Unraveling the Security Pitfalls that Stem from Core Cloud Benefits through Analyzing Various DoS Attacks, Detection and Prevention

S.B. Ribin Jones, Research Scholar, Dept. of Computer Science & Engineering, VISTAS, Chennai, India.

Dr.N. Kumar, Associate Professor, Dept. of Computer Science & Engineering, VISTAS, Chennai, India.

Abstract--- Cloud Computing has become center of attraction for Private and Public Sectors due to its features such as On-Demand services, flexible Pay-as-you-go etc. Virtualization as the centre the Cloud can be extended and presented as any number of services which revolve around fundamental architecture with IaaS, SaaS and PaaS. The benefits of cloud that looks appealing from all the other perspectives looks very discouraging when looked at from the security perspective. Conversely, to seek answers this research paper looks at the aspects of traditionally threatening DDoS attacks in Cloud Computing and, how it managed to adapt into Cloud in various forms. Moreover it also presents the aspects of the Cloud Components that can cause the harmful effects of DDoS attacks with a simple exploit. Moreover the core elements of Cloud IDPS and its limitations are discussed. The limitations in prevention and detection of such attacks suggest the requirement for strong Cloud feature based monitoring. The Cloud features are defined in form of QoS requirements and are negotiated while performing SLA (Service Level Agreement). All the features that are delivered as functional and performance metrics are presented and their role in improvising the Cloud Security has been discussed. Consequently based on the performed research various undefined aspects that are attributing to security threats in Cloud were identified and are defined appropriately.

Keywords--- Cloud Computing, DDoS, EDoS, IDPS, SLA.

I. Introduction

Cloud computing as a provider of services puts available resources to effective use through virtualization [2]. This way, among other distributed computing paradigm it thrives through offering; readily available resources for on-demand access, pay-as-you-go dynamic billing for resource usage, utilize the extra hardware capabilities from the aspect of storage, processing and communication, absolute null in-house depreciation losses, etc [1]. This core benefits attracts organizations indifferently from Government sectors and private industries to migrate to Cloud Services [3].

Besides to suit various needs of the industries the Cloud computing offers service oriented architecture that specifies the service requirement in organized manner as; Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS) [2]. More specific services can also to derived and provided under XaaS (any thin as a Service) paradigm [2][3]. This allows organizations to migrate the entire IT infrastructure or individual or group of elements to Cloud as the need arrives. Among those services IaaS is a huge business because it allows the complete migration of the industry [9]. IaaS Cloud stands superior over premise bounded infrastructure through effective application of virtualization over all available resources [17].

Virtualization allows cloud to generate any number of virtual machines (VMs) from the server, to host the client service [7]. Client services are therefore entitled to receive VMs and resources in an unlimited basis based on the processing requirement.

When in need, the resources are dynamically allocated and returned when they are idle [6]. Web servers and other client request processing services faces service outages due to various reasons such as occasional benign flash flooding of resources, running of complex application, network congestion, maintenance outages etc [27]. These outages can be completely eliminated with insightful application of auto scaling and service on-demand features. Unlike traditional computing, this makes the basic Cloud architecture dynamic and extendable to host any number of applications, Operating systems (OS), hardware operations and network components [27]. This way, unlike traditional computing the Cloud achieves the maximum extent of virtualization. For instance, a single VM can host an OS or various VMs can host a single application.

DOI: 10.5373/JARDCS/V11/20192603
ISSN 1943-023X

Received: 19 July 2019/Accepted: 18 August 2019

Cloud requires needs of user to be well defined and catered appropriately. This demands the Cloud Service Provider (CSP) to provision the resources based upon the negotiable Service Level Agreements (SLAs) that determines the Quality of Service (QoS) requirement for the offered service [4]. SLA is a contract signed between the consumer and the CSP agreeing upon various performance and functional requirements necessary for the service to meet user need. The resource usage and VM access in cloud is expected to be highly dynamic in nature so becomes the nature of the cyber attacks on the Cloud. Moreover the vulnerability has the scope to spread to various industries and is not confineable to perimeter based defense as in on-premise or traditional distributed computing at the least in public and hybrid Cloud [6]. This way Cloud not only becomes easy target of attack but also becomes the hatching ground for developing various versions of attacks. It is more likely, for an attacker to host a Command and Control platform in Cloud than other platforms because it requires to host and monitor the attacks across diverse platforms [11]. Such scenarios question the applicability of robust looking traditional security measure in Cloud Computing. As the cloud attempts to further narrow the gap between the technology and business, Cloud applications becomes more sensitive and requires more robust security solutions [8]. For instance, the traditional Distributed Denial of Service attack when performed on Cloud it inflict business (currency) loss to clients and evolve as EDoS (Economic Denial of Service) attack [18].

1.1. Need for DDoS, IDPS and SLA, Survey

A simple DoS attack to a complicated EDoS attack can be performed within the Cloud or launched from the Cloud with ease. Therefore the types of attack that was once well categorized and anticipated becomes complex to categorize and predict in the Cloud. As a result number of DoS/DDoS based incidents increases in such a way that every enterprise is expected to face at least 3 DDoS attack every month, which was not the case five years back [22]. Therefore thorough literature survey is required to identify various versions of DDoS attack. As well as the features of Cloud that can cause the effects of the DDoS attack becomes inevitable.

Moreover various functional component of complete Cloud IDPS needs to be sorted out in the same taxonomy to understand the limitation and to derive the possibilities of improvements.

SLA is marked with the shooting up of violations whenever the service surpasses the bounds of pre-determined QoS. Even if the attacker carefully evade the IDPS system he may not have the resource to know SLA policy, so there is a greater chance these violations can indicate the presence of the malicious entity apart from service faults. Therefore various QoS aspects of the Cloud from both functional and performance perspective is required to be placed in the DDoS survey paper to guide the researches to design better Detection and Prevention Systems.

1.2. Survey methodology

A thorough literature survey is performed by collecting numerous survey papers related to Cloud based *Dos/DDoS attacks; Detection, Prevention and Mitigation;* as well as *SLA implications*, since those three aspects are identified as *focus of the research*.

The exhaustive search is performed in all the notable indexing services to make sure all the notable research works were surveyed. However, almost all collected papers miss out on encompassing the importance of the three aspects of the research focus. Hence they are lacking to offer the future researches to thrive and achieve proper Cloud security goals. Therefore we attempts to provide short and crisp taxonomy on all these three aspects from the connotation of DoS/DDoS, since DDoS attack has been proved to a highest challenge for security system to face [22].

1.3. Organization

We present a brief introduction about Cloud and its various features and how they are susceptible to attacks in Section 1. It also discusses about importance of looking at the cloud vulnerability towards DDoS attack from a different perspective than the traditional approach. Section 2 presents the taxonomy of DDoS attacks hosted in Cloud. It also list out characteristics of attacks that can mimic the DDoS attacks in all the components of cloud computing. Section 3 offers a concise taxonomy on Cloud Security from the core aspects of Prevention, Detection and Response of DDoS attacks. Section 4 discusses about the various pit falls in Cloud Security and how the integration of SLA violation based monitoring is essential for the effective Cloud Security. Section 5 lists all the functional and performance based QoS metrics required for SLA agreements. The Section 6 concludes the article with pointing out the future direction for research. Finally the Reference section is listed only with the chosen papers that are considered suitable for this research.

DOI: 10.5373/JARDCS/V11/20192603
ISSN 1943-023X

Received: 19 July 2019/Accepted: 18 August 2019

II. Taxonomy of ClouD Hosted DDoS Attacks

Traditional DoS/DDoS attacks were enhanced to exploit various features of Cloud [5]. The improvisation denotes, not only how many and wide number of options that are readily available to exploit in Cloud, but also how easily they can be maneuvered. There is lot of reference for Cloud hosted TCP SYN, HTTP, UDP Flood attacks, ICMP, DNS Reflective attacks etc [16]. However the intention of this work to show the evolved attacks, therefore the list of all Cloud Specific attacks are listed in Table I.

Table I: Types of DDoS attacks

Types	Abbreviation	Description
EDoS	Economic Denial of Sustainability	EDOS through covert invocation of virtual resource or virtual nodes, exploit the Cloud pricing model [1].
CI-DDoS	Cloud-internal Distributed Denial of Service	Compromised VMs ran by C&C module attacks the residing cloud host and behaves as normal VMs, can overload the hosting Cloud and disrupt further processing [31] .
X-DoS	XML Denial of Service	Sends web services with oversized XML messages to surpass the processing potential of the server [5].
DX-DDoS	Distributed XML DoS	This attack aims at crashing the cluster of web servers through complicating XML messages, which can struck the parsing mechanism [17].
H-DDoS	HTTP Denial of Service	Attackers hide the malicious content in the HTTP requests to bypass the web proxy conditions to launch DoS & DDoS attacks [10].
HX-DDoS	HTTP XML DoS	Floods the virtual or physical communication channels of Cloud hosted web servers by combining HTTP & XML messages [8].
DNS-DDoS	Domain Name System DoS	DNS Deployed in Cloud hosts both virtual and physical components from the pool of IP addresses. Therefore even a complicated amplification attack is easier to perform in Cloud Data Centers [17].
MeM Cached DDoS	Memory Cached DDoS	Cloud Servers have Object-caching mechanism to speed up web server session [26]. If MeMCache is exposed, attackers can generate reflective UDP requests towards server. Server attempts to generate response and may clog the network or hangs.

The attack that focuses upon internal/external vulnerabilities to flood server/servers, cloud platforms and other Internet based platforms is DDoS attack [5]. The attack that focuses on inflicting money loss is EDoS attack and it is also a version of DDoS attack [10]. Apart from the listed DDoS attacks, there are possibilities for more versions of DDoS attacks that can be maneuvered and still can go unnoticed so such exploits were carefully studied and presented as follows. In other word, various user friendly Cloud components are exploitable in such a way to imitate a DoS/DDoS attack. They are listed as follows;

Cloud Supervisor Exploits: Hypervisor usually have inbuilt security management and vulnerability patching services [7]. However if the Cloud Supervisor itself is compromised then the entire cloud can be compromised [27]. Similarly if the QoS Scheduler is compromised, though cloud offers wide array of options to tune the Scheduler the service qualities can be degraded [23]. This way Cloud Computing exhibit Single Point-of-Failure possibilities [27]. For instance, through leasing a guest VM, attacker can install an OS that carries code to hack the hypervisor to host C&C module.

Cloud Scheduler Exploit: Cloud Supervisor or Hypervisor comprises a Scheduler that can perform priority scheduling as well as different types of automatic and manually supervised Scheduling to meet the SLA requirements [23]. Based on the SLA requirement, the VMM (Virtual Machine Manager) chose the scheduling algorithm and then allot the application to dynamic pool of VMs. However, if the Scheduler is compromised, attackers can perform cheeky yet devastating operations such as; prioritizing the non priority VM operations, turn the high priory operations to low priority, replace the running algorithm for instance FIFO (First In First Out) to LIFO (Last In First Out), etc. If numerous VMs are running then the Scheduler exploit can impact Cloud processing as a DDoS attack. VM Sprawling Exploit: VMM provides management policy that does not allow another VM to start when processing VMs are idle [27]. However if the VMM is compromised then the attacker can keep invoking VMs even if it goes to idle state. This way, the attacker can use up all the virtual resources and halt the genuine VM access. Energy exploit: Nowadays to control greenhouse gas emissions Cloud facilities are monitored with stringent energy consumption rules. Consecutively the CSP (Cloud Service Provider) deploys hardware, storage, network and software with the Cloud abstraction level of energy conserving provisions to achieve Green Computing benefits. However attackers though performing VM migration, overloading the VMs with complicated workloads, not allowing the VMs from halting etc can increase the energy consumption and make the CSP to be penalized for consumption violations [28]. Privilege Violations: Hypervisor only have VM privileges to host and run the Virtual Machines [26]. However if the attackers hacks the host systems then it allows the attacker to mess up with Hypervisor and VM privileges towards complete meltdown of the Cloud Systems [24].

DOI: 10.5373/JARDCS/V11/20192603
ISSN 1943-023X

Received: 19 July 2019/Accepted: 18 August 2019

Attackers can also reverse engineer this hacking process by running malevolent codes in VMs to crack the VM privilege and gain access to the root privilege of host machine.

VM Migration Exploits: Cloud Supervisor provides features to complete transfer of applications and resources from traditional Systems to Cloud Systems or within Cloud Systems in case of overloads [26]. However an attacker through using this feature can initiate a small or large scale VM Migration process without the knowledge of the Cloud Supervisor/Hypervisor. This can impact the cloud systems as a DDoS attack if more VMs are migrated. This way an attacker can reduce the performance of the Cloud Services and can cause serious damages to SLA objectives [6]. Storage Exploits: Cloud supports numerous VMs to run and access I/O storage disk concurrently [7]. Disk access such as in Network Attached Storage (NAS) allows accessing of the storage resources through networks [11]. Therefore DDoS intended attacker, through issuing large number of disk accesses can cause I/O Contention in local storage and network congestion in NAS.

Network exploits: Hypervisor has an inbuilt network emulation component for network device virtualization. It provides IP address to every VM and treats them as virtual LAN [17]. VM forwards packets to hypervisor through physical device to another VM. Packets can be routed through host domain to a remote VM or to a System. Consequently DDoS attack can be generated within cloud by deploying various VMs to clog the hypervisor and the physical device. Interrupt and Timer Exploits: Hypervisor also contain Interrupt Request (IRQ) module, Programmable Interrupt Controller (PIT) etc to generate virtual interrupts in accordance with physical interrupts [7]. Simple obstruction of virtual interrupt mechanism with a DoS attack hosted from a compromised VM can crash the host.

III. Cloud Security Discussion

Cloud offers provision for IDPS (Intrusion Detection & Prevention System). Cloud Distributed IDS (DIDS) scale and monitor across physical and virtual networks [21]. Cloud IDPS is custom built with capabilities involve Host-based IDS (HIDS), Network-based IDS (NIDS), Hypervisor-based IDS (HyIDS) etc [5][29]. Moreover the Cloud IDPS performs various operations that are classifiable under three main categories, they are; attack prevention, attack detection and attack response and recovery as depicted in fig.1.

3.1 Attack prevention

Prevention is a collection of precautionary and proactive measures grouped in an attempt to eliminate the possibilities for an attack to take place. This is analogues to deploying Transport Layer Security (TLS) in an attempt to prevent wide array of attack from happening [29]. The functional components involve algorithms, methods, policies, rules etc to automatically take decision and deploy action that guards the resources from attacks [32]. It has a set of Assessment tools that can be applied periodically and automatically to scan for vulnerabilities across various components of Cloud. If the vulnerabilities are detected it can be patched to eliminate the risk. e.g. port 80 marks http if the security is the prime concern the report will suggest moving it to port 443 to access secure http [13].

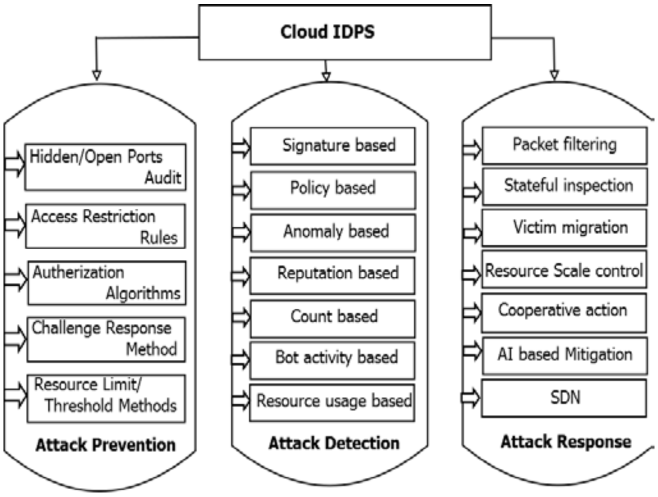

Fig. 1: Detailed security parameters of Cloud IDPS system

DOI: 10.5373/JARDCS/V11/20192603
ISSN 1943-023X

Received: 19 July 2019/Accepted: 18 August 2019

Hidden Port is a technique to hide the ports of the server and present a proxy for external application [13]. This prevents the direct access of the sensible resources [6]. However presenting an open port is advisable for general services to minimize the proxy overhead. Periodic audit on open port server will suggest whether to increase or decrease the security of hidden sensible servers.

Access restriction dictates the terms for clients in accessing the resources. It makes sure only the service is available to benign users and discards or delays the malicious entries [18].

Authorization identifies the clients with their resources [17], measures such as PKI (public key infrastructure) are part of the authorization policy.

Challenge response as a Crypto puzzle such as CAPTCHA, One time password etc has become integral part of the IDPS to differentiate manual use from auto generated requests [1]. One time password can validate the request originator too.

Resource Limit/Threshold methods in general holds an upper limit [11], beyond which the IDPS performs passive scan for attacks. This works as the emergency set up to deal with Zero-day situation. This situation arises when there are no methods to detect an ongoing attack. Every time an attacker programs a new attack to circumvent existing vulnerability database of IDPS it can strike as a Zero-day attack.

3.2 Attack Detection

Attack Detection services is the primary response system. It attempts to detect an ongoing attack with minimal response time [33]. Cloud DoS/DDoS detection is made up of various types of detection procedures to monitor and detect the attack without fail as illustrated in fig. 1.

Signature-based detection is a simple but effective pattern matching system [12]. It contains the pattern or binaries of all the existing attacks and matches it with ongoing traffic. If it finds a match then deduce it as attack with 100% accuracy.

Policy based detection thrives through enforcing compliable policies [9]. The defined policies are then converted into restrictive rules for monitoring the intrusion. For instance, if the policy instructs the client application to perform SSL with Server then the client application that does not perform SSL can be detected as threat and be blocked [28].

Anomaly Detection attempts to observe the behavior of the traffic to find differing pattern from normal pattern [18]. Observing the behavioral change in TCP handshake, ICMP echo requests, client web access behavior, session duration, HTTP request etc are useful in detecting the attacks. It not only helps in detecting ongoing attack but also helps in passive analysis of back logs such as headers of all protocols.

Reputation based detection is analogues to ranking system where the past behavior of the clients were taken in to attack and used to rate it [6]. The clients with poor ranking may end up in the black list for blocking.

Count based or Flow based detection Attempts to detect unusual increase in flow or activities with identity; such as IP address specific packets/unit time counting mechanism to detect DDoS floods [20].

Bot activity based detection: The virtual clients and server mostly resides in the same physical component. So Cloud has the unique opportunity for detecting zombies and tracking the Botnet based on the malevolent activities of VMs [8]. For instance a set of VM sends packets to a black listed server instead of sending it to a genuine server, instead of performing destined operation VM’s attempt to access known vulnerability etc are samples for Bot activity detection.

Resource usage based or threshold based detection performs monitoring by placing a max limit for resource access, if it exceeds then it is detected as attack [21].

3.3 Attack Response

The response is the set of procedures that are automatically deployable if the detection alarm goes off [30]. However there are two types of response reactive and proactive response [24].

Reactive response works with detection and the proactive response uses set of rules and algorithms to automatically act to various adverse situations without waiting for the detection to complete.

Packet filtering is the mechanism that works in tandem with detection to mark and eliminate the infected packets [6].

Received: 19 July 2019/Accepted: 18 August 2019

Stateful inspection is performed to follow various states of the VM machine [6]. As a proactive response if any VM is not responding properly even if a threat is not detected it denotes it is faulty and requires to be replaced. Hence the Cloud based Stateful inspection not only works in tandem with attack detection but also with fault tolerance.

Victim migration is the crucial step in response. If a certain VM is deceased stopping it abruptly will cause the loss of data and affects the credibility of the Cloud. Therefore the processing data is strategically backed up with checkpoint and are made migrate-able in case of malfunctioning of VMs [24]. Cloud can migrate single or set of VMs to VMs in ready state and resume the process from the previous checkpoint.

Resource Scale control is an emergency response system which can take actions in case if the scaling of resource goes out of control [30]. It may or may not have permission to filter the packets or to halt the VMs but can pause the running VMs and migrate it in to other servers with better performance. Hence if the DDoS attack is evasive then it could end up getting migrated into other servers due to scale control [31].

Cooperative Action has become necessary since the boundaries of Cloud are getting more volatile with its growth. This requires a Distributed IDPS system with excellent distributed response system [9]. Cooperative response is marked by the automatic sharing of knowledge and methods essential to safe guard the collective resources [21]. This may be governed by an agreed upon common policy.

Artificial Intelligence based response is a round the clock automatic response system [21]. It may works differently than the manual configuration but still it is necessary to deflect the attacks that are not followed by the skilled professionals [33]. Therefore response from artificial intelligence requires cross examining the detection with set of algorithms to make sure the threat is real to take immediate actions. Semi automatic detections works only after the professional approval.

SDN (Software Defined Networks) is relatively new architecture that improves the performance of Cloud by decoupling redundant data forwarding functions and network controls [8]. Effective programming with SDN can helps in Cloud hardening process and to remove risk causing elements.

Through implementing these mechanisms, Cloud seems to have offered better attack monitoring, detection and filtering possibilities. However the security challenge in Cloud is more elaborate and unprecedented, the following section presents a research narrative on such challenges.

IV. Cloud Security Undefined Constrains

The complication is security arises from its benefits. This section therefore attempts to define the undefined security complications for enhancing the productivity of the Cloud research.

4.1Unboundability for attacks

Cloud in performing Auto Scaling not only can scale across platforms but also can scale across multiple management Boundaries [6]. At certain level, Cloud needs to seamlessly integrate with various elements across boundaries to sustain its Clients. This helps the exploit to spread across various management boundaries. Whenever there is a dynamic access from new boundaries it could keep on spreading. This way, an exploit has numerous opportunities to scale and conquer new boundaries regardless of its perimeter defense. Traditional attacks only managed to spread from server to clients. Cloud attacks could spread from server to server with ease.

4.2 Boundability challenges protection

In spite of sharing a common working environment, in Cloud models such as hybrid Cloud each resource owners may try to secure their own infrastructures and end up viewing other resource management monitoring their resources as breach in security. This rigidity could limit the scope of monitoring a compromise in other friendly Clouds [21]. It also allows enough room for the compromise to hide its existence and allow it to improvise and strike the more secure cloud while the common application is running.

4.3 Hatching Ground Availability

Moreover in public clouds the user is allowed to try different things such as implementing unusual codes in SaaS Cloud that could either have implemented a breach or malfunction. Besides, a single exploit can be hatched to create or to extend into many more complex exploits [17]. Once it succeeds, due to the platform independent nature of Cloud it could attempts to attack more secure private Clouds too.

DOI: 10.5373/JARDCS/V11/20192603
ISSN 1943-023X

Received: 19 July 2019/Accepted: 18 August 2019

4.4 Bountiful opportunities

A single vulnerability on dynamic VM after used by 'n' users can spread to untraceable number of VMs across boundaries due to the volatile usage policy [28]. Consequently the Bot Owner who intend to compromise few VMs to constitute Botnet end up compromising numerous VMs effortlessly. Consequently to constitute a DDoS attack the attacker doesn't have to generate pseudo floods but by sending genuine i/o request from its Botnet can cause the same effect in Storage area networks [12].

4.5 Productive enormity

Apart from spreading Cloud also offer unprecedented chance to convert attacks into revenue [23]. For instance, after hijacking a Cloud attacker can demand ransom from CSP to allow regular operation of services. To avoid loss of reputation and to ensure business continuity, CSP may have to offer the ransom. Another good example is the use of Botnet for stealth mining of Bitcoins in Cloud [31].

4.6 Unduly Tolerability

High priority services like Video Conferencing mostly be accommodated and performed better with superior QoS Management, Load Balancing, Scheduling and Protocol Security such as IP Sec, etc [25]. However for ordinary and low priority services Clouds still remains hatching ground for DDoS/EDoS attacks. Due to its poor following of fault and SLA violations, it is prone to tolerate more faults even if it is caused by an exploit.

4.7 Outsiders inside

In other systems DDoS attack is hosted externally; but in cloud the attack can be housed both externally and internally. E.g. in Internet based client/server setup, the clients are usually considered as external or remote components that access the server [8]. However in Cloud the client and server could be residing in the same server and are internal in nature. Only requirement for the remote computer to become an insider is a Cloud interface.

4.8 Untracability

Owing to the quick change of hands and VM interoperability features an exploit is not easy to be contained. Any number of VMs is instantly accessible to any number of applications at any time across Clouds [25]. As a result, a single exploit in a VM could have gotten into any application and to any Cloud in an instant. Though the security management may not keep track of the compromise, the attacker can keep track of the compromise through his C&C module [29].

4.9 Loss of specificity

Traditionally, when the computing is bound to physical devices it is easy to specify the details of attack such as target machine IP, Mac, time of attack etc [13]. Conversely, if the same attack could have happened in the VM, due to its highly dynamic nature such details can't be specified.

4.10 Lavishness in Entertaining attack

The objective of DDoS attack is to flood all processing capability of the server and halt its operation, thus making it inaccessible to genuine clients [13].

Cloud through offering dynamic brokering services can help tackling the maximum brunt of any DDoS attack and still can process the genuine users. Therefore in general, the Cloud is viewed as the provision to alleviate variety of DDoS attack and flash floods [9]. On the contrary, it could also be looked at as going easy on attacks by tolerating it and entertaining it.

4.11 Volatile networking

Cloud network constitutes VAN (Virtual Application Network) &VLAN (Virtual LAN) with Virtual IP address offered for every Virtual clients, Virtual switch and Virtual servers [30]. Cloud Platform offers internal Open Virtual Switch (OVS) and external Open Flow Switch (OFS) to constitute and manage virtual networks. There are issues concerning VAN that impedes Cloud IDPS to cope up with this criterion. Since the VAN constitutes virtual components that works in tandem with physical components, if Cloud IDPS attempts to do a deep packet inspection it requires to look into the VAN and physical vLAN setup together thus consumes more time [17]. Unlike physical networking VAN in Cloud are more complex software programs. Therefore it causes unprecedented deployment, configuration and other software problems and is vulnerable to various software exploits.

DOI: 10.5373/JARDCS/V11/20192603
ISSN 1943-023X

Received: 19 July 2019/Accepted: 18 August 2019

4.12 Maskability

Byzantine faults are the once even thought the component is faulty it does not generate detectable errors but it appears to function as normal [24]. Typical VM exploit if managed to act as the Byzantine fault, it can elude fault and risk detection systems. For instance, allowing a single exploited VMs to participate in Bigdata processing [3] through masking it as genuine will create erroneous result in every level of data processing which is enough to corrupt the entire outcome.

4.13 Pressure of Non Performance

In highly paid Bigdata processing Clouds, there is no threshold for processing requests. Even if the DDoS attack is constituted, in a pressure to meet the QoS requirements the Cloud may end up extending the virtual nodes and resources without invoking the filtering capabilities to avoid false positives [29]. Detecting cluster of DDoS/EDoS attack is further made complicated since nowadays any DDoS can exhibit the behavior of normal usage e.g. Botnet attacks [12].

4.14 Unlimited scope for attack innovation

The traditional DDoS when performed on Cloud it inflict currency loss to clients and evolve as EDoS (Economic Denial of Service) attack [10].

Seemingly DoS/DDoS attack has evolved more capabilities in Cloud to perform vicious operation such as corrupting big data processing, performing stealth big data processing, causing financial loss, gaining stealth profit etc. Moreover as the user friendly features evolve more options keeps opening up for an attackers to exploit [32].

V. Metrics that Distinguishes the Cloud

Cloud Services relies upon delivering the agreed upon QoS (Quality of Service) to the Clients. For that reason, QoS is carefully chosen and negotiated to establish a SLA (Service Level Agreement) between the Service provider and the Consumer before providing of the Cloud Service [29]. Various third party applications are involved in negotiations of QoS based SLA metrics before the service is delivered. They are; Meta Negotiator [4]: As the name implies it negotiates services between user and service provider. It is where user selects services by specifying their prescriptions such as Protocol, Security, Memory, Storage, Processing, along with various QoS requirements. Next in line is Meta Broker [27]: Involves meta data to select appropriate broker to deploy services for specified user requirements.

Broker [23]: It is the prime component which can communicates with Automatic Service Deployer (ADS) or has the privilege to interact directly with virtual and physical resources in accomplishing the service goals of the users. Quit often Cloud Broker is involved in negotiations as well as with the renegotiation and attempts to deal with the service complications smoothly [5] [8].

Finally Automatic Service Deployer [4]: is responsible for deploying services through appropriate selection of resources without expecting the manual interaction.

However a Cloud Hypervisor or Supervisory component contains a Self-Management Module which is responsible for performing QoS scheduling based on the SLA [23]. It offers two types of SLAs; they are dynamic and static SLA [14]. Static SLA retains the initial SLA agreement throughout the processing and it does not support renegotiations.

Whereas the Dynamic SLA allows changes and renegotiations to suit the service fluctuations, however it is costly than static SLA [24]. Moreover the SLA involves obligations such as service pricing, and penalties in case of agreement violations [3][14].

Every SLA violation is treated differently for different scenarios. For instance the SLA in mission critical applications is more seriously monitored than other applications where certain degree of SLA violation is allowed. The SLA violation may indicate the node (VM) failure, link failure, etc]. Whether the element which caused SLA violation is further allowed for processing or replaced with other node is often determined based on the QoS requirements and priorities.

5.1. Functional SLA Metrics of Cloud Services

SLA metrics covers diverse parameters that impact the Cloud Services [15] are listed as follows:

DOI: 10.5373/JARDCS/V11/20192603
ISSN 1943-023X

Received: 19 July 2019/Accepted: 18 August 2019

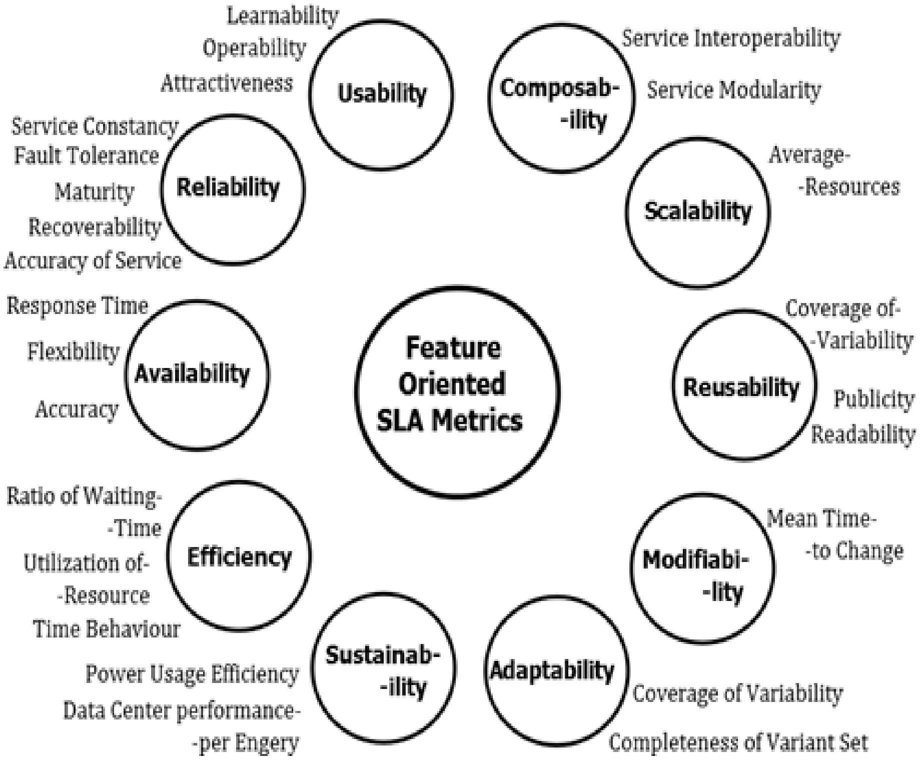

Fig. 2: Functional SLA Metrics that measures the Cloud Features

The functional and performance measure are enlisted in figures 2 and 3 respectively. However describing all the metrics is not the motive of this research, instead to point out all the aspects of the metrics which helps in optimizing the DoS/DDoS Prevention, Detection, and Mitigation if incorporated with Cloud IDPS system.

Reliability [3]: Ensures the services are functioning without errors and serving the purpose. Following Reliability is essential for Prevention.

Availability [9]: Not only ensures the resources are available but it is also accessible on time. Following violations in availability metrics can help in quick attack detection & mitigation.

Efficiency [23]: Makes sure that the resources are delivered on time. It also ensures that the resources are put to better use. Oscillations in efficiency if monitored can improvise detection & mitigation.

Sustainability [15]: It attempt to reduce carbon footprint. Following it is essential for proactive detection, mitigation and prevention.

Modifiability [32]: Measures the customizable nature of a Cloud service. It may help in protection and detection.

Adaptability [29]*:* Provides metrics to measure the capabilities of a service to adjust to various situations in enhancing the utilization. It is essential to enhance Distributed IDPS.

Reusability [3]: Measures the levels to which a Cloud module or component is usable to multiple applications. It can help in improvising all the three components of IDPS.

Scalability [25]: Not only ensures resources are dynamically involved but also measures whether it is performing to the user requirement. Following violation can help to enhance detection & mitigation.

Composability [3]: Ensures basic unit level standards to make interoperability possible and also makes sure it is performed smooth and seamless. It can help in early detection.

Usability [19]: Measures usefulness from the user point of view. It could help in deducing a zero-day attack. EDoS attack if not detected early reflects in usability.

DOI: 10.5373/JARDCS/V11/20192603
ISSN 1943-023X

Received: 19 July 2019/Accepted: 18 August 2019

5.2. Performance defined SLA Metrics of Cloud Services

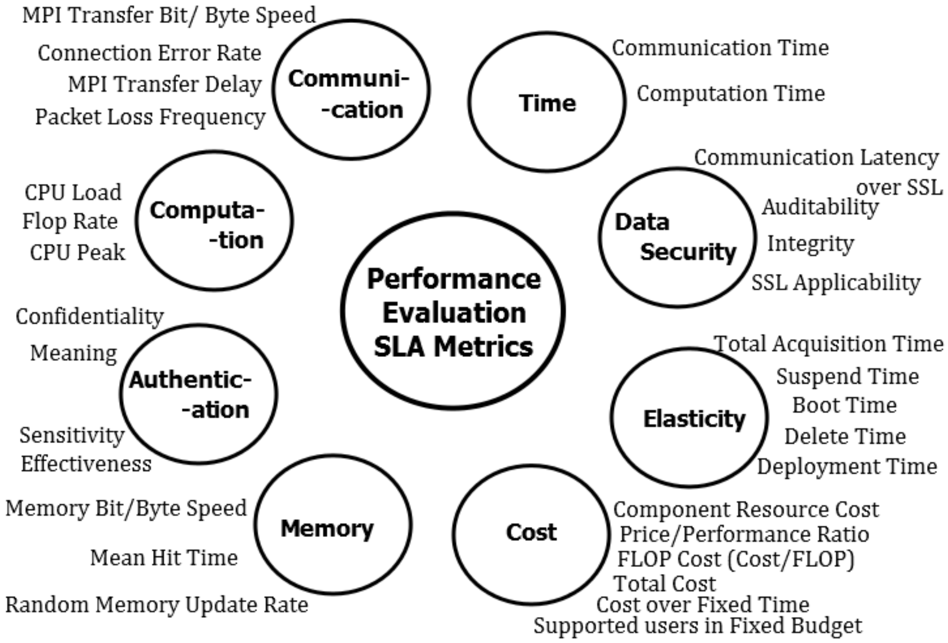

Fig. 3: SLA Metrics that measures the Cloud Performance

Communication [25]: Provides metrics to measure the performance of the communication. SLA violations in communication indicate fault or breach.

Computation [14]: Measures processing performance of the Cloud system. It can reflect the presence of DDoS attack.

Authentication [23]: Provides metrics to evaluate the required need for securing the resources from illicit access of attacker by making sure various aspects of security.

Memory [31]: the metrics involved will help to evaluate various aspects of memory. SLA violations in memory often indicate the unhealthy access and monitoring memory violation will enhance the DoS/DDoS detection and reaction.

Cost [19]: Provides various metrics to convert the service usage into the price of service. It is actively monitored to provide pay-as-you-go type of bills. Integrating metrics from the cost with intrusion for both passive and active vulnerability assessment as well as for active monitoring will helps to curb EDoS attack and other aspects which cause loss of money either advertently or inadvertently.

Elasticity [15]: It provides metrics to follow complete cycle of VMs. This is required for the smooth expand and contract the Cloud resources in timely manner. This can work along nicely with proactive and reactive attack monitoring systems.

Data Security [30]: Covers complete aspect of security. It is involved in Software Engineering process, to operation support aspects of Cloud.

Time [19]: Helps in active measurement of communication time and processing time of individual VMs and entire set of VMS involved in a Service. Hence it is a critical component to reduce reaction for attack response.

5.3 Result Evaluation

Cloud attacks often struck as a zero day attack, in such cases the prevention fails for the lack of proactive preventive measures. Therefore the attack detection becomes significant. However to understand the real-time industry level detection standards various statistical pie chart plots were obtained from the leading Cloud security service providers ‘ARBOR networks’. They are analyzed as follows.

DOI: 10.5373/JARDCS/V11/20192603
ISSN 1943-023X

Received: 19 July 2019/Accepted: 18 August 2019

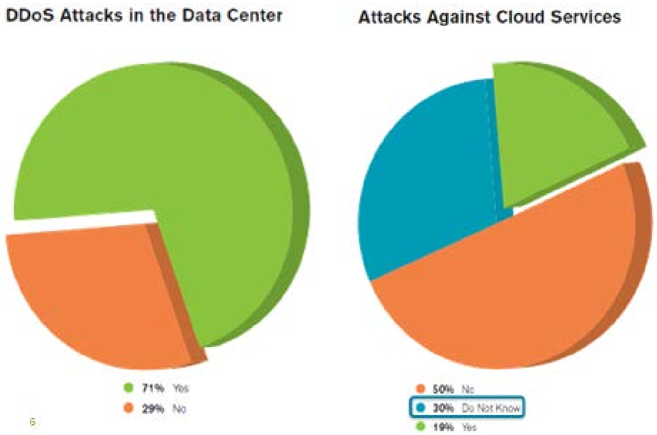

Fig. 4 & 5: Attack against Data Centers in every months & Attack against Cloud Services every month

Detection of attack is not effectively happening in the Cloud, for instance the pie chart as in fig.5 shows 30% of the times the attack is not detected. The 30% do not know cases substantiates; that the DDoS attacks that were once very strongly felt has now become unnoticeable and became undetectable. Therefore if an attack corners single-point-of-failure such as hypervisor or Scheduler, if the mitigation is not put into effect immediately, then the attack could manage to crash the entire Cloud for the lack of preemptive detection and effective mitigation techniques. It shows that the Cloud still lacks the timely response techniques for detection and mitigation to curb the attack at its early stage.

Moreover the figure 4 &6 shows there are 71% chance for 1 to10 DDoS attack to strike at any Data Centers. This shows there is a *massive weakness* in Cloud that helps the attackers to grow their potential. Thus new types of attacks are keep surfacing.

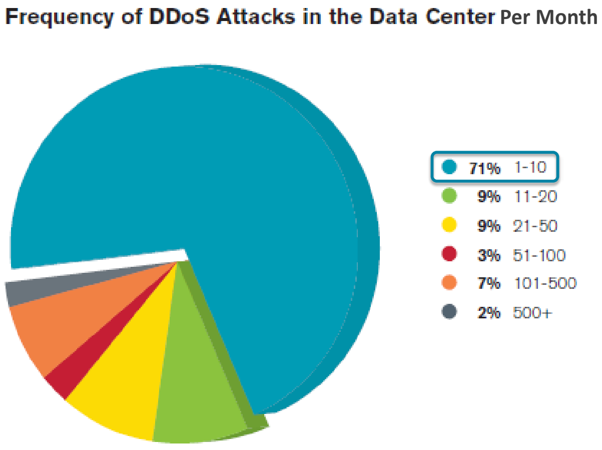

Fig.6: Shows the frequency of the DDoS attacks detected monthly for a third party managed Data Centers

There is the fair chance that the 19% as in figure 5 were the once who are aware of DDoS attack and attempts to follow the attacks either with automatic or manual observations. The same can't be said about the rest because traditionally the DDoS attack can be immediately felt in terms of flooding, exceptional conception of processing power or memory etc. Nowadays with the advent of SAN and Cloud the servers are already a Server farms or Data center. This is also stretchable to any number of servers with the automatic implementation of Cloud. This way the Datacenters may not fail the client but may incur loss to company for exceptional use of resources.

However the C&C controlled Virtual Nodes are expected to generate more SLA violations, since the attacker does not confine to the SLA negotiations. If the service surpasses the bounds of pre-determined QoS the SLA violations shoots up, these violations may indicate the presence of the malicious entity. Therefore SLA violation or QoS violation is a good place to look for security breach and DDoS attack.

DOI: 10.5373/JARDCS/V11/20192603
ISSN 1943-023X

Received: 19 July 2019/Accepted: 18 August 2019

VI. Conclusion and Future Scope

Various forms of DoS/DDoS attack that threatens the Cloud have been surveyed and tabulated. The features that pave way for attacks that intends to create the effect of DoS/DDoS has be analyzed and listed in specific to every Cloud operating components. The phases of security in mitigating DoS/DDoS attack, i.e. Prevention, Detection, and Response has been studied carefully and are categorized. The DDoS/EDoS poses unprecedented challenges to Cloud that hinders the Cloud IDPS, such aspects are unusual and not yet been properly studied comprehensively. Therefore various such challenges that are unique to Cloud have been examined and are defined. This shows the need for enforcing SLA metrics into Cloud IDPS for getting better and real-time applicable results. Therefore various functional and performance QoS metrics that are negotiable in SLA agreements has been enlisted by marking their applicability in various aspects of DoS/DDoS mitigation system. Finally a result analysis is performed to understand the real-time implications of DDoS/EDoS mitigation. The result suggests, taking the DoS/DDoS detection level improvement more seriously to overcome the present lag in performance.

Consequently according to this research, integrating and fine tuning the DoS/DDoS detection with SLA violation monitoring capabilities is required to enable IDPS to offer proper Cloud level solution. Given that, the Cloud SLA based Security can be able to detect more swiftly and effectively than other detection methods.

References

[1] Ahmad Shawahna, Marwan Abu-Amara, Ashraf S. H. Mahmoud, and Yahya Osais, “EDoS-ADS: An Enhanced Mitigation Technique Against Economic Denial of Sustainability EDoS Attacks”, *IEEE Transactions On Cloud Computing*, Feb. 2018.

[2] Bhaskar Prasad Rimal, Erunmi Choi, and Ian Lump, "A Taxonomy and Survey of Cloud Computing Systems," *IEEE Fith International Joint Conference on INC, IMS and IDC*, pp. 44-51, Aug. 2009.

[3] Haluk Demirkan and Dursun Delen, "Leveraging the capabilities of service-oriented decision support systems: Putting analytics and big data in cloud," *Elsevier Decision Support Systems*, vol.55, pp. 412–421, April 2013.

[4] Ivona Brandic, Vincent C. Emeakaroha, Michael Maurer, Schahram Dustdar, Sandor Acs, Attila Kertesz, and Gabor Kecskemeti, "LAYSI: A Layered Approach for SLA-Violation Propagation in Self-manageable Cloud Infrastructures", *34th Annual IEEE Computer Software and Applications Conference Workshops*, July 2010.

[5] Andrew Carlin, Mohammad Hammoudeh and Omar Aldabbas, "Defence for Distributed Denial of Service Attacks in Cloud Computing", *Elsevier The International Conference on Advanced Wireless, Information, and Communication Technologies*, vol. 73, pp. 490-497, 2015.

[6] Gaurav Somani, Manoj Singh Gaur, Dheeraj Sanghi, Mauro Conti and Rajkumar Buyya, "DDoS attacks in cloud computing: Issues, taxonomy, and future directions", *Elsevier Computer Communications*, vol. 107, pp. 30-48, 2017.

[7] Diego Perez-Botero, Jakub Szefer and Ruby B. Lee, "Characterizing Hypervisor Vulnerabilities in Cloud Computing Servers," *ACM Proceedings of the international workshop on Security in cloud computing*, pp.3-10, May 2013.

[8] Adrien Bonguet and, Martine Bellaiche, "A Survey of Denial-of-Service and Distributed Denial of Service Attacks and Defenses in Cloud Computing", *MDPI Future Internet*, Vol.9, Iss.43, 2017.

[9] Modi. C, Patel. D, Borisaniya. B, Patel. A and, Rajarajan. M, “A survey on security issues and solutions at different layers of Cloud computing”, *The Journal of Supercomputing*, 63(2), pp. 561-592, 2013.

[10] Uttam Kumar and Bhavesh N. Gohil, “A Survey on Intrusion Detection Systems for Cloud Computing Environment”, *International Journal of Computer Applications*, Vol. 109, No. 1, pp. 6-15, Jan. 2015.

[11] Tianwei Zhang and Ruby B. Lee, “ Host-based DoS Attacks and Defense in the Cloud”, *ACM HASP*, June (2017).

[12] Udhayan J, Anitha R and Hamsapriya T, "Lightweight C&C based botnet detection using Aho-Corasick NFA", *International Journal of Network Security & Its Applications (IJNSA)*, Vol.2, No.4, Oct 2010.

[13] Q. Jia , H. Wang , D. Fleck , F. Li , A. Stavrou , W. Powell , Catch me if you can: a cloud-enabled DDoS defense, *In: Dependable Systems and Networks (DSN), 2014 44th Annual IEEE/IFIP International Conference on, IEEE*, 2014, pp. 264–275 .

[14] Saurabh Kumar Garg, Srinivasa K. Gopalaiyengar, and Rajkumar Buyya, "SLA-Based Resource Provisioning for Heterogeneous Workloads in a Virtualized Cloud Datacenter", *ICA3PP, Part I, LNCS* 7016, pp. 371–384, 2011.

[15] Amid Khatibi Bardsiri, and Seyyed Mohsen Hashemi, "QoS Metrics for Cloud Computing Services Evaluation", *MECS International Journal of Intelligent Systems and Applications*, vol.6, no.12, pp.27-33, 2014.

DOI: 10.5373/JARDCS/V11/20192603
ISSN 1943-023X

Received: 19 July 2019/Accepted: 18 August 2019

[16] Marwan Darwish, Abdelkader Ouda and Luiz Fernando Capretz, "Cloud-based DDoS Attacks and Defenses", *IEEE International Conference on Information Society*, pp.67-71, 2013.

[17] Ishrat Ahmad and, Humayun Bakht, "Security Challenges from Abuse of Cloud Service Threat", *International Journal of Computing and Digital Systems,* Vol.8, No.1, Jan 2019.

[18] A. Sukhada Bhingarkar and, B. Deven Shah, "A Survey: Securing Cloud Infrastructure against EDoS Attack", *Int'l Conf. Grid & Cloud Computing and Applications,* pp 16-22, 2015.

[19] Mona Eisa, Muhammad Younas and, Kashinath Basu, "Analysis and Representation of QoS Attributes in Cloud Service Selection", *IEEE 32nd International Conference on Advanced Information Networking and Applications (AINA),* Aug 2018.

[20] J. Udhayan1, T. Hamsapriya, and, N.A. Vasanthi, "DDoS Attack Detection through Flow Analysis and Traffic Modeling", *SPIT* 2011, LNICST 62, pp. 89–94, 2012.

[21] Preeti Mishra, Emmanuel S. Pilli, Vijay Varadharajan and, Udaya Tupakula, "Intrusion detection techniques in cloud environment: A survey", *Elsevier Journal of Network and Computer Applications,* Vol. 77, pp.18–47, 2017.

[22] Muhammad Kazim and, Shao Ying Zhu, "A survey on top security threats in cloud computing", *International Journal of Advanced Computer Science and Applications*, Vol. 6, No. 3, 2015.

[23] Sukhpal Singh and, Inderveer Chana, "A Survey on Resource Scheduling in Cloud Computing:Issues and Challenges", *Springer Journal of Grid Computing* (2016) 14:217–264.

[24] S. Gokulakrishnan, J.M. Gnanasekar, "Peer-toPeer convoluted fault recognition to conquer Single-Point stoppage in Cloud systems*", International Journal of Pure and Applied Mathematics,* Vol.116 No. 21, pp. 559-577, 2017.

[25] Bin Wanga, Zhengwei Qi, Ruhui Maa, Haibing Guana and, Athanasios V. Vasilakos,"A survey on data center networking for cloud computing", *Elsevier Computer Networks*, Vol. 91, pp.528–547, 2015.

[26] Tianwei Zhang, Yinqian Zhang and, Ruby B. Lee, "DoS Attacks on Your Memory in the Cloud ", *Proceedings of the ACM on Asia Conference on Computer and Communications Security*, pp. 253-265, April 2017.

[27] Tariqul Islam, D. Manivannan and, Sherali Zeadally,"A Classification and Characterization of Security Threats in Cloud Computing", *International Journal on Next-Generation Computing,* 2016.

[28] Francesco Palmieri, Sergio Ricciardi, Ugo Fiore, Massimo Ficco and, Aniello Castiglion, "Energy-Oriented Denial of Service Attacks: an Emerging Menace for Large Cloud Infrastructures", *The Journal of Supercomputing Springer*, Vol. 71, Iss. 5, pp 1620–1641, May 2015.

[29] Issa M. Khalil 1, Abdallah Khreishah and, Muhammad Azeem, "Cloud Computing Security: A Survey", *Computers Journal*, Vol.3, pp. 1-35, 2014.

[30] Benny Rochwerger, Johan Tordsson, Carmelo Ragusa, David Breitgand, Stuart Clayman, Amir Epstein, David Hadas, Eliezer Levy, Irit Loy, Alessandro Maraschini, Philippe Massonet, Henar Mu˜noz, Kenneth Nagin, Giovanni Toffetti and, Massimo Villari, "RESERVOIR – When one cloud is not enough",

[31] Rashid Tahir, Muhammad Huzaifa, Anupam Das, Mohammad Ahmad, Carl Gunter, Fareed Zaffar, Matthew Caesar and, Nikita Borisov, "Mining on Someone Else's Dime:", Mitigating Covert Mining Operations in Clouds and Enterprises",

[32] Tanja Vos, Paolo Tonella, Joachim Wegener, Mark Harman, Wishnu Prasetya, Yarden Nir-Buchbinder and, Shmuel Ur, "Testing of Future Internet Applications Running in the Cloud",

[33] Ahmed Patel, Mona Taghavi, Kaveh Bakhtiyari and, Joaquim Celestino Júnior, "An Intrusion Detection And Prevention System In Cloud Computing: A Systematic Review",

DOI: 10.5373/JARDCS/V11/20192603
ISSN 1943-023X

Received: 19 July 2019/Accepted: 18 August 2019