www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 7 Issue 3 March 2018, Page No. 23742-23752
Index Copernicus Value (2015): 58.10, 76.25 (2016) DOI: 10.18535/ijecs/v7i3.15

Survey of new attack models on Cloud Infrastructure

Har Preet Singh,
Technical University of Berlin,

***Abstract*—**
Cloud Computing is currently most useful technol- ogy around the globe which offers an innovative business models for infrastructure to the enterprise , software services to the end users and the easy to deploy platform to the developer on Internet using virtual machine , for the quick and easy accessibility. It is Internet driven technology, which gives pool of resources such as Storage , Network , Application on demand basis. As the technology is driven over the Internet and virtual machine and allow resource pooling their are various kind of security problem arise relate to the model architecture, multi-tenancy, elasticity, data confidentiality, authentication and authorization. Various kind of attack could happen in cloud infrastructure ,as there is no exact definition about the attack and attack model but here we try to group into a various levels eg. Network level, host level and application level and few other attacks and the solution to prevent the attacks. In this paper we will discuss about the different kind of attacks and solution on cloud services

***Index Terms*—Cloud Computing, Security, Attack models**

Introduction

IN this paper, we will be discussing about the various security issue and different kind of attacks possible in the cloud infrastructure.Before that understanding about the topic is quite needed before getting into the details further. There are various definition exist for the cloud computing in terms of business, usage , resources , utilization and even more. Basically cloud computing describes the approach of making IT infrastructures available over a computer network without them having to be installed on the local computer.in general

, cloud computing describes the provision of IT infrastructure such as storage space , computing power or application soft- ware as a service over the Internet. For case, a small start- up company may need the require or the monetary assets required to purchase numerous computing assets but may need to take off its alternatives open for a future extension, in case successful, making Cloud Computing especially fitting in such a case. In this setting, the company would essentially pay for what is really utilized given that assets can be discharged when they are no longer required. In a Cloud network, clients do not claim the computing servers. They can access various services without the burden of Cloud management and their information can be accessed by way of numerous gadgets (such as smartphones, sensors, tablets, etc.).

let's have a look into in mode details:

Cloud Computing

NIST Definition [1] : cloud computing is a model for enabling ubiquitous, convenient, on-demand network access

Dr. -Ing. Marius-Iulian Corici, Fraunhofer FOCUS ,Berlin (marius-iulian.corici@fokus.fraunhofer.de) to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is com- posed of five essential characteristics, three service models, and four deployment models.

A. Essential Characteristics

1) On-demand self-service: consumer can unilaterally ar- rangement computing capabilities, such as server time and network capacity, as required consequently without requiring human interaction with each benefit supplier.

2) Broad network access: Capabilities are accessible over the network and accessed through standard instruments that advance utilizes by heterogeneous lean or thick client plat- forms (e.g.,

portable phones, tablets, tablets, and workstations).

3) Resource pooling: The providers computing assets are pooled to serve numerous consumers utilizing a multi-tenant show, with diverse physical and virtual assets dynamically allocated and reassigned according to consumer demand. There is a sense of area autonomy in that the client, for the most part, generally has no control or information over the correct location of the given assets but may be able to indicate the location at a higher level of reflection (e.g., nation, state, or datacenter). Examples of resources include storage, processing, memory, and network bandwidth.

4) Rapid elasticity: Capabilities can be flexibly provisioned and discharged, in a few cases naturally, to scale quickly outward and internal commensurate with the request. To the customer, the capabilities accessible for provisioning fre- quently show up to be boundless and can be appropriated in any amount at any time.

5) Measured service: Cloud systems naturally control and optimize resource utilization by leveraging a metering ca- pability at a few level of reflection fitting to the sort of benefit (e.g., storage, processing, bandwidth, and active user accounts). Resource utilization can be monitored, controlled, and detailed, giving straightforwardness for both the supplier and consumer of the utilized service.

Service Models

6) Software as a Service (SaaS): [1] The capability pro- vided to the consumer is to use the providers applications running on a cloud infrastructure. The applications are acces- sible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user specific application configuration settings.

7) Platform as a Service (PaaS): [1] The capability pro- vided to the consumer is to deploy onto the cloud infras- tructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.

8) Infrastructure as a Service (IaaS): [1] The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls).

Deployment Models

9) Private cloud: The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises.

10)Community cloud: The cloud infrastructure is provi- sioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises.

11)Public cloud: The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider.

12)Hybrid cloud: The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, com- munity, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds). To viably address

the cloud security issues, we require to get it the compound security challenges in an all-encompassing way. Especially, we require to

- investigate various cloud security attributes including vulnerabilities, threats, risks, and attack models
- identify the security requirements including confidential- ity, integrity, availability, transparency, etc
- identify the involved parties (clients, service provides, outsiders, insiders) and the role of each party in the attack-defense cycle
- understand the impact of security on various cloud de- ployment models (public, community, private, hybrid)

Challanges And Issues

While there is a developing propensity toward the adop- tion of cloud computing by organizations, statistical anal- yses (Figure 1) of the challenges appear an disturbing drift in terms of security. International Data Corporation conducted a ponder of 244 IT executives, and out of the nine focuses raised, security was highlighted as the most genuine concern by around 74.6% of the respondents.

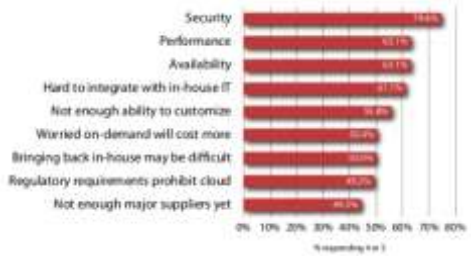

Figure (1) : IDC Survey Report

There are different perspective includes while choosing the cloud benefit and the comes about uncovers that security is a major concern in the cloud computing this is not as it depended on the give but moreover the assaults and benefit which can influence all kind of suppliers. we will check the different security challenges and angle in the cloud and the conceivable kind of assaults in the paper.

Security Challenges

Security in the cloud has become a major issue because of the worldwide usage of distributed systems and network computing (Shen & Tong, 2010b). Hence, security in the cloud environment emerged as the most significant barrier to faster and more widespread adoption of cloud computing (Chen, Paxson, & Katz, 2010). IS security issues and threats in cloud computing have been researched from various perspectives. In truth in appear abhor toward of the reality that the diverse issues in cloud computing have been inspected from different points of view, a correct definition of threats is misplaced in this space, in this way making it troublesome for specialists to center on the change nature of these threats. In this way, a basic format of threats is required to classify threats particular to the varying estimations of cloud computing.

A. Security Principal

Security in Cloud Computing is fundamental when making services. Upgrading the operating systems of virtual machines, ensuring availability, isolating clients, person information, executing confirmation components, encryption or planning VPN and VLAN are but a few outlines of what needs to be considered [2]. Here is a list of the security perspectives that challenge Cloud Computing.

1) Identity, Authentication, Authorization: Identity empow- ers characterizing a user through the utilize of a login. Au- thentication is utilized to affirm the users credentials. This is done in a secure, dependable and sensible way [3]. When verification is add up to, the Cloud authorization affirms the users rights. Course consolidates a centralized catalog, identity organization, favored client and get to organization, role-based get to control and division of commitments among principal highlights. In the extension, the benefits provider can as frequently as conceivable offer a free trial period. For case, in the summer of 2012, assailants (clients for a free period) gotten to Mat Honas data (creator for Wired Magazine) Apple, Gmail and Twitter accounts [3]. They erased all his person data in those accounts.

2) Confidentiality: A noxious assailant in a virtual machine can tune in to another virtual machine [4]. An attacker can exceptionally effortlessly distinguish the information center of the Virtual Machine (VM) and can too get information about the IP address and the domain name of the data center. In expansion, a VM can extricate private cryptographic keys being utilized in other VMs on the same physical server, which along these lines suggests the hazard of information spillage [3]. It is hence vital to ensure the

privacy of VM information. For illustration, the Amazon EC2 stage (Seattle, Washington, WA, USA) [5] was helpless to secrecy issues [4]. In any case, presently, with Amazon Web Benefit (AWS), the client has the alternative to oversee their possess encryption keys [6].

3) Integrity: Phishing, extortion and misuse of software vulnerabilities, traffic hijacking can listen in exercises and exchanges, manipulate data, return distorted data and redirect clients to illegitimate sites. Essentially, weak interfaces and Application Program Interface APIs cannot secure clients from coincidental or noxious endeavors [3]. For case, Hewlett- Packard (Palo Alto,California, CA, USA) proposes an As- tuteness Virtual Machines Design [7].

4) Isolation: Cloud Computing must have a level of iso- lation among all the VM data and the hypervisor [8,9]. In Infrastructure as a Service (IaaS), it means isolating VMs storage, processing memory and access path networks. In Platform as a Service (PaaS): running services and API calls must be isolated. Moreover, in Software as a Service (SaaS): isolation amongst transactions must be achieved.Isolation of the user cloud be at client and the server end both.

5) Availability: Illegitimate users consume much of the victims processing control, memory, disk space or network transmission capacity. It moreover causes system slowdowns, which anticipates authentic clients from utilizing the benefit. Thus, the VM gets to be inaccessible, causing a Denial of Service (DoS) or Distributed Denial of Service (DDoS). For case, a DDoS assault with compromised Internet of Things gadgets happen on Dyn (DNS foundation) [10] and deadened a few cloud computing-based sites such as GitHub [11].

Type Of Attacks

Before knowing approximately security administration in the cloud, its fundamental to dissect the different conceivable vulnerabilities and assaults in a cloud environment.their is no exact definition for the attacks in the cloud computing and various attack can occurs in different layers of computation, In this paper, the attacks and Top security threats in cloud com- puting is classified as network level, host level and application level. [13]

A. Network Level

In public cloud architecture the information moves to or from the organization, guarantee confidentiality and integrity. The network level security chance is classified as three sorts such as guaranteeing the information confidentiality, avail- ability and integrity. The information and resources already restricted to a private network are presently uncovered to the Internet, share open network having a place to a third-party cloud supplier. If The user is not using HTTPS (but utilizing HTTP) so it increment the hazard much more. The types of possible network level security issues and thread which are :

1) DNS Attack: It translate the domain name to an IP address, Since domain name is simpler to keep in mind rather than IP address. The client using IP address in not feasible since has been routed to some other cloud instead of the one he inquired. The sender and a receiver get rerouted through a few fiendish connection. DNS security measures are taken, still the route selected between the sender and receiver cause security issues [14].

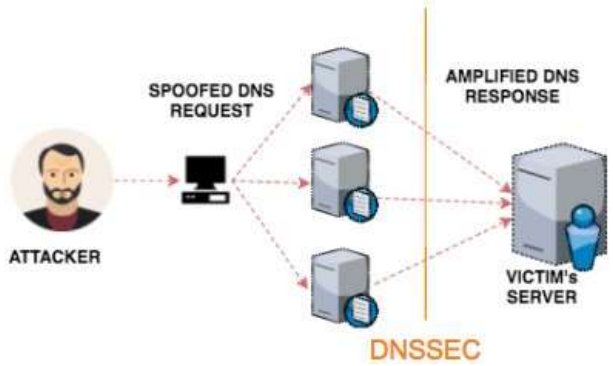

Figure (2) : DNS Attack

DNS attack can be prevent by DNSSEC which stands for domain name system security extensions to reduce the effect of DNS threats. DNSSEC are a set of the Internet standards that the DNS security mechanism to ensure the authenticity and integrity expand the data.

DOS Attack: Dos attack is an attack it drives the system component to restrain, or indeed end, normal services. The network is inaccessible by flooding it, disturbing it, sticking it, or crashing it. The issue in Denial of service on the web is inconceivable to anticipate. DoS attacks can be avoided with a firewall but they have configured properly.

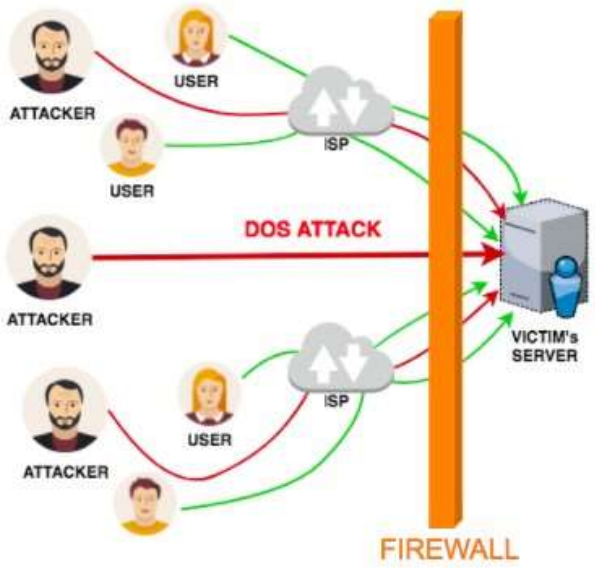

Figure (2) : DoS Attack Firewall is not only enough to avoid this kind of attacks even if the firewall is not configured properly still attacker have chance to attack the service.Proper firewall configuration and the regular routine check up can help to avoid these challenges.

2) DDoS: A DDoS is a DoS that uses a high number of has to make the attack indeed more disruptive. The number of hosts can reach hundreds of thousands. Most of the time, the machines proprietors are uninformed that their machines were already infested and corrupted through a Trojan or a backdoor program. The activities driving to a DoS or DDoS, the extreme objective of which is to compromise the avail- ability of the Cloud, can take put remotely or locally from the victims or users service. It for the most part targets the victims communication bandwidth, computational resources, memory buffers, network protocols or the victims application processing logic. This area particularly addresses DoS and DDoS connected to Cloud Computing systems. DoS and DDoS are not particular to Cloud systems, but they completely apply to them. Riquet et al. [21] consider the affect of DDoS attacks on Cloud Computing with a defense such as an IDS (snort [22]) and a commercial firewall. Their tests appear that distributed attacks stay undetected, indeed with security solutions. As specified in [23], DoS or DDoS assaults on Cloud Computing can be direct or indirect. In direct attacks, the target service or host machine is foreordained in spite of the fact that collateral damages may result in indirect DoS or DDoS by denying access to other services facilitated on the same machine or network. There is indeed a situation called race in power, initiated by a Cloud mechanism that migrates overflowed services to other machines. Cloud elasticity can be used to relieve the impacts of the assault, but it is completely conceivable that it will basically spread the workload, inother words, coordinate the assault to many other servers. Somani et al. [24] illustrate that DDoS attacks in clouds influence the victim server along with a few other parts: virtual servers on physical servers, network resources, and service providers. They conclude that these parts could be affected collaterally, indeed on the off chance that they are not the actual targets of the attack. Concurring to [25], a DoS or DDoS attack can have two goals. The to begin with comprises in overwhelming the target system resources or the network connections, by taking advantage of the superior capacity of the attacker, compared to what the system is able of coping with in terms of CPU or bandwidth for instance. The moment comprises of misusing vulnerabilities in the system by sending particular malicious packets (not essentially at a huge rate).

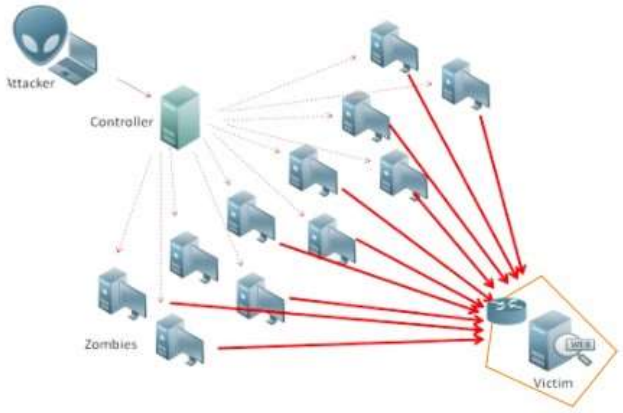

Figure (3) : DDoS Attack Distributed Denial of Service

attack is a DoS attack that occurs from more than one source, and from more than one location at the same time. DDoS attacks that comes from many ”dummy” computers at the same time to flood the server. This is harder to trace or so that they can use more bandwidth.

3) Sniffer Attack: [15]There are such sorts of applica- tion that dispatch attack by capture the packets when they streaming in the network and on the off chance that the information that is transferred by these packets is not use encryption, at that point it can be read as well as there is a chance that the

data that streaming through the network can be captured or traced. A sniffer program, through the (NIC) guarantees that data or traffic connected to other systems which also exist on the network is also gets recorded. This can accomplish by setting the Network Interface Card (NIC) in indiscriminate mode, at that point in promiscuous mode it will track all information, transmitted on the same network. A malicious-sniffing-detection platform that is based on Address Resolution Protocol (ARP) and Round Trip Time (RTT) , that is fundamentally utilized to distinguish a sniffing-system that is running on a organize [16].

4) Issue of Reused IP Address: [15]Each node of the net- work is has an IP address thus an IP address is unquestionably a finite quantity. There are a large number of cases that are related to reuse of IP address issue have been observed. When a client or user moves out to the network at that point IP address that is related with him earlier is assigned to new users. This now and then may be risks to security of the new user since there is a continuously certain time-lag between the alter of the past IP address in the DNS server and the clearing of that specific address from DNS caches. Consequently, we can watch that in spite of the fact that the past IP-address is assigned to the new client but still there is always a chances of accessing the data by other user and it is not negligible since the address still exists in the DNS server cache and the data belonging to that specific user can gotten to be available to other user and that is violating the privacy of original user.

B. Host Level

Cloud service provider do not publicly share information related to their host platforms, host operating systems, and processes that are in place to secure the hosts, since hackers can trying to intrude into the cloud service. The host level security issues are :

1) Hypervisor: Hypervisor is defined as controller called as Virtual machine manager (VMM) that allows multiple OS runs on single machine at a time. If number of Operating system running on hardware platform, security issues get increased, because single hardware unit is difficult to monitor multiple operating systems.[13] eg.:- guest system tries to run malicious code on the host system and get control of the system and block other guest OS, even it can make changes to any guest OS. Advanced cloud protection system can be developed, in order to monitor the guest VMs and inter communication among the various infrastructure components [17]

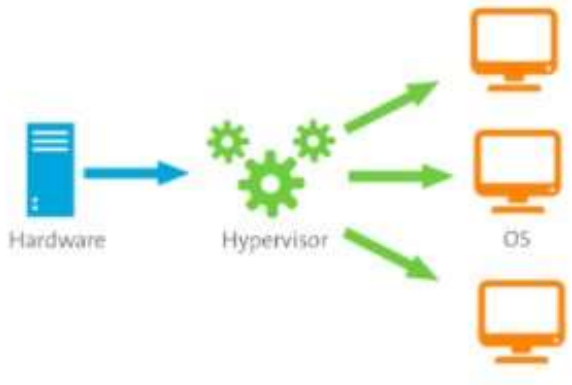

Figure (4) : Hypervisor Attack

Virtualization platform is software. Major virtualization platform vendors are VMware, Xen and microsoft. Its impor- tant to secure the layer of software that sits between hardware and virtual servers. The isolation of customer VMs from each other in a multitenant environment, it is very important to protect the hypervisors from unauthorized users[18]. To protect the hypervisor, Current solutions utilize a VM security agent and a security appliance to offload the scanning part, tackling the execution perspective of resource consumption. In any case, these guest operating systems are still defenseless to misuses, custom threats an in-guest security solution may not be able to detect in a convenient manner. Ultimately, the security solution depends on the data given by the working

system and, in case that system is compromised, the whole security suite could be bypassed. This opens up the same can of worms as traditional single-guest security, but that presently remediation is far more cumbersome as virtual infrastructures come with far more dependencies.

2) Securing Virtual Server: Customers of Iaas have full access to the virtualized guest VMs that are hosted and isolated from each other by hypervisor technology. Virtual server may be accessible on the Internet, so sufficient network access preventive steps should be taken to restrict access to virtual instances. The IaaS platform creates a risk due to self provisioning of new virtual server, that leads to create insecure virtual servers. Securing the virtual server in the cloud requires strong operational security procedures. Some recommendations are

- Protect the integrity of the image from unauthorized users.
- Secure the private keys in the public cloud.
- Keep the decryption keys away from the cloud.
- Do not allow password-based authentication for shell access.
- Require role-based access password
- Run a host firewall and open only the minimum ports necessary to support the services on an instance.
- Run only the required services and turn off the unused services
- Enable system auditing and event logging.
- Secure the log events to a dedicated log server.
- Keep the log server separate with higher security protec- tion, including accessing controls.

C. Application Level

A few company hosts an applications in Internet that nu- merous user utilize without considering about Where, how, by whom the services are given, so legitimate security instrument ought to adjust. The sorts of Application level security threats are

1) Cookie Poisoning: [19] Cookie poisoning is an exertion by an unauthorized person to get to and control aspects of the information in a cookie, more often than not in order to steal someones identity or financial data. Numerous distinctive sorts of hacking that center on taking data from cookies can be called cookie poisoning, including theft of passwords, credit card numbers or other identifiers that are put away on cookie files.

The items inside a cookie that are subject to cookie poi- soning are often called parameters. Effective endeavors at cookie poisoning will accurately distinguish the parameters that contain usable information, such as selecting a credit card number from a transaction that too incorporates things like a session ID, timestamps and other data about purchases.

The common strategy for securing information against cookie poisoning includes encrypting the requests or trans-actions. Various services can help clients and end clients to encrypt sent information so that it is no longer transparent to those who can use cookie poisoning to access it.

2) Backdoor and Debug: [20] Developers frequently work on code and write their coding with a backdoor. Some time recently making the website live, programmers may also leave certain debug options running in order to re-examine the website. At times, these backdoor or debug options contain passage points which can permit a hacker simple get to to sensitive information. Hence, uncommon consideration must be given to backdoor and investigate alternatives that empower hackers to gain privileged access and trespass into applications. many applications contain backdoors or debug options open, to provide programmers or developers unrestricted easy access. However, when the website goes live and left open, these entry points offer easy access to hackers, who can compromise all your sensitive data and lead to serious damage. Surprisingly, some backdoors are so significant they allow visitors to log into applications without using a password. This type of backdoor access grants users many other privileges. For in- stance, banking websites offer their customers a wide range of facilities and online financial services; these allow customers such functions as checking their balances and implementing online money transfers. While developing the money transfer application, the programmer might have left few debugging options and the website went live with them. In the event that a money transfer application contains a flaw unknown to the bank officials, a disastrous situation can ensue as hackers can use an unaddressable flaw to break into the banks website

and manipulate various features. In this type of scenario, hackers can do a lot. Backdoor and debug options have the potential of allowing hackers to extract any amount of money from any given account. They can also steal crucial information and cause immeasurable damages to the bank. Our knowledgeable have extensive experience with IT security services in financial services as well as in the general IT security services market. We are extremely knowledgeable in understanding how these attacks take place and offer both IT security assessment services and managed IT security. We offer a comprehensive web application security assessment package. Our services effectively detect existing loopholes in web applications, as well as locating and identifying undetected debug options inadvertently left within applications.

3) SQL Injection: Attackers inserted a malicious code into a standard SQL code and it allow unauthorized person to download the entire database or interact it in other illicit ways. The unauthorized user can access the sensitive data. This will be avoided the usage of dynamically generated SQL in the code.

Common Steps to Avoid SQL Injection , some generic best practices that could be utilized by any application to avoid SQL Injection.[21]

- Parameterized Queries: SQL Injection arises from an attacker's manipulation of query data to modify query logic. The best method of preventing SQL Injectionattacks is thereby to separate the logic of a query from its data. This will prevent commands inserted from user input from being executed.
- Validate input: The vast majority of SQL Injection checks can be prevented by properly validating user input for both type and format.
- Stored Procedures: Consider using stored procedures. They require a very specific parameter format, which makes them less susceptible to SQL Injection attacks.

4) Cross Site Scripting: Like all injection attacks, XSS takes advantage of the fact that browsers cant tell valid markup from attacker-controlled markup they simply execute whatever markup text they receive. The attack circumvents the Same Origin Policy (SOP), a security measure used in Web browser programming languages such as JavaScript and Ajax. Simply put, Same Origin Policy requires everything on a Web page to come from the same source. When Same Origin Policy is not enforced, an attacker might inject a script and modify the Web page to suit his own purposes, perhaps to extract data that will allow the attacker to impersonate an authenticated user or perhaps to input malicious code for the browser to execute. There are a number of security controls that can be used in concert to drastically reduce or entirely remove the threat of cross-site scripting. They include: Input validation - determines if an end users input matches the expected format. For example, a browser-side script would not be expected in a phone number field. Content Security Policy (CSP) - restricts which scripts can be run or loaded on a Web page. Output encoding - tells the browser that certain characters it is going to receive should be treated as display text, rather than executable code. A typical web page will contain many contexts including, but not limited to: HTML body, HTML attribute, script and CSS. Each of these output contexts relies on different character encodings to prevent the execution of cross-site scripting payloads. Many web languages and frame-works have template engines available that can automatically set the output context for variable data which will be included in the final Web page. Blacklist input validation, including Web application firewalls (WAFs), should not be counted on to prevent cross-site scripting attacks. Blacklists are inherently a reactive security measure, dependent upon lists that are often out of date and incomplete. Output encoding and content- security policies are the strongest solution to the problems XSS attacks pose, but do have limitations: output encoding must be properly set for the expected output context and CSP policies need to be configured so that they are as restrictive as possible.[22]

Few More Possible Threats

A. Hijacking Account

Cloud account hijacking is a process in which an individual or organizations cloud account is stolen or hijacked by an at- tacker. Cloud account hijacking is a common tactic in identity theft schemes in which the attacker uses the stolen account information to conduct malicious or unauthorized activity.

When cloud account hijacking occurs, an attacker

typically uses a compromised email account or other credentials to impersonate the account owner. [23] While cloud computing carries with it a wealth of benefits to organizations, includ- ing reduced capital costs and on-demand resources, it also provides cyber criminals with an environment ripe for attack, since huge amounts of data are housed in one place. Because the data is stored and accessed on devices and resources often shared across many different users, the risks presented by cloud account hijacking are plentiful. There are simple, effective steps businesses and organizations can take to keep their data secure on the cloud. Be sure to:

- Check with your service provider to make sure they have conducted background checks on employees who have physical access to the servers in their data centers.
- Have a strong method of authentication for cloud app users.
- Make sure all of your data is securely backed up in the event that your data is lost in the cloud.
- Restrict the IP addresses allowed to access cloud applica- tions. Some cloud apps provide tools to specify allowable IP ranges, forcing users to access the application only through corporate networks or VPNs.
- Require multi-factor authentication. Several tools exist that require users to enter static passwords as well as dynamic one-time passwords, which can be delivered via SMS, hardware tokens, biometrics, or other schemes.
- Encrypt sensitive data before it goes to the cloud.

B. Insider Threat

This is the worst-case scenario for both cloud providers and cloud clients, i.e. a malicious system administrator working for the cloud provider. Because of her business role in the cloud provider, the insider can use her authorized user rights to ac- cess sensitive data. For example, an administrator responsible for performing regular backups of the systems where client resources are hosted (virtual machines, data stores), could exploit the fact that she has access to backups and thus ex filtrate sensitive user data. Detecting such indirect access to data, can be a challenging task. Depending on the insiders motives, the result of such an attack in a cloud infrastructure will vary from data leakage to severe corruption of the affected systems and data. Either way, the business impact for the provider will be significant. All common cloud types (IaaS, PaaS, SaaS) are equally affected by insider attacks as long as the insider has (or can gain) access to the data centers or cloud management systems. Someone could argue that the aforementioned impact of an insider threat in the cloud is similar to the impact of an insider in the classic outsourcing paradigm. This is partially true, since the decision to outsource is coupled with an innate risk of exposing sensitive data to an outsider, though cloud computing differentiates due to the fact that it offers a holistic solution to outsourcing via IaaS and PaaS. Hence, cloud computing paradigm could be utilized in order to outsource vast parts of the infrastructure instead of specific services, such as web hosting or application hosting. [24]

C. Malware Injection

One of the clouds functionality called Infrastructure as a Service (IaaS in short) which offers Virtualization of devices, storage and network does not have a secured registration process. It means that anyone having a proper credit card can sign up for cloud and can instantly start using the cloud. Due to this any cloud network could become a victim of malicious attack, spam mails and other such criminals.

- Authorized registration and validation processes.
- Prevention of frauds by monitoring credit card processes.
- Absolute examination of network traffic.
- Keeping an eye on blacklisted stuff for ones network

D. Insecure APIs

Application User Interface, software and other interfaces are shared among the users of a particular cloud. Security in sharing such resources is merely dependent on the security policies used by respective API and software. APIs and soft- ware which are going to be shared upon the cloud, should have tight security in every aspects it authentication or encryption in order to avoid any malicious attacks.

- Inspect thoroughly the security standards of the

cloud provider.

- Make sure that strict authentication along with encrypted transmission are populated.

E. Data Breach

Keeping a backup of your data off line may reduce the risk of data loss, but will increase the risk of data exposure. A virtual machine can easily access your side channel timing information to derive the private cryptographic keys used by other virtual machines in the same network. The outstanding features of multitenancy. If not architectured properly may allow an attacker to reach to the users data.

- Select a proper and reliable Cloud provider.
- Install proper encryption system to ensure the data secu- rity

F. Cloud Abuse

One of the clouds functionality called Infrastructure as a Service (IaaS in short) which offers Virtualization of devices, storage and network does not have a secured registration process. It means that anyone having a proper credit card can sign up for cloud and can instantly start using the cloud. Due to this any cloud network could become a victim of malicious attack, Spam mails and other such crimes. *Loss of Data*

Compromising of important data caused due to deletion, alteration, unlinking a record and storing of data on unreliable medium, is another serious threat. It leads to loss of important data, reputation (for businesses), trust of customers and some- times even the customers. Sometimes the loss of data may cause severe legal and policy compliance issues.

- Enforce powerful API security.
- Secure data with SSL encryption.
- Check for the integrity of the data running time duration as well as designing time duration.
- Explore the backup and collection plans of the provider.

Future Scope

As there is not exact definition for attack in cloud com- puting but still various threats still emerging which can be avoided to bring more security.Major future work could be on Data Classification based on Security Level of security includes confidentiality, encryption, integrity and storage etc. that are selected based on the type of data. There is a scope of distinguishes the security issue and different type attack and solution and Security considerations and provisions for virtualization along with the optimum use of the cloud infrastructure also needs to be focused and addressed under Optimization of resource Utilization.In Rapid Application de- livery is dramatically transforming how software is designed , created and delivered a good adoption of Dev Ops technique can help to update the OS and other security thread in a cloud automatically , correct approach will help to secure and prevent attacks.

Conclusion

cloud computing describes the provision of IT infrastruc- ture such as storage space , computing power or application software as a service over the Internet.and have five essential characteristic includes on demand self service, broad network access , resource pooling , rapid elasticity and measured ser- vices, with three service models know as Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a service (IaaS).Few deployment model enrich the capabilities of cloud computing.The growth of technology led various specious issue which has been discussed in the paper as thread and other security concern.As there is no really model or definition to define attacks we break down into three layers as network, host and application.Various issue and solution discussed but still the appropriate solution for few of the vulnerability can not be complete avoided.Continues changes
, upgrade and routine check can help to observe the threat and track the issue which causing problems. In 2017, Wanna Cry attack , damaged various windows operated machines the attacked was combination of Cross Site Scripting and the Mal ware Injection and the recent solution emerged to adapt Dev Ops in automated way. Security is in cloud is always a major concern which can not be totally avoided but a secure setup
, trusted infrastructure , attack preventing techniques , which are discuss in the paper , can help to prevent the attacks.

References

[1] Peter Mell , Timothy Grance , *The NIST Definition of Cloud Computing* ,NIST

Special Publication 800-145 Available online :http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800- 145.pdf

[2] Sridhar , T. *Cloud Computing: Infrastructure and Implementation Topics.* Int. Protoc. J. CISCO 2009, 12, 4

[3] Los, R., Gray, D., Shackleford, D., Sullivan, B. *The Notorious Nine: Cloud Computing Top Threats in 2013*; *CSA, Cloud Security Alliance: 2013.*

[4] Ristenpart, T.; Tromer, E.; Shacham, H.; Savage, S. *Hey, You, Get off of My Cloud: Exploring Information Leakage in Third-party Compute Clouds./* In CCS09, *Proceedings of the 16th ACM Conference on Com- puter and Communications Security*, Chicago, IL, USA, 913 November 2009; ACM: New York, NY, USA, 2009; pp. 199212.

[5] Amazon, EC2. Available online: https://aws.amazon.com/ec2

[6] Service, A.W. 2017. Available online: https://aws.amazon.com/compliance/data-privacy-faq/

[7] Hewlett-Packard. Security Overview of the Integrity Virtual Machines Architecture.

[8] Hashizume, K.; Rosado, D.; Fernandez-Medina, E.; Fernandez, E. An analysis of security issues for cloud computing. J. Int. Serv. Appl. 2013, 4, 5.

[9] Gonzalez, N.; Miers, C.; Redigolo, F.; Carvalho, T.; Simplicio, M.; de Sousa, G.; Pourzandi, M. A Quantitative Analysis of Current Security Concerns and Solutions for Cloud Computing. In Proceedings of the 2011 IEEE Third International Conference on Cloud Computing Technology and Science (CloudCom), Athens, Greece, 29 November1 December 2011; pp. 231238.

[10] KrebsonSecurity. DDoS on Dyn Impacts Twitter, Spotify, Reddit. Avail- able online: https://krebsonsecurity.com/2016/10/ddos-on-dyn-impacts- twitter-spotify-reddit/

[11] Khandelwal, Massive DDoS Attacks against Dyn DNS 2016. Available online: http://thehackernews.com/ 2016/10/dyn-dns-ddos.html

[12] Adrien Bonguet and Martine Bellaiche ,A Survey of Danial-Of-Service and Distributed Denial of Service attacks and defenses in Cloud Com- puting Available online: http://www.mdpi.com/1999-5903/9/3/43

[13] R. Charanya et al. / International Journal of Engineering and Technology (IJET) , Levels of Security Issues in Cloud Computing Available Online: http://www.enggjournals.com/ijet/docs/IJET13-05-02-199.pdf

[14] Char Sample, Senior Scientist, BBN Technologies, Diana Kelley, Part- ner, Security Curve, Cloud computing security: Routing and DNS security threats,

[15] Neha Khandelwal , Chetan Kumar ,ISSN: 2278-621X . Security in Cloud: Attacks & Prevention Techniques ,International Journal of Latest Trends in Engineering and Technology (IJLTET) ,86

[16] Dean J, Ghemawat S, Map Reduce: simplified data processing on large clusters. Communication of the ACM, Volume 51, Pages 107-113, ACM 2008.

[17] Daniel Petri, What You Need to Know About Securing Your Vir- tual Network, Jan. 8, 2009.http://www.petri.co.il/what-you-need-toknow- about-vmware-virtualization-security.htm/.

[18] Jinpeng Wei, Xiaolan Zhang, Glenn Ammons, Vasanth Bala, Peng Ning. Managing security of virtual machine images in a cloud environment. CCSW '09: Proceedings of the 2009 ACM workshop on Cloud computing security pages 91-96. November 2009.

[19] Cookie Poisoning resource from: https://www.techopedia.com/definition/16076/cookie-poisoning

[20] Hacker4Lease , backdoor and debug options, http://hacker4lease.wpengine.com/attack-methods/backdoor-and-debug- options/

[21] Srinivasan Sundara Rajan , Cloud Security Series — SQL Intejection and SaaS http://cloudcomputing.sys-con.com/node/1624391

[22] Cross Site Scripting (XSS) http://searchsoftwarequality.techtarget.com/definition/cross-site-scripting

[23] Nate Lord, Cloud Hijacking ,https://digitalguardian.com/blog/what- cloud-account-hijacking

[24] Miltiadis Kandias, Nikos Virvilis, Dimitris Gritza- lis ,The Insider Threat in Cloud Computing

[25] ,https://www.infosec.aueb.gr/Publications/CRITISCloud

[26] Cloud Computing thread and its solution https://www.clickssl.net/blog/top-8-cloud-computing-threats-and-its- security-solutions