ISSN: 0976-3031

Available Online at http://www.recentscientific.com

CODEN: IJRSFP (USA)

International Journal of Recent Scientific Research
Vol. 9, Issue, 11(B), pp. 29545-29556, November, 2018

International Journal of Recent Scientific Research

DOI: 10.24327/IJRSR

Research Article

SURVEY OF REAL CASE STUDIES OF VARIOUS NETWORK BASED ATTACKS IN DIFFERENT CLOUDS

Lomte S. S[1]., Poonam M. Rokade[2] and Manza R.R[3]

[1]Matoshree Pratishthan Group of Institutions, Khupsarwadi, Nanded
[2]Department of Computer Science & IT, Dr. B.A.M.U., Aurangabad
[3]Department of Computer Science & IT, Dr. B.A.M.U., Aurangabad

DOI: http://dx.doi.org/10.24327/ijrsr.2018.0911.2880

ARTICLE INFO

Article History:
Received 13th August, 2018
Received in revised form 11th September, 2018
Accepted 8th October, 2018
Published online 28th November, 2018

Key Words:

Cloud computing, security, attacks types, security case studies, WannaCry ransomeware, real-world cases

ABSTRACT

Cloud computing is essentially the most rising technology today. It provides various resources such as software, hardware, computing devices, processors, storage, and so on to its users' on demand in pay-as-you-go approach. Because of its distribute environment and introduction of the web, this computing is also liable to various attacks like DoS attack, Session Hijacking, Man-in-the-middle attack, and many others., accordingly the more than a few security concerns arises. For that reason, it is main to protect the cloud against hackers through constructing distinctive algorithms. This paper elaborates quite a lot of security concerns and widespread attacks in cloud. Beside of this it also excited about various attacks, actual world attacks happened and the treatments of attacks furnished by using researchers. We have also described how the India is becoming the paradise for cybercriminals across the globe and being targeted the business. In this paper we have taken survey of attacks in different cloud from the year 2005 to 20018. Especially, we have taken a high-level view on the report of cybersecurity and internet threats, specially on the healthcare systems. The recapitulation of ransom ware from the year 2015 to 2016 has shown, as well as the global impact of Wanna Cry ransom ware has been graphically described.

INTRODUCTION

Cloud computing is a today's technological innovation presents a vast list of benefits for just about every business and governmental, small or medium sized organizations [1]. It's web based computing [2, 3] that supplies services to sharing resources, servers, applications, stores and process the dataover the network and employs massive crew or sectors of servers, which runs on low price patron pc technology. Due to storing, sharing and having access to the significant amount of dataover the network, management and security is the important issues [4]. It is completely web based technology where client's details being stored within the data center of the cloud provider services such as Google, Amazon, Facebook, Salesforce.Com and Microsoft, and so forth [5] and such colossal companies depend upon this kind of computing [4].Customers can lessen their charges on software/hardware infrastructure as good as upkeep due to the fact that customers put their exclusive data corresponding to business personal information or bank important points, etc., and non-personal data into cloud. The restricted control over the data could intent quite a lot of security problems and threats which includes the data leakage, insecure access, data availability and insider attacks [5]. Various services like drop box, flicker, face book, picasa achieved a widespread popularity for saving, organizing and managing the pictorial data which arises quite a lot of security and privacy challenges [4].

Security is the predominant difficulty in cloud computing and famous as a processing service expected to broaden the security of data. The cloud is the major source for the hackers to attack the information system and causes the leakage of information due to the internal or external attackers. The majorsecurity challenge is that the owner of the data won't have control of the location of datasince if one wants to exploits the advantages of utilizing cloud computing, he must also utilize the resource allocation and scheduling provided by the clouds.

To achieve excellent cloud security moreover to data server security, following security facets must be considered:

- ***Physical Security:*** All of the infrastructures of cloud including servers, routers, storage devices, and different add-ons must be physically secure and monitored.

Corresponding author:* **Lomte S. S
Matoshree Pratishthan Group of Institutions, Khupsarwadi, Nanded

- ***Network Security:*** Use many network security tactics services to firewalls; Virtual Private networks (VPNs), secure routers, intrusion detection systems, network sniffers, etc.
- ***Host security:*** Use this technique such as securing operating system; use virus protection and malware protection to put in force web browser security.
- ***Application Security:*** Secure applications that are running on your system. The cloud provider must follow and aid to secure development process.
- ***Identity Management:*** Identifying and authenticating enterprising customers using systems and methods.
- ***Business Control:*** Implement rules, processes and practices to govern access, assets, use and management of data [5].

Security in Cloud Environment

With a purpose to provide and improve the security in cloud environment, following goals must be carried out:

- ***Integrity:*** The data should be modified in cloud through the authorized individual only for higher security. Man-in-the-middle attack is a kind of attack where the websites between the two devices communicating and manipulating the data via the hackers by way of eavesdropping the private data.
- ***Confidentiality:*** The users should be aware of which data is stored in cloud and its accessibility to maintain confidentiality of data and understanding its classification.
- ***Availability and Management:*** It is concerning the knowledge on hand to the person to whom it is predicament, in order that data will have to now not be leaked or there will probably be minimum information harm.
- ***Authenticity:*** There are number of unambiguous persons who can access the information and it is not recognized who is permitted to knowledge. Henceforth, the licensed person and assistance cloud must have interchangeability administration entity.
- ***Storage and maintenance:*** The data is saved dynamically in cloud servers; hence the consumer is unaware about the location of knowledge in cloud environment. The data in cloud uncovered to loss or harm due to an atmosphere disaster or server failure, if that's the case the recovery is very essential.
- ***Monitoring and Incident Response:*** it is essential to continuous monitoring of the cloud infrastructure to assure compliance with client security insurance policies and auditing requirements.
- ***Policy Management:*** Defining and implementing rules for exact actions equivalent to auditing or proof of compliance.
- ***Privacy:*** Protect Personally Identifiable Information (PII) within the cloud from adversarial attacks or attacks that purpose to discover the identity of the person that PII related to.

Cloud computing environments are easy targeted by intruders and pose new risks and threats to an institution because of its provider and operational models, the underlying technologies, and their dispensed nature that depends on the network for its working [6]. Thus, Intrusion Detection Systems (IDS) are efficient security mechanisms to handle most of the threats of cloud computing, due to the fact that security is without doubt one of the most outstanding challenges that prevent the acceleration of cloud adoption [7]. As a consequence, the effectiveness of the IDS is a valuable obstacle for cloud security, which impacts homes of visibility and robustness. IDS can believe to be effective if:

1. It has a good visibility of the internal state of the monitored system.
2. It has a high robustness against attacks.
3. It may possibly avoid any pretence attempts.

IDS need crucial information from monitored process to analyze for strong attacks detection. If IDS deployed to dwell with monitored then it may well maintain a greater visibility of internal state of the monitored system, in order that higher robustness against evasion will also be accomplished as a consequence.

Cloud Computing Attacks

It's important to have the knowledge regarding to the attacks before developing or deploying any system for security in cloud. The attacks restrict some foremost security issues services such as Authentication, Integration in cloud. As companies are moving towards cloud computing, care ought to be taken towards hackers. The attacks which criminals or hackers may make an attempt may just comprise the next:

Denial-of-Service Attacks (DoS)

DoS attack is probably the most risk attack over the web. Its goal is to change or modify the data and gaining illegal access. In addition, it goals the availability of the server which is the major component of cloud computing. The attacker tries to get access to prevent the authorized consumer from accessing the services provided by cloud service provider. The attacker quite often sends extra quantity of requests to the cloud server so that more network traffic creates and the connection between the machines gets interrupted. If the attacker used spoofed IP, then it's hard to observe attacks. Spoofed IP is used to be certain that compromised computing device remains undetected and attacker can use it for different distinctive type of attacks [2,8]. However, it's viable to stop and block the attack if the source of attack is saved consistent. This entails emails with automated responses. If the false e-mail address is in reality belongs to any one, this may overwhelm that person’s account.

This severe threat would result in business lose and even discontinuance to quite a lot of organizations of users together with government services, manufacturing, and outlets, heath care data support, logistics, and cloud provider vendors. It breaks down the efficiency of the targeted server; also preclude professional users from getting access to the subscribed services and utilizing the elemental need of server’s availability. The growth of DDoS mitigation options in the cloud and the adoption of cloud are two major points complement each other. Distributed Denial of Service Attack is a modified form of DoS attack. These are inclined to network level and cloud infrastructure level threats, and are probably of three varieties described under:

Network Depletion Attack

The attacker consumes all of the bandwidth of particular network by using flooding targeted network with malicious site visitors. Later, it intercepts the respectable visitors from achieving the targeted network. This attack once more classified into two varieties:

Flood attack

It happens through Network and Application layers. e.g. HTTP (Hypertext Transfer Protocol), ICMP (Web Control Massage Protocol, used for IP operations, diagnostics and errors), and many others. It tries to saturate the network bandwidth to prevent it from responding to legitimate user traffic. Flooding will also be direct attack in opposition to the network or application or software, or reflective attacks via zombies. When DDoS attacks are initiated by using gaining illegal access to a couple compromised computers referred to as Zombies, which degrades the efficiency and throughput of the network.

Amplification attack

Attacker initiates the attack by way of networking devices memory of routers which have in-built Broadcast characteristic. Using the broadcast address attacker transmit packets to the networking devices. Then these devices further send those packets in variety of broadcast address, thereafter these machine will send a reply to targeted system so that you can lead to have malicious traffic.

Spoofing

This is to falsify the foundation of a network packet to bypass filters, hide the source of an attack or to attain access to restricted resources or services.

User to root

It targets to gain administrator (root) access privileges for a non-authorized account.

Oversized XML

The attacker sends a several megabytes XML document encapsulated with elements, attributes o namespaces with massive names or contents. The Document Objects Model (DOM) parses document into memory of their entirety to be analyzed which increases memory specifications.

Coercive Parsing

The attacker sends malformed XML for clogging up CPU cycles by means of including many namespaces declarations or via using very deeply nested XML structures.

Web service-addressing Spoofing

This is an extension of the spoofing attack where the Reply To or Fault To address in a SOAP (Simple Object Access Protocol) header is falsified leading to a reflective attack.

Reflective attack

Request messages are sent to reflector machines via zombie machines containing the spoofed source IP deal with of the victim. The specific replies to those requests are then dispatched to the victimcausing flooding [11].

Resource Depletion Attack

In this attack the attacker upends or exhausts the processing capabilities or memory of the server. The attacks that targets the server assets or resources as given below:

Protocol exploit attack

Attacker finds and avail certain feature of protocol used by victim after which consume the surplus amount of resources from it.
e.g. TCP SYN attack

Port scanning

Commonly used in the first stage of an attack and are available in many forms services to TCP (Transmission Control Protocol), TCP-SYN, SYN-ACK (SYNchronize and AC Knowledge), TCP ECHO, ICMP (Web control Message Protocol) SWEEP and so on.

Malformed Packet attack

Attacker sends the data packet which is wrapped with the malicious information to the victim's server to crash it.
e.g. IP address attack and IP Packet option attack

Application attack

Attacker finds an exploit in the application protocol. Attacker target any of the application protocol like HTTP, HTTPS (Hypertext Transfer Protocol Secure), DNS (Domain Name System), SMPT (Simple Mail Transfer Protocol), FTP (File Transfer Protocol), VoIP (Voice over IP) and different application protocols which have exploitable weaknesses.

Cloud Malware – Injection attack

Malware mainly referred as Malicious Software that designed to compromise the, confidentiality, availability or integrity of computer programs. The penalties of Malware Injection attack system can degrade computer operations; spam e-mail exalts unwanted product; services or activities in distasteful and even illegal. Additionally, the private, company or fiscal expertise theft can occur. The application installation remotely makes it possible for hackers to control and reveal computer activities. Malware is more hazardous than the phrases Virus. It additionally encompasses Worms, Trojan Horses, Rootkits, spyware, adware, crimeware, robot (botnet) clients, and many others.

Side Channel attack

In this attack, the attacker runs a virtual machine on the same physical host of the victim's virtual machine, and takes the advantages of a shared Physical component (e.g. Processor cache) to steal the information (e.g. A cryptographic key) from victim [2]. In other words, the attacker tries to retrieve the value of cryptographic key through monitoring the activity of the processor cache. That is large and needs tens of virtual machines to launch because attacker managed somehow to place his virtual machine on the victim's Physical host. Moreover, a co-residency examine is required after launching virtual machine. Trojans and an identical construction on the system are aid to compromise the system [9].

Authentication attacks

The authenticated consumer has something or knows something. The attacker in most cases goals the mechanism used to secure the authentication process and the approaches used.

Presently, there's only IaaS granting this style of protection and data encryption among the architecture of SaaS (software-as-a-service), PaaS (Platform-as-a-service) and IaaS (Infrastructure-as-a-Service).

Man-In-The-middle (MITM) Cryptographic attacks

It's mainly provided in SaaS environment of cloud. This attack is implemented when an attacker places himself between two users [10], i.e. attacker intercepts the communication channel which is established between legitimateusers and modifies the communication between client and server without their knowledge [9].
e.g. Wrapping attacks, SSL (comfy Socket Layer) attack, and so forth.

Session Hijacking

In this attack the session identity issued to the authenticated users shouldn't be protected accurately, which in turn can be utilized for spoofing identity. Session side-jacking captures login sequence by the use of packet sniffing tools and gain access to the consumer's session key encryption. The communication channel can avoid this kind of session hijacking attack.

Insider attack

This attack happens as a result of the authentication crisis and privileged authority and acts like genuine or licensed object. In this attack the attacker is present throughout the system and executed through malicious employees at provider's or user's location, so it is a passive entity. Consequently, attacker can damage or steals confidential information and performs modifications to damage the services and computation. As attacker acts like an authenticate entity, it is complicated to detect this sort of attack.

Many hacking attempt had been made in latest prior years on private and public classified web based storage system. Some examples of those are given under:

As per McAfee, August 2012 reports over few years over 72 company's databases are hacked across countries globally.

- Germany losses billion Euros annually due to electronic attacks on its databases.
- In 2012, due to cyber-attack on Amazon Web Services customers were not in a position to access Webflix for round 12 hours.
- Globally one new malware is developed each 2 seconds.
- European government bodies report 4-5 hacking attempts on their system every day [3]

Types of Web Services attacks

Most addressed attacks are denial of service attacks followed by using XML injection attacks. Techniques to handle attacks predominantly focus on attack detection measures. For the reason that web Service attacks are not able to be thoroughly eradicated, penetration and automation testing will have to be executed as part of every development. This will likely assurance brought security as well as lower attacks web services [8].

Web services are the major method for the exchange of key information between applications. It makes most important component to the web service security and web service attack a serious threat to the integrity and availability of data. The various web services attacks are ranging from injection attacks to Denial of service attacks. The elaboration is as beneath:

SQL Injection attack

These are very fashioned in web serviceenvironment. Most of the web services have improperly coded blocks that fail to filter non-validated consumer inputs. These inject and embed themselves as a parameter in a SQL statementtrying to run non-administrative commands.

XML Injection attack

XML Injection vulnerability arises, when any service fails to validate malicious XML content. The malicious XML injection content into any service can alter the working logic.

XPath Injection attack

This attack targets services or applications that use XPath as a language to convert consumer supplied input to query XML documents. With the aid of sending malformedinput, unauthorized information such as structure of XML document is obtained.

Denial of Serviceattack

It renders the target machine unresponsive via depriving the provider of resources.

Exploration

DOS Attack

In 2005, writer Zheng J. *et al*. Proposed a vector quantization basedintrusion detection system on web services to attain better true detection rates [12]. Chonka A., *et al*. (2009) specializes in attack detection and prevention by means of creating filter defense approach to protect towards XML based DOS [13]. Writer Pinzon C., *et al*. Proposed an architecture in 2010 that attempt to preventweb services against DOS attack. The structure used is based on real time, intelligent agent to use reasoning within a time bound to categories DOS attack [14]. Ficco M., *et al*., has proposed an approach in 2011 for identifying and attack detection on web services which can be intrusion tolerant [15]. Suriadi S., Stebila D. (2011) used the clientpuzzles for effectiveness of a cryptographic authentication technique for accessgrant to preclude attack [16]. Authors Pinzon CI, *et al*. (2011) used an approach that combining the capabilities of Case Based Reasoning (CBR) as well as multi-agent methods for protecting web services in opposition to SOAP messages [17]. Mainka C., & Jensen M. (2012) introduces the mechanism with adaptive rule updates for attack detection and mitigation [18]. Falkenberge A. *Et al*. (2013) did the automated plug-in established on Black box testing for web Service attack analysis [19]. Altmeier C., Mainka C. (2015) used adaptable algorithm for testing web services via parsing incoming XML messages for attack detection [20]. Chan GY, *et al*. (2015) proposed fuzzy rule

based intrusion detection system [21]. Gruschka N. *et al*.(2006) makes a speciality of attack prevention gateway system based on schema hardening as well as WSDL Compiler to defend the services by filtering the SOAP messages [22].

XPath Injection, XML Injection, SQL Injection

Loh YS., *et al*. (2006) designed and carried out as architecture as well as filtering coverage and tested to prevent web services attack such as Injection, Coercive parsing [23]. Vieira M., *et al*. (2006) focused on vulnerability detection and studied the evaluation of current vulnerability scanners against 300 public web services to identify security flaws of SQL, XPath injection [24]. Antunes N., *et al*. (2009) detected SQL injection attack using penetration testing tool [25]. Laranjeiro N., *et al*., proposed system (2010) to prevent SQL/XPath injection attacks on web services by combining statement learning as well as Service protection [26]. These authors also performed detection for the identical attacks in 2009 based on idea of anomaly detection [27]. In 2010 Patel V, *et al*. [28] and in 2008 authors Siddhavatam I, *et al*.J [29] recognized XML injection and DOS attacks. Asmawi A., *et al*. Designed architecture (2012) for attack prevention against XPath injection. They use a run time monitoring mechanism to determine malicious queries and prevention [30]. Chana GY, *et al*. Proposed (2012) hybrid learning, universal approximation model to observe XML SOAP based attacks on web services [31]. Rajaram Ak, et al. (2013) focused on XML injection attack detection with pluggable API as well as security services in the middleware to detect and overcome the attacks [32]. Tao Z. (2013) offered XML injection attack detection system on XML based SOAP message tree verification [33]. Gupta AN, *et al*. designed system (2016) established an interception, detection and logging module for XML attack detection [34]. Rosa TM, *et al*. (2013), proposed hybrid technique for XML injection attack on web services that applies ontology on the knowledge database for knowledge based detection [35]. Appelt D., *et al*. (2014), has proposed the vulnerability detection over the SQL injection. This vulnerability detection in web services is based on mutation operated related automated testing approach [36]. Salas P., *et al*. (2015) used fault injection technique on web services for XML injection vulnerabilities [37].

Attacks Occurs in Different Cloud

XML Signature Wrapping Attack

In October 2011, a German researcher Jorg Schwenk of Ruhr University Bochum found and reported a cryptographic hole in Amazon's EC2 and S3 services. They identified vulnerabilities in signature wrapping or XML rewriting techniques has been known since 2005 and advanced cross site scripting utilized by some AWS services. The flaw was located in the web services (WS) security protocol and enabled attackers to trick servers into authorizing digitally signed SOAP (Simple Object Access Protocol) messages to be altered. The attacker hijacked control interfaces which can be used to manage resources of cloud computing. This may permit to attacker to create, modify, delete machine images, and alter administrative passwords and settings.

As an answer, a redundant bit (STAMP bit) will be added onto signature price while appended in the SOAP header. This bit will probably be transmitted while therapeutic massage is protested with through a third occasion during the transfer. After reaching the message to its destination the STAMP bit is checked. If it has been modified, then the new signature value is sent to the server generated by browser. Then the new value is sent back to the server to change the authenticity checking [38].

Malware Injection

In May 2009, the Treasury department of U.S. Moved to a cloud platform for Bureau of Engraving and Printing (BEP), which has four web deal with URLs that focuses to one public website. These URLs are BEP.gov, BEP.treas.Gov, Moneyfactory.gov and Moneyfactory.com. The webhosting organization used by BEP had intrusion, so therefore countless web pages (BEP & non-BEP) had been affected.

Roger Thompson who's the chief research officer for Anti-Virus Guard (AVG) discovered malicious code used to be injected into the affected pages. The hackers brought a tiny snippet of a virtually undetectable iframe (Inline Frame) HTML code that redirected viewers to a Ukrainian Website. From there, quite a lot of web based attacks had been launched utilizingeasy-to-purchase malicious toolkit known as Eleonore Exploit Pack. First time users had been affected best. Second time whilst returning to the website attacks weren't leaded more, which is complicated for regulation enforcement to track the perpetrators. To preclude this sort of attack, the server operator needs to check for and make the most iFrame code. Firefox customers will have to install NoScript and set "Plugins | Forbid iFrame" option. Window user should have to ensure they've installed all security updates and have an active anti-malware guard running [39].

In June 2011, Brazilian cyber criminals deliberately launched the attacks as spam/phishing campaigns on Amazon web services, which ambitions users in Brazil notably. Customers receive spoofed emails with links with having the malicious domains hosted by Amazon. Attackers installed a style of malicious documents on victim's machines. One aspect acted as a rootkit (sort of malicious program, activated at any time when a user's system boots up) and disabled the installed anti-malware applications. Moreover, downloaded components during attack tried to retrieve login information from a list of nine Brazilian banks and two other international banks, steal digital certificates from eTokens saved on the machine, and accumulate distinct knowledge concerning the pc itself i.e. used by some banks as part of an authentication routine. The utilization of FAT (File Allocation Table) system structure is the solution, which determine the code or software that a patron is going to run [40].

Social Engineering attack

This attack depends closely on human interaction and quite often deceit other people to break down normal security approaches. The hackers used a social engineering attack in 2012 to thoroughly destroy the digital life of technical writer Mat Honam's by deleting the datafrom his iPad, MacBook and iPod remotely. The hackers take competencies of blind spot between the identification verification techniques used by Amazon and Apple. The hackers found the victim's online web addresses @me.com, which is associated Apple ID account. The hackers called the Amazon customer service and waiting

to add credit card number to the victim's account. All of the information like name, billing address and associated email address found on the web by means of hackers and asked by the representative the hacker on victim's account. Representative added the brand new credit card onto the account after the victorious answering from hacker. After ending the call, the hacker called back to the Amazon customer service and explained concerning the misplaced of access to his account. Then the Amazon representative requested to the hacker for his billing address and credit card related to the account. Hacker supplied the new credit card information from the previous phone call. As soon as the representative will get the information from the hacker they add new email address to the victim's account. Then by logging into Amazon's website the hacker requested for password reset the email address he just created. Now the hacker had access to the victim's Amazon account and credit card information on file. Then the hacker called Apple technical support and request for password reset on victim's email account @me.Com. The Apple offered yet another alternative even though the hacker does no longer answer the security questions. The Apple representative need only last 4 digits of victim's credit card and billing address then they issued the temporary password. Once the hacker had access to the victim's Apple iCloud account, the entire information from the victim's iPad, MacBook and iPod account was erased remotely.

Apple temporarily disabled its client's capability to reset an AppleID password over the phone. Instead, customers must use Apple's online "iForgot" system. They work on much stronger authentication password system to prove the customers who they are saying they are. Amazon customer service representatives will not exchange account setting like credit card or email addresses by using cell phone [41].

Account Hijacking

It happens because of credential theft which results in access sensitive information by attackers and compromises the confidentiality, integrity and availability of supplied services. e.g. eavesdropping on transaction/sensitive events, manipulation of data returning falsified information, and redirection to illegitimate sites.

In July 2012, the UGNazi hacker group exploited a main flaw in Google's gmail password recovery process and AT&T's voicemail system. It allowed the team to access the CEO of CloudFare's personal gmail account. The hacker deceived AT&T's process into redirecting the victim's cell phone to a fraudulent voicemail box. The hacker first visited the gmail and start for account recovery function for victim's personal e-mail handle. A voicemail message was recorded on the compromised voicemail box to sound like someone used to be answering the phone. From Google, a call was placed to the victim, but the victim didn't recognize the number so he let the call go to voicemail. Google's system used to be dodged by using the fraudulent voicemail and a temporary PIN were once left (which allowed the password to be reset) within the voicemail. Then the hacker was logged into the victim's gmail account and delivered his email address to the function 'account recovery control". The hackers have been stayed less than 2 hours. They used that personal gmail account for approximately 1 hour 35 minutes and CloudFare's email account for roughly 28 minutes, despite the fact that probably interrupted several occasions as their staff reset passwords and sessions. In addition, they put together the visual timeline under for better understanding of the events occurred. The email about contemporary password has been changed was received to Cloud Fare's account. So when the victimstarts to change the password, an email is sent to the hacker informing that victim changed password, however hacker changed the password right immediately. Both the users continue going back and forth to get control over the account. In short time, the hacker is able to remove victim's cell phone and e-mail addresses authorized for account recovery. As a result, the victim is averted from resetting the gmail account. The Google's account recovery system allowed two-factor authentication setup on the victim's Cloud Fare account which is to be bypassed and the hacker had access to the account. Hackers used victim's administrative privileges to change passwords on different administrative account. CloudFare's operations team suspended the victim's account, res*et al*l CloudFare's employee email passwords, and cleared all web mail sessions that terminated the access of the email system from hackers [42].

CSO supplies news, analysis and research on an extensive variety of security and risk management topics. It focuses areas include information security, physical security, business continuity, identification and access administration, loss prevention and more. CSO online. in is published with the aid of IDG (International Data Group Company) Media Private Limited. It is mentioned that Google fixed the flaw within the Google enterprise application account recovery system by using no longer permitting a user to get around two-factor authentication. Cloud Fare has stopped emailing blind copies of password resets and other transactional messages to administrative accounts [43].

In July 2012, cloud storage service 'Dropbox' informed that the hackers used usernames and passwords which are stolen from third party sites. Best the Dropbox account users received spam emails enclosed in a file. It was improved after receiving complain from users. The company believed customers who use the stolen password on a multiple websites make it simpler for hackers to access their accounts on different websites. The two-element authentication often known as Strong Authentication is applied into the company's security controls to prevent a repeat attack. The user proves his identity into properties: the user is aware of something like password, PIN, etc. User should have something like ATM card, and/or the something the user is like biometric attribute equivalent to fingerprint. The organization launched new automated mechanisms to identify suspicious activities and a brand new web page to show all logins [44].

Traffic Flooding

This attack occurs as a result of gigantic amounts of traffic and results in a network or services down. When a network or service weighted down with packets, it cannot able to process specific connection requests for the reason that it initiates incomplete connection requests. Eventually, the host's memory buffer turns into full, and so there cannot make any additional connections, so outcome is Denial of service.

A cloud-based password storage and management company named as Last Pass had announced that its server has very

likely hacked. No any data leakage reports were heard but the company insisted to the client about to take caution to ensure that their information is riskless. Because the security professionals found out an unusual behavior within the database servers with having extra traffic going out as in comparison with incoming data. This was a hacking activity assumed by means of the company and is concerned to siphoning which stored the consumer's sensitive data and login credentials. The master Passwords (passwords that defend lists of passwords to access different web sites and on-line services in the cloud) were right away converted to protect patrons from possible knowledge leakage.

The Last Pass enhanced its encryption algorithm to protect customer's data and convey additional remedies to secure sensitive data on its server in order to preclude this situation from happening again [45].

Wireless Local Area Network attack

To perform attacks similar to Man-in-middle, accidental organization, identity theft, denial of service, Network injection attacks, and so forth. The hacker breaks into a licensed user's wireless local network.

In January 2011, Thomas Roth a German researcher used cloud computing to crack wireless networks which relied on pre-shared passphrases, equivalent to in homes and small firms. Therefore of this attack revealed that wireless computing which depends on pre-shared key (WPA-PSK→Wi-Fi protected Access-Pre-Shared-Key) system for security is essentially insecure. Roth's program was run on Amazon's Elastic Cloud Computing (EC2) system. As Amazon cloud has colossal power therefore the program was capable to run via 400,000 possible passwords per second. It would typically cost tens of thousands of dollars to purchase the computers to run the program; however, Roth claims that a usual password can be guessed by means of EC2 and his software in about six minutes. The sort of EC2 computers used in the attack bills $.28 cents per minute, so $1.68 is all it took to hack into a wireless network.

WPA-PSK is believed to be secure because the computing power needed to run via the entire potentialities of passphrases in huge. However, cloud computing provides this type of computing power today at very cheap rate. It is strongly recommended that as much as 20 characters are enough to create a passphrase that are not able to be cracked, however the extra characters included, the strong passphrase will be. Quite a lot of symbols, letters and numbers must be included in the passphrase and must be changed regularly. Dictionary words and letter substitution (i.e. "c1c3" instead of "nice" should be avoided) [46, 47].

Persistent attack

The second largest healthcare provider Anthem in the U.S. Used was compromised for 78 million patient records exposure data breach in February 2015. The attack traced by way of Symantec to a well-funded Black Vine attack team that has association with a China-based IT security organization, called Topsec [49].

In keeping with file [52], in Q1, 2015 cloud services were most of the DDoS attack targets. DDoS attacks targeting services regarding cloud computing has grown up from 19 percentage two years in the past, to reach up to 33 percentages as much as 2017 [53]. Lizard Squad planned attacks on Sony gaming servers and Microsoft is the first illustration of DDoS attacks that targets cloud providers. In early 2015, Rack space servers and Amazon EC2 servers the cloud service vendors have been additionally attacked [54, 55].

In March 2015, a heavy DDoS attack targeted the Greatfire.Org website which belongs to Chinese Censorship watchdog activist group that monitors Chinese web blocks. This attack cost the company of $30,000 daily on Amazon EC2 cloud [54, 56].The Arbor Networks mentioned yet another dangerous attack that has been started known as Smoke screening attack which has parallel impact on to DDoS attack. This attack used to plan dataor information breach behind a DDoS. While the entire staff is distracted in stopping or mitigating from the present DDoS attack, the attacker may just plan to do different attacks to harm the target. According to [57], Neustar report, around 50% of the organizations were affected with the "Smoke screening attack" whilst they have been best preventing or mitigating DDoS.

India: A Haven for Cybercriminals

India is among the lucrative places to launch and an increase in cyber-attacks due to its digitization. According to the report in 2016, the number of attacks through bots greater than tripled. In 2015, attacks had been 1.3 %, however reached 10.4 % in 2016. Amongst all the threats, the highest was through bots. The term Botnet (bots) is a blend of the words "robot" and "network". It is a network of private computer systems, each of which is running one or more bots and contaminated with malicious software and controlled as a group without the owner's knowledge. It may be used to perform DDoS attack, steal data, send spam, and enables the attacker to access the device and its connection. The owner can control the botnet using command and control (C&C) software [48].

China was the origin of bot activity and has emerged as targeted for cybercrime in 2015 due to many industries up and coming economies. His rise of 84% in bot-associated activity in nation occurred. Chinese executive announced plans in 2013 to broaden broadband coverage for the rural and urban areas with the aid of 2020. Probably the most milestones for the multi-pronged strategy aimed to bring fixed broadband connections to 400 million Chinese households by 2015. Additionally, costs were kept low and broadband speeds have increased. This all make the country an appealing target for cybercriminals searching to compromise a fresh source of high-speed, internet connected computers. Bot endeavor in the U.S. by contrast, fell via 67%. Following table shows the malicious activity due to bots in different nations and the global impact of bots by percentage (See Table 1):

Table 1 Malicious activity due to bots across the globe

	2015 Country/ Region	2015 Bots % of Global	Percent Change Bots in Country/ Region	2014 Country/ Region	2014 Bots Percentage of Global
1	China	46.1%	+84.0%	China	16.5%
2	United States	8.0%	-67.4%	United States	16.1%
3	Taiwan	5.8%	-54.8%	Taiwan	8.5%
4	Turkey	4.5%	+29.2%	Italy	5.5%
5	Italy	2.4%	-71.2%	Hungary	4.9%
6	Hungary	2.2%	-69.7%	Brazil	4.3%
7	Germany	2.0%	-58.0%	Japan	3.4%
8	Brazil	2.0%	-70.1%	Germany	3.1%
9	France	1.7%	-57.9%	Canada	3.0%
10	Spain	1.7%	-44.5%	Poland	2.8%

Businesses targeted in India in 2016

The Symantec Corporation or Symantec is an American software company that provides cybersecurity software and services. In line with the Symantec Internet Security ThreatReport 2017, India ranks fifth in ransomware attacks globally. There was 36% increase in ransomware attacks globally. The Tarun Kaura, the director of Solution Product Management for Asia Pacific and Japan stated Symantec; cybercriminals have prompted unusual phases of disruption with the aid of focusing their exploits on relatively simple IT tools and cloud services. He mentioned "The cybercriminals understand the security mechanism of enterprises. For instance, earlier the malware was spread through .exe files, but now it is through word document. As soon as the cybercriminals have access to credentials, they may be able to compromise computing property".

Within the top wholesale alternate and mining industries, one in 84 industries was once infected by way of malware and one in 85 industries in mining have been impacted. The industries littered with spam mail had been mining 74%, wholesale trade 61.7%, finance, insurance, and real estate 59.5% [48].

In February 2015, 78 million people records were exposed in a main data breach at Anthem, which is a second greatest healthcare provider in the U.S. Symantec traced the attack to a well-funded attack group, named Black Vine, that has association with a China-based IT security institution, referred to as To psec. Black Vine is responsible for carrying out cyber espionage campaigns, against a couple of industries, together with energy and aerospace, using advanced, custom-developed malware.

Over excessive-profile targets of cyber espionage in 2015 incorporated the White House, the Pentagon, the German Bundestag, and the U.S. Government's Office of Personnel Management, which lost 21.5 million personnel files, including sensitive information such as health and financial history, arrest records, and even fingerprint data. These attacks are part of a rising tide of subtle, well-resourced, and persistent cyber espionage attacks around the globe. Targets include state secrets, intellectual property equivalent to design, patents, and plans, and as evidenced via recentdatabreaches, personal information.

On 31st December 2015, the BBC's (British Broadcasting Corporation) websites were unavailable early in the morning because of a colossal webattack. Its associated services in the UK including iPlayer catch-up service and iPlayer Radio app taken down for several hours on New year's evening. It's to be greatest ever DDoS attack according to New World Hacking, the Anti-Islamic State organization that claimed accountability. The attacker claimed that the BBC's scale offered a risk for them to test their capabilities and claim the attack reached a peak of 602 Gbps bandwidth.

Top Five DDoS Attack Traffic

The majority of DDoS attacks were ICMP flood attacks, where a large volume of (typically) 'ping' requests eventually overload the target until it can no longer handle legitimate traffic. The table 2 given below presents the top five DDoS attack traffic seen by Symantec's Global Intelligence Network [52].

Table 2 Top five DDoS attacks scrutinized by Symantec

	2015 Attacks	2015 Attack Rate	2014 Attacks	2014 Attack Rate
1	Generic ICMP Flood Attack	85.7%	DNS Amplification Attack	29.4%
2	Generic TCP Syn Flood Denial of Service Attack	6.4%	Generic ICMP Flood Attack	17.2%
3	Generic Ping Broadcast (Smurf) Denial of Service Attack	2.1%	Generic Ping Broadcast (Smurf) Denial of Service Attack	16.8%
4	Generic Teardrop/ Land Denial of Service Attack	2.0%	Generic Teardrop/Land Denial of Service Attack	7.2%
5	RFProwl Denial of Service Attack	0.6%	Generic ICMP Unreachable Denial of Service Attack	5.7%

The National Health Service (NHS), England was launched in 1948, reported the investigation by the Controller and Auditor General about WannaCry Cyber-attack in April 2018. On 12 could 2017, a massive ransom ware attack occurred across a wide range sectors, including health care, government, telecommunications and gas. To date, WannaCry has spread to over 300,000 systems in over 150 countries. The countries that appear to be the most affected are Russia and China, probably because of the high percentage of legacy software, with significant impacts elsewhere, particularly to the UK National Health Services (NHS) [52], although it was not the certain target. At 4 pm NHS declared the cyber-attack a major incident and applied its emergency arrangements to maintain health and patient care.

In the evening, a cyber-security researcher activated a "Kill-Switch" in its code so that WannaCry stopped locking gadgets. WannaCry ransomware affected as a minimum 80 (34 infected and locked out of devices, of which 25 had been acute trusts and 46 not infected but reported disruption out of 236 trusts throughout England on the grounds that of both either infected with the aid of ransomware or became off their devices or systems as precaution.

Further 603 primary care and other NHS organizations were also infected, together with 595 GP practices. This attack affected NHS services within the week from 12 may to 19 may 2017. The health department and NHS England worked with NHS Digital, NHS improvement, the National Cyber Security Centre, the National Cyber Crime Agency and others to respond to the attack. Enormous quantities of appointments and operations have been cancelled and in five areas patients had to

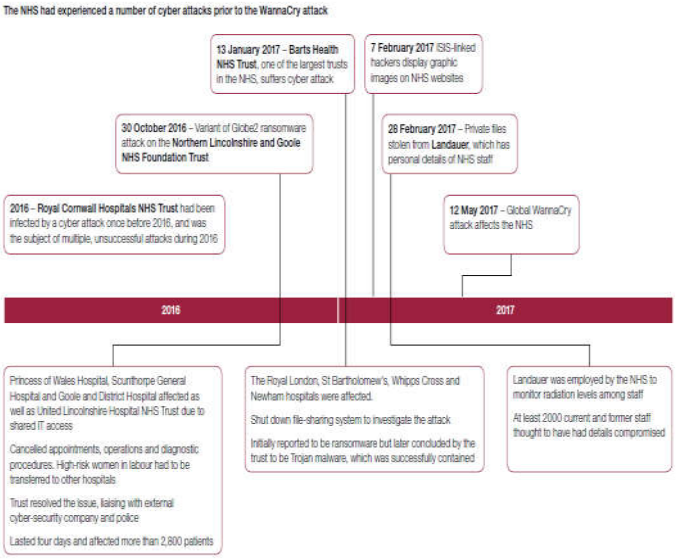
travel further to travel to accident and emergency departments. The NHS organizations paid the ransom, but the department does not know the cost of disruption to services.

More than a few individual NHS trusts had been attacked earlier than 12 May 2017, even though WannaCry was the largest cyberattack. The England's largest trusts, Barts Health NHS trust had been infected by earlier cyberattack and Lincolnshire Goole NHS Foundation Trust had been infected via ransomware attack in October 2016, which results in the cancellation of 2,800 appointments.NHS organizationsacross England had been affected by the WannaCry attack. Figure 3 sets out the location of the trusts affected and shows the:

• 34 trusts infected by the WannaCry malware; and
• 46 trusts now not infected with the aid of the malware but reporting disruption [50].(see Figure 1)

Cyber Attacks on the NHS in 2016 and 2017 before 12 May 2017

WannaCry spreads by way of SMB, Server Message Block protocol running over ports 445 and 139, on the whole used by Windows machines to communicate with file systems over a network. Once effectually installed, this ransome ware scans for and propagates to other at-risk devices. WannaCry tests to look if backdoors (like DoublePulsar) are already on previously infected machines. DoublePulsar is backdoor implant tool developed by the U.S. National security Agency's (NSA) Equation Group that was leaked by The Shadow Brokers in early 2017. The tool infected more than 200,000 Microsoft Windows computers in just a few weeks and was used alongside Eternal Blue in the May 2017 Wanna Cry ransomware attack (see Fig.1) [51].



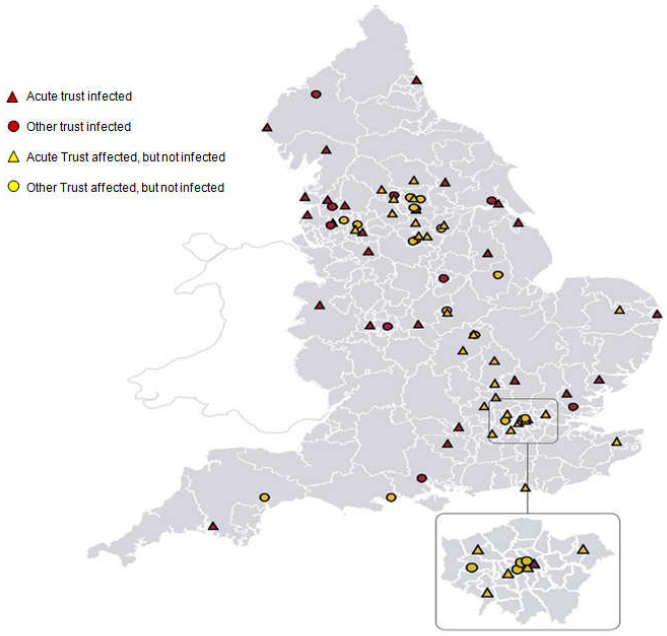
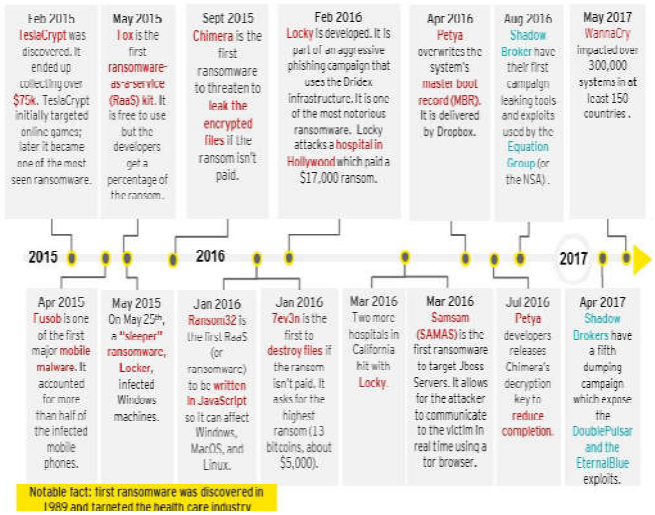


Fig 1 Trusts affected by the cyber attack

Disruption to front-line services affected all parts of the country but was concentrated in the North HNS region and the Midlands and East NHS region

Recap of Notable Ransomware Events



Global Impact of WannaCry

There are approximately 30–40 publicly named corporations among the probably hundreds of thousands that were impacted by the ransomware. Examples include the Russian Interior Ministry, Telefonica (Spain's largest telecommunications company) and FedEx. The UK NHS was badly hit, with 16 of the 47 NHS trusts being affected, and routine surgery and healthcare professional or doctor appointments being canceled because the service recovers. There are reports that in China over 40,000 organizations had been affected, together with over 60 academic institutions (see fig.2).

Fig 2 Global impact of WannaCry Ransomware

CONCLUSION

As cloud computing security has been a foremost task in latest years. Consequently, more than a few mechanisms had been developed by the researchers to defend and improve the security of cloud computing systems in opposition to attacks. In this paper we have offered real world cases where the attacks have been occurred in the company's cloud. We now have discussed distinctive forms of attacks equivalent to social engineering attacks, XML signature wrapping attacks, malware injection, data manipulation, account hijacking, SYN flood and wireless field network attacks, and so forth. However, DoSis the intense threat and increasing its attack rate in distinct areas.

Symantec take a fresh appear each and every year on the structure and contents of the report. Also makes a specialty of the threats and reports the findings, tracks industry trends, and so on from their research. Symantec highlights the most important developments and look to future trends. This goes beyond simply looking at computer systems, smartphones, and other products, and extends into extensive ideas like national security, the economy, data protection, and privacy.

In this paper, we have taken a high-level view on the reports of cybersecurity and internet threats, peculiarly on the healthcare systems, underlining the first rate changes and developments. Nonetheless, we ought to no longer forget that cybercrime will not be victimless. For example, ransomware locks folks out of their desktops, retaining treasured family photos to ransom, hijacking unfinished manuscripts for novels, and blocking access to tax returns, banking records, and other valuable documents. Moreover, there are not any ensures that paying the ransom will release these padlocks. Corporations, as well as home users, have end up victims, and relying on backups is almost always the last line of security when cybersecurity should rather be the primary. Targeted attacks steal invaluable intellectual property from businesses, and a data breach can shred an organization's reputation-even threatening its survival. Cyber insurance claims are developing in quantity and price, pushing premiums even better. In the broadest sense, cybersecurity problems threaten national security and economic growth, which ultimately affects us all.

To mitigate attacks, staff must be educated and expert on the risks posed through spear-phishing emails and other malicious email attacks, together with the place to internally report such makes an attempt. At the same time companies should detect the networks for abnormal and suspicious conduct, and correlate it with risk intelligence from experts.

References

1. Varsha R Moulia*, KP Jevitha, "Web Services Attacks and Security- A Systematic Literature Review", 6th International Conference On Advances In Computing & Communications, ICACC 2016, 6-8, September 2016, Cochin, India, Procedia Computer Science 93 (2016) 870 – 877.
2. R. Ramya, G. Kesavaraj, A Survey on Denial of Service Attack in Cloud Computing Environment, *International Journal of Advanced Research in Education & Technology* (IJARET), Vol. 2, Issue 3 (July - Sept. 2015)
3. Gazala Matloob, "A Survey on cloud computing security Issues and its possible solutions", IJARCS,March 2017.
4. Shivali Munjal, Shelly Garg, "Enhancing Data security and storage in cloud computing Environment", IJCSIT, Vol.6, 2015.
5. Elham Abd Al Latif Al Badawi, Ahmed Kayed, "Survey on Enhancing the Data Security of the Cloud Computing Environment By Using Data Segregation Technique", IJRRAS, May 2015.
6. Prachi Tembhare, Neeraj SHukla, "An Integrated and Improved Scheme for Efficient Intrusion Detection in Cloud", *International Journal of Scientific Research in Computer Science and Engineering*, Vol.5, Issu.3, pp.74-78, June 2017.
7. Marwa Elsayed, Mohammad Zulkernine, "A Classification of Intrusion Detection Systems in the Cloud", *Journal of Information Processing, Information Processing Society of Japan*, Vol.23, No.4, 392-401, July 2015.
8. Kirtesh Agrawal, Nikita Bhatt, "Survey on DDoS Attack in Cloud environment", *International Journal of Innovative and Emerging Research in Engineering, vol.2, Issue.3, 2015.*
9. Prachi Tembhare, Neeraj Shukla, "A study on Various attacks and Intrusion Detection Systems in Cloud", IJARCCE,vol.5, Special Issue 3, November 2016.
10. Ajey Singh, Dr. Maneesh Shrivastava, "Overview of Attacks on Cloud Computing", *International Journal of Engineering and Innovative Technology* (IJEIT), VII.1, Issue 4, April 2012.
11. Andrew Carlin, Mohammad Hammoudeh, Omar Aldabbas, "Defence for Distributed Denial of Service Attacks in Cloud Computing", International Conference on Advanced Wireless, Information, and communication Technologies (AWICT 2015).
12. Zheng J, & Hu MZ, "Intrusion detection of DoS/DDoS and probing attacks for web services", Advances in Web-Age Information Management; 2005. p. 333-344.
13. Chonka A, Zhou W, & Xiang Y., "Defending grid web services from xdos attacks by sota", IEEE International Conference on Pervasive Computing and Communications; 2009. p. 1-6.
14. Pinzón C, De Paz JF, Zato C, & Pérez J., "Protecting web services against dos attacks: A case-based reasoning approach", Hybrid Artificial Intelligence Systems; 2010. p. 229-236.

15. Ficco M, & Rak M., "Intrusion tolerant approach for denial of service attacks to web services", First International Conference on Data Compression, Communications and Processing; 2011. p. 285-292.
16. Suriadi S, Stebila D, Clark A, & Liu H., "Defending web services against denial of service attacks using client puzzles", IEEE International Conference on Web Services; 2011. p. 25-32.
17. Pinzón CI, Bajo J, De Paz JF, & Corchado JM. S-MAS, "An adaptive hierarchical distributed multi-agent architecture for blocking malicious SOAP messages within Web Services environments", Expert Systems with Applications; 2011. p. 5486-5499.
18. Mainka C, Jensen M, Iacono LL, & Schwenk J. XSpRES, "Robust and Effective XML Signatures for Web Services", CLOSER; 2012. p. 187-197.
19. Falkenberg A, Mainka C, Somorovsky J, & Schwenk J., "A new approach towards DoS penetration testing on web services", IEEE 20th International Conference on Web Services; 2013. p. 491-498.
20. Altmeier C, Mainka C, Somorovsky J, & Schwenk J., "AdIDoS-Adaptive and Intelligent Fully-Automatic Detection of Denial-of-Service Weaknesses in Web Services", Data Privacy Management, and Security Assurance; 2015. p.65.
21. Chana GY, Chuaa FF, & Leeb CS., "Fuzzy association rules vs fuzzy associative patterns in defending against web service attacks", 12th International Conference on Fuzzy Systems and Knowledge Discovery ; 2015. p. 524-529.
22. Gruschka N, & Luttenberger N., "Protecting web services from dos attacks by soap message validation", Security and privacy in dynamic environments; 2006. p. 171-182.
23. Loh YS, Yau WC, Wong CT, & Ho WC., "Design and Implementation of an XML Firewall", International Conference on Computational Intelligence and Security; 2006. p. 1147-1150.
24. Vieira M, Antunes N, & Madeira H., "Using web security scanners to detect vulnerabilities in web services", IEEE/IFIP International Conference on Dependable Systems & Networks; 2009. p. 566-571.
25. Antunes N, & Vieira M., "Detecting SQL injection vulnerabilities in web services", Fourth Latin-American Symposium on Dependable Computing; 2009. p. 17-24.
26. Laranjeiro N, Vieira M, & Madeira H. A, "Learning-Based Approach to Secure Web Services from SQL/XPath Injection Attacks", IEEE 16th Pacific Rim International Symposium on Dependable Computing; 2010. p. 191-198.
27. Laranjeiro N, Vieira M, & Madeira H., "Protecting Database Centric Web Services against SQL/XPath Injection Attacks", Database and Expert Systems Applications; 2009. p. 271-278.
28. Patel V, Mohandas R, & Pais AR, "Attacks on Web Services and mitigation schemes", International Conference Security and Cryptography; 2010. p. 1-6.
29. Siddavatam I, & Gadge J., "Comprehensive test mechanism to detect attack on Web Service", 16th IEEE International Conference on Networks; 2008. p. 1-6.23.
30. Asmawi A, Affendey LS, Udzir NI, & Mahmod R, "Model-based system architecture for preventing XPath injection in database-centric web services environment", 7th International Conference on Computing and Convergence Technology; 2012. p. 621-625.
31. Chan GY, Lee CS, & Heng SH, "Policy-enhanced ANFIS model to counter SOAP-related attacks", Knowledge-Based Systems; 2012. p. 64-76.
32. Rajaram AK, Babu BC, & Kishore Kumar RC, "API based security solutions for communication among web services", Fifth International Conference on Advanced Computing; 2013. p. 571-575.
33. Tao Z., "Detection and service security mechanism of xml injection attacks", Information Computing and Applications; 2013. p. 67-75.
34. Gupta AN, & Thilagam PS., "Detection of XML Signature Wrapping Attack Using Node Counting", 3rd International Symposium on Big Data and Cloud Computing Challenges; 2016. p. 57-63.
35. Rosa TM, Santin AO, & Malucelli A., "Mitigating xml injection 0-day attacks through strategy-based detection systems", Security & Privacy; 2013. p. 11(4), 46-53.
36. Appelt D, Nguyen CD, Briand, LC, & Alshahwan N., "Automated testing for SQL injection vulnerabilities: an input mutation approach", International Symposium on Software Testing and Analysis; 2014. p. 259-269.
37. Salas P, Invert M, De Geus PL, & Martins E., "Security Testing Methodology for Evaluation of Web Services Robustness-Case: XML Injection",. IEEE World Congress on Services; 2015. p. 303-310.
38. A. Hickey, "Researchers uncover 'massive security flaws' in Amazon cloud", Available: http://www.crn.com/news/ cloud/231901911/re
39. M. Kronfield, "Treasury Dept. has cloud hacked", Available: http://www.gsnmagazine.com/article/20691/treasury_dept_has_cloud_hacked
40. D. Fisher, "Attackers using Amazon cloud to host malware", Available: http://threatpost.com/en_us/blogs/attackers-using-amazon-cloud-hostmalware-060611
41. J. Pepitone, "Hack attack exposes major gap in Amazon and Apple security", Available: http://money.cnn.com/2012/08/07/technology/mathonan-hacked/index.htm
42. M. Prince, "The four critical security flaws that resulted in last Friday's hack", Available: http://blog.cloudflare.com/the-four-critical-securityflaws-that-resulte
43. L. Tung, "CloudFare boss's Gmail hacked in redirect attack on 4Chan", Available: http://www.cso.com.au/article/426515/cloudflare_boss_gmail_hacked_redirect_attack_4chan/
44. Kiril, "LassPass possibly hacked, cloud security concerns on the rise", Available:http://www.cloudtweaks.com/2011/05/lastpass-possiblyhacked-cloud-security-concerns-on-the-rise/
45. PC World Staff, "Cloud computing used to hack wireless passwords",

Available: www.pcworld.com/article/216434/cloud_computing_used_to_hack_wireless_passwords.html
46. Chimere Barron, Huiming Yu and Justin Zhan, "Cloud Computing Security Case Studies and Research", Proceedings of the World Congress on Engineering , Vol II, WCE 2013, July 3-5, 2013, London, U.K.
47. www.csoonline.in
48. Internet SecurityThreat Report (ISTR), Symantec, Volume 21, April 2016.
49. Investigation: WannaCry cyber attack and NHS, National Audit Office, HC 414, Session 2017-2019, 25 April 2018.
50. "WannaCry" ransomware attack, EY Technical Intelligence Analysis, May 2017
51. https://www.infosecurity-magazine.com/news/q1-2015-ddos-attacks-spike/, Security and technical news, "Q12015 DDoS attacks spike, targeting cloud", Latest Access Time for the website is 19 January 2018.
52. Fadi SHAAR, Ahmet EFE, "DDoS Attacks and Impacts on Various Cloud Computing Components", *International Journal of Information Security Science*, Vol.7, No.1
53. G. Somani, M. Singh, D. Sanghi, M. Conti, and R. Buyya, "DDoS attacks in cloud computing: Issues,taxonomy, and future directions," Computer. Communications., vol. 107, pp. 30–48, 2017.
54. R. V Deshmukh and K. K. Devadkar, "Understanding DDoS Attack & Its Effect in Cloud Environment", Procedia Computer Science., vol. 49, pp.202–210, 2015.
55. https://nakedsecurity.sophos.com/2015/03/20/greatfireorg-faces-daily-30000-bill-from-ddos-attack/L,"Greatfire.org faces daily $30,000 bill from DDoS attack", Latest Access Time for the website is 22 January 2018.
56. Neustar News, "DDoS attacks and impact report finds unpredictable DDoS landscape", https://nscdn.neustar.biz/creative_services/biz/neustar/www/resources/whitepapers/it-security/ddos/2016-fall-ddosrepo

How to cite this article:

Lomte S. S *et al*.2018, Survey of Real Case Studies of Various Network Based Attacks Indifferent Clouds. *Int J Recent Sci Res.* 9(11), pp. 29545-29556. DOI: http://dx.doi.org/10.24327/ijrsr.2018.0911.2880

****