International Journal of Computing and Digital Systems
ISSN (2210-142X)
Int. J. Com. Dig. Sys. 8, No.1 (Jan-2019)
http://dx.doi.org/10.12785/ijcds/080103

Security Challenges from Abuse of Cloud Service Threat

Ishrat Ahmad[1] and Humayun Bakht[1]

[1] *School of Management, Cardiff Metropolitan University, UK*

Received 19 Aug. 2018, Revised 7 Dec. 2018, Accepted 17 Dec. 2018, Published 1 Jan. 2019

Abstract: Cloud computing is an ever-growing technology that leverages dynamic and versatile provision of computational resources and services. In spite of countless benefits that cloud service has to offer, there is always a security concern for new threats and risks. The paper provides a useful introduction to the rising security issues of Abuse of cloud service threat, which has no standard security measures to mitigate its risks and vulnerabilities. The threat can result an unbearable system gridlock and can make cloud services unavailable or even complete shutdown. The study has identified the potential challenges, as BotNet, BotCloud, Shared Technology Vulnerability and Malicious Insiders, from Abuse of cloud service threat. It has further described the attacking methods, impacts and the reasons due to the identified challenges. The study has evaluated the current available solutions and proposed mitigating security controls for the security risks and challenges from Abuse of cloud services threat.

Keywords: abuse of cloud service, DDoS, botnet, botcloud, shared technology vulnerability, malicious insiders

1. INTRODUCTION

Cloud services allow access to unlimited free resources to any scale of organizations or individuals. The resources such as processor power, servers, memory, disk space or network bandwidth, can be rented at affordable cost instead of buying and maintaining them. Conversely, with just an anonymous registry any attacker can use array of cloud servers to crack an encryption key in minutes and can stage a DDoS attack (distributed denial-of- service), resulting an unbearable system gridlock, services slowdown and leaving cloud customers confused and frustrated [1]. In real cases, cloud service providers fail to provide security and privacy for customers' assets like the way they claim guarantee for protection. Typically, the regulatory bodies provide some quick evaluation on the identified threats and suggest to their audit solutions instead of proposing in-depth compilation of security risks and areas of concern [1].

According to Cloud Security Alliance [2-4], Abuse of cloud services has been identified as one of the top threats in cloud computing. Few other studies [3-14] have also identified the threat and its consequences. However, they have only conferred about the importance of implementing mitigation techniques for the identified threat, but no standard methods have been suggested.

Although, some research works [4, 15–18] have been done on particular context to formulate strategies for security challenges from the identified threat, but failed to provide a holistic overview of the issues and still need defined model of security controls accepted by both academia and IT industry.

This study has identified that there is lack of security standard defined for Abuse of cloud service threat. The threat, itself is specially related to the shared, on-demand nature of cloud computing and affects following security attributes as confidentiality, repudiation and availability. To the best knowledge of the researchers, no similar work existed by the time of publication.

The rest of the paper is organized as follow: section 2 discusses Abuse of cloud services threat and identifies its challenges. Section 3 discusses about the major challenges from the threat and their available solutions. Section 4 narrates overall evaluation and the direction of the study. Section 5 concludes the paper with future references.

2. ABUSE OF CLOUD SERVICE THREAT

The term "abuse of cloud services" refers to the fact of exploiting the cloud services to perform unethical or malicious activities by the cloud users in order to acquire benefits or financial gain. Cloud providers offer free unlimited trial period of cloud services with poor registration process and weak fraud detection capabilities. It helps a user with cloud computing model knowledge and a valid credit card to access cloud services in order to organize a cyber-crime [1]. It allows legitimate cloud

E-mail address: ahmad.ishrat611@yahoo.com, humayunbakht@yahoo.co.uk

customers to deploy, configure hosting environment and control their own applications on the cloud platform, which lead to create scope for the attackers to inject malicious codes.

Few studies [4, 19-22] have identified some experiments of how easy and inexpensive are to create malicious attacks by abusing cloud resources and services. Even some employees of service provider have the privilege of accessing customers' sensitive data and may be allured to abuse this privilege in an inappropriate way. A research study [17] has showed that 84% of cloud users still consider it as serious threat. The cloud service providers are incompetent in detecting attacks within their networks and hence no generation of alerts or termination of any account takes place [17].

Due to shared technology vulnerabilities, threats are hard to control for massive parallelism infrastructure. A virtualization hypervisors are not enough to address gap for strong compartmentalization multitenant architecture in cloud computing, hence exhibits flaws and risk of accessing compromising customers' sensitive data. Attackers can abuse this feature by renting VM to hack service engine through other customers' VMs in order to breach and compromise confidential data by breaking the isolation feature that separates customers' data. [23].

Typically, research community focuses more into technical aspects of cloud security, however, even traditional insider threat has been studied for decades, but cloud insider threat issues has not received much attention, and hence, some serious approaches are needed to overcome the impact of it. Critical cloud computing risks do not just hover around security and privacy aspects, but also affect legal, operational and business management area [24]. It seems that various managerial and organizational employee related problems, from both cloud providers and customers, may also trigger potential failure of cloud computing adoption.

Another major issue to consider is the Malicious Insider, who can have easy access to potential sensitive information and can involved into an organized crime. System administrators with high privilege roles can use their privileged access to multiple customers' data residing on same physical servers and that can be leaked or sold to other parties of interest.

From the discussion above, it is consequent that major challenges may occur from Abuse of cloud services threat are as DDoS, Botnet/BotCloud, Malicious insiders and Shared technology vulnerabilities.

Some of the typical major factors to invoke the attacking methods are listed as below:

- Free unlimited or trails periods of cloud services
- Weak user registration and verification process
- Free VOIP to activate account for SMS in registration process
- No credit card, SMS, email verification, CAPTCHA control
- Basic security controls
- Legitimate user deploy/control and hosting configuration of application on the cloud platform
- Resource sharing, Multitenancy
- Weak fraud detection process
- No internal alert or limit traffic generation
- Lack of standard hiring process
- Less visibility of employee's code of practices
- IT service under single management
- Roles & administration access control
- Lack of transparency of provider's policies and procedures

Fig 1 below shows the breakdown of Abuse of cloud services threat into major challenges as DDoS, BotNet/BotCloud, Malicious Insider and Shared Technology Vulnerabilities:

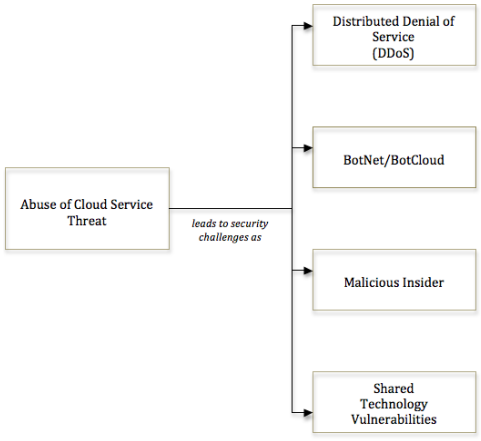

Figure 1. Major Challenges from Abuse of Cloud Service Threat

Fig 2 below shows some of the potential attacking methods that can be used to initiate the major challenges from Abuse of cloud service threat:

Security Challenges	Potential Attacking Methods
Distributed Denial of Service (DDoS)	Malicious coding; CAPTCHA control; spam; virus; password and key cracking; identity theft; hacking; phishing; organized crime; social engine attacks; shell coding; account / service hacking; malware attacks;
BotNet / BotCloud	Cryptocurrency; BitCoin mining; shell coding; malware attacks; account service hacking; spoofing; identity theft; host hopping attack; service engine attacks;
Malicious Insider	Organized crime; identity theft; account service hacking; espionage; eavesdropping; spoofing
Shared Technology Vulnerabilities	Cross site-scripting; tampering; shell coding; host hopping; service engine attacks;

Figure 2. Attacking Methods to initiate the threats

Fig 3 below lists the potential impacts as what can happen due to the identified challenges above:

<table>
<tr><th>Security Challenges</th><th colspan="5">Potential Impacts that might occur from the Security Challenges</th></tr>
<tr><td>Distributed Denial of Services (DDoS)</td><td rowspan="3">Service disruption / failures / unavailable; Traffic slowdown / gridlock; Business discontinuity; Consumption of bandwidth / processing power, storage, networks, memory; Billing customers;</td><td></td><td></td><td rowspan="3"></td><td rowspan="4">Data loss, theft, breaches, leakage, lock-in; Unauthorized access; Reputation & Brand image;</td></tr>
<tr><td>BotNet/BotCloud</td><td rowspan="3">Financial fraudulent & impact;</td><td rowspan="4">Compliance violations & Legal ramifications;</td></tr>
<tr><td>Malicious Insider</td><td rowspan="2">Privacy; Data scavenging;</td></tr>
<tr><td>Shared Technology Vulnerabilities</td><td colspan="2"></td></tr>
</table>

Figure 2. Potential Impact from the threat

A study [20] has identified a research experiment by Pedram Hayati (a security professional at BAE system), which was conducted to evaluate top five cloud providers' defense mechanism in preventing malicious usages of services. The research found out how cloud infrastructure can be misused for cyber-crimes to launch malicious attack, like a botCloud. A series of experiment was carried out for 21 days on undisclosed five top common cloud providers' infrastructure. Different types of malicious traffic were sent from remotely controlled cloud instances to some servers. First experiment was to investigate the cloud providers' security posture in the event of outbound malicious traffic originating from its network. The second was to investigate if the cloud providers can detect the traffic transmitted within internal network instances. The next was to investigate the security defense of malicious traffic coming from external network. The last one was to investigate if more time for execution of malicious activity of non-stop DDoS attacks for 48 hours along with generated volume of traffic would trigger the cloud service providers' attention. The results were found that the five top cloud service providers did not reset or terminate inbound or outbound network traffic connection. There was no awareness of internal malicious traffic, no limiting of any traffic, no generation of alerts or suspension of any accounts, as temporarily or permanently.

A similar kind of research [21] has been conducted by Rob Regan and Oscar Salazar (two security associates for Bishop Fox). The research was to show, how easy it is to create a legal botNet by using free available cloud resources. The research has developed a process to create distinct email accounts using free email services, which then automatically click the confirmation link to activate the account. They have managed to develop a platform to create 30,000 email addresses for a single person. A central system was used to launch and control malicious activities through virtual private network. The researchers did crypto-currency and Bitcoin mining using free computing power available from various service providers. The abuse was possible due to lack of users' verification during account creation process. Amongst 150 PaaS and IaaS service offerings, about 100 did not execute any SMS, credit card or CAPTCHAs verification. The researchers further disclosed the reason for their devious scheme is to raise awareness of problems in security measures for abusing of cloud resources. Regan further remarked that even for SMS verification, some online freely available VoIP could be used to activate new accounts, such as Google Voice or Phone Burner. The verification processes need to be addressed by service providers and also need to improve anti-automation techniques, as it is a vulnerability issue and charges bills to customers.

The threat Abuse of cloud services is severe and more alarming to the cloud service provider than cloud customers. A cloud service provider might harm their brand reputation and may result in blacklisting; therefore they must ensure all possible measures for preventing such threats [17]. While there are small numbers of defensive techniques exist for cloud customers' end, however, the customers should comprehend by the risk and related protection mechanism that to be followed when needed.

3. Major Challenges from Abuse of Cloud Service Threat and Available Solutions

The section discusses the major challenges that may arise due to Abuse of cloud services threat along with their available existing solutions:

A. BotNet / BotCloud Challenge

1) Introduction: A computer is told to be a bot when it is infected by some malicious software or malware, which then act like a zombie. Bot is the short form of robot. When a bot occurs, the computer performs automated tasks over the Internet without any acknowledgement. Typically, BotNet occurs when an attacker infects a large number of computers over a network, or to a group of cloud instances called BotCloud. The malicious activities can be done using commanded and controlled servers by an attacker through communication channels formed by network protocols like Internet Relay Chat Protocol (IRC), Hypertext Transfer Protocol (HTTP), File Transfer Protocol (FTP) or Simple Mail Transfer Protocol (SMTP), in order to compromise large number of hosts [4, 19]. Infection path can be achieved through browser exploits, network services exploits, P2P networks, OS exploits, client application vulnerabilities, e-mail attachments or unsolicited, download Internet files, etc. VM instances can also act as bots, by either getting infected from other customer's malware VMs, or due to deliberate installation of bot software by some malicious users [4]. The attacker would use these BotNets or BotCloud, typically, to send spam messages, spamdexing, spread viruses, worms, trojans, rootkit, spyware, backdoor, downloader, adware, ransomeware,

attack servers, mining bitcoins, DDoS attacks, access login details, cyber-attacks or other fraudulent activities [11].

2) Solutions: BotNet can be detected at ISP level with a heuristic signature based method as DNS and IDS; at LAN level with Honeypot, Cooke [25] and Riordan [26]; and at computer level with some hints, such as strange process names, browser behaviour, filenames, startup programmes, window services, slow network connections, anti-virus software disable, host file changes and unknown network connections [27].

In case of malware in masses or at IoT devices for Telnet services, IoTPOT and IoTBOX can be implemented [28]. IoTPOT emulates various devices (like CPU architectures) to analyze ongoing attacks in-depth with a frontend low-interaction responder cooperating with backend high-interactions virtual environments, called IoTBOX, which is a tailored version of IoT and sandbox that operates various virtual environments used by embedded systems for CPU architectures. They together control all network related options, like outbound traffic of C&C communications or DDoS attacks, and has the ability to learn unknown command interactions [28]

B. Denial of Service (DoS) Challenge

1) Introduction: A Denial of Service (DoS) attack is a cyber-attack in where the perpetrator makes unavailable of accessing information, data, network, storage or other services from its legitimate users by provisionally or indefinitely targeting a machine or network connections over the Internet [4, 17, 24]. Distributed Denial of Service (DDoS) is where, multiple numbers of machines or network resources are involved in sending a large number of requests for consuming cloud resources [4, 17].

Another form of DoS attack is Asymmetric application-level DoS attacks, which is capable of shutting down an application by using small attack payload as 100 bytes [23]. The DoS attacks are usually achieved by exploiting the vulnerabilities, like in web server or applications etc., and overloading the victim machine by sending many requests collectively in order to consume most cloud resources, such as network bandwidth, memory or computation powers, and therefore, causing in delay of cloud services or completely make unavailable of resources and services [4, 17].

DoS can be initiated by following steps as first to identify network topology by exploiting the multiplexing nature of a router to get a clear picture of the network, then to gain access of enough hosts and lastly to carry the attack [29]. An example of initiating DoS attack is like that cloud users request in XML and the request is sent to HTML protocol which in turn build system interface with REST protocol, this makes XML attack more vulnerable and attacks to REST are easy to implement [30]. The occurrence of the risks from DoS attacks usually lead to financial losses, reputation damage and business crisis. Typically, an organization needs to devote a huge amount of time and money in order to get back to normal business operations after any DoS attack.

2) Solutions: A study [4] has suggested that DoS attacks can be detected at the network level using sensors at the boundary as VLANs and has also identified the existence of different approaches for inbound detection from other researchers. The author has suggested VMI-based IDS technique as it can directly inspect any machine state and can detect malicious software running on the host. During unexpected increase of traffic, a port scanning can be performed to detect any DDoS attacks [31].

Port scanning might not be a straightforward process, as it includes monitoring of all machines, which can become legal issues as privacy invasion of customers' machines [19]. Port scanning is required to send a message in a network from a remote host, which can be used to check for vulnerable points in the network services during a potential attack. Although, inbound port scan detection techniques were proposed, but yet, research work is needed for outbound detection in cloud. An extrusion detection technique can be used at the domain of ISP for tracing outgoing spam.

The study [23] has introduced to some of researches for DDoS attacks detection as follow: A highly effective flooded DoS attacks detective Covariance-matrix method [32], application level detection with counter measure DoS attack was introduced [33] and Game Theory defense mechanisms to stop co-residence DoS attacks [34].

Another study [35] has overviewed with DDoS attacks, detection methods, source to trace back and details about organizing DDoS attacks. A study [30] has explained how XML and REST protocol are easy to attack and proposed a comber approach as filtering tree that has five filters to detect and resolve XML and HTTP DDoS attacks.

A hop-count method was found out in [36] that is used to prevent DDoS attack by determining the value from received IP packet. In their research they proposed approach for storing the hop-count values so to save searching time and filtering in preventing DDoS attacks.

A SOA Based Tracing Approach algorithm was used to reconstruct the path and trace back the source of DDoS and then filter by cloud. Generally, service providers cannot differentiate between good and bad traffic, even though, it is difficult to trace back the origin of an attack as the attacker uses spoofing IP address [37].

A DDoS defense mechanism was proposed by [38], that is capable of monitoring flows from two-way traffic and can detect and prevent DDoS attacks autonomously. However, a large number of network domains are required for implementing the mechanism.

A study [17] has suggested using hop-count filtering technique that helps to in reducing attacks by 90%. The other technique was involving IDS in VM, in where the targeted applications can be transferred to another VMs that is hosted on different server. However, no outbound traffic specifications have been provided by the study.

An Intrusion Prevention Systems (IPS) was suggested by [5] in identifying attacking point through pre-existing signatures, however, it is ineffective with legitimate content with bad intentions, even firewalls are ineffective as they can be easily bypassed. An avoidance strategy called Service Migration was proposed by [33], which has a monitoring agent and an application constantly probing each other to observe available bandwidth from both directions. If the application found the available bandwidth degrades below a certain threshold, it starts sending large number of UDP packets to the monitoring agent for help. Once the monitoring agent found bandwidth degradation or UDP packets, it migrates the application to different free subnet, or optionally hopping the application every few minutes. The approach requires re-programming DNS entry, which takes about few seconds to reassign an IP address.

DoS prevention strategy is however not enough to defend this attack completely, as the adversaries are usually anonymous and the key components are to be identified at first. The key is to identify the origin and generation of absurd and meaningless continuous nonstop traffic that vexed to flood the connection link. Hence tracing back to the malicious attacking point is necessary step to consider.

C. Shared Technology Vulnerability Challenge

Cloud computing services offer provision of resources at infrastructure, platform and software level. The basic design concept of cloud computing architecture is to separate the applications, operating system and hardware from each other. For instance, if an operating system fails, rather shutting down the whole system, the application can just be migrated into another server by using virtualization technology [1]. The virtualization technology is the key element of cloud computing. It has been broadly used to provide dynamic resource allocation and service provisioning, and with such technology, many operating systems can co-reside on the same physical machine without any confliction to one another. In general, the mechanism of virtualization, including multi tenancy, provides better server utilization and data center consolidation with ease and speed of provisioning, hence better capital expenditures on hardware and enhancement on operational productivity and efficiencies by organizations [39].

Traditional system security is often based on perimeter access control, however in cloud, security perimeters are not physical, but virtual. Cloud does not have underlying fixed infrastructure and allow customer's service infrastructure to run on cloud service provider's hardware along with other cloud users' software, hence posses security challenges. Although virtualization is a primary defense mechanism, but however, all resources are not virtualized and all virtualized environments are not bug free. Incorrect configurations of network virtualization might allow users access to sensitive areas of infrastructure or to other users' resources. There are some limitations of shared virtualization technology, such as, the transferring of virtual server from one physical machine to another is not possible unless the processors are from the same manufacturer; and another problem was the increased risk of voiding SLA that do not support VMs.

The much discussed and researched issues ever in cloud are multi-tenancy and resource sharing and virtualizations. However, the issues remain underserved regardless of number of various approaches provided to identify the concerns. The issues from multi-tenancy and virtualization problems can create much exaggeration and impact on the whole cloud environment. As a virtual environment is more complex than traditional physical environment, hence it requires new approaches and more sophisticated, efficient and generic secured techniques in mitigating any potential attacks.

1) Virtualization:

a) Introduction: The term virtualization is the creation of a virtual form of a resource such as operating system, storage device, CPU, memory, application or network resources. It is a technique that allows user to create, copy, share, migrate and roll back virtual machines [39]. The virtualization technique isolates lower level functionalities, i.e. to hide physical characteristics of a platform, and facilitate portability of higher-level functions and does sharing and aggregation of physical resources with a dedicated resource view for users' platform [39]. It is the process of partitioning a physical server into multiple virtual servers. In virtualization, the host machine is the actual physical machine, on which virtualization is implemented to create the guests or Virtual Machines (VMs). The term Virtual Machine is basically a physical hardware abstraction.

Due to co-residencies, the VM technique has the potential to facilitate adversaries to execute cross-VM attacks and timing attacks [29]. A case study conducted by UCSD and MIT on Amazon's EC2 VM instances and has found four weaknesses, which can be used to stage and execute side-channel attacks [40]. The results were as that it is possible to determine physical infrastructure where a VM instance resides; and whether two VM instances resides on the same physical server; to create VM instances on the same physical server of the targeted VM instances; to exploit or leakage information from one VM instance to the other that resides on the same physical server [40]. Similar kind of security risks and concerns has been classified by CSA as follows: At architectural level, VMs connected to a network can be a target by other VMs on the same network; Any security vulnerability

in the hypervisor or management software enables VMs at risk; A new infrastructure can be deployed easily by cloning and copying images in a virtual environment, which establishes configuration drift and potential challenges for controlling and accounting rapid growth of new virtual environments.

b) Solution: An Advanced Cloud Protection System (ACPS) was proposed in [41] to protect and monitor the integrity of guest VMs and cloud infrastructure components. The system can block suspicious activity and notifies the security system.

2) Virtual Machine Monitor or Hypervisors:

a) Introduction: Virtual Machine Monitor or Hypervisor is an abstraction low-level software or firmware or small application that sits between VMs and physical machine hardware, and runs on top of this hardware layer. It implements, control, monitor and isolates vCPU, vMemory, events channels, I/O controls and memory access and shared on the host hardware [23, 39]. Hypervisors allows multiple VMs to run on a single machine. If hypervisors is compromised, then VMs are likely to get infected and can bring whole cloud down [11, 23, 42].

b) Solution: A study [23] showed an attack as Hyperjacking, in where, an attacker creates and runs a thin hypervisors to take control over underlying operating system that would lead to have access and manipulate cloud users' data, allows eavesdropping or disrupt cloud services. The study also found the mechanism for reducing hypervisors attacks by enabling guest VMs to run in native mode with minimal computational components, or by employing a hierarchical secure virtualization model, which will quarantine threat and take control on virtualization [23]. The migration of VM, for example during fault tolerance, load balancing or maintenance, exposes the content to the network leading to compromise security attributes as data integrity and confidentiality. During VM rollback, it is necessary to take image copy, for just in case, to avoid re-enable disabled accounts or passwords. Even when VMs are offline, it can be instantiated using an image that has a malicious code and can be used as proliferation of malware attack by infecting other VMs [42].

VMMs are not secured enough and have bugs that allow guest users to exploit by malicious code and bypass certain security restrictions or gain system privileges. As an example, Microsoft Virtual PC and Virtual Server allow privilege to guest operating system user so to run code on the host or in another guest operating system. VMM can be made as 'root secure' so that no privilege is accessed within the virtualized guest environment and hence no interference with the host system. Besides, VMMs isolation, inspection and interposition properties needed to be achieved. Subahini and Kavitha (2011)

A study [44] has proposed TinyChecker, a system to protect VMs against hypervisors by using nested virtualization methods. The system uses context based and on-demand checking to identify and rectify any failure. However, it does generate small performances overhead. A study [17] has suggested in implementing proper isolation among VMs in order to prevent leakage. The authors have suggested of having proper access controls and risks assessments so to avoid unauthorized access to sensitive business data.

A study [45] has demonstrated how a security assessment as Cloud-Trust can measure the security status of IaaS cloud computing systems and service providers' offerings, and be used to estimate probabilities of threats intrusion and detection. These measure the value of specific cloud system security controls, which includes optional security features offered by leading commercial cloud service providers.

Systems must include monitoring mechanism in order to ensure performance ability and that the security level is being maintained according to business requirements. Like traditional system infrastructure, the ability to monitor security of cloud domains and to identify and inspect the causes and responsibilities behind security infringements are absolutely necessary.

3) Intrusion Detection Systems (IDS):

a) Introduction: Intrusion Detection Systems (IDS) is a hardware or software device installed on the network or host to monitor and report of any suspected infringement within the network system. It is used in combination with existing security devices so to enhance the capabilities of network security and verify network requests before accessing to cloud servers. It must be implemented at inbound and outbound boundaries to observe and track abnormal activities, which are often overlooked by firewalls, and send alerts to system administrator. IDS management system can monitor Virtual Machine status and workload, and can be started, stopped or recovered at any time [40].

b) Solution: A Virtual Intrusion Detection System (V-IDS) in [46] was proposed, which is a software or hardware based that monitor network and host activity to report, analyze and provides automatic alarm to management. The author proposed two methods for analysis: Attack Signature by static packet filtering like firewall rationale and Anomaly Detection by Heuristics approach.

A study of anomalies detection system as Unsupervised Behavior Learning (UBL) has been proposed to predict unknown performance anomalies for IaaS layer [47]. The UBL prototype is a host-based IDS, leverages Self-Organizing Maps and has been built on Xen platform, to capture dynamic system behaviors and achieves scalable learning approach by virtualization and distributing the learning tasks amongst other

hosts. The results claimed by the authors in [47] from the prototype were high prediction accuracy and raising alarms up to 47 seconds prior to attacks. However, UBL is as not effective in detecting distributed anomalies behaviors, like DDoS attacks, due to less monitoring capabilities. Instead a signature-based approach implemented at the source host and allows detection of large-scale distributed DDoS attacks. The authors [20] suggested in combining the evidences of suspicious networks or host activity from multiple distributed hosts and networks and collaborative IDS as solutions.

Another study [48] proposed collaborative IDS that use IPSs to design overlay protective networks ring around customers' applications. However, it forms unpreventable side-effects damage. A detection mechanism against malicious activity was proposed in [20] that will avoid side effect damages through source-based detection and considerations of system metrics and scalability support by autonomous collaborative distributed detection system.

A study [5] has proposed three secured ways to cloud environment as follow: First is to secure transmission with tunneling and by using of virtual circuits. Second is to secure the servers by placing IDS, separating servers for different applications, storing hashed values, data replication and threshold for server load. Third is to secure the client side by using digital signatures for authentications, one time password, authentication for every write, distributed storage, local servers for avoid network congestion and temporary storing on local disk for single session.

4) Side Channel Attacks:

a) Introduction: Side channel attacks are conducted by gaining access to the physical node where the targeted virtual machine is hosted. The technique can be achieved by creating enough virtual machines until one is created on the physical machine of the victim's VM. Later, the attacker collects necessary information to execute the attack by exploiting shared CPU and memory caches, or by examining control signals and traffic patterns to infer sensitive information from the victim virtual machine [23]. A potential attacker can analyse the physical characteristics of cryptosystem implementation through conducting side channel attack in order to collect information as timing, power consumption, electromagnetic leaks and so on and can exploit the system [23].

b) Solution: The author has identified a number of researches on side channel attack and has discussed the available mitigation techniques briefly, such as for L2 convert channels, cache memory, AES encryption, dynamic cache coloring etc. [23].

The study in [29] has discussed vulnerabilities that may be exploited by attackers and have drawn threat models with defense strategies through attribute-driven methodology. The defense strategies proposed have some deficiencies, which are discussed as follows. For Cross-VM attack via side channels, the defense strategy proposed was placement prevention, co-residency detection and NoHype. However, placement prevention does not stop brute-force strategy (simply launches instances and checks co-residence by the target). Co-residency detection strategy was only on L2 cache side-channel; other side channels can also get exploited. NoHype was proposed, but existing hardware inflicts restrictions to implement it, plus, live VM migration is not convenient with this new method. By rule, an isolated virtual machine should not have access by other resources, however, attacks on hypervisor can take control to access virtual machines instances or host server, such as Virtual machine-based rootkits.

5) Multi-tenancy:

a) Introduction: The term multi-tenancy refers to sharing of resources by utilizing virtualization technology, in where any resource object is reusable. A typical example of multi-tenancy is when two or more VMs of different customers share the same physical machine by resource allocation policy [29]. While it is an opportunity benefit and economic efficiency for cloud service providers, but security experts define it as exposure of security risks and threats and provides vulnerabilities to the cloud [29]. A potential attacker, who could be a legitimate user, can take advantage of co-residencies to stage an attack. A potential attacker can hire a storage space and scan the resource for any sensitive data of previous customers. Security attributes as confidentiality can be compromised when resource objects are reused.

A study in [22] has identified threat as Host Hopping Attack, which exploits resource sharing characteristics of cloud computing. Due to lack of secured isolation mechanism of resources, malicious attackers can hop from one host to another causing severe damage like distorting image and reputation, gaining illegal access to sensitive information or interrupting services. Furthermore, the study showed that service engines are IaaS platform, used to manage customers' resources, often rented by customers as well. Attackers can abuse this feature by renting VM to hack service engine through other customers' VMs in order to breach and compromise confidential data by breaking the isolation feature that separates customers' data.

b) Solution: The authors narrated that cyber criminals are exploiting and misusing cloud computing services due to weak registration process and lack of security controls, and pointed out that extensive research is required to identify the risks and impact of the such threat as abusing of cloud services [22].

An attack model was reconstructed in a study by [31]. The study proposed the resource allocation mechanism, which will minimize the surface layer attack. However, the model was constructed not fully but partially, and needed evaluation empirically.

6) Outsourcing:

a) Introduction: Three categories of public cloud exist according to NIST: 1) Services are provided at no cost; supported by advertisements; limited to personal but non-commercial use; collected information from registration and the use of the service produces digital marketing for advertisements to customers; no encrypted protection features; search engine and e-mail services. 2) Services are fee-based; terms of service delivery are non-negotiable but modifiable at any discretion; free of advertisements; protection mechanisms are configurable to some extent. 3) Services are fee-based; terms of service delivery are negotiable; services can be tailored and costs depend on it. Eventually, the organizations are responsible for security and privacy of the outsourced services by choosing the public cloud. While organization can choose to have an exclusive private cloud deployment, yet outsourcing applications or data to another organization are done through a public cloud, and then again, the concern of security and privacy implications always exists.

b) Solution: During outsourcing, the organizations physically lose control over their applications or data, hence to address the security concerns for outsourcing, the service providers must assure customers secured computing and data storage [29]. The main concerns from outsourcing organizational resources are the continuity, security and privacy of the services. In terms of services continuity, there could be downtime Internet or network access that may lead to unavailability of services.

An approach that can be considered is to take services from a certified cloud service provider with the appropriate rating for the level of controls and security required by organizational prospective.

7) Application Programming Interfaces (APIs):

a) Introduction: Application Programming Interfaces or API is an enabler for service delivery model. It is a set of protocols and standard to enable the programmatic controls for the development of applications and serves as an interface that provides self-provisioning of cloud hardware, software and platforms to cloud users and helps with load balancing among application servers. It is a gateway for communication between cloud services layers to other services [17, 39]. Based on cloud service models requirement, APIs can enable control from simple URL manipulations to complex SOA programming and helps to hide complex IT management processes and practices to user services [39]. Infrastructure as a Service API offers to access, create and manage cloud resources like storage, compute, network, VMs etc. Platform as a Service API offers access to cloud storage and to deploy and manage software modules. Software as a Service API offers basic connection of applications to cloud infrastructure like export and import browsing functionalities using HTTPs and URI methods. [17, 39].

A study [39] notified that security flaws on APIs and interfaces could lead many security challenges and tend to compromise security attributes as data integrity, confidentiality and availability. Cloud vendors offer APIs to third party for services to customers; therefore, any leak to the APIs can result to have access to sensitive information or security keys by third party [17].

Each cloud service provider has a unique API, which is why it is difficult to obtain interoperability amongst applications from different cloud vendors [39]. The security challenge as vendor lock-in or data lock-in creates wide range of potential risks and constraints, from customer reliability issues to service providers business continuity. Customers cannot easily extract their business data or applications, while being getting frustrated and vulnerable in price increases. On the other hand, service provider goes out of business, loss cost control and flexibility in system configuration [39].

b) Solution: A study by [46] provides a schematic novel architecture of cloud middleware API, which organizes local management system of each domain while maintaining a secure API that helps to exchange information through modifying each VM status for secured information.

Cloud service providers can enhance their service offerings by standardizing and providing compatible APIs, data format and low cost data conversion during cloud implementation process, which in turn will provide support during service failovers and migration of data and systems when switching multiple cloud vendors platforms for backups [11].

A study by [49] showed some name of organizations who are working for standardization and interoperability in cloud systems, as follow: Open Grid Forum (OPF) is for discussing cloud computing related standards; Internet Engineering Task Force (IETF) promotes the standardization and best practice of distributed computing related techniques; Open Cloud Standards Incubator aims to clarify the interoperability between several cloud systems; Open Cloud Computing Interface Working Group (CCI-WG) designs resource management API for IaaS; others like Storage Network Industry Association (SNIA), Cloud Security Alliance (CSA) and Open Cloud Consortium (OCC) has started working on cloud storage, security and intercommunication standards respectively.

The research [50] has suggested an ontology-based approach to implement an automatic determination and solutions for interoperability issues amongst different cloud vendors. They further believed that an ontology-based approach could be helpful in terms of security and sensitivity of data and storage in cloud services [50]. However, the ontology provided in the study was a simple preview of cloud computing offerings and needed extensive in-depth research on interoperability of each layer cloud service and deployment

models, and while covering legal issues simultaneously between cloud vendors.

A universal cloud APIs need to be developed that will aim to construct an open and standardized interfaces that could integrate cloud-based applications, mobile apps and wearable apps together in order to share assets with other apps and systems. The target can be obtained, by considering a singular common programmatic point of contact, which can cover the whole cloud infrastructure stack and emerging cloud technologies. The value of APIs integration applications is gaining importance because the focus of the trend is on the cloud, mobile and IoT as means for business development and digital transformation.

D. Malicious Insiders Challenge

1) Introduction: Malicious insider is the potential for an individual, from current or ex-employee, supplier, vendors, clients, contractor or other business partner, who has or had authorised access to organisational information processing facilities, like system, network or data and attempt to abuse the privileges by damaging employer's assets, reputation or by leaking sensitive information for financial gain or revenge [51]. Or sometimes, they may create some unintentional attack through email services or social engineering due to lack of proper user guidance and training.

Typically, the malicious insiders access the system to look for vulnerable or susceptible points, in order to launch program to infect system (example, by creating botNet for command and control), from on-premises or remote location, and perform disreputable and malicious activities. They can install viruses, steal credential, data, currency, or do data manipulations and much more.

Malicious insiders have been considered as one of the cloud security challenges that can happen to any organization, whereas, security related incidents reported have been due to exploits originating from inside the organizations. For various reasons employees get engage into malicious acts such as workplace conflicts, job termination, dissatisfaction, private life issues, destitution, personal business advantage or financial gain [15]. Trusted insiders have credentials to access organizational information processing units and are usually hard to be identified and monitored because they are already inside the organization, system or network and are not breaking any defense system, unlike outside hackers. Even, system administrators or information security managers with high privilege roles can use their privileged access to multiple customers' data residing on same physical servers and that can be leaked or sold to other parties of interest. Unfortunately, cloud providers hides such issues due to reputation and customer trust concerns [22]. Malicious attackers exploit unlimited resources and set up rogue clouds to attract individuals to host their business data and applications, causing their identity at risk and lead to financial fraud [22]. Limiting access control to system users can be a mitigating approach, but then again, it also hamper the tasks that privileged system users have to maintain in terms of business productivity. Cloud system administrators have responsibilities for managing, governing and maintaining complete cloud environment [17].

Although cloud customers has most access to the infrastructure at IaaS, yet, it is totally undetectable by the customer whether there was any unauthorized access by a malicious administrator, who has usually access to the physical infrastructure which is not controlled by the customer.

2) Solution: The researchers from [52] have studied some others' techniques in light with encryption keys, but they opinioned that the techniques have high performance overhead and impractical to use.

Two studies [23, 53] have discussed not to introduce the associated keys to the cloud system but to keep it with the customer, which could be a potential way to defend the attack. Another study [14] has proposed security tools to use, such as, data loss prevention system, anomalous behavior pattern detection, format preserving and encryption, authentication and authorization technologies.

The study [23] further discussed that decryption key has to be saved somewhere in the cloud, which could be easily manageable to retrieve by administrator who has access to physical memory used by the customer's virtual systems to store encrypted keys.

A study by [15] has proposed some suggestions as to strengthen the registration process with effective security techniques and to control unauthorized and illegal access of confidential data on cloud platform.

Traditional security controls on cloud insider threats are not adequate for cloud infrastructure and need much attention and researched upon. The impact of such attack is massive and can affect every infrastructure in cloud business. Technical solutions are there to defend and minimize the impact from the threat. However, some other issues related to insider threats as physical monitoring, screening policies during recruitment, complying with business rules and guidelines and all other business factors are as equally important as technical security controls.

During recruitment of an employee, it is advisable to both cloud service providers and customers to have a strict screening policy for employees, not only educational and professional background to check, but also character references and criminal activities records must need to be considered with relevant regulations and business requirements during recruitment process. A background investigation may find whether the potential employee has been fired from prior job, credit check, shows medical history, school dropout and like.

4. DISCUSSION & EVALUATION

From the study, it was found out that there is a reasonable level of awareness exists in considering the amount of attention required for cloud security. Both cloud service providers and consumers should be aware of

security issues associated with cloud computing. It is also logical, because most prominent cloud security related incidents reported have been due to lack of concern about technical infrastructure and management guidance maintenances. In order to avoid major challenges like BotNet, Bot Cloud or Shared Technology Vulnerability to occur, some important steps need to be ensured through information processing facilities and managerial components.

Information security controls must be addressed during organisational project development phase. It must ensure to check with departmental representatives for a new or any update of information security controls in requirement analysis and specification. Moreover, special security professionals, regulatory bodies and law enforcement authorities should be included, who can advise for much effective control practices during implementation of information security controls for a project. Besides, it is also important for managers to give review of information processing and procedures to employees of respective departments regularly. Such practices help the employees to get updated with their information system processing and can compliance with appropriate security policies, standards and business requirements.

Regarding operational procedures and responsibilities, any new information systems, upgrades and new versions should be validated through acceptance testing, which are based on related criteria in order to avoid any shared technology potholes or vulnerabilities. A cloud service provider must be aware of the fact that different types of malicious attacks can be sent from remotely controlled cloud instances to some servers for cyber crimes. It is absolutely crucial and necessary to have a proper mechanism for system administration and communication security in the organisation. Both cloud service providers and consumers must have knowledge about unsafe email or link and should be aware of its consequences. Typically, an email system is decentralized and very inexpensive to create spam, which is why it can be sent to everybody at anywhere, consuming users' bandwidth, steeling personal information and such alike may lead serious consequences to the users. Unwanted emails can be avoided by getting right software or anti-spam filters.

The cloud vendors could also enhance their service offerings by doing regular monitoring and maintaining up-to-date applications and technical infrastructure to run the information processing facilities seamlessly and competently. It is very fundamental and crucial to maintain antivirus software controls to opt out from malicious attacks. The antivirus software should also be regularly checked and updated with new versions on the systems.

Resources allocation and management should be considered as a very major control measure in order to avoid shared technology vulnerabilities issues. Besides, defining principles for resource allocation and management, organisations should also have mechanisms to evaluate, direct and monitor the allocation and management of software and hardware resources for outsourcing. During resources allocation for outsourcing, a review and approve mechanism should be in existence in order to mitigate risk occurrences. If any resource management abnormalities or problems get noticed, appropriate actions should be performed instantaneously.

To identify any risks associated with architecture is very crucial and a process should exist to identify and report for an action during taking place. In terms of data lock-in or for backups, cloud service providers may also consider in using standardized APIs and boost their service offerings. During adverse circumstances, such compatible APIs amongst service providers will help to migrate customers' data inexpensively and hence making services even more reliable and trustworthy.

Cloud security related incidents reported have been due to exploits originating from inside the organizations. Malicious insiders have been considered as one of the cloud security challenges that can happen to any organisation and need to be aware of certainly. Management should always observe regularly whether the employees are complying with the agreement policies and maintaining the code of conduct.

An organization must define job roles and responsibilities based on the hierarchy of the management level. It is necessary of maintaining rigorous screening policies for a potential employee in accordance with relevant regulations and business requirements during the recruitment process, which will help to identify any background testimony of criminal records. Besides checking educational and professional background, other character references or criminal activities background must be checked during recruitment process.

Both managers and employees are responsible to protect and maintain necessary security controls. Managers must ensure contract covers all compliances with agency information security policies. They must also make sure that employees fully understand policies and receive proper training and information security support access. On the other hand, employees must comply with the policies and accomplish necessary technical adeptness to carry out the required security controls. Sometimes employees do not follow the process, intentionally or unlikely, and they just leave unattended storage media or confidential papers on desk, which is a risk issue to sensitive information. Organisation must have assets handling policies according to business requirements. Any removal media as disks, documents, and software and like should be protected from unauthorised access or corruption. Unwanted media should be destroyed physically or overwritten securely in order to reduce

security breach incidents. It is also necessary for an organisation to have restricted process to access program source code. Organisations must produce restriction process for installation of software on operational system by unauthorised users. There should be restrictions or limitations to any modifications or alterations of software packages, even by authorised users.

The cloud service providers should maintain a practice of getting feedback from customers. They should enhance their service facilities by understanding customers' needs and respond to any discrepancies without any delay.

Typically, most of the organisations have a strategic planning to determine the requirements for business continuity, disaster recovery and risk assessment during an adverse situation. It is important for all organisations, especially executive level of management, to understand the security incidents that can take place and how business continuity, disaster recovery and risk assessment process can actually help to recover from any adverse circumstances. A business continuity, disaster recovery and risk assessment system can help to identify security incidents, to analyse the impact of the incidents, to generate alarm or to notify the concern person, to update security controls at regular intervals for future references and many more.

Organisations should establish a management channel process to report any observed or suspected security weakness in information system and services. The reporting system should also help to record any adverse incidents like user activity, system admin login, malicious activities, faults, corrections and so on. The system must respond quickly to changing risk and report immediately to concern person by defining what, when, where and how any observation is taking place.

Auditing security controls has a big part to play for verification of operational systems, which should be properly planned and reviewed regularly to minimise business process disruption. An organisation should maintain auditing security controls at regular interval in order to avoid any business disruptions. A process to develop mitigation strategy for each identified risk should exist within the organisation for future references.

It is necessary for both cloud service providers and potential users to carefully consider and evaluate the security posture and all the possible business risks from both sides before actually set off for the mutual agreement. Cloud security posture is feasible only if the appropriate defensive measures are in places. If it is properly planned and deployed, the cloud will bring positive functionalities and economic benefits. The cloud security system must be able to identify any incident or risk that may appear abruptly and take instant initiative to address it. The security measures are suppose to be in place in order to defense any vulnerabilities in the system and hence decreasing the consequences of any attack.

The potential next step is to implement a Detection and Prevention framework with security measures for mitigating and overcoming the security risks and challenges from the threat. The framework must define major security control processes across areas of business strategic plans, network, shared technology and human resources in cloud computing. The control processes must cover security measures for strategic planning for business continuity, disaster recovery and risk assessment. The control processes must also cover registration, resource allocation, asset and employment inventory system, management and universal cloud APIs process. The framework can be embedded into general auditing process of business and organizations for security purposes. The framework must be presented in generic approach so that both technical and non-technical audiences can take advantage of the benefits. The framework should provide recommendation to business policy-makers, cloud service providers, customers and end-users on how to deal with this serious Abuse of cloud services threat.

5. CONCLUSION

Cloud security mitigation techniques has not reached the level of transparency and hence, the journey of understanding and accepting cloud computing services still remains uncharted for many organizations or individuals. While mitigation techniques for different security issues are actively being researched, however, the study shows that there is still insignificancy in research on Abuse of Cloud Services threat, in particular. The study has provided a constructive introduction to the rising security issues of Abuse of Cloud Services threat along with the potential challenges and risks in a holistic way and has established awareness of BotNet, DDoS, Shared Technology Vulnerabilities and Malicious Insider challenges.

For future reference, a generic detection and prevention framework will be developed with some relevant security measures for each identified challenge discussed in this study. The proposed framework of individual security measures will be global standard and generalized in terms of every layer of cloud service and deployment models. Furthermore, the proposed framework will add to the literature of risks and areas of concern related to Abuse of cloud services threat in cloud computing environment.

REFERENCES

[1] Ahmad, H. Bakht, and U. Mohan, "Cloud Computing – Threats and Challenges," *J. Comput. Manag. Stud.*, vol. 1, no. 1, 2017

[2] CSA, "Cloud Security Allainace - The Notorious Nine," *Infoworld*, 2013.

[3] B. S. Al-Attab and H. S. Fadewar, "Security Issues and Challenges in Cloud Computing," *Int. J. Emerg. Sci. Eng.*, vol. 2, no. 7, pp. 22–26, 2014.

[4] J. Lindemann, "Towards abuse detection and prevention in IaaS cloud computing," *Proc. - 10th Int. Conf. Availability, Reliab. Secur. ARES 2015*, pp. 211–217, 2015

[5] A. Aich and A. Sen, "Study on Cloud Security Risk and Remedy," *Int. J. Grid Distrib. Comput.*, vol. 8, no. 2, pp. 155–166, 2015.

[6] M. A. Hossain and S. Taslima, "A Study on Threatened Risks for Cloud Computing Security- How to Overcome These Risks," *Int. J. Adv. Res. Comput. Sci. Softw. Eng.*, 2016.

[7] M. M. Rahaman, M. S. Bin Alam, S. Islam, and T. Rahman, "An Effective Cloud Computing With its Security in the Cloud: A Smart Survey," *Int. J. Eng. Sci. Comput.*, vol. 6, no. 6, 2016.

[8] J. Singh, "Cyber-Attacks in Cloud Computing: A Case Study," *Int. J. Electron. Inf. Eng.*, vol. 1, no. 2, pp. 78–87, 2014.

[9] S. Kaur and S. Khurmi, "A Review on Security Issues in Cloud Computing," *IJCST Int. J. Comput. Sci. Technol.*, vol. 7, no. 1, 2016.

[10] V. Ashktorab and S. R. Taghizadeh, "Security Threats and Countermeasure in Cloud Computing," *Int. J. Appl. or Innov. Eng. Manag.*, vol. 1, no. 2, pp. 234–245, 2012.

[11] T. Kajiyama, "Cloud computing security : how risks and threats are affecting cloud adoption decisions," San Diego State University, 2013.

[12] S. Mewada, U. Singh and P. Sharma, "Security Enhancement in Cloud Computing." *Int J Sci Res Comput Sci Eng* 1:31–37, 2013.

[13] K. Lee, "Security Threats in Cloud Computing Environments." *Int J Secur Its Appl* 6:25–32, 2012

[14] T.-S. Chou, "Security Threats on Cloud Computing Vulnerabilities," *Int. J. Comput. Sci. Inf. Technol.*, vol. 5, no. 3, pp. 79–88, 2013.

[15] M. Omar, "IntroductiInsider threats: Detecting and controlling malicious insiderson and Background," *Researchgate*, 2015.

[16] A. Shahzad and A. Litchfield, "Virtualization Technology: Cross-VM Cache Side Channel Attacks make it Vulnerable." *Australas Conf Inf Syst*, 2015

[17] M. Kazim and S. Y. Zhu, "A survey on top security threats in cloud computing," *Int. J. Adv. Comput. Sci. Appl.*, vol. 6, no. 3, pp. 109–113, 2015.

[18] J. Szefer and R. B. Lee, "BitDeposit : Deterring Attacks and Abuses of Cloud Computing Services Through Economic Measures," *IEEE*, no. May, 2013.

[19] K. Clark, M. Warnier, and F. M. T. Brazier, "BOTCLOUDS The Future of Cloud-based Botnets?," *NLnet Foundation*, 2011.

[20] H. Badis, G. Doyen, and R. Khatoun, "A Collaborative Approach for a Source based Detection of Botclouds," 2014.

[21] M. Anderson, "Black Hat 2014: How to Hack the Cloud to Mine Crypto Currency." *IEEE Spectre*, 2014

[22] Y. A. Hamza and M. D. Omar, "Cloud Computing Security: Abuse and Nefarious Use of Cloud Computing," *Int. J. Comput. Eng. Res.*, vol. 3, no. 6, pp. 22–27, 2013.

[23] M. M. Alani, "Securing the Cloud: Threats, Attacks and Mitigation Techniques," *J. Adv. Comput. Sci. Technol.*, vol. 3, no. 2, pp. 202–213, 2014.

[24] A. Dutta, G. C. A. Peng, and A. Choudhary, "Risks in Enterprise Cloud Computing: The Perspective of IT Experts," *J. Comput. Inf. Syst.*, 2013.

[25] E. Cooke, F. Jahanian, and D. Mcpherson, "The Zombie Roundup: Understanding, Detecting, and Disrupting Botnets," 2005.

[26] J. Riordan, D. Zamboni, and Y. Duponchel, "Billy Goat, an Accurate Worm-Detection System," 2005

[27] D. Barroso, *Botnets - The Silent Threat*, vol. 15, no. 3. 2007.

[28] Y. Pa, S. Suzuki, K. Yoshioka, T. Matsumoto, T. Kasama and C. Rossow, "IoTPOT: Analysing the Rise of IoT Compromises.", *In: WOOT'15 Proceedings of the 9th USENIX Conference on Offensive Technologies*, 2015

[29] Z. Xiao and Y. Xiao, "Security and Privacy in Cloud Computing," *IEEE Commun. Surv. Tutorials*, vol. 15, no. 2, pp. 843–859, Jan. 2012.

[30] T. Karnwal, S. Thandapanii, and A. Gnanasekaran, "A Filter Tree Approach to Protect Cloud Computing against XML DDoS and HTTP DDoS Attack," Springer, Berlin, Heidelberg, 2013, pp. 459–469.

[31] H. Aljahdali, A. Albatli, P. Garraghan, P. Townend, L. Lau, and J. Xu, "Multi-Tenancy in Cloud Computing," in *IEEE 8th International Symposium on Service Oriented System Engineering (SOSE)*, 2014, pp. 344–351.

[32] M. Ismail, A. Aborujilah, S. Musa and A. Shahzad A, "Detecting flooding based DoS attack in cloud computing environment using covariance matrix approach." *In: Proceedings of the 7th International Conference on Ubiquitous Information Management and Communication - ICUIMC '13. ACM Press, New York, New York, USA, pp 1–6*, 2013

[33] H. Liu, "A new form of DoS Attack in a Cloud and its Avoidance Mechanism." *ACM Computer Network*, 2010

[34] H. Bedi and S. Shiva, "Securing Cloud Infrastructure Against Co-Resident DoS Attacks Using Game Theoretic Defense Mechanisms." *ICACCI*, 2012

[35] S. Yu, *Distributed Denial of Service Attack and Defence*. 2013.

[36] V. Chouhan and S. Peddoju, "Hierarchical Storage Technique for Maintaining Hop-Count to Prevent DDoS Attack in Cloud Computing." *In: Proceedings of International Conference on Advances in Computing*. Springer, New Delhi, pp 511–518, 2013

[37] L. Yang, T. Zhang, J. Song, J. Wang and P. Chen, "Defense of DDoS attack for cloud computing.", *In: 2012 IEEE International Conference on Computer Science and Automation Engineering (CSAE)*. IEEE, pp 626–629, 2012

[38] J. Mirkovic and P. Reiher, "D-WARD: A Source-End Defense Against Flooding Denial-of-Service Attacks.", *IEEE Trans Dependable Security Computing* 2:216–232, 2005

[39] T. Mather, S. Kumaraswamy, and S. Latif, *Cloud Security and Privacy An Enterprise Perspective on Risks and Complaince*. O'Reilly, 2009.

[40] N. Gonzalez, C. Miers, F. Redígolo, M. Simplício, T. Carvalho, M. Näslund, and M. Pourzandi, "A quantitative analysis of current security concerns and solutions for cloud computing," *J. Cloud Comput. Adv. Syst. Appl.*, vol. 1, no. 1, p. 11, 2012.

[41] F. Lombardi and R. Pietro, "Secure virtualization for cloud computing." *Journal of Network Computing Application.* doi: 10.1016/j.jnca.2010.06.008, 2010

[42] K. Hashizume, "A reference architecture for cloud computing and its security applications," Florida Atlantic University, 2013.

[43] S. Subashini and V. Kavitha, "A survey on security issues in service models of cloud," *J. Netw. Comput. Appl.*, 2011.

[44] C. Tan, Y. Xia, H. Chen H and B. Zang B, "TinyChecker: Transparent Protection of VMs against Hypervisor Failures with Nested Virtualization.", I*n: Dependable Systems and Networks Workshops (DSN-W), 2012 IEEE/IFIP 42nd International Conference*, 2012

[45] D. Gonzales, J. Kaplan, E. Saltzman, Z. Winkelman and D. Woods, "Cloud-Trust—a Security Assessment Model for Infrastructure as a Service (IaaS) Clouds.", *IEEE Trans Cloud* Computing 5:523–536 . doi: 10.1109/TCC.2015.2415794, 2017

[46] Donadio, "Virtual Intrusion Detection Systems in the Cloud," *Wiley Online Libr.*, vol. 17, no. 3, pp. 113–128, 2012.

[47] D. J. Dean, H. Nguyen, and X. Gu, "UBL: Unsupervised Behavior Learning for Predicting Performance Anomalies in Virtualized Cloud Systems," 2012.

[48] J. François, I. Aib, and R. Boutaba, "FireCol: A Collaborative Protection Network for the Detection of Flooding DDoS Attacks," *IEEE*, 2012.

[49] L. Qian, Z. Luo, Y. Du, and L. Guo, "Cloud Computing : An Overview," *Springer*, pp. 626–631, 2009.

[50] D. Androcec, N. Vrcek, and J. Seva, "Cloud Computing Ontologies : A Systematic Review," in *MOPAS The Third International Conference on Models and Ontology-based Design of Protocols, Architectures and Services*, 2012, no. c, pp. 9–14.

[51] D. Costa, "CERT Definition of Insider Threat" - *Updated. In: SEI Carnegie Mellon University*., 2017
[52] M. Kandias, N. Virvilis, and D. Gritzalis, "The Insider Threat in Cloud Computing," 2011.
[53] W. R. Claycomb and A. Nicoll, "Insider Threats to Cloud Computing: Directions for New Research Challenges," 2012.

Dr. Ishrat Ahmad has achieved her PhD degree from Cardiff Metropolitan University, UK. She has done her BSc in Computer Science and Engineering and MSc in Data Warehousing. She is a Software Quality Assurance Engineer by profession. Email: ahmad.ishrat611@yahoo.com

Dr. Humayun Bakht is a Director of Studies / PhD supervisor at the Cardiff Metropolitan University / London School of Commerce. Dr. Bakht is a regular contributor of both academic and non academic articles. He has also authored several books including 'Mobile Ad-hoc Networking' and 'A Roadmap to PhD'. Email: humayunbakht@yahoo.co.uk