Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 73 (2015) 490 – 497

Procedia Computer Science

The International Conference on Advanced Wireless, Information, and Communication Technologies (AWICT 2015)

Defence for Distributed Denial of Service Attacks in Cloud Computing

Andrew Carlin[a] , Mohammad Hammoudeh[b] , Omar Aldabbas[c]

[a, b] School of Computing, Mathematics & Digital Technology, Manchester Metropolitan University, Manchester, UK

[c] Faculty of Engineering, Al-Balqa Applied University, Jordan

Abstract

Cloud computing offers users high-end and scalable infrastructure at an affordable cost. Virtualisation is the key to unlocking cloud computing. Although virtualisation has great benefits to the users, the complexity in its structure, introduces unseen and forcible threats to the security of the data and to the system infrastructure. This investigates the exploitation of compromised virtual machines to execute large-scale Distributed Denial-of-Service (DDoS) attacks. A critical review of most recent intrusion detection and prevention systems to mitigate potential DDoS attacks is presented.

Peer-review under responsibility of organizing committee of the International Conference on Advanced Wireless, Information, and Communication Technologies (AWICT 2015)

Keywords: Cloud Computing Security, Virtualisation, Distributed Denial of Service, Intrusion Detection, Intrusion Prevention.

1. Introduction

Cloud computing enables ubiquitous, on-demand Internet access to computing resources (e.g., storage, applications, servers, and services) that can be provisioned with minimal interaction with service providers. The cloud delivers the demand of users for near consistent access to their information, resources and data [1]. Many businesses have already implemented cloud computing given its characteristics such as on-demand self-service, broad network access, resource pooling, rapid elasticity and measured services [2]. These characteristics allow users to focus on their own businesses processes, while the computing resources are managed by a Cloud Service Provider (CSP). The cloud model reduces business costs by simplifying the process of installing hardware and software updates and ensuring availability and adaptability of computing resources.

Peer-review under responsibility of organizing committee of the International Conference on Advanced Wireless, Information, and Communication Technologies (AWICT 2015)

doi:10.1016/j.procs.2015.12.037

The cloud computing model depends on maintaining an agreed level of trust between clients and providers, which is essential to ensure that company's data is secure and that the agreed Quality of Service (QoS) is met. There is also trust from the providers to the clients to avoid malicious activity against the provider from insider attacks or security flaws in cloud-based applications. Clients behaviour on the cloud is monitored by the CSP. Unusual discrepancies in resource utilisation affect trust in the client and consequently affect the services they receive [3].

One concern that has hindered the acceptance of cloud computing is the concern of security of all stakeholders from CSPs, to clients and to end-users. The power of the cloud is an attractive resource for exploitation from assailants to launch further attacks. For example, Amazon's Elastic Computing Cloud Service (EC2) was used in 2011 to attack Sony's online entertainment systems [4]. This shows the potential of the low-cost cloud power, which can be utilised by malicious users. Once successfully compromised, the cloud becomes a potential threat to both the cloud itself and to external targets [5]. For example, the biggest DDoS attack in the Norwegian history interrupted online payment systems of five banks, three airlines, two telecommunication companies, and one insurance company. This attack was committed by a person demonstrating the computing power of the cloud [6].

There is a meaningful increase in attacks on CSP. Such attacks frequently use hacked or setup accounts to install commands and control servers to perform malicious activities. It has been observed that attacks on routers that control traffic and provide the Internet backbone are growing in line with other cybersecurity issues. Distributed Denial of Service (DDoS) attacks, such as those against Cloudflare and Spamhaus, are increasingly exploiting the Simple Network Management Protocol (SNMP). In the month of May 2014, fourteen separate DDoS attacks made use of SNMP amplified reflection attacks [7]. This highlights the rate at which attacks are evolving and demonstrates the importance of constantly evolving defence systems. Problems are further complicated by the various setup models of the cloud and the accountability of all parties for security in each of these setups [8].

In this paper, we examine the cloud's open secure architecture advantages in brief, and focus on DDoS security threats in the cloud model along with the existing methods to defend against them with their pros and cons. The following section briefly identifies the main cloud security vulnerabilities. Section III gives a classification of intrusion detection in the cloud and highlights the main challenges facing their deployment. Section IV presents the latest developments in the areas Virtual Machin (VM) security. Section V, presents a review of the recent defence systems against DDoS in the cloud. Section VI concludes the paper and highlights future research directions.

2. Common Cloud Vulnerabilities

The elasticity, openness and large amount of data stored in clouds make them tempting targets for attackers. Cloud models inherit the weaknesses in its enabling technologies, e.g., virtualisation, and since it runs through standard Internet protocols. The cloud characteristics that provide its flexibility and scalability also bring new threats that can be amplified by the anonymity of the Internet. Attacks can target globally without concern over geographical location of their victims. Codes and tools for launching attacks against systems are readily available on the Internet and require minimal user skills to execute.

Cloud clients want guarantees for their data integrity and confidentiality. These responsibilities are handed to an external agency, which can leave clients feeling vulnerable given that they no longer control where their data is physically residing and the legal frameworks around its protection. They also have concerns about new vulnerabilities, such as SQL injection and buffer overflow, which can be compromised through web browser weaknesses. Since user interactions with the cloud are governed by traditional internet protocols, attacks become more difficult to detect and distributed attacks are easier to implement [9].

This paper focuses on the immense increase in the number of DDoS attacks. The majority of these attacks flood service resources to block or delay response for legitimate user requests. Table 1 describes the main attacks aimed at causing this type of interruption. Unlike traditional networks DDoS attacks, DDoS against cloud results in the potential for disruption that crosses traditional organisational boundaries. This is because the data is managed by a CSP and the data for different organisations may be stored on the same physical hardware. Therefore, the scalability of cloud is what presents its main security challenges when compared to traditional networks.

Table 1. Main DDoS Attacks

Type of Attack	How it works
Flooding	Occurs through network and application layers, e.g., HTTP, ICMP etc. It tries to saturate the network bandwidth to prevent it from responding to legitimate user traffic. Flooding can be direct attack against the network or application, or reflective attacks via zombies.
Spoofing	Used to falsify the origin of a network packet to bypass filters, hide the source of an attack or to gain access to restricted resources or services.
User to root	Aims to gain administrator (root) access privileges for a non-authorised account.
Port Scanning	Often used in the first stages of an attack and come in many forms such as TCP SYN, TCP ACK, TCP ECHO, TCMP SWEEP etc.
Oversized XML	The attacker sends a several megabytes XML document, which contains elements, attributes or namespaces with large names or content. The Document Object Model (DOM) parses documents into memory in their entirety to be analysed, which increases memory requirements by a factor of 2-30.
Coercive Parsing	The attacker sends malformed XML aimed a clogging up CPU cycles by incorporating many namespace declarations or by simply using very deeply nested XML structures.
Web Service-addressing Spoofing	This is an extension of the spoofing attack where the ReplyTo or FaultTo address in a SOAP 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 address of the victim. The genuine replies to these requests are then sent to the victim causing flooding.

3. IDSs Classification and Challenges

Firewalls can be effective in stopping external attacks, but have no effect on internal attacks where cloud users attempt to gain unauthorised privileges. In general, Intrusion Detection Systems (IDS) designed for cloud computing can be classified into four main categories [10]: (1) Host-based IDS (HIDS) monitors and analyses log files, security access and user login information to detect intrusive behavior. (2) Network-based IDS (NIDS) monitors IP and transport layer headers with behaviour being compared with previously observed behaviour in real time. (3) Hypervisor-based IDS (HyIDS) allows users to monitor and analyse communication between VMs, within the hypervisor based virtual network and between the hypervisor and VMs. (4) Distributed IDS (DIDS) consists of a number of IDSs, HIDS and NIDS, placed across a large network. These individual IDSs communicate with each other via a central analyser, which aggregates system information from the different IDSs.

Intrusion Detection and Prevention System (IDPS) is an invaluable tool in the early detection of malicious activity, which helps to prevent attacks from succeeding. They can also gather forensic evidence. Traditional IDPS are largely inefficient when applied to cloud environments given their openness. The authors of [8] investigate the requirements of IDPS in the cloud by asking the following questions:

1) What criteria and requirements should an IDPS meet to be deployed on cloud computing environments?

2) Which methods or techniques can satisfy these requirements?

The list below outlines some of the challenges that traditional IDPS is unable to counter:

- Current IDPS technologies can not be adequately applied to new network paradigms such mobile networks.
- They do not scale to handle cloud requirements and satisfy the requirements of high-speed networks.
- The traffic profiles of networks changes frequently making the audit data that was used to train IDPS systems unsuitable.
- They generate high false alarm rate [11].
- There is no uniform standard or metric for evaluating an IDPS, which can often lead to misleading information as to their effectiveness.
- It is very difficult to identify internal intrusion given that correctly configuring the systems and implementing organisational policies is a difficult task.

4. VM Common Security Vulnerabilities and Defence Mechanisms

Virtualisation is the main enabling technology of the cloud computing model. Therefore, its security needs to be

considered as the foundations of any proposed system. Specifically, the fundamental weaknesses in the VM architecture need to be understood for security to be improved across other layers.

A significant security feature of VM is isolation. Isolation is intended to allow multiple users to co-habit the same physical host without data leakage occurring between users. However, scaling using VMs can still allow some issues to be exploited. These systems can expose memory and process management functionalities meaning that some users can obtain administration privileges. Defence methods against attacks on isolation can be divided into those that isolate the running of VMs and those that focus on the isolation of shared resources [12]. The first of these approaches can limit the ability of the system to schedule the work of legitimate VMs. To implement the second method, a mediation and monitoring process is necessary to analysis resource requests and to assign these requests to VMs. In addition, to implement the policies necessary to apply isolation takes many OS hooks and this is challenging to impose across a distributed system.

Volokyta [13] presents a VM Monitor to secure VMs. The presented system intercepts system calls and maintains a log file of system warnings. The author does not give the practical design details or evaluation results, which makes it is hard to determine the level of security provided by this approach. Nevertheless, VM management systems are often part of security design specifications.

Lui et al. [14] presents a framework for combating user-level security in SaaS, where many individual users access a single instance of an application using VMs to manage access. Metrics of the executables running in VMs are taken and compared to a reference table of trusted measurements. In this framework, a trusted VM is used to monitor other VM instances, meaning that the status of the measurement module should be noted to ensure that the system can be trusted.

In [12], a system that records the behaviour of VMs to obtain traces to calculate Aggressive Conflict of Interest Relation or Aggressive in Ally with Relation is proposed. In this system, specific monitoring methods are not required, but a trade-off is created between security and resource utilisations.

Another approach in [15], called virVMs, is to use N-version programming in the construction of VMs. virVMs attempt to introduce diversity in VM design that can avoid a sequence of events that leads to failure. This approach lends itself to automation making it scalable, but it can make the development of compatible systems difficult.

To summarise, virtualisation is a key underlying technology in the cloud computing model. It poses a number of security issues that need to be addressed. A benefit of virtualisation is its ability to allow users to isolate VMs and resources, which enhance security. A number of systems have been presented in the literature to monitor and enforce the principles of isolation and thus secure the virtualisation layer. The systems reviewed could be made more effective if monitoring VMs could also make use of the scalable nature of the cloud. This means that monitoring VMs could increase in number, ensuring the efficient management of resources and monitoring of isolation throughout periods of operation.

5. Defence Mechanisms against DDoS in the Cloud

DDoS attacks have two implications on CSPs; either they become incapable to deliver their users with the service as defined in their QoS agreement or they have their resources compromised to launch an attack against another location. This section analyses proposed systems aimed at protecting a cloud against DDoS attacks.

A filtering tree that acts as a service broker within an Service Oriented Architecture (SOA) model is presented in [9]. The authors examine the insecurities in standardised cloud APIs and how these can be exploited in provisioning, management and monitoring of services. They propose adding a signature reference element to each SOAP request to ensure that it comes from a legitimate source. Double signatures are generated using hashed characteristics of each SOAP envelope, such as the number of child or header elements. The client IP address is kept in the message header along with a puzzle that is stored as part of the WSDL file. The suggested system has to scan each packet individually, which can lead to a bottleneck in DDoS situations.

In [16], a trace-back and filter system is proposed to protect the cloud from DDoS attacks. SOA trace-back is used by adding a tag to SOA packets to record the route taken. This system can not identify the source of attack, because the tag is only added to the packet once it is relatively close to the server. The tests used in the paper do not consider spoofed IP addresses or the fact that an attacker is likely to make use of zombie machines.

Another trace-back model is presented in [17], which uses Data Protection Manager (DPM) and training data to inform the filters in a neural network. The future of DPM may be limited with the introduction of IPv6. This system

has a success rate of correctly identifying approximately 75% of attack traffic, though its ability to detect currently unknown attacks is not researched. This system has a significant time variation in the detection rate of attack traffic from 20ms to 1s; an overhead that could cause disruption to legitimate users when accessing systems.

An approach to protect web services against DDoS at the application layer is proposed in [18]. The system is designed to protect against Oversized XML, Oversized Encryption, HTTP flooding, Web Service-addressing spoofing and Coercive parsing. A reverse proxy is used as a filter to intercept all service requests. This filter adds no overheads on the cloud and users notice no effect to their service. The web service only accepts requests that come from the defence system. However, the defence server could be susceptible to flooding attacks particularly from insiders. To add extra security to this approach, strong authentication requirements need to be forced on users attempting to connect to the web services.

In [19], an approach to prevent Low and Slow (LOS) application layer DDoS attacks is presented. LOS attacks are infrequently detected using pattern matching or threshold measuring techniques due to their low resource consumption tactic. This reference-based system mitigates attacks by using a software defined infrastructure. The authors of [20-22] describe techniques used for detecting LOS DDoS. These techniques introduce a 'healing' approach that migrates legitimate users from compromised to newly generated VMs. The use of 'Shark Tanks' is presented as isolation areas for potentially malicious traffic. This allows monitoring suspect users, while continuing to receive a suitable level of application access in case a legitimate user is wrongly redirected. The locations of the Shark Tanks are disguised using OpenFlow switches. Two concrete implementations of the design are put forward in [19]. However, the results of these implementations are not compared against each other or existing systems.

To restrict information that attackers can find through scanning attacks, [23] use the autonomous generation properties of the cloud to base service delivery on randomly generated and assigned proxy nodes. Attacking machines using spoofed IP addresses become ineffective, as they will not receive server reassignment messages. Strong authentication methods are introduced to prevent external attackers from accessing proxy nodes. This system entirely depends on the IP addresses of key components being kept hidden, but there is no description of how this can be achieved. Currently, all of the datasets used to generate the models used by the system are stored centrally by the application server, which makes it a target for attackers.

The authors of [23] propose a greedy algorithm that provides a 'near-optimal' means for assigning users to proxy nodes allowing these to be 'shuffled' when an attack is detected against a proxy node. The repeated shuffling of users between newly generated nodes allows the system to identify the insiders launching the attack. This approach is extended in [24], where new selection of algorithms to optimise runtime reassignment plans is introduced. Both approaches use the number of persistent bots, which contains the intelligence for migrating servers as a key metric for calculating the optimised 'shuffling' pattern. However, in the real-world this value can only be estimated.

Another extension of [23] is presented in [24] to allow it to deliver security across the application layer and for anonymous users by removing the need for strong client authentication. This creates a generic DDoS protection product that can be deployed by non-ISP organisations. Both [23] and [24] do not describe how the attack is detected by the proxy node. Implementation overheads are dependent on the number of needed shuffles and the size of the geographical area covered, which could be global.

In [12], individual cloud users are protected by creating clones of virtual IPS as required to filter traffic. A queuing procedure is defined to calculate the number of IPS clones required to defeat a DDoS attack. The authors assume that in order to defeat DDoS attacks, the defence system must have access to greater resources than those of the attackers; this was proven to be feasible in [25]. This implies that DDoS attacks are unlikely to affect an entire cloud service. Yet, the cloud resources available to individual clients are limited, which makes them susceptible to DDoS attacks. The published theoretical evaluation results shows that the IPS cloning solution is effective and that the cloud contains enough idle resources to overcome the attack.

Huang [26] presented a low reflection ratio mitigation system that consists of source checking, counting, attack detection, turning test and question generation modules. This system is designed to be implemented before the IaaS. This system considers the computational efficiency and overheads in the implementation and their effect on legitimate users. A blacklist, whitelist, block list and unknown are used to categorise incoming packets based on IP addresses; these are maintained by administrators using APIs. Such APIs opens the system to malicious manipulation from insiders. The system shows an operational degradation of 8.5% when monitoring traffic against a blacklist of 100,000 addresses.

The system proposed in [27] addresses some of the limitations of overlay networks in hiding the location of target servers through the use of gateway routers. It protects clouds from insider attacks and compromised user host machines. There is no need for migration of network items to other hosts. The approach removes the need to monitor all network traffic resulting in lower computational overhead. Each proxy node contains a Bloom filter, which is a data structure that can efficiently test for the presence of certain values. When an attack warning is issued, more user proxy machines are deployed with the number of users assigned to each being halved until attackers are identified. Published simulation results are very promising; however, a real-world testing is needed to achieve realistic performance measurement.

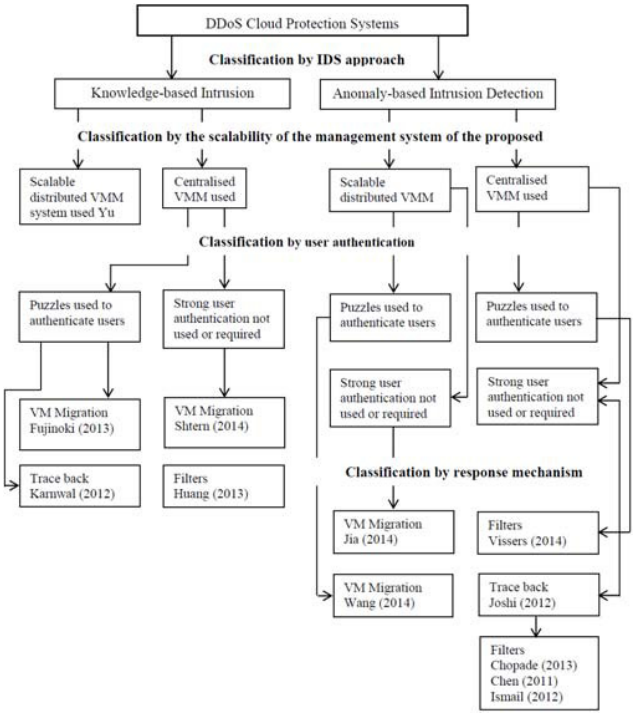

Fig. 1. Classification of DDoS cloud protection systems

Tripathi et al. [28] investigate the use of Hadoop for DDoS defence. Hadoop uses the MapReduce framework for processing large volumes of data. This method replaces the standard First in First Out (FIFO) scheduling mechanism with a Self-Adaptive MapReduce (SAMR) scheduling. SAMR breaks jobs into tasks that are then allocated to map nodes. The advantage of SAMR is that it reads the historical data that is stored on each node and adapts its task distribution based on this information. By classifying the performance of nodes, the time of task execution can be improved by up to 25%. This approach is only suitable for a behaviour based IDS.

In [29], DDoS flooding detection tool is proposed. The authros introduce a distance estimation based method to estimate traffic rates. The distance is calculated using the Time-To-Live (TTL) of a packet. Exponential smoothing is then implemented to calculate the real-time measurement of the roundtrip of IP traffic. Finally, absolute deviation is used to decide if the behaviour is abnormal. This approach attempts to overcome the reliance on attribute dependences that can be spoofed or the time delays associated with traffic monitoring. Since ISPs should be responsible for implementing filters on traffic as they receive the packets; this practice is unlikely to be adopted.

In [30], a review of systems to protect against DDoS attacks in Wireless Body Area Networks (WBANs) is presented. WBANs devices are resource constrained, which makes them ideally joined to the cloud, where the complex computational requirements can be performed. A number of low-overhead systems has been proposed specifically for WBANS. For example, [31] is a system that places IDS' at different locations in the cloud that collaborate to share attack alerts. This system assumes that a node will have the available bandwidth to send an alert

when it is under attack. Another IDPS system proposed in [32] uses a statistical method to create and apply a covariance matrix of network behaviour. A behaviour-based system proposed in [33]. It presents a training period to create a nominal profile with attribute value pairs. The system calculates a score for every packet. These scores are then used to determine which packets to drop in an attack scenario. This approach delivers a high-speed system with minimal memory requirements and an acceptable level of filtering accuracy.

Based on the review of these recent approaches, it is evident that the cloud model introduces new security vulnerabilities. Most of the proposed defence models focus largely on a single type or point of attack. However, we started to observe new systems that rely on the cloud itself for defence against large-scale DDoS attacks. This enables systems to adopt the scalability features of the cloud enhancing security for all parties. It is also essential to think of security models in terms of protecting individual clients and their services as well as the cloud as a whole. To develop an effective defence system, aspects of these research systems need to be integrated to protect against a wider range of attacks. This requires efforts to be directed towards the secure integration of the fundamental cloud technologies to avoid further vulnerabilities being introduced to the model.

6. Conclusion

With virtualisation being a key underlying technology of the cloud model, there are a number of similarities between proposed IDPSs. A number of these use VMs as system management units. Others migrate users to new VMs through either physical or logical migration. This allows these systems to make use of the elasticity and scalability of the cloud paradigm to provide a more effective response to an attack and helps to reduce bottlenecks in the system.

We identify two main research avenues to be followed. First, the intrusion is attempting to compromise VMs to launch a DDoS attack against a target that is external to the cloud. Once the intrusion is detected, a counter-measure is to be deployed, which in this case will be a calibrated firewall. Although this is may appear to be a simplistic fix to exiting systems, it is not a solution that is widely adopted by CSPs because it adds to their overheads, while not directly protecting their own infrastructure. Second, develop defence mechanisms for the more traditional cloud intrusion, where the target of the attack is the cloud or an element within the cloud itself. Resources relevant to this scenario will be based in a Eucalyptus cloud system.

7. Reference

[1] M. Mackay*, et al.*, "Security-oriented cloud computing platform for critical infrastructures," *Computer Law & Security Review,* vol. 28, pp. 679-686, 2012.

[2] C. Rong*, et al.*, "Beyond lightning: A survey on security challenges in cloud computing," *Comput. Electr. Eng.,* vol. 39, pp. 47-54, 2013.

[3] J. Jang-Jaccard and S. Nepal, "A survey of emerging threats in cybersecurity," *Journal of Computer and System Sciences,* vol. 80, pp. 973-993, 2014.

[4] Galante J.*, et al.* (2011, May 14, 2015). *Sony network Breach shows Amazon Cloud's appeal for hackers*. Available: http://bloomberg.com/news/2011-05-15/sony-attack-shows-amazon-s-cloud-service-lures-hackers-at-pennies-an-hour.html

[5] Cloud_Security_Alliance. (2010, Top Threats to Cloud Computing V1.0. Available: http://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf

[6] W. Wei. (2014, May 14, 2015). *Sony Playstation Network Taken Down By DDoS Attack. The Hackers News*. Available: http://thehackernews.com/2014/08/sony-playstation-network-taken-down-by_24.html

[7] S. Khandelwal, "SNMP Reflection DDoS Attacks on the Rise. The Hackers News," 2014.

[8] A. Patel*, et al.*, "An intrusion detection and prevention system in cloud computing: A systematic review," *Journal of Network and Computer Applications,* vol. 36, pp. 25-41, 2013.

[9] T. Karnwal*, et al.*, "A comber approach to protect cloud computing against XML DDoS and HTTP DDoS attack," in *Electrical, Electronics and Computer Science, 2012 IEEE Students' Conference*, 2012, pp. 1-5.

[10] C. Modi*, et al.*, "A survey of intrusion detection techniques in Cloud," *Journal of Network and Computer Applications,* vol. 36, pp. 42-57, 2013.

[11] S. X. Wu and W. Banzhaf, "The use of computational intelligence in intrusion detection systems: A review," *Applied Soft Computing,* vol. 10, pp. 1-35, 2010.
[12] S. Yu*, et al.*, "A Security-Awareness Virtual Machine Management Scheme Based on Chinese Wall Policy in Cloud Computing," *The Scientific World Journal,* vol. 2014, p. 12, 2014.
[13] A. Volokyta*, et al.*, "Secure virtualization in cloud computing," in *Modern Problems of Radio Engineering Telecommunications and Computer Science, 2012 International Conference on*, 2012, pp. 395-395.
[14] L. Qian*, et al.*, "An In-VM Measuring Framework for Increasing Virtual Machine Security in Clouds," *Security & Privacy, IEEE,* vol. 8, pp. 56-62, 2010.
[15] D. Williams*, et al.*, "Security through Diversity: Leveraging Virtual Machine Technology," *Security & Privacy, IEEE,* vol. 7, pp. 26-33, 2009.
[16] Y. Lanjuan*, et al.*, "Defense of DDoS attack for cloud computing," in *Computer Science and Automation Engineering (CSAE), 2012 IEEE International Conference on*, 2012, pp. 626-629.
[17] B. Joshi*, et al.*, "Securing cloud computing environment against DDoS attacks," in *Computer Communication and Informatics (ICCCI), 2012 International Conference on*, 2012, pp. 1-5.
[18] T. Vissers*, et al.*, "DDoS defense system for web services in a cloud environment," *Future Generation Computer Systems,* vol. 37, pp. 37-45, 2014.
[19] M. Shtern*, et al.*, "Towards Mitigation of Low and Slow Application DDoS Attacks," presented at the Proceedings of the 2014 IEEE International Conference on Cloud Engineering, 2014.
[20] P. C. Senthilmahesh*, et al.*, "DDoS Attacks Defense System Using Information Metrics," in *Proceedings of the Third International Conference on Trends in Information, Telecommunication and Computing*. vol. 150, V. V. Das, Ed., ed: Springer New York, 2013, pp. 25-30.
[21] R. Mathew and V. Katkar, "Survey of low rate DoS attack detection mechanisms," presented at the Proceedings of the International Conference & Workshop on Emerging Trends in Technology, Mumbai, Maharashtra, India, 2011.
[22] Y. Tang, "Countermeasures on Application Level Low-Rate Denial-of-Service Attack," in *Information and Communications Security*. vol. 7618, T. Chim and T. Yuen, Eds., 2012, pp. 70-80.
[23] H. Wang*, et al.*, "A moving target DDoS defense mechanism," *Computer Communications,* vol. 46, pp. 10-21, 2014.
[24] J. Quan*, et al.*, "Catch Me If You Can: A Cloud-Enabled DDoS Defense," in *Dependable Systems and Networks (DSN), 2014 44th Annual IEEE/IFIP International Conference on*, 2014, pp. 264-275.
[25] D. Moore*, et al.*, "Inferring Internet denial-of-service activity," *ACM Trans. Comput. Syst.,* vol. 24, pp. 115-139, 2006.
[26] V. S. Huang*, et al.*, "A DDoS Mitigation System with Multi-stage Detection and Text-Based Turing Testing in Cloud Computing," in *Advanced Information Networking and Applications Workshops (WAINA), 2013 27th International Conference on*, 2013, pp. 655-662.
[27] H. Fujinoki, "Dynamic Binary User-Splits to Protect Cloud Servers from DDoS Attacks," presented at the Proceedings of the Second International Conference on Innovative Computing and Cloud Computing, Wuhan, China, 2013.
[28] S. Tripathi*, et al.*, ". Hadoop Based Defense Solution to Handle Distributed Denial of Service (DDoS) Attacks," *Journal of Information Security,* 2013.
[29] S. S. Chapade*, et al.*, "Securing Cloud Servers Against Flooding Based DDOS Attacks," in *Communication Systems and Network Technologies (CSNT), 2013 International Conference on*, 2013, pp. 524-528.
[30] R. Latif*, et al.*, "Distributed Denial of Service (DDoS) Attack in Cloud- Assisted Wireless Body Area Networks: A Systematic Literature Review," *J. Med. Syst.,* vol. 38, pp. 1-10, 2014.
[31] L. Chi-Chun*, et al.*, "A Cooperative Intrusion Detection System Framework for Cloud Computing Networks," in *Parallel Processing Workshops, 2010 39th International Conference on*, 2010, pp. 280-284.
[32] M. N. Ismail*, et al.*, "Detecting flooding based DoS attack in cloud computing environment using covariance matrix approach," presented at the Proceedings of the 7th International Conference on Ubiquitous Information Management and Communication, Kota Kinabalu, Malaysia, 2013.
[33] C. Qi*, et al.*, "CBF: A Packet Filtering Method for DDoS Attack Defense in Cloud Environment," in *Dependable, Autonomic and Secure Computing (DASC), 2011 IEEE Ninth International Conference on*, 2011, pp. 427-434.