Cyber-Attacks in Cloud Computing: A Case Study

Jitendra Singh

Department of Computer Science, PGDAV College, University of Delhi
Ring Road, Nehru Nagar, New Delhi, India, PIN-110065, India
(Email: jitendra.singh0705@gmail.com)

(Received June 6, 2014; revised and accepted Aug. 17, 2014)

Abstract

Cloud computing has emerged from the legacy system; consequently, threats applicable in legacy system are equally applicable to cloud computing. In addition, cloud specific new threats have also emerged due to the various reasons including, multi-tenancy, access from anywhere, control of cloud, etc. Considering the significance of cloud security, this work is an attempt to identify the major threat factors to cloud security that may be critical in cloud environment. It also highlights the various methods employed by the attackers to cause the damage. To accomplish our objective, we have reviewed the major publication related to cyber security. It is revealed that cyber-attacks are industry specific and vary significantly from one industry type to another. Finally, we have conducted the case study on cyber-attacks that are already occurred in cloud paradigm. Cyber-attacks were highlighted by categorizing them into phishing attacks and distributed denial of services. This work will be profoundly helpful to the industry and researchers in understanding the various cloud specific cyber-attack and enable them to evolve the strategy to counter them more effectively.

Keywords: Cyber security, cloud Attack, cybercrime, resource protection, cloud threat

1 Introduction

Enterprises and individual users prefer outsourcing their services on the web, instead of maintaining the resources of their own. Outsourcing of technical resources enables the organization to concentrate on business need instead of technical aspect that is managed by the experts in Information Technology (IT) area. To facilitate such users, a web based paradigm known as cloud computing has emerged and offering the services on utility model [13]. The major goal of Cloud computing is to reduce the operating cost, increase throughput, increase the reliability and availability [12].

To cater the need of wide variety of users, cloud is offering three types of services. These services include Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS) [17]. In IaaS, users are offered the computing capabilities such as processor, RAM, Storage, etc. as Services [4]. All these resources are offered on rent basis from the cloud instead of private services [9]. The appealing feature of the IaaS is that the users do not need to change the infrastructure periodically, which gets outdated in every three years due to the Murphy's Law. Users are also free from updating the operating system, installing the new patches that are frequently needed to plug the exploited vulnerabilities.

In PaaS, development environment is offered as a service; whereas in SaaS, applications are offered as services. In SaaS environment, applications subscribed are available for use without any delay, while in legacy system user has to wait for months or sometimes for years to get the application developed. Google docs, invoices, cloud ERP, etc. is some of the prominent examples of SaaS based services. All the cloud services (IaaS, PaaS, and SaaS) are offered via public, private or community based deployment model. All these cloud deployment models have been classified depending upon the ownership held by the cloud user. If the cloud resources are under the control of cloud users, then it is known as private model (aka on-premises model), whereas if the cloud resources are under the control of cloud provider in that case it is known as public cloud (aka hosted model). In public model, resources are accessed with the help of software known as clients that connect to the cloud server remotely. Desktop, Laptop, Smartphones, etc. are some of the clients that can be utilized to access the cloud resources.

Despite of the above advantages, Cloud computing has also lead to the emergence of various challenges. Various factors need to be considered before the cloud adoption. Many of these issues are attributed due to the remote availability of resources, location of data center in other country, no control on data center, etc. All the above issues pave the fertile ground to the cyber attacker to determine the vulnerabilities and exploit the cloud resources. Many of the authors have considered security as the major challenge [6, 13].

2 Security in Cloud Computing

Security in the cloud computing is a major challenge and retarding the proliferation of cloud computing [8, 19, 28]. Understanding the criticality involved in cloud security, various working groups and standard organizations have been formed to take up cloud security. Cloud security alliance (CSA), NIST, ENISA, etc. are some of the prominent groups working for the cloud security and suggesting their recommendations, releasing the guidelines, to secure the cloud. Among all the above groups, Cloud security alliance is entirely committed for the cloud security. Many of the significant documents have already been published by CSA related to the cloud security.

To identify the major contemporary threats, CSA has published the report on the top threats. Although, similar report was also published earlier in 2010 titling 'Top Threats to Cloud Computing V1.0' [8], but the new study was required due to the change in methodologies by the attackers and to examine the current security trend in cloud computing. The report is published with the title 'The Notorious Nine Cloud Computing Top Threats in 2013' [7]. In this study, CSA has reviewed thousands of article related to cloud threat, asked from a number of experts and visited the different website. Correspondingly, the group has identified the major threats on cloud computing that have significant impact in cloud computing. In this most recent report, experts have identified the following nine critical threats to cloud security (ranked in order of severity):

1). Data Breaches

2). Data Loss

3). Account Hijacking

4). Insecure APIs

5). Denial of Service

6). Malicious Insiders

7). Abuse of Cloud Services

8). Insufficient Due Diligence

9). Shared Technology Issues.

2.1 Data Breaches and Data Loss

Once the information is available to any entity, other than the owner then it is known as data breach. It is more critical in cloud computing where the data is under the control of third party and promotes the resource sharing among many users. Cloud computing has also opened the new avenue of attacks including side channel attack. In this attack, the adversary can use virtual machine's side channel timing information to extract the private cryptographic key used in other's VM on the same physical server. Multi-tenancy architecture of cloud computing also offers more vulnerability, if it is not properly designed. Flaw exist in one user's database can affect the safety and security of others data stored in the same cloud.

Data loss is the other key issue related to cloud security. In data loss users are losing the information stored, whereas in data breaches, information is stolen by the adversaries. For instance to secure the data, user may opt for data security. But loss in encryption key may result in data loss. Similarly, to prevent the catastrophic loss if the user is storing the data in backup devices, it means data is more vulnerable to attack. Data breaches is applicable in IaaS, PaaS and SaaS deployment model of the cloud computing. It is believed that this threat is still relevant.

2.2 Account Hijacking and Denial of Service

Account hijacking exists in legacy system, where adversary takes over the control of user's account. In cloud paradigm it poses additional challenges. For instance, if credential is stolen by the adversary then he can eves drop, modify, information even worst can direct cloud users to illegitimate web site. In the denial of services, illegitimate users are using the cloud resources and denying the legitimate users from accessing the resources. In cloud computing distributed denial of services (DDoS) attacks are frequently caused.

2.3 Insecure APIs

Cloud providers are offering their API's to the developers so that they can develop the application to connect to their cloud. These API's are openly available and can easily be used by the developer community. But it has been observed that the API's that are offered are not secured enough, as needed for the cloud environment. This vulnerability has been observed due to third party usage of cloud APIs. Consequently, insecure API's make the cloud vulnerable to various attacks.

2.4 Abuse of Cloud Services and Malicious Insider

Cloud providers maintain the huge resources. Once the cloud users subscribe for the cloud resources they are passed under the control of subscribed users. This subscriber may be an adversary. Consequently, huge resources come under the disposal of adversary that can be utilized by him in various analyses. In legacy system, to buy such resources required huge investment, consequently huge computation was not possible.

User's rights are given to perform certain task for the smooth functioning of the organization. However, it has been observed that these services are mis-utilized, particularly by the power user, for instance System administrator.

The other major threat is malicious insider, in which someone from the inside only facilitates in external attacks. These passages may be provided intentionally or un-intentionally. Opening of the mail that has received by the user and clicking the link provided aims of knowing more about the users organization falls under the category of un-intentional attack.

2.5 Undue Diligence, Selection for Cloud Selection

Many of the users are selecting the cloud due to huge infrastructure, minimum upfront cost, security offered by the cloud, etc. Considering the huge potential growth many new cloud provider have emerged and continue to emerge on daily basis. Consequently, it is imperative to conduct the sufficient background check of the cloud provider, security offered, regulatory compliance, etc. used by them. Necessary contract related to data availability is also need to be placed to avoid any future disputes.

2.6 Shared Technology Usage

In the IaaS model of cloud, resources such as processor, memory, bandwidth etc. are utilized by the subscribers on shared basis. Similarly, in SaaS environment, same application is shared among many users. In cloud, Hypervisor have significant role in isolation and resource provisioning. Since, all the users are on the top layer of hypervisor, if the security of the hypervisor is compromised, security of the entire cloud may be breached at once.

3 Study on Cyber-Attack in Cloud Computing

Cloud resources are the attractive ground for the cyber-criminals due to the huge resources available at the centralized place. Accessibility by anyone subscribing, and from anywhere is highly suitable for cyber criminals. Now, they can access the resources from any part of the world and any time, even the use of device is not restricting the usage of cloud resources. Consequently, huge cloud resources under the disposal of adversary pose major threats to the cloud and web users. They are utilizing cloud resources in many of their cyber-attacks.

McAfee and Guardian analytics have uncovered sophisticated attack that are targeting to financial services. Before, it was considered that cyber-crime is confined to the Europe but the study revealed that it is reached to other parts of the world, including US and Columbia. These attacks are automated and targeting the account with huge balance. In addition, they have also targeted the credit union, large global bank, and regional bank. From these fraudulent activities they could manage to transfer $78 million (USD) from various accounts of Financial Institutions.

3.1 Review of Cloud Threats

Being a new paradigm and concentration of resources, there is great threat to cloud computing. Twelve major threats have been identified by the [11]. Identified threats have been denoted as T1 to T12. Abuse and nefarious use of cloud has been named as T1, insecure interfaces as T2, malicious insiders as T3, etc. Other threats and their nomenclature have discussed in Table 1.

Critically of these threats can be identified with the number of attacks that have already taken place. As per the study conducted by [1], T2 (Insecure interfaces and APIs) have been considered as the major threat, it is followed by T5 (Data loss or leakage). Ranking of other threats can be determined by Figure 1 [11].

Table 1: Threats in cloud computing

Abuse and Nefarious Use of Cloud Computing	Insecure Interfaces and APIs	Malicious Insiders	Shared Technology Issues	Data Loss or Leakage	Account or Service Hijacking
T1	T2	T3	T4	T5	T6
Unknown Risk Profile	Cloud related malware	Natural Disaster	Closure of cloud services	Cloud related malware	Inadequate Infrastructure Design and Planning
T7	T8	T9	T10	T11	T12

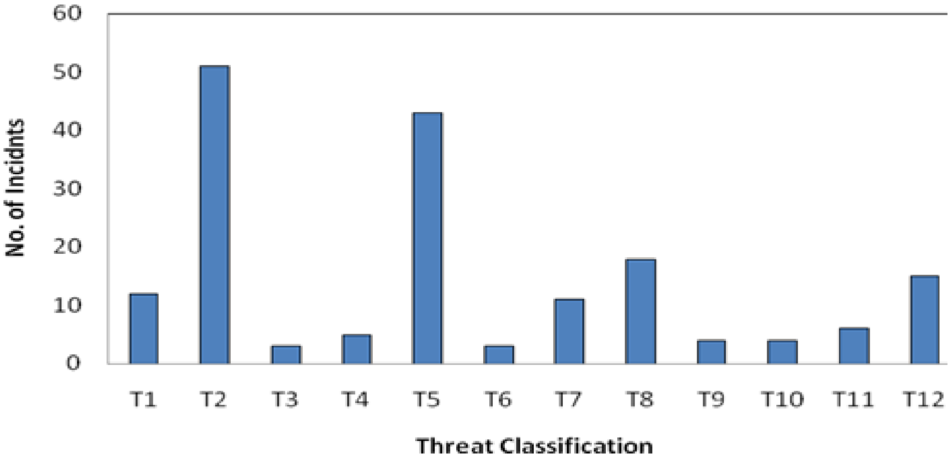

Figure 1: Threat classification

Once we further drilled down to identify which cloud is most affected (determined by the number of incidents that took place), while comparing to other clouds big cloud giant's (Google, Amazon, Microsoft etc.) are primarily targeted by the cyber criminals. Number of incidents that took place in different cloud has been illustrated in Figure 2.

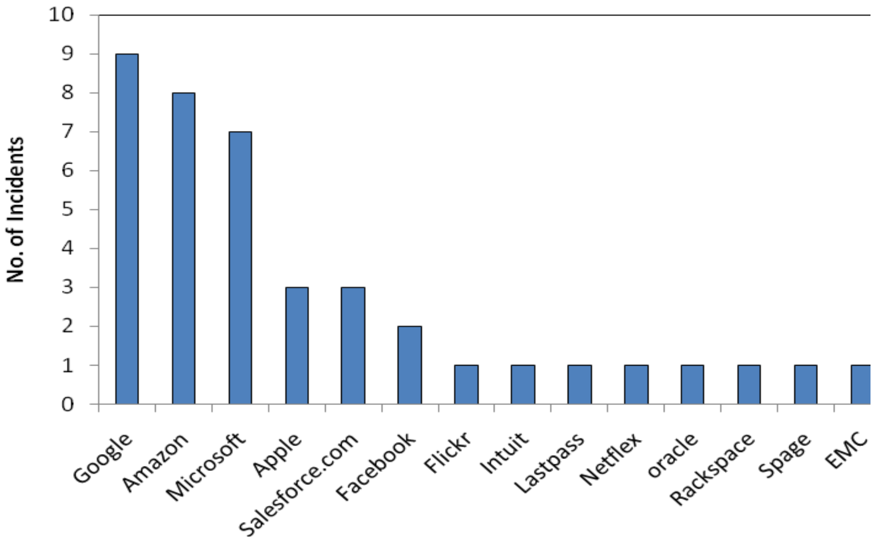

Figure 2: Number of incidents reported in major cloud

3.2 Study on the Type of Industry Targeted

Recently, IBM security services, 'cyber security intelligence index has carried out the study to figure out the industry that is most attacked by cyber criminals. As per this study, finance and infrastructure, ICT, & health and social services are the prominent industry types that are attracting to cyber-criminal in huge number. From the total cyber-attack that took place 20.9% were directed to finance and insurance domain.

Majority of the attacks are caused by the outsiders and consisting of 50% of the total attackers [15]. However, malicious insiders are equally a cause of cyber-attack, and causing 20% of the overall attack. The key objectives of these attacks were to harm the ICT users in one way or the other and the same has been illustrated in the Figure 3 [1].

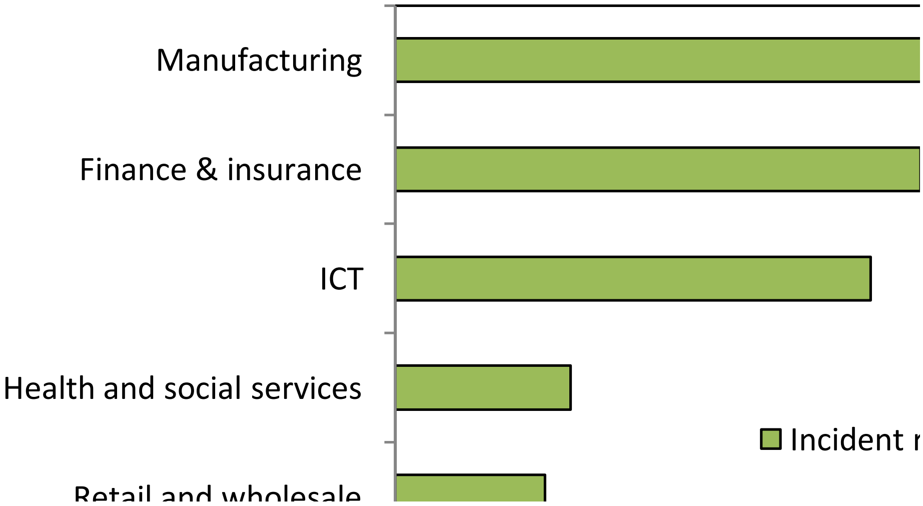

Figure 3: Attack incident rates as per the industry (Source: [15])

3.3 Categories of Cyber-Attack in Cloud

As per the study conducted by AlertLogic on its customer, it was observed that more than 45,000 security incidents were verified between 01April 2012 to 30 Sept 2012 [1]. In this study, cloud computing was categorized into hosted cloud and enterprise data center. Hosted model is similar to public model where the resources are under the control of cloud provider. The other model (enterprise model) is privately owned model where the resources are under the control of the owner. Study revealed that hosted cloud security is better than the enterprise data center. Cyber-attacks that are taking place in hosted data center and enterprises data center are not same [1]. However, for our study we have considered the common factors that are applicable in both the model to compare them which is more secure.

Study has considered the incidents which are caused by malware/botnet, Brute force attack, and web app attack in hosted and enterprise model. Incidents along with their definition have been depicted in Table 2.

Table 2: Incident descriptions and their definitions

S.No.	Incident Descriptions	Definitions
1.	Malware/botnet	Malicious software deployed on a host and gets involved in unscrupulous activities, such as data destruction, information gathering or creation of backdoors.
2.	Brute force	Exploit attempts enumerating a large number of combinations typically involving multiple credential failures, in hopes of finding a weak door.
3.	Web app Attack	Attacks targeting the presentation, logic or database layer of web apps

As per the Alertlogic's study, Enterprise data center are much affected with the Malware activities that account to 49%, and followed by Brute force attack with 49%. Whereas, it is less frequent in hosted model [1]. Same is also illustrated in Figure 4 [1]. In hosted model, web application attacks are more relative to the enterprise model and account for 52% of the total attack [1]. Majority of these attacks are taking place with automated software.

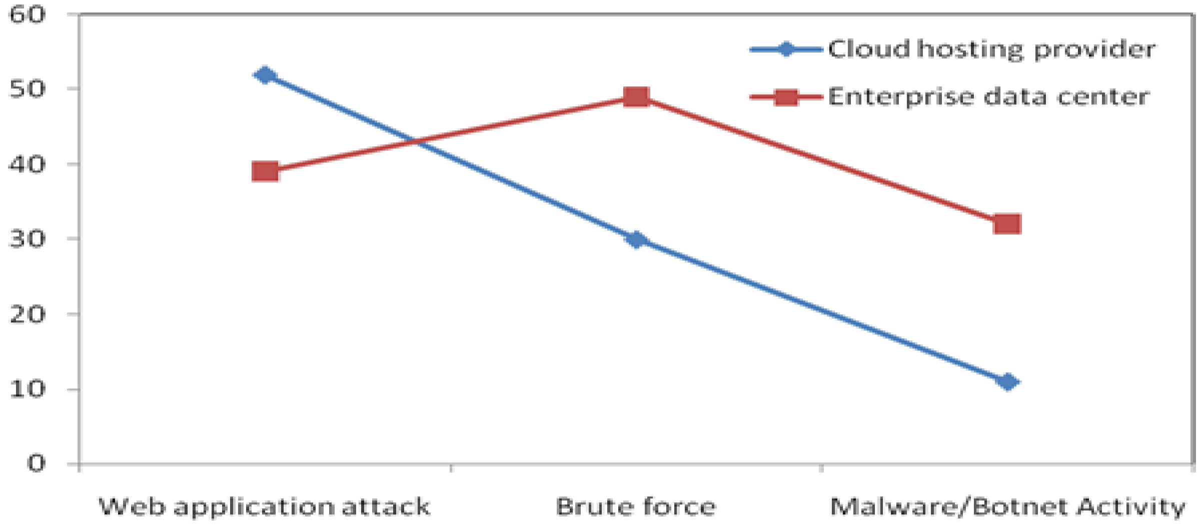

Figure 4: Categories of attack on hosted and enterprise data center

With the help of Figure 4, it can be concluded that hosted model of cloud is more secure relative to the enterprise model when we consider brute force attack or the malware/botnet attack. However, web application attacks are more in hosted model of cloud in comparison to the enterprise model.

4 A Case Study on Cyber-Attacks in Cloud

Information security is all about Confidentiality, Integrity & availability (CIA) [6]. Among the CIA, administration are more focused on confidentiality and integrity due to the involvement of regulatory compliances. Lack of focus on availability makes it more vulnerable to attacks. Recent attacks that took place in cloud are the examples of security hole exploited by cyber-criminals. Cyber attackers resort the cloud and leveraging it various platforms for malware infection and data ex-filtration. DBaaS is one of the services that are attacked by the cyber-crime [13]. This is revealed by the recent study titling 'Assessing the threat of DBaaS landscape' carried out by security outfit Imperva to analyze how the DBaaS is affected by the cyber criminals.

4.1 Identifying the Major Factors of Cyber Crime

To study the major breaches in cyberspace particularly cloud computing, we have identified the factors that can have significant impact on cloud security. To attain this objective, we have reviewed the literature published in prominent research journals. Further, we have also reviewed the publications from the varieties of working groups active in this domain including cloud security alliance, ENISA, NIST, etc. Survey and findings of security organizations, for instance Kaspersky, Micro-trend, and McAfee has been extensively reviewed.

By reviewing the literature [3, 6, 13, 21, 22, 27] it is revealed that DDoS is the major threat in cloud computing and need to be addressed at appropriate level. In DDoS, legitimate users are denied the resources due to the excessive use by non-legitimate users [21, 29]. Further identified the other characteristics of DDoS attack and revealed that average DDoS exist for 19 hours. It further highlights that 28% of the threats generate from the US while 35% from china. [2] Released the demographic report on how the Denial of services effecting the users globally. Whereas [6, 15, 23, 24, 25] have identified phishing as major threat. Study reveals that major frauds are taking place due to the phishing attacks and same is growing at phenomenal rate. Spear phishing is also an appealing method to the cyber attackers for attacking the various users reveals ThreatSim.

From the above review it is concluded that DDoS and Phishing are the major threats and need extensive study for their occurrences and damage caused.

4.2 Phishing Attacks in Cloud

In the phishing attacks, users are working on a fraudulent side that appears to be legitimate site. Phishing sites are created to obtain the users credential. The other phishing attack is through the e-mail, where users received the e-mail from the adversaries. E-mail received appears as legitimate mail from the known source. Such mails provide very concise or no information and provides the link to know more about it. Once clicked on the embedded link sent, malware gets installed on the user's PC. A number of phishing attacks have already occurred in the cloud. Some of them have been discussed in the upcoming sub-section.

4.2.1 Longline Phishing

Longline phishing is a new type of attack that is occurring in the cloud. In this type of attack, adversaries take the advantage of email services and sought the personal information from the users. Attackers sent the mail to the cloud user tricking him to click the link [18].

4.2.2 Spear Phish Attack on Raythe

Defense company Raythe have also encountered the phishing attack in its cloud. It was a spear phishing attack, an email was sent to the employees to access an application through this e-mail link. However no damage was reported due to the outgoing filters that were in place.

4.2.3 Phishing Attack on Microsoft Employees

Recently, some of the phishing attacks occurred on the account of Microsoft employee that was maintained on social media and emails [11]. These accounts were targeted phishing attack. It occurred to obtained the law enforcement information inquiries.

4.2.4 Phishing Attack on Dropbox

Phishing attack is also uncovered in Dropbox users account by the security firm Appriver [10]. This attack phishes victim's password via bogus email once succeeded then users computers are infected with malware. They send an official appearing mail to reset the password once clicked by the user on the reset button a malware gets installed on the user's browser.

4.2.5 Phishing Attack on South Carolina

Another major phishing attack observed at South Carolina [26]. The data breaches have stolen millions of social security numbers, bank account information and thousands of credit card and debit card information. When investigated, it is uncovered that at least one of the employees has clicked on the embedded link containing the malware. However, the source from where attacker received the employee's credential remained unknown. Attacker were not confined themselves with this attack only, instead gained the access of more system and deployed the malware on them to get more credentials.

4.2.6 Phishing Attack on Amazon and Apple

One of the major data breach occurred with Apple and Amazon [18]. In this breach, Honan's accounts on Apple and Amazon were compromised. In these attacks, victim has lost all his information stored in his account. Additionally, he has lost the photo and video of his 18 years daughter, which he has not stored anywhere else.

4.2.7 Phishing Attack on DBaaS

Recent trend is to offer database as a Service. In this model user can subscribe for the relational database to leverage this cloud offering. Amazon and Microsoft both are offering DBaaS. Users can benefit by these services by subscribing to it and pay for its usage.

But a recent report by Imperva highlights that DBaaS is extremely risky and can be exploited by Command and Control (C & C) Server, if necessary precautions are not observed [16]. To examine the vulnerabilities, [16] conducted the research and concluded that cloud subscription is fairly risky due to the fact that same database can be shared/ subscribed by the adversaries. This will result in easy access and attack on database. To support their claim they have carried out a research that revealed that mail sent to a user may lead to execute the malware in his system and connect the users system to remote location that is controlled by the adversaries. OLEDB provides the necessary connectivity to connect the database. In addition, report revealed that vulnerabilities existing in the database provide further ground to attack DBaaS.

4.3 DDoS Attack in Cloud Computing

Distributed denial of services is the other category of prominent cyber-attack that is taking place in cloud computing. Distributed denial of services attack is the cyber-attack in which a number of computers are used to attack the single destination. Compromised computer are known as Zombie. Due to DDoS, legitimate users are denied the resources, since they are utilized by non-legitimate users.

DDoS exploit the volumetric technique or the amplification technique. In the volumetric technique huge volume of traffic is directed to the network in order to consume the bandwidth or resource-sapping exhausts. State exhaustion attacks such as TCP SYN flood, and idle session attacks are the example of misuse of state nature of TCP and causes the resource exhaustion.

In the amplification technique, attackers take the help of victim to increase the traffic. An amplification technique, attacker exploits the attacked resource. Attacked botnet send out a DNS query of about 60 bytes to an open recursive DNS resolver that respond with response message up to 400 bytes, increasing the amount of traffic by more than the factor of 60.

Upcoming sub-section discussed the major DDoS attacks that have already been caused.

4.3.1 Attack on Spamhous

Spamhous is a spam avoiding company. Recently, DDoS attack took place in spamhous project [20]. The attack exploited the DNS Servers, open DNS resolver's capability. In this attack, peak attack traffic has reached to the capacity of the server. The peak attack traffic has reached to the volume of 300 gigabit per second. To handle the issue spamhous released a press note advising the internet community to check the traffic leaving their network to stop spoofed sending addresses is not leaving their network and to lock down any open DNS resolver [20].

4.3.2 Security Breach in Sony

Security breach on Sony has alerted the whole internet community [5]. Attack has exposed 100 million account records. Attackers not remained concentrated on this attack instead an additional attack occurred on Sony's online entertainment that exposed additional 25 million users. To determine the reasons, company constituted an investigation team. It was revealed that attack took place due to the availability of two servers behind the firewall. The two servers were web server and the application servers. Attacker exploited the vulnerabilities of application servers and attacked the web Server [5].

4.3.3 DDoS Attack Took Place on Bitbuchet

Bitbuchet is a development company that hosted it's infrastructure on cloud. It has subscribed to Amazon EC2 [18]. In 2009, all of sudden this service went down. As a result, whole production came down. Problem continued for several hours (19 hours approx.), before the services were restored. Once the Amazon pin pointed the problem, and then only it could be put on [18].

5 Conclusion

Security in cloud computing is a critical issue considering the privacy and regulatory acts. A number of organizations and working group are putting their efforts to strengthen the security in cloud computing. Working groups are releasing their drafts and report on critical security threats and recommending various methods to counter them. Although various study reveals that hosted model is more secure relative to the on-premises cloud model. Yet, many attacks are targeting the hosted model to exploit the vulnerabilities. DDoS and Phishing are the major method employed to attack the cloud. Finally, in the light of phishing and DDoS attack that took place in many of the cloud revealed, it can be concluded that they are causing huge financial losses, damage to privacy of data. Although a number of solutions are existing that are countering various attacks, still there is further need to strengthen the security in hosted as well as on premises cloud, in order to restore the confidence of users.

References

[1] AlertLogic, “Targeted attacks and opportunistic hacks, state of cloud security report spring 2013”, available at https://www.alertlogic.com/alert-logic-releases-2013-state-of-cloud-security-report/.

[2] Arbor, “Arbor Special Report: Worldwide Infrastructure Security Report”, Volume IX, 2014, available at http://pages.arbornetworks.com/rs/arbor/images/WISR2014.pdf.

[3] J. Archer, A. Boehme, D. Cullinane, P. Kurtz, N.J. Reavis. “Top threats to cloud computing”, version 1.0. Cloud security alliance retrieved 7 May 2011, accessed from http://www.cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf.

[4] B. Boss, P. Malladi, D. Quan, L. Legregni, and H. Hall “Cloud computing”, 2009. http://www.ibm.com/developerswork/websphere/zones/hipods/library.html.

[5] E. Chickowski, “Sony Still Digging Its Way Out of Breach Investigation”, Fallout ,02 Apr 2013, available at http://www.darkreading.com/attacks-breaches/sony-still-digging-its-way-out-of-breach/229402823.

[6] M. Cobb, “How cyber-criminal attack the cloud”, information week (dark reading), (2013), available at http://www.darkreading.com/attacks-breaches/how-cybercriminals-attack-the-cloud/240153610.

[7] CSA (2013), “The Notorious Nine Cloud Computing Top Threats in 2013”, Available at https://downloads.cloudsecurityalliance.org/initiatives/top_threats/The_Notorious_ Nine_Cloud_Computing_Top_Threats_in_2013.pdf.

[8] CSA, “Top Threats to Cloud Computing”, 2010, V1.0.

[9] Ericka Chickowski,Sony Still Digging Its Way Out of Breach Investigation, Fallout ,02 Apr 2013, available at http://www.darkreading.com/attacks-breaches/sony-still-digging-its-way-out-of-breach/229402823.

[10] A. Goscinski, M. Brock, “Toward dynamic and attribute based publication, discovery and selection for cloud computing”, *Future Generation Computer Systems*, vol. 26, pp. 947-970, 2010.

[11] C. Green, “Dropbox hit by Zeus phishing attack”, Oct 2013, available at http://www.information-age.com/technology/security/123457411/-dropbox-hit-by-zeus-phishing-attack.

[12] A. Hall, “Recent phishing attack targets select Microsoft employees”(accessed on 24 Jan 2014) available at https://blogs.technet.com/b/trustworthycomputing/archive/2014/ 01/24/post.aspx (accessed on 01 Feb 2014).

[13] B. Hayes, “Cloud computing”, *Communications of the ACM*, vol. 51, no. 7, 2008.

[14] A. Hutchings, R.G. Smith, and L. James “Cloud computing for small business: Criminal and security threats and prevention measures”, Trends & issues in crime and criminal justice, no. 456, May 2013.

[15] IBM, “Security service cyber security intelligence index”, IBM Global technology services security services, 2011

[16] IMPERVA, “Hacker intelligence initiative”, Monthly Trend Report. Report no. 18, Dec 2013.

[17] D. Marcus, D. and R. Sherstobitoff, “Dissecting operation high roller”, Mcfee, white paper, 2012, available at http://www.mcafee.com/us/resources/reports/rp-operation-high-roller.pdf.

[18] P. Mell, and T. Grance, "The NIST definition of cloud computing", Special Publication 800-145, National Institute of Standards and Technology, 2011, available at http://csrc.nist.gov/ publications/ PubsSPs.html#800-145.

[19] C. Metz, “DDoS attack rains down on Amaon cloud”, Oct 2009, available on http://www.theregister.co.uk/2009/10/05/amazon_bitbucket_outage/(accessed on 1 Feb 2014).

[20] NIST, 2011, NIST cloud computing program retrieved 21 May 2011, fromhttp://www.nist.gov/itl/cloud/.

[21] B. Prince, "Spamhaus DDoS attack renews talk of DNS server security", Apr 2013, available at http://www.darkreading.com/attacks-breaches/spamhaus-ddos-spotlights-dns-server-secu/240152167.

[22] S.H. Shin, and K. Kobara, “Towards secure cloud storage”, *Demo for CloudCom2010*, Dec. 2010.

[23] S. Srinivasamurthy, and D. Q. Liu, "Survey on cloud computing security", *in Proceeding of Conference on Cloud Computing (CloudCom.'10)*, 2010.

[24] Md. Tanzim Khorshed, A.B.M. Shawkat Ali & Saleh A. Wasimi, “A survey on gaps, threat remediation challenges and some thoughts for proactive attack detection in cloud computing”, *Future Generation Computer Systems*, vol. 28, no. 6, pp. 833–851, 2012.

[25] Verizon,"The truth about DDOS Attacks", 2013, available at http://www.verizonenterprise. com/ products/security/managed/.

[26] R. Westervelt, “Phishing attack, stolen credentials sparked South Carolina breach”, available at http://searchsecurity.techtarget.com/news/2240172466/Phishing-attack-stolen-credentials-sparked-South-Carolina-breach?asrc=EM_NLN_19698566 &track=NL-102&ad=883490.

[27] D. Windser, “Databases in the cloud- a new target for cyber criminals”, CloudPro, 2013, available at http://www.cloudpro.co.uk/cloud-essentials/cloud-security/3639/databases-in-the-cloud-a-new-target-for-cyber-criminals.

[28] G. Wrenn, CISSP, ISSEP, Unisys Secure Cloud Addressing the Top Threats of Cloud Computing, (online) (2010), White Paper, http://www.unisys.com/unisys/unisys/inc/pdf/whitepapers/38507380-000.pdf (accessed May 26, 2011).

[29] L. Yan, C. Rong, G. Zhao, “Strengthen cloud computing security with federal identity management using hierarchical identity-based cryptography”, *in Proceeding of 1st International Conference on Cloud Computing (CloudCom 2009),* pp. 167-177, Beijing, China, Dec. 1-4, 2009.

Jitendra Singh has pursued his masters in computer science that is followed by PhD in computer science, in the area of cloud computing. He has qualified the prestigious UGC-NET examination conducted by the UGC of India. He has more than 11 years of teaching experience. During his academic career, he has taught to the students of Bachelor and Master Courses. He is also involved with the Stratford University, USA, India Campus, as a part time faculty from more than 2 and half years. He has contributed more than dozen of research papers in the area of cloud computing. Many of them are published in reputed journals. In addition, he is also author of two books titling ‘Cloud computing for beginner to researcher’ and ‘Data structure simplified: Implementation using C++”. His research areas of interest are cloud computing, Networking, Security, etc.