in Security and Privacy (SP), 2011 IEEE Symposium on. 2011. IEEE.

[28] Keller, E., et al. NoHype: virtualized cloud infrastructure without the virtualization. in ACM SIGARCH Computer Architecture News. 2010. ACM.

[29] Szefer, J., et al. Eliminating the hypervisor attack surface for a more secure cloud. in Proceedings of the 18th ACM conference on Computer and communications security. 2011. ACM.

[30] Xia, Y., Y. Liu, and H. Chen. Architecture support for guest-transparent VM protection from untrusted hypervisor and physical attacks. in High Performance Computer Architecture (HPCA2013), 2013 IEEE 19th International Symposium on. 2013. IEEE.

[31] Wu, J., et al., C2detector: a covert channel detection framework in cloud computing. Security and Communication Networks, 2014. 7(3): p. 544-557.

[32] The API is everything for cloud computing http://www.infoworld.com/article/2627516/paas/the-api-is-everything-for-cloud-computing.html, 2010.

[33] Šilić, M., J. Krolo, and G. Delač. Security vulnerabilities in modern web browser architecture. in MIPRO, 2010 Proceedings of the 33rd International Convention. 2010. IEEE.

[34] Tsai, W.-T., Z. Jin, and X. Bai. Internetware computing: issues and perspective. in Proceedings of the First Asia-Pacific Symposium on Internetware. 2009. ACM.

[35] Kalloniatis, C., et al., Towards the design of secure and privacy-oriented information systems in the cloud: Identifying the major concepts. Computer Standards & Interfaces, 2014. 36(4): p. 759-775.

[36] Kene, S.G. and D.P. Theng. A review on intrusion detection techniques for cloud computing and security challenges. in Electronics and Communication Systems (ICECS), 2015 2nd International Conference on. 2015. IEEE.

[37] Milenkoski, A., et al., Evaluating computer intrusion detection systems: A survey of common practices. ACM Computing Surveys (CSUR), 2015. 48(1): p. 12.

[38] Hlavacs, H., et al. Energy consumption side-channel attack at virtual machines in a cloud. in Dependable, Autonomic and Secure Computing (DASC), 2011 IEEE Ninth International Conference on. 2011. IEEE.

[39] Zhang, Y., et al. Cross-VM side channels and their use to extract private keys. in Proceedings of the 2012 ACM conference on Computer and communications security. 2012. ACM.

[40] Hund, R., C. Willems, and T. Holz. Practical timing side channel attacks against kernel space ASLR. in Security and Privacy (SP), 2013 IEEE Symposium on. 2013. IEEE.

[41] Liu, F., et al. Last-level cache side-channel attacks are practical. in Security and Privacy (SP), 2015 IEEE Symposium on. 2015. IEEE.

[42] Younis, Y.A., et al. A new prime and probe cache side-channel attack for cloud computing. in Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing (CIT/IUCC/DASC/PICOM), 2015 IEEE International Conference on. 2015. IEEE.

[43] Yarom, Y. and K. Falkner. FLUSH+ RELOAD: A High Resolution, Low Noise, L3 Cache Side-Channel Attack. in USENIX Security. 2014.

[44] Liu, F., L. Ren, and H. Bai, Mitigating Cross-VM Side Channel Attack on Multiple Tenants Cloud Platform. JCP, 2014. 9(4): p. 1005-1013.

[45] Kim, T., M. Peinado, and G. Mainar-Ruiz. STEALTHMEM: System-Level Protection Against Cache-Based Side Channel Attacks in the Cloud. in USENIX Security symposium. 2012.

[46] Szefer, J. and R.B. Lee. Architectural support for hypervisor-secure virtualization. in ACM SIGPLAN Notices. 2012. ACM.

[47] Shoundic, S., et al. Extended-HyperWall: Hardware support for rollback secure virtualization. in Advances in Computing, Communications and Informatics (ICACCI), 2016 International Conference on. 2016. IEEE.

[48] Xia, Y., et al. Defending against vm rollback attack. in Dependable Systems and Networks Workshops (DSN-W), 2012 IEEE/IFIP 42nd International Conference on. 2012. IEEE.

[49] Yeh, J.-R., H.-C. Hsiao, and A.-C. Pang. Migrant Attack: A Multi-resource DoS Attack on Cloud Virtual Machine Migration Schemes. in Information Security (AsiaJCIS), 2016 11th Asia Joint Conference on. 2016. IEEE.

[50] Habiba, U., et al., Cloud identity management security issues & solutions: a taxonomy. Complex Adaptive Systems Modeling, 2014. 2(1): p. 5.

[51] McIntosh, M. and P. Austel. XML signature element wrapping attacks and countermeasures. in Proceedings of the 2005 workshop on Secure web services. 2005. ACM.

[52] Rahaman, M.A., R. Marten, and A. Schaad, An inline approach for secure soap requests and early validation. OWASP AppSec Europe, 2006. 1.

[53] Rahaman, M.A., A. Schaad, and M. Rits. Towards secure SOAP message exchange in a SOA. in Proceedings of the 3rd ACM workshop on Secure web services. 2006. ACM.

[54] Jensen, M., et al. On the effectiveness of xml schema validation for countering xml signature wrapping attacks. in Securing Services on the Cloud (IWSSC), 2011 1st International Workshop on. 2011. IEEE.

[55] Gupta, A.N. and P.S. Thilagam. Detection of XML Signature Wrapping Attack Using Node Counting. in Proceedings of the 3rd International Symposium on Big Data and Cloud Computing Challenges (ISBCC–16'). 2016. Springer.

[56] Kaur, N. and M. Singh. Botnet and botnet detection techniques in cyber realm. in Inventive Computation Technologies (ICICT), International Conference on. 2016. IEEE.

[57] Kumar, R. and B. Gupta, Neural Network Based Approach for Stepping Stone Detection under Delay and Chaff Perturbations. Procedia Computer Science, 2016. 85: p. 155-165.

[58] He, T. and L. Tong. A signal processing perspective to stepping-stone detection. in Information Sciences and Systems, 2006 40th Annual Conference on. 2006. IEEE.

[59] Kuo, Y.-W. and S. Huang. Stepping-stone detection algorithm based on order preserving mapping. in Parallel and Distributed Systems, 2007 International Conference on. 2007. IEEE.

[60] Kuo, Y.-W. and S.-H.S. Huang. An algorithm to detect stepping-stones in the presence of chaff packets. in Parallel and Distributed Systems, 2008. ICPADS'08. 14th IEEE International Conference on. 2008. IEEE.

[61] Huang, S.-H.S. and W. Ding, A Hybrid Stepping-Stone Detection Algorithm to Counter Packet Jittering Evasion. Journal of Information Assurance & Security, 2014. 9(2).

[62] Kampasi, A., et al., Improving stepping stone detection algorithms using anomaly detection techniques. 2007: Computer Science Department, University of Texas at Austin.

[63] Kourai, K., T. Azumi, and S. Chiba. A self-protection mechanism against stepping-stone attacks for IaaS clouds. in Ubiquitous Intelligence & Computing and 9th International Conference on Autonomic & Trusted Computing (UIC/ATC), 2012 9th International Conference on. 2012. IEEE.

[64] Kuo, Y.-w. and S.-H.S. Huang. Detecting stepping-stone connection using association rule mining. in Availability, Reliability and Security, 2009. ARES'09. International Conference on. 2009. IEEE.

[65] Gopalan, K. Audio steganography using bit modification. in Acoustics, Speech, and Signal Processing, 2003. Proceedings.(ICASSP'03). 2003 IEEE International Conference on. 2003. IEEE.

[66] Rhoads, G.B., Audio steganography. 2001, Google Patents.

[67] Jayaram, P., H. Ranganatha, and H. Anupama, Information hiding using audio steganography–a survey. The International Journal of Multimedia & Its Applications (IJMA) Vol, 2011. 3: p. 86-96.

[68] Liu, B., et al. Thwarting audio steganography attacks in cloud storage systems. in Cloud and Service Computing (CSC), 2011 International Conference on. 2011. IEEE.

[69] Thangavel, M., S. Nithya, and R. Sindhuja, Denial of Service (DoS) Attacks Over Cloud Environment: A Literature Survey, in Advancing Cloud Database Systems and Capacity Planning With Dynamic Applications. 2017, IGI Global. p. 289-319.

[70] Yatagai, T., T. Isohara, and I. Sasase. Detection of HTTP-GET flood attack based on analysis of page access behavior. in Communications, Computers and Signal Processing, 2007. PacRim 2007. IEEE Pacific Rim Conference on. 2007. IEEE.

[71] Chonka, A., et al., Cloud security defence to protect cloud computing against HTTP-DoS and XML-DoS attacks. Journal of Network and Computer Applications, 2011. 34(4): p. 1097-1107.

[72] Shruthi, B. and Y. Nijagunarya, X-DoS (XML Denial of Service) Attack Strategy on Cloud Computing. Imperial Journal of Interdisciplinary Research, 2016. 2(12).

[73] Jensen, M., et al. Soa and web services: New technologies, new standards-new attacks. in Web Services, 2007. ECOWS'07. Fifth European Conference on. 2007. IEEE.

[74] Angaitkar, A.V., N. Shekokar, and M. Maurya, The Countering the XDoS Attack for Securing the Web Services. International Journal of Computer Science and Information Technologies, 2014. 5(3): p. 3907-3911.

[75] Chonka, A. and J. Abawajy. Detecting and mitigating HX-DoS attacks against cloud web services. in Network-Based Information Systems (NBiS), 2012 15th International Conference on. 2012. IEEE.

[76] Anitha, E. and S. Malliga. A packet marking approach to protect cloud environment against DDoS attacks. in Information Communication and Embedded Systems (ICICES), 2013 International Conference on. 2013. IEEE.

[77] Shamsolmoali, P. and M. Zareapoor. Statistical-based filtering system against DDOS attacks in cloud computing. in Advances in Computing, Communications and Informatics (ICACCI, 2014 International Conference on. 2014. IEEE.

[78] VivinSandar, S. and S. Shenai, Economic denial of sustainability (edos) in cloud services using http and xml based ddos attacks. International Journal of Computer Applications, 2012. 41(20).

[79] Sqalli, M.H., F. Al-Haidari, and K. Salah. Edos-shield-a two-steps mitigation technique against edos attacks in cloud computing. in Utility and Cloud Computing (UCC), 2011 Fourth IEEE International Conference on. 2011. IEEE.

[80] Kumar, M.N., et al. Mitigating economic denial of sustainability (edos) in cloud computing using in-cloud scrubber service. in Computational Intelligence and Communication Networks (CICN), 2012 Fourth International Conference on. 2012. IEEE.

[81] Ismail, M.N., et al. Detecting flooding based DoS attack in cloud computing environment using covariance matrix approach. in Proceedings of the 7th International Conference on Ubiquitous Information Management and Communication. 2013. ACM.

[82] Maiti, S., C. Garai, and R. Dasgupta. A detection mechanism of DoS attack using adaptive NSA algorithm in cloud environment. in Computing, Communication and Security (ICCCS), 2015 International Conference on. 2015. IEEE.

[83] Devare, A., et al., A System for Denial-of-Service Attack Detection Based on Multivariate Correlation Analysis. 2016.

[84] Jin, C., H. Wang, and K.G. Shin. Hop-count filtering: an effective defense against spoofed DDoS traffic. in Proceedings of the 10th ACM conference on Computer and communications security. 2003. ACM.

[85] Mukaddam, A. and I.H. Elhajj. Round trip time to improve hop count filtering. in Broadband Networks and Fast Internet (RELABIRA), 2012 Symposium on. 2012. IEEE.

[86] Dou, W., Q. Chen, and J. Chen, A confidence-based filtering method for DDoS attack defense in cloud environment. Future Generation Computer Systems, 2013. 29(7): p. 1838-1850.

[87] Mamtesh, R.N., An Improved Defense Mechanism Based on Packet Filtering to Mitigate DDOS Attack in Cloud Computing Environment.

[88] Luo, Y.-B., B.-S. Wang, and G.-L. Cai. Effectiveness of port hopping as a moving target defense. in Security Technology (SecTech), 2014 7th International Conference on. 2014. IEEE.

[89] Senie, D. and P. Ferguson, Network ingress filtering: Defeating denial of service attacks which employ IP source address spoofing. Network, 1998.

[90] Yaar, A., A. Perrig, and D. Song. Pi: A path identification mechanism to defend against DDoS attacks. in Security and Privacy, 2003. Proceedings. 2003 Symposium on. 2003. IEEE.

[91] www.securityaffairs.co, Homograph Phishing Attacks are almost impossible to detect on major browsers. 2017.

[92] Tan, C.L. and K.L. Chiew. Phishing Webpage Detection Using Weighted URL Tokens for Identity Keywords Retrieval. in 9th International Conference on Robotic, Vision, Signal Processing and Power Applications. 2017. Springer.

[93] Xiang, G., et al., Cantina+: A feature-rich machine learning framework for detecting phishing web sites. ACM Transactions on Information and System Security (TISSEC), 2011. 14(2): p. 21.

[94] Deng, Q., et al. A Phishing Webpage Detecting Algorithm Using Webpage Noise and N-Gram. in International Conference on Cloud Computing and Security. 2016. Springer.

[95] Man-in-the-Cloud Attacks Want Your Dropbox, Google Drive Files. pcmag, http://in.pcmag.com/google-drive/94851/news/man-in-the-cloud-attacks-want-your-dropbox-google-drive-file, 2015.

[96] Lee, S., et al., Two factor authentication for cloud computing. Journal of information and communication convergence engineering, 2010. 8(4): p. 427-432.

[97] Fernandez, E., N. Yoshioka, and H. Washizaki. Cloud Access Security Broker (CASB): A pattern for accessing secure cloud services. in Procs. of 4th AsianPLoP (Pattern Languages of Programs) 2015. 2015.

Authors

Aaqib Iqbal Wani has a Masters in Computer Science and Engineering from SMVD University, India and a Bachelors in Computer Science and Engineering from Bharath University, India. His areas of expertise are Cloud Computing and Networking.

Zubair Ahmad Lone has a Masters in Computer Science and Engineering from SMVD University, India and a Bachelors in Information Technology from MIET, India. His areas of expertise include Neural networks and Discrete Mathematics.