IJCSE International Journal of Computer Sciences and Engineering Open Access
Review Paper Vol.-7, Issue-7, July 2019 E-ISSN: 2347-2693

Analyzing the Secure Virtualization schemes and preventions from DDoS flooding Zoombie attacks

Amit K. Chaturvedi[1*], Punit Kumar[2], Kalpana Sharma[3]

[1]Dept. of MCA, Govt. Engineering College, Ajmer, Rajasthan, India
[2,3]Dept. of CS, Bhagwant University, Ajmer, Rajasthan, India

[*]*Corresponding Author: amit0581@gmail.com, Tel.: 9829265881*

DOI: https://doi.org/10.26438/ijcse/v7i7.223229 | Available online at: www.ijcseonline.org

Accepted: 10/Jul/2019, Published: 31/Jul/2019

***Abstract*—** As Cloud computing emerges as a dominant paradigm in distributed systems, it is important to fully understand the underlying technologies that make clouds possible. One technology, and perhaps the most important, is the virtualization. Recently virtualization, through the use of hypervisors, has become widely used and well understood by many. Distributed Denial of Service (DDoS) attacks typically focus high quantity of IP packets at specific network entry elements; usually any form of hardware that operates on a Blacklist pattern is quickly overrun. As in the cloud computing, a large number of tenants or VM clients share the common hardware, DDoS attacks have the potential of having much greater impact than against single tenanted architectures. In this paper, various secure virtualization schemes and preventions from DDoS flooding zombie attacks are analyzed. Security threats are discussed and preventive measures from DDoS attacks and protection solutions are presented so that the companies can take the appropriate action accordingly.

***Keywords*—**DDoS, flooding, attack, Cloud, recovery, prevention, secure, virtualization.

I. INTRODUCTION

The number of internet users is growing exponentially all over the world. Online average user's time on internet is also increasing, as well as organizations of service sector are providing more online services than ever before. Internet is presently not only the need of the work for industry but now it is the part of life for a common man throughout the world. Hence, the more user's data like text, images, audio and video contents are uploaded on the internet storage. The public, industries, and govt schemes all are now more dependent on the internet based solutions. As the important public information like images, text, audio, and video are saved on internet storages. The number of internet attacks are also increasing like, attacks on banking data, personal data, organizational information etc. Presently, most internet services that we access either through mobile gadgets, laptops by using small android based applications, also called Apps. These apps are the light-weight applications and we only access these services when we are connected with the internet i.e. data is not with the mobile gadgets or device nor with the application, it is stored on the online storage media.
In cloud computing, variety of services required for designing an application either on social issues, related with business, or related with health care, etc. The development of these services in cloud is now very easy with very less efforts and management. Any of such application needs internet connectivity for the execution, here hackers find the gap. They either join themselves with the application's execution process as a part of it by any means, or they get access of the online storage by some other means. The cloud servers can be accessed through internet, the more use of cloud computing leads it toward the more cyber-attacks.

There are variety of attacks that we know as Botnet attacks, DDoS attacks, click fraud, phishing fraud, key logging, bitcoins fraud, spamming, sniffing traffic, spreading new malware, google AdSense abuse, password stealer and mass identity theft with bots. Like worms propagation, the botnet also propagate itself, similarly like virus, botnet also keep it hidden from detection. Botnet has an integrated control and command system that's why it attack similar numerous standardization unaccompanied tools. It spurs with a very high infected by botnet, bots are also known as a zombie, that's why a botnet is also called zombie network.

II. RELATED WORK

Security and privacy are the important factors for building the confidence towards the use of virtualization based applications. Researchers are regularly raising the security issues in architecture of cloud computing as well as its implementation through virtualization. During the study of

these issues, following contributions are important to consider.

Andrew J. Younge, Robert Henschel, and his team had presented the analysis of virtualization technologies for high performance computing environments. As Cloud computing emerges as a dominant paradigm in distributed systems, it is important to fully understand the underlying technologies that make clouds possible. One technology, and perhaps the most important, is virtualization. Recently virtualization, through the use of hypervisors, has become widely used and well understood by many. However, there are a large spread of different hypervisors, each with their own advantages and disadvantages. This manuscript provides an in-depth analysis of some of today's commonly accepted virtualization technologies from feature comparison to performance analysis, focusing on the applicability to High Performance Computing environments using Future Grid resources. The results indicate virtualization sometimes introduces slight performance impacts depending on the hypervisor type, however the benefits of such technologies are profound and not all virtualization technologies are equal [1].

Farzad Sabahi presented his findings on the Secure Virtualization for Cloud Environment Using Hypervisor-based Technology. According to him Cloud computing is one of today's most exciting technologies, because it can reduce the cost and complexity of applications, and it is flexible and scalable. These benefits changed cloud computing from a dreamy idea into one of the fastest growing technologies today. Actually, virtualization technology is built on virtualization technology which is an old technology and has had security issues that must be addressed before cloud technology is affected by them. In addition, the virtualization technology has limit security capabilities in order to secure wide area environment such as the cloud. Therefore, the development of a robust security system requires changes in traditional virtualization architecture. This paper proposes new security architecture in a hypervisor-based virtualization technology in order to secure the cloud environment [2].

Durairaj. M, Kannan.P presented a study on virtualization techniques and challenges in cloud computing. Cloud computing is a modern technology that increase application potentialities in terms of functioning, elastic resource management and collaborative execution approach. The central part of cloud computing is virtualization which enables industry or academic IT resources through ondemand allocation dynamically. The resources have different forms such as network, server, storage, application and client. This paper focus as on how virtualization helps to improve elasticity of the resources in cloud computing environment. In addition to, this paper gives a detailed review on open source virtualization techniques, challenges and future research direction [3].

Ms Jayshri Damodar Pagare, Dr. Nitin A Koli presented a technical review report on analysis of virtualization technologies by comparison of Xen and KVM hypervisors. Hypervisors are widely used in cloud environments and virtualization through the use of hypervisors has become widely used. This paper reviews in depth analysis of virtualization technologies experimented by researchers from feature comparison to performance analysis and it will be useful for researchers to work on appropriate hypervisors [4].

V RaviTeja Kanakala, V.Krishna Reddy, K.Thirupathi Rao, presented the analysis on Virtualization Technologies in Cloud. Virtualization was one of the trending research technologies in the IT industry now days. Organizations which were working for the advancement in Cloud Computing were concentrating more on virtualization technology. Virtualization technology brought many changes in the functionality of cloud computing technology through which solutions for very long lasting problems were found. One such solution found by virtualization technique is 'hypervisor' which is a software layer inserted between the hardware and the operating system was solving many of the security issues. In this paper we will discuss about virtualization technologies in different areas of cloud computing [5].

Gabriel Cephas Obasuyi, Arif Sari discussed the Security Challenges of Virtualization Hypervisors in Virtualized Hardware Environment. The concept of virtualization machines is not new, but it is increasing vastly and gaining popularity in the IT world. Hypervisors are also popular for security as a means of isolation. The virtualization of information technology infrastructure creates the enablement of IT resources to be shared and used on several other devices and applications; this increases the growth of business needs. The environment created by virtualization is not restricted to any configuration physically or execution. The resources of a computer are shared logically. Hypervisors help in virtualization of hardware that is a software interact with the physical system, enabling or providing virtualized hardware environment to support multiple running operating system simultaneously utilizing one physical server. This paper explores the benefits, types and security issues of Virtualization Hypervisor in virtualized hardware environment [6].

V. A. Meshram, V. V. Meshram, P. V. Khandare , Dr. S. R. Sakhare published a survey paper on Cloud Computing and Virtualization Security. They presented that Cloud computing is one important domain in now days, the meaning of cloud computing is computing is in cloud. In this paper, we explained different term related with cloud

computing like deployment model of cloud, service models of cloud, also we focuses on need of virtualization, different risk associated with the it and different solution for different risk associated with virtualization [7].

Kanika, Navjot Sidhu presented an analysis of Virtualization: Vulnerabilities and Attacks over the Virtualized Cloud Computing. Cloud computing is the fastest growing technology in the IT world. The technology offers reduced IT costs and provides on the demand services to the individual users as well as organizations over the internet. The means of cloud computing is obtained by the virtualization of the resources such as hardware, platform, operating system and storages devices. Virtualization permits multiple operating systems to run on the same physical machine. Multiple tenants are unaware of the presence of the other tenant with whom they are sharing the resources. The co-existence of multiple virtual machines can be exploited to gain the access over other tenant's data or attack to deny of services. The significant concern is insuring the security and providing isolation between multiple operating systems. The paper explores various kinds of vulnerabilities and attacks associated with the virtualization [8].

Syed Asad Hussain, Mehwish Fatima, Atif Saeed, Imran Raza, Raja Khurram Shahzad discussed the "Multilevel classification of security concerns in cloud computing. Threats jeopardize some basic security requirements in a cloud. These threats generally constitute privacy breach, data leakage and unauthorized data access at different cloud layers. This paper presents a novel multilevel classification model of different security attacks across different cloud services at each layer. It also identifies attack types and risk levels associated with different cloud services at these layers. The risks are ranked as low, medium and high. The intensity of these risk levels depends upon the position of cloud layers. The attacks get more severe for lower layers where infrastructure and platform are involved. The intensity of these risk levels is also associated with security requirements of data encryption, multi-tenancy, data privacy, authentication and authorization for different cloud services. The multilevel classification model leads to the provision of dynamic security contract for each cloud layer that dynamically decides about security requirements for cloud consumer and provider [9].

Theepan Moorthy and Sathish Gopalakrishnan, discussed the IO and data management for infrastructure as a service FPGA accelerators. We describe the design of a non-operating-system based embedded system to automate the management, reordering, and movement of data produced by FPGA accelerators within data centre environments. In upcoming cloud computing environments, where FPGA acceleration may be leveraged via Infrastructure as a Service (IaaS), end users will no longer have full access to the underlying hardware resources. We envision a partially reconfigurable FPGA region that end-users can access for their custom acceleration needs, and a static "template" region offered by the data centre to manage all Input/Output (IO) data requirements to the FPGA. Thus our low-level software controlled system allows for standard DDR access to off-chip memory, as well as DMA movement of data to and from SATA based SSDs, and access to Ethernet stream links. Two use cases of FPGA accelerators are presented as experimental examples to demonstrate the area and performance costs of integrating our data-management system alongside such accelerators. Comparisons are also made to fully custom data management solutions implemented solely in RTL Verilog to determine the tradeoffs in using our system in regards to development time, area, and performance. We find that for a class of accelerators in which the physical data rate of an IO channel is the limiting bottleneck to accelerator throughput, our solution offers drastically reduced logic development time spent on data management without any associated performance losses in doing so. However, for a class of applications where the IO channel is not the bottle-neck, our solution trades off increased area usage to save on design times and to maintain acceptable system throughput in the face of degraded IO throughput [10].

Diego Perez-Botero, Jakub Szefer and Ruby B. Lee, discussed the characterizing Hypervisor Vulnerabilities in Cloud Computing Servers. The rise of the Cloud Computing paradigm has led to security concerns, taking into account that resources are shared and mediated by a Hypervisor which may be targeted by rogue guest VMs and remote attackers. In order to better define the threats to which a cloud server's Hypervisor is exposed, we conducted a thorough analysis of the codebase of two popular open-source Hypervisors, Xen and KVM, followed by an extensive study of the vulnerability reports associated with them. Based on our findings, we propose a characterization of Hypervisor Vulnerabilities comprised of three dimensions: the trigger source (i.e. where the attacker is located), the attack vector (i.e. the Hypervisor functionality that enables the security breach), and the attack target (i.e. the runtime domain that is compromised). This can be used to understand potential paths different attacks can take, and which vulnerabilities enable them. Moreover, most common paths can be discovered to learn where the defences should be focused, or conversely, least common paths can be used to find yet-unexplored ways attackers may use to get into the system [11].

Swati Pawar, Sarvesh Singh discussed the performance comparison of VMware and Xen Hypervisor on Guest OS. Virtualization has become a critical element in today's enterprise network. It makes more efficient use of server resources and setup different types of servers within both

public and private cloud platforms. Hypervisor plays an important role in the virtualization of hardware. It provides a virtualized hardware environment to support running multiple operating systems concurrently using one physical server. This paper focuses on the performance comparison of guest operating system (Microsoft Window Server 2008 r2, 64-bit) under virtual environment by using two most useful hypervisors Citrix XenServer 6.5 and VMware ESXi 6.0. Their different parameters such as CPU, disk, memory and system response time are calculated to show the performance level of Guest OS in both hypervisors [12].

III. DDOS FLOODING ZOMBIE ATTACKS

DDoS attack means to the deployment of large number of internet bots may be from hundreds to hundreds of thousands. These bots may attack a single server, network or application with an irresistible number of requests, packets, or messages, which then denying service to legitimate users. These DDoS attacks carried out for a variety of reasons, such as extortion, revenge, or politics. DDoS attacks are measured by a few megabits per second (Mbps) to several hundred gigabits per second (Gbps), or even more than one terabit per second (Tbps), which is basically a measure of how many of it or traffic they send at the target per second. It is important to note that not all DDoS attacks are bandwidth focused. For example, network protocol attacks are low bandwidth with many packets per second (PPS).

Distributed Denial of Service (DDoS) attacks typically focus high quantity of IP packets at specific network entry elements; usually any form of hardware that operates on a Blacklist pattern is quickly overrun. As in the cloud computing, a large number of tenants or VM clients share the common hardware. DDoS attacks have the potential of having much greater impact than against single tenanted architectures.

Now, let us first understand that what a zombie machine is. A zombie is a computer connected to the Internet that has been compromised by a hacker, computer virus or trojan horse program and can be used to perform malicious tasks of one sort or another under remote direction. Botnets of zombie computers are often used to spread e-mail spam and launch denial-of-service attacks (DOS attacks). Most owners of "zombie" computers are unaware that their system is being used in this way. Because the owner tends to be unaware and don't take any prevention measures, these computers are abstractly compared to invented zombies.

There are basically two types DDoS flooding attacks : (1) Direct attacks and , (2) Reflector attacks. In the direct attacks, the attacker directly attacks the victim's computer by using the Zombie machines to send a flood of packets to the victim. In respect to the OSI layer, the direct attacks can be classified into two types : (i) application-layer DDoS attacks and (ii) network-layer DDoS attacks.

For the second type of attack, i.e. reflector attacks, the attacker uses the zombie machines or spoofing the source IP address of the victim server in order to send request messages to reflector machines. Therefore, the reflector machines send their replies to the given address which, in turn, makes packet flooding at that site of the victim server. ICMP ECHO reply flood, SYN ACK (RST) flood, DNS flood, Smurf attack and Fraggle attack are considered as the most well-known reflector attacks. Such attacks makes use of a potentially legitimate third party component to send the attack traffic to the victim's machine and ultimately hiding the attackers' own identity because the attacker send packets to the reflector servers with a source IP address set to their victim's IP, therefore the victim's machine is indirectly overloaded with the response packets. A common example for this type of attack is Reflective DNS Response attack.

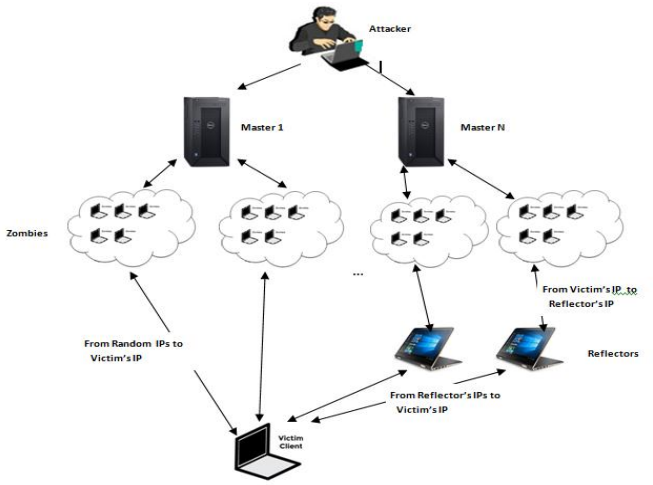

Figure 1: Architecture of the flooding zombie reflector DDoS attack

As shown in the figure 1 attacker divides its tasks in multiple masters and then these master controls multiple zombie clouds, which may consists hundreds of zombie systems. These zombies communicate with the victim or client using random IPs directly or by using the Reflectors.

IV. SECURITY THREAT UNDER DDOS ATTACK

In many cases a DDoS attack is designed to divert the victim from other criminal activity at their site, such as data theft or network infiltration etc. The attacker keeps busy its victim for fighting off against that DDoS attack, and in the mean time attacker steals victim's important data or perform malicious tasks at their site. Recently, the number of DDoS attacks are increasing both in frequency and severity. Some of the well known DDoS attacks are listed below.

1. GitHub with 1.35 Tbps : On Feb. 28, 2018, GitHub—a popular developer platform—was hit with a sudden onslaught of traffic that clocked in at 1.35 terabits per second. If that sounds like a lot, that's because it is—that amount of traffic is not only massive, it's record-breaking. According to GitHub, the traffic was traced back to "over a thousand different autonomous systems (ASNs) across tens of thousands of unique endpoints". The worse is that GitHub was not entirely unprepared for a DDoS attack—they simply had no way of knowing that an attack of this scale would be launched.

2. Occupy Central, Hong Kong with 500 Gbps : The PopVote DDoS attack was carried out in 2014 and targeted the Hong Kong-based grassroots movement known as Occupy Central. The movement was campaigning for a more democratic voting system. The attack barraged servers with packets disguised as legitimate traffic, and was executed with not one, not two, but five botnets. This resulted in peak traffic levels of 500 gigabits per second. In response to their activities, attacker(s) sent large amounts of traffic to three of Occupy Central's web hosting services, as well as two independent sites, PopVote, an online mock election site, and Apple Daily, a news site, neither of which were owned by Occupy Central but openly supported its cause.

3. CloudFlare with 400 Gbps : In 2014, security provider and content delivery network CloudFlare was slammed by approximately 400 gigabits per second of traffic. The attack was directed at a single CloudFlare customer and targeted servers in Europe and was launched with the help of a vulnerability in the Network Time Protocol (NTP), a networking protocol for computer clock synchronization. Even though the attack was directed at just one of CloudFlare's customers, it was so powerful that it affected CloudFlare's own network.

4. Spamhaus with 300 Gbps : In 2013, a DDoS attack was launched against Spamhaus, a nonprofit threat intelligence provider. Although Spamhaus, as an anti-spam organization, was and is regularly threatened and attacked, this DDoS attack was large enough to knock their website offline, as well as part of their email services. Like the 2014 attack on CloudFlare mentioned above, this attack utilized reflection to overload Spamhaus' servers with 300 gigabits of traffic per second.

5. U.S. Banks with 60 Gbps: In 2012, not one, not two, but a whopping six U.S. banks were targeted by a string of DDoS attacks. The victims were no small-town banks either: They included Bank of America, JP Morgan Chase, U.S. Bancorp, Citigroup and PNC Bank. The attack was carried out by hundreds of hijacked servers, which each created peak floods of more than 60 gigabits of traffic per second. At the time, these attacks were unique in their persistence: Rather than trying to execute one attack and then backing down, the perpetrator(s) barraged their targets with a multitude of methods in order to find one that worked. So, even if a bank was equipped to deal with a few types of DDoS attacks, they were helpless against other types.

6. OpIsrael : This was launched on 14th Nov, 2012 in the Gaza Strip by Israel Defence Forces as "Operation Pillar of Cloud" and it is a cyber-attack campaign against the Anonymous cyber group with the following objectives :

a. Ensure communication channels availability in the Gaza Strip, and provide alternative communication methods in case of an Israeli communication blackout as part of the military operation.
b. Take down Israeli and Israeli-related Websites.
c. Deface Israeli sites and promote anti-Israeli agendas.
d. Stop the violence.

7. RefRef : It is a Perl-based DoS attack tool developed by the Hacktivist group that uses a vulnerability in MySQL to perform an SQL injection involving the MySQL BENCHMARK() function.

DDos attacks are not only increasing but also more bigger and overwhelming than ever before. From independent websites to multinational banks, it seems like no one is immune. In fact, a 2017 report from Cisco found that the number of DD0S attacks exceeding 1 gigabit per second of traffic will rise to 3.1 million by 2021. As anonymous cyber groups are involved in such types of attacks and the internet world raised strong protest against it.

V. PREVENTIVE MEASURES FROM DDOS ATTACKS AND PROTECTION SOLUTIONS

By taking the experience from the past, it can be clearly understood that such DDoS attack will be growing larger and more destructive in the future, we cannot stop them but preventive measures can be taken for security and be more alert from being a victim or the part of it unknowingly.

On the basis of business goal, the DDoS attack's deployment mode is chosen either (i) proactive, or (ii) reactive. A proactive mode delivers the highest resolution detection capabilities and is commonly used for real-time apps such as voice, video and gaming. With a proactive mode, detection is always on, and you're provided with an inline tool that gives 100 percent visibility through packet analysis.

On the other hand, a reactive mode detects anomalies by analyzing metadata, as well as by leveraging the flow data available from switches and edge routers. A reactive mode is more cost-effective than a proactive one, but it doesn't have the ability to respond in real-time. Proactive mode of deployment will be best suitable for the Protect critical DNS

services, and Protect real-time IMS infrastructure, whereas reactive most is best suitable for the Volumetric attack protection, Protect external hosted client, and Business customer scrubbing service. Bi-directional protection and Protect internal hosted clients may use either proactive or reactive deployment modes as per their requirements. With proactive mode the security services may be managed within the customer premises, but reactive mode may be applied to provide security services wtih the clean pipe.

There are many different methods for DDoS detection like (i) Flow Sampling, (ii) Packet Analysis, and (iii) Mirrored Data Packets. In Flow Sampling, the router samples packets and then exports a datagram that contains information about those packets. It is highly scalable and all the nearby routers support this type of technology. Hence it is a popular choice with the limitation that it gives limited snapshot of the traffic and doesn't allow for detailed analysis. Packet Analysis is good choice when a high performance DDoS mitigation device is deployed in path. It can instantly detect and mitigate anomalies. It continuously processing all incoming asymmetric traffic and can also process all outgoing symmetric traffic. Mirrored Data Packets provides the full details for in-depth analysis and can detect anomalies quickly, although these packets don't operate in the path of traffic. The limitation of this method is that it can be difficult to scale up.

VI. CONCLUSION AND FUTURE SCOPE

Recently virtualization using hypervisors has become widely used, which is a software layer inserted between the hardware and the operating system for solving and managing many security issues by means of isolation. There are a large spread of different hypervisors each with their own advantages and disadvantages. The virtualization sometimes introduces slight performance impacts depending on the hypervisor type. Secure virtualization for cloud environment using hypervisor-based technology is the emerging research area. The virtualization of IT infrastructure creates the enablement of IT resources to be shared and used on several other devices and applications to increase the growth of the business needs. The environment created by virtualization is not restricted to any configuration physically or execution. The virtualization technology has limited security capabilities in order to secure wide area environment such as the cloud. Therefore, the development of a robust security system requires changes in traditional virtualization architecture. Virtualization also helps to improve elasticity of the resources allocation in cloud computing environment. Virtualization technology brought many changes in the functionality of cloud computing technology through which solutions for very long lasting problems were found. Virtualization permits multiple operating systems to run on the same physical machine. Multiple tenants are unaware of the presence of the other tenant with whom they are sharing the resources. The co-existence of multiple virtual machines can be exploited to gain the access over other tenant's data or attack to deny of services.

DDoS flooding based zombie attacks are more frequent in future and be more dangerous because attackers will be more advanced with updated web-based tools and panic with malicious motives. So, using preventive measures and be more vigilant with the updated knowledge will be the solution to safe ourselves from such attacks.

ACKNOWLEDGMENT *(HEADING 5)*

The authors are thankful to all the contributors directly or indirectly related to the development of this papers.

REFERENCES

[1]. Andrew J. Younge, Robert Henschel, James T. Brown, Gregor von Laszewski, Judy Qiu, Geoffrey C. Fox, "Analysis of Virtualization Technologies for High Performance Computing Environments", 2011 IEEE 4th International Conference on Cloud Computing, ISSN : 978-0-7695-4460-1/11, pp. 9-16.

[2]. Farzad Sabahi, "Secure Virtualization for Cloud Environment Using Hypervisor-based Technology", International Journal of Machine Learning and Computing, Vol. 2, No. 1, February 2012, pp. 39-45

[3]. Durairaj. M, Kannan.P, "A Study On Virtualization Techniques And Challenges In Cloud Computing", INTERNATIONAL JOURNAL OF SCIENTIFIC & TECHNOLOGY RESEARCH, VOLUME 3, ISSUE 11, NOVEMBER 2014, ISSN 2277-8616, pp. 147-151

[4]. Ms Jayshri Damodar Pagare, Dr. Nitin A Koli, "A technical review on comparison of Xen and KVM hypervisors: An analysis of virtualization technologies", International Journal of Advanced Research in Computer and Communication Engineering, Vol. 3, Issue 12, December 2014, ISSN (Online) : 2278-1021 , ISSN (Print) : 2319-5940, pp. 8828-8832

[5]. V RaviTeja Kanakala, V.Krishna Reddy, K.Thirupathi Rao, "Analysis on Virtualization Technologies in Cloud", International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 3 Issue 7, July 2014, pp 2567-2574.

[6]. Gabriel Cephas Obasuyi, Arif Sari, "Security Challenges of Virtualization Hypervisors in Virtualized Hardware Environment", Int. J. Communications, Network and System Sciences, 2015, Vol. 8, pp. 260-273, http://dx.doi.org/10.4236/ijcns.2015.87026

[7]. V. A. Meshram, V. V. Meshram, P. V. Khandare , Dr. S. R. Sakhare, "Cloud Computing and Virtualization Security: A Survey", International Journal of Computer Trends and Technology (IJCTT) – volume 12 number 4 – Jun 2014, ISSN: 2231-5381, pp. 167-170

[8]. Kanika, Navjot Sidhu, "Analysis of Virtualization: Vulnerabilities and Attacks over the Virtualized Cloud Computing", International Journal of Emerging Technologies in Computational and Applied Sciences (IJETCAS), Vol. 8(issue 5), March-May, 2014, pp. 391-396

[9]. Syed Asad Hussain, Mehwish Fatima, Atif Saeed, Imran Raza, Raja Khurram Shahzad, "Multilevel classification of security

concerns in cloud computing", Applied Computing and Informatics, 2016, ISSN: 2210-8327, pp.1-9
[10]. Theepan Moorthy and Sathish Gopalakrishnan, "IO and data management for infrastructure as a service FPGA accelerators", Journal of Cloud Computing: Advances, Systems and Applications, 2017, pp. 1-23
[11]. Diego Perez-Botero, Jakub Szefer and Ruby B. Lee, "Characterizing Hypervisor Vulnerabilities in Cloud Computing Servers", in Proceedings of the Workshop on Security in Cloud Computing (SCC), May 2013.
[12]. Swati Pawar, Sarvesh Singh, "Performance Comparison of VMware and Xen Hypervisor on Guest OS", International Journal of Innovative Computer Science & Engineering, Volume 2 Issue 3; July-August-2015; Page No. 56-60

Authors Profile

Dr. Amit Chaturvedi obtained the Ph.D. degree in Mar, 2012. He is presently teaching in the Govt. Engineering College, Ajmer. He has 17 years long PG teaching experience. Five doctorate degrees are awarded under his supervision. He has published around 71 research papers in national/international Journals and conference. He has written three text books in the computer science subjects. Presently he is working on the subjects of cloud computing and multicast communication in adhoc networks..

Mr. Punit Kumar obtained the MCA degree in may 1999 from IBS, BR Ambedkar Univ, Agra and pursuing Ph.D. in Computer Sc from Bhagwant University, Ajmer.

