I. J. Computer Network and Information Security, **2018, 3, 25-36**
Published Online March 2018 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2018.03.04

Cyber Attacks in Cloud Computing: Modelling Multi-stage Attacks using Probability Density Curves

Aaron Zimba
Department of Computer Science and Technology University of Science and Technology Beijing Beijing 100083, China
E-mail: azimba@xs.ustb.edu.cn

Victoria Chama
Department of Computer Science and IT Mulungushi University Kabwe 80415, Zambia
E-mail: vchama@mu.ac.zm

Received: 07 October 2017; Accepted: 27 December 2017; Published: 08 March 2018

Abstract—Cyber attacks in cloud computing more often than not tend to exploit vulnerabilities and weaknesses found in the underlying structural components of the cloud. Such vulnerabilities and weaknesses have drawn interest from various attack profiles ranging from script kiddies to APTs. Regardless of the attack profile, cyber attackers have come to leverage the interdependencies exhibited amongst these vulnerabilities by chaining exploits together to effectuate complex interlinked attack paths. Such chaining of vulnerabilities in cloud components results in multi-stage attacks where the attacker traverses different segments of the cloud residing in different layers to reach the target. In this paper, we partition the cloud into three different layers to show how multi-stage attacks on Confidentiality, Integrity and Availability (CIA) interleave with the SaaS, PaaS and IaaS cloud computing service models. Further, we generate multi-stage attack paths based on the vulnerabilities exhibited in the components across the partitioned cloud layers. Furthermore, we model the constituents of multi-stage attack events as discrete random Bernoulli variables to characterize the attack path pursued by a given attack profile. We generate probability density curves of the associated resultant attack paths to infer on the nature of the attack and recommend a hierarchical security mitigation process based on the nature of the attack nodes.

Index Terms—Cloud computing, multi-stage attack, attack path, vulnerability, probability density curves.

I. INTRODUCTION

The advancement of computing technology has seen the unfolding of resilient computing solutions which harness a myriad of technologies via integration. Cloud computing has emerged as one of the new computing paradigms which has attracted providers and users alike. The benefits offered by cloud computing are irresistibly attractive to both entities and are not limited to operational costs, capital investment, flexibility, convenience etc [1] [2]. Though not a pristine technology itself, cloud computing leverages not only new computing technologies but also utilizes the Internet to deliver a product that's consumable to almost any part of the world with network connectivity. Server utilization, for example, is one underutilized aspect where data centers in the US use between 6% ~ 20% of the actual throughput with Google's servers averaging ~ 40% [3] as evidenced by lack of virtualization. However, cloud computing introduces virtualization and economies of scale where users share computing resources and services thus improving the overall throughput. This has attracted Cloud Service Providers (CSP) to minimize on costs while users are drawn by the flexibility of pay-as-you-go and the convenience thereof.

Nonetheless, this new approach to computing is not without challenges. It's quite apparent that cloud computing inadvertently inherits the challenges cast by the underlying technologies. One of the most echoed concerns in this regard is security [4]. Since cloud computing is built on various technologies having their own challenges, the security concerns introduced by cloud computing are complex in nature in that they are a web of intertwined security challenges emanating from the participating technologies. In addition, when users outsource computing services from the cloud, they likewise lose control of their data [5]. Will their data be readily accessible from anywhere at any time? The availability aspect of security begs this question. When the data is stored in the cloud data centers even as is traverses the appropriate networks, what guarantee does the user have that their data is not seen by unauthorized persons? Confidentiality concerns cast this question. And in the vein of transferring and processing the data, is the data itself free of alteration? Integrity concerns beg that such security concerns be addressed. Therefore, cloud computing needs to address security concerns directed not

Copyright © 2018 MECS

IPR2025-01083
Orca Security EX1011 Page 1

only towards Confidentiality, Integrity and Availability (henceforth referred as CIA) of user data but even that of the cloud infrastructure as well. Since there are different cyber-attacks directed towards the various components that constitute the cloud infrastructure, the resulting attack surface is so wide that it requires consideration of the interconnection amongst the attacks. There exists in the cloud simple attacks which exploit the ignorance of benign users and carefully crafted complex attacks such as APTs [6] [7] [8] which all pose respective attack vectors. Attackers can integrate these attack vectors with the resultant being complex attack paths traversing different aspects of the cloud to reach the final goal. The effectiveness of each of these attack paths likewise varies and composition and implementation methodologies adopted by attackers are of great importance in as far as addressing cloud security challenges is concerned. Virtualization, which is the major technology upon which cloud computing is built has a very wide spectrum of attack vectors targeting both virtual machines residing in the cloud data centers and those on the network during migration instances. As opposed to conventional cyber-attacks whose goals might at times be abstract, multi-stage cyber-attacks employ a sophisticated level of reconnaissance, surveillance and data exfiltration [9] and this calls for a different approach when addressing and countering the attacks thereof. In light of the above, modeling attacks of this nature calls for the reflection of the appropriate threat actor profiles in the corresponding attack model formulation.

We thus in this paper, for attack path consideration purposes, partition the cloud infrastructure into an abstraction of three layers namely the Application, Virtual and Physical Layer and consider the associated CIA attacks therein. Partitioning the cloud in this manner captures all the three cloud computing service models SaaS, IaaS and PaaS [10] and hence the associated attacks thereof. We furthermore engage conditional probabilities and Common Vulnerability Scoring System (CVSS) [11] [12] to characterize the resultant attack paths and generate probability density curves for the given attack scenarios. The identified critical nodes and edges go on to serve as inputs when formulating measures to thwart the respective attack attempts.

The rest of the paper is structured as follows: Section II describes layer partitioning of the cloud infrastructure while the attack taxonomy and the threat model are presented in Section III. Cloud attacks and their corresponding ingress paths are discussed in Section IV. Illustrative results are presented in Section V and we draw the conclusion in Section VI.

II. Cloud Infrastructure Layer Partitioning

One of the major challenges encountered in addressing security concerns in cloud computing is defining the category of the cloud to which a concern pertains to. Cloud computing can be viewed from either a service model or a deployment model perspective [10]. Viewing cloud attacks from the classifications of the former casts uncertainty on other attacks not captured in the latter and the opposite is true. We therefore combine the two views and partition the end result into an abstraction of three layers namely the Application Layer, Virtual Layer and Physical Layer. The layered cloud architecture is shown in Figure 1 below depicting cloud attacks at each layer. Such a layered approach captures the all the attacks whether viewed from a service or deployment model perspective. We expound Figure 1 as follows:

A. Physical Layer

This layer compromises real-world physical resources that make up the cloud infrastructure. There are three main components in this layer: networking devices, storage devices and physical servers. Therefore consideration of cloud attacks at this layer should not only be focused on individual components but even attacks directed towards the intercommunication amongst these physical components.

1) Networking Components

This comprises a collection of different network devices and media which in turn serve as the backbone of communication in the entire cloud infrastructure. Such components include but not limited to switches, routers, bridges etc and we consider CIA attacks on these components. Confidentiality attacks herein encompass unauthorized viewing of configuration information as well as data traversing these devices. Integrity attacks in this respect pertain to any unauthorized modification of configuration settings or user data traversing therein. Availability attacks seek to make these devices unusable and mainly constitutes the various forms of Denial of Service (DoS) attacks actualized by the various cloud components or otherwise.

2) Storage Devices

Storage components are responsible for storage of cloud data and proving file system services. The storage devices make up cloud data centers and are distributed in a typical cloud computing offering [13]. Storage components usually come in two flavors either as local storage e.g. Storage Area Network (SAN) [14] or network storage e.g. Network Attached Storage (NAS) [15]. In the case of SAN, the devices are directly attached to server components and thus access to storage data has to go through the server. In this case, the server component acts as a key node in any attack directed towards the storage component. Failure to fully exploit the server as a pivot to attacking storage data thwarts the attack attempt. On the contrary, in NAS the storage devices are connected to the cloud infrastructure directly on the network via networking components. Physical servers in this case do not act as key nodes as access to storage components is directly over the network to authenticated users and applications. CIA attacks likewise seek to access, modify or make data unavailable on these components which typically employ some form of RAID architecture [16] for resilience.

3) Physical Servers

IPR2025-01083
Orca Security EX1011 Page 2

These entities provide computational services to cloud users by employing virtualization to achieve maximum efficiency. Physical servers typically run a hypervisor [17], a minimal operating system capable of virtualizing different hardware resources of a desired operating system, hence virtual machine. Details of the virtual machines are discussed in the subsequent sub-sections. CIA attacks on physical servers include confidentiality attacks on the server as it processes user data, data exfiltration and service unavailability achieved by some attacks discussed later in this paper.

B. *Virtual Layer*

This layer comprises different logical otherwise virtual resources which are hosted and supported by the physical layer below. A virtual machine (VM) is the major component at this layer and is supported by various virtual resources not limited to virtual networking components and virtual disks. A VM is simply an abstraction of CPU, memory, network resources offered to a cloud user as though it were an independent system. The hypervisor achieves virtualization of multiple virtual machines by running the Virtual Machine Manager (VMM) which starts, stops or reloads a given virtual machine. VMs run OS specific applications and the VMs are thus independent one from the other although they would share the same physical resources if they reside on the same physical platform. Virtual layer components, though transparent to the user, collaboratively serve Application layer software platforms and applications for both SaaS and PaaS. IaaS if fully manifest at this layer. Since cloud computing is centered on virtualization [18], most of cloud attacks reside at this layer as it is apparent this is the interface layer of both the physical and application layer. CIA attacks herein are directed not only on the underlying virtual components but the user data handled thereof. These include attacks on VMs, hypervisors, virtual routers and switches, Software Defined Networking (SDN) etc. We consider these attacks in detail in Section IV.

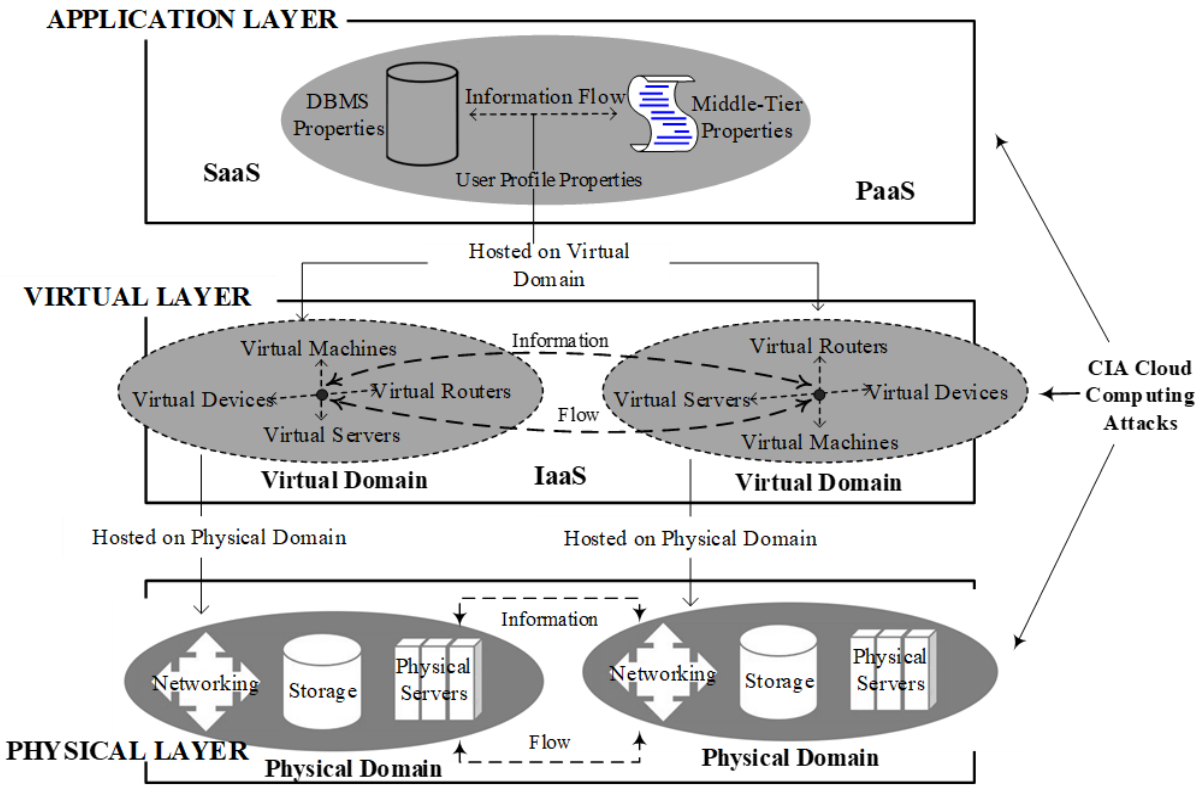

Fig.1. Layered View of Attacks on Cloud Computing

C. *Application Layer*

The application layer is directly supported and hosted by the virtual layer and it provides resources for software applications and platforms. This layer reflects SaaS with some overlapping of PaaS. It's worth noting, however, that not all cloud implementations host application resources on the virtual layer. Other implementations, as the case of critical infrastructure with a degree of resilience host application resources directly on the physical layer. This is important in attack path formulation as some additional components are removed from the overall attack chain. CIA attacks at this layer mainly encompasses attacks on user data both in SaaS and PaaS. It's worth noting that an attack emanating from the application layer can traverse the cloud infrastructure all the way to the physical layer provided all pivotal nodes along the attack path are exploitable.

D. *Layer Domains and Information Flow*

Components within a layer are usually organized into logical groups to serve specific users or for efficiency purposes. The logical groups form layer domains enforced

IPR2025-01083
Orca Security EX1011 Page 3

by a domain policy hence the physical, virtual and application domain. Therefore, data can move either horizontally at a given layer from one logical domain to another or vertically from a domain in the upper layer (Application or Virtual Layer) or from a lower layer (Physical or Virtual Layer) to a domain in a different layer altogether. Therefore cloud attacks in this respect would be intra-layer or inter-layer attacks respectively.

The information flow found in the cloud infrastructure can be classified as either one that holds application data or management data. Application data is the actual user data stored on cloud storage devices. Most attacks in the cloud are directed towards application data. Instances of application data breaches via various attack vectors are not uncommon even amongst major cloud vendors [19] [20]. Cloud users are responsible for their data's security in the PaaS and IaaS offering whilst the provider is responsible for data security in SaaS. Management data is the data used for managing the various cloud components at each layer. This includes SDN configuration, VM settings, user profile properties, DBMS properties, middle-tier properties and all other information that enables the operation of the cloud infrastructure. Unlike application data, management data is the sole responsibility of the cloud provider. Though insufficient protection of management data can foster attacks such as insider attacks, we in this paper consider mainly application data as goal of a given attack unless otherwise stated. Therefore, even in consideration of insider attacks, we only consider those that are mainly targeted against user data and not management data.

III. Attack Taxonomy and Threat Model

Having defined the components that constitute the cloud infrastructure, we now endeavor to classify cloud attacks pertaining a given approach and furthermore define the threat model of the attacks.

A. The Attacks Taxonomy

As seen in Figure 1, cyber-attacks in the cloud can be sub-divided as attacks on the Application, Virtual and Physical layer. Attacks on the physical layer are directed towards physical servers, storage devices or networking components. The target data is either management or application data and the nature of the attack seeks to breach tenets of the CIA triad. Likewise, attacks on the virtual layer are directed towards VMs, virtual servers, virtual networking components and other virtual devices such as hypervisors. The attacks seek to steal data, modify it and or make it inaccessible hence CIA attacks on application and or management data. In the same manner, attacks on the application layer target middle-tier properties, user profiles, DBMS properties and the associated data. These attacks likewise are CIA attacks on management and application data. We summarize, as depicted in Figure 2 below, the attack taxonomy of cloud attacks from a layered structure standpoint.

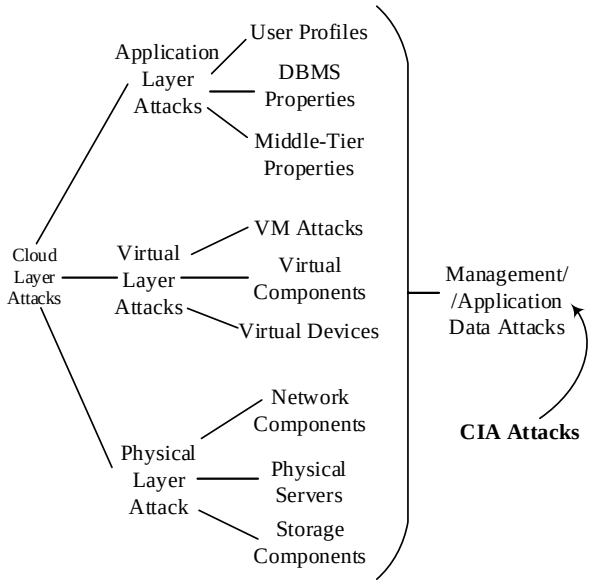

Fig.2. Summarized Cloud Attacks Taxonomy

Regardless of the cloud layer and target data, i.e. whether application or management data as shown in Figure 2, cloud attacks seek to breach tenets of the CIA triad and we henceforth categorize any given attack at a layer as a confidentiality, integrity or availability attack.

B. The Threat Model

We now define our threat model for which all considered attacks are valid. We consider attacks that compromise the confidentiality, integrity and availability of client application data. We do not include management data due to the constraints imposed by initial attack sources. We use attack graphs [21] [22] to model cyber-attacks across different cloud layers. The overall attack process is described as a composition of discrete units serving basic building blocks which when correctly implemented lead to the actualization of the attack. These units include: ***Attack Source*** unit, ***Cloud Layer*** unit and ***Node*** units. Using these three units, we classify a given multi-stage attack as either *Intra-layer* or *Inter-Layer*. The threat actor, otherwise attacking agent, is a skillful technical actor using a myriad of attack vectors, even malware whenever necessary. The diagram below in figure 3 illustrates the attack model.

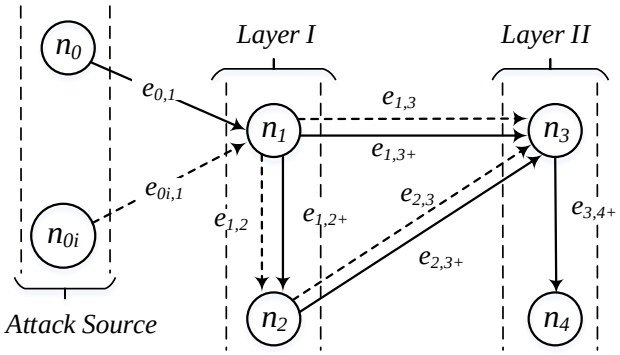

Fig.3. The Attack Model

IPR2025-01083
Orca Security EX1011 Page 4

The attacker traverses the cloud network moving from one node to the other by exploiting vulnerabilities exhibited in the nodes. Attack graph nodes represent the different cloud components at different layers of the cloud structure. Nodes without vulnerabilities of interest to the attacker cannot be traversed, hence cannot be attacked. Details on how these vulnerabilities are exploited are explained in the proceeding section.

1) Attack Source

This unit comprises nodes depicting the different types of network environments from which a cyber-attack can originate. Generally, an attack can originate from the Internet outside the cloud network, from within the private network of the cloud service provider or from a trusted third party like a cloud security broker or any other entity that shares a trust relationship with the cloud provider's network. A discrete node in this unit is denoted as n_0 where n_{0i} denotes a set of the three attack sources as earlier described. Therefore, the edge $e_{0,j}$ denotes an attack from a specified attack source to a node n_j at certain layer of the cloud. The probability of infiltrating a given attack source is a subjective value determined by the security analyst depending on the security configurations and susceptibility to cyber-attacks of a given source.

2) Cloud Layer

We differentiate two categories of cloud layers namely Layer I and Layer II. Both Layer I and II can be any of the earlier described three layers (Application, Virtual or Physical). This is to mean that from a given entry attack source, the attacker can enter any of the three cloud layers. This implies that the attack is multi-directional. Thus an attack can start from the virtual layer and proceed upwards or downwards to the adjacent layers. Alternatively, if the entry point is the uppermost or lowermost layer, the attack can propagate downwards or upwards respectively to the adjacent layers.

3) Attack Nodes

The nodes of the attack graph are symbolic representations of the different vulnerable cloud components. We differentiate two types of nodes; *pivot* nodes and *goal* nodes.

Pivot nodes: These are any nodes used by the attacker as stepping stones to reach the next node. If a pivot node is required to be exploited before reaching a given node, then such a pivot node is a critical node. Failure to exploit such a node thwarts the whole attack process. Since the attack is multi-stage, the attacker discovers vulnerable nodes in the cloud network via reconnaissance attacks and lateral movement in the case of an APT. Pivot nodes are represented by the node set $\{n_1; n_2; n_3\}$ and their corresponding edge set $\{e_{1,2+}; e_{1,3+}; e_{2,3+}; e_{3,4+}\}$. These are shown by the solid edge transitions.

Goal nodes: These are nodes which the attacker seeks to reach in order to breach the data. If no further attainment of pivot nodes is required, then the last node in the attack path is the actual goal. These are denoted by the node set $\{n_2; n_3; n_4\}$ and the corresponding edges $\{e_{1,2}; e_{1,3}; e_{2,3}; e_{3,4}\}$. It's worth noting that node n_1 cannot be a goal node as the attacks are multi-stage thereby requiring of at least traversal one node before reaching the target.

4) Multi-stage Attack Category

We further subdivide the multi-stage attacks into two categories; *intra-layer* and *inter-layer*. Intra-layer multi-stage attacks present those attacks that occur within a given layer but exploit multiple nodes to breach the target. Intra-layer attacks for Layer I are those depicting a traversal from node $n_1 \rightarrow n_2$ denoted by edge transitions $e_{1,2}$ and $e_{1,2+}$. Intra-layer attacks in Layer II are depicted by a traversal from $n_3 \rightarrow n_4$ denoted by the edge transition $e_{3,4+}$. Inter-layer multi-stage attacks are those attacks which leverage a pivot node in one layer to reach a node in another layer. These are depicted by traversal from $n_1 \rightarrow n_3$ and $n_2 \rightarrow n_3$ with the corresponding attack edge sets $\{e_{1,3}; e_{1,3+}\}$ and $\{e_{2,3}; e_{2,3+}\}$ respectively. In so doing, we classify any given cloud attack as either intra-layer multi-stage or inter-layer multi-stage cloud attack. Figure 4 below illustrates these two types of multi-stage attacks.

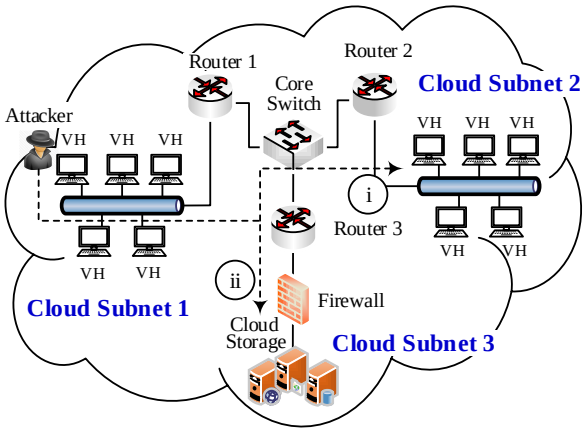

Fig.4. Intra-layer and Inter-layer multi-stage Attacks

The cloud network above comprises three subnets with subnet 1 and two residing on the same layer (virtual layer) while subnet 3 resides on the physical layer housing client data. Subnet 1 and 2 contain different client VMs (Virtual Machines) or VH (Virtual Hosts) whereas subnet 3 contains physical data storage.

Attack scenario ***i*** represents an intra-layer multi-stage attack in that despite the attacker residing in a different subnet 1, he still lies in the same layer as subnet 2. A typical attack of this nature is a side channel attack [23] where the attacker needs to establish local network co-residency on the same layer to effectuate the attack.

Attack scenario ***ii*** represents an inter-layer multi-stage attack because the attacker and the victim reside in different layers. In this case, the attacker needs to exploit pivot nodes either in subnet 2 or vulnerable network devices e.g. routers, switches etc in order to reach the target in subnet 3. A common typical attack of this nature is a DDOS (Distributed Denial of Service) [24] where the attacker first compromises a set of zombie VMs in either

Copyright © 2018 MECS

IPR2025-01083
Orca Security EX1011 Page 5

subnet 1 and or 2 to launch the attack directed towards a victim in subnet 3. In this case, the exploited VMs act as pivot nodes and only do so because of the presence of an exploitable vulnerability. It's worth noting that in this case, the targeted victim might not necessarily be a discrete node such as a SAN server but it could also be subnet housing the data storage server. This is evidenced in a Link aggregation DOS [25] attack where the attacker seeks to bring down an entire subnet hosting a server of a certain application.

It's apparent from the attack model that the success of a multi-stage attack is heavily dependent on pivot nodes. If a pivot node is not traversable, i.e. does not exhibit any vulnerability to be exploited, then the multi-stage attack is not possible. Therefore, to determine reachability of nodes in a given attack scenario, we deduce the reachability matrix representative of the attack graph's adjacency matrix. The resultant matrix for the above attack graph is a square matrix of the 5th order denoted by Equation (1) below as:

$$R_M = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix} \quad (1)$$

Though the vertex degree of node $n_2$is higher than that of node n_1, the node n_1 is the actual isthmus of graph. This is echoed by the fact that node n_1 represents the entry node of the graph without which node n_2 is not reachable. Therefore, node n_1 is the critical node. Since the exploitation of a given node in the attack network might be dependent on another node, the full joint probability can be expressed as conditional probabilities of child nodes conditioned by parent nodes as:

$$Pr(n_0, \dots, n_i) = \prod_{i=1}^{n} Pr(n_i \mid parents\ (n_i)) \quad (2)$$

Where a child node has more than one parent node, the resultant probability of traversal can be expressed as either probability of union or intersection of events depending on whether the attack events are mutually exclusive or otherwise. Following from Equation (1) and (2), the full joint probability of the attack network in figure 3 is calculated as:

$$\Pr(n_0, n_1, n_2, n_3, n_4) = \Pr(n_0) \cdot \Pr(n_1|n_0) \cdot \Pr(n_2|n_1) \cdot \Pr(n_3|n_1, n_2) \cdot \Pr(n_4|n_3) \quad (3)$$

Therefore, the probability of reaching the critical node n_1 by traversing the isthmus edge from the attack source can be expressed as:

$$\Pr(n_1) = \Pr(n_1|n_0) \quad (4)$$

The probability $\Pr(n_0)$ as earlier stated, is given as a subjective belief based on expert knowledge. In the same manner as Equation (4), we calculate the conditional probabilities of traversing other nodes in the attack network:

$$\Pr(n_2) = \Pr(n_2|n_1) \quad (5)$$

$$\Pr(n_4) = \Pr(n_4|n_3) \quad (6)$$

$$\Pr(n_3) = \Pr(n_3|n_1, n_2) = \Pr(n_3|n_1) \cdot \Pr(n_3|n_2) \quad (7)$$

Since the child node n_3 is conditioned on two parents n_1 and n_2 , Equation (7) could also be expressed a disjunction of attack events in the scenario where the attack events from the parent nodes are independent one from the other. We use the above Equations (3) – (7) further in computations of conditional probabilities in the results' sections. We now endeavor to categorically characterize attacks in cloud computing components as documented in literature for later application in the results segment.

IV. Cloud Computing Ingress Attacks

There are a lot of cyber-attacks witnessed in various cloud environments which leverage either the vulnerabilities present in cloud components or misconfigurations depending on the design pattern. All of these attacks breach at least one tenet of the CIA triad. Before we generate probability density curves, we make our paper compact and self-contained by endeavoring to characterize the most common types of these attacks and how they generate virtual attack paths as the attack progresses. Most of the attacks are directed towards cloud components within a given layer or across different layers. Therefore, the attacks considered henceforth constitute both intra-layer and inter-layer multi-stage attacks so long they utilize some form of pivot nodes to enhance the attack. The goal of a given attack differs one from the other and ranges from attacking client VMs to compromising actual servers or bringing the entire cloud network down in the case of a DOS attack.

A. *Hyperjacking*

A hyper-jacking attack [26] targets the operating system (OS) providing the virtualization in a cloud environment. The goal of the attack it to take control of all the VM Oss that are running on top of the hypervisor. The naming implies that the hypervisor is technically hijacked and in so doing the attacker is capable of controlling the guest operating systems thereby breaching any of the targeted CIA tenets. The attacker achieves this by installing a rogue hypervisor beneath or just on top of the original hypervisor but before the VM OS stack. Alternatively the attacker can directly get hold of the hypervisor depending on the pursued attack vector. From such a position, the attacker is able to compromise client data or monitor their activities and implant APT malware to harvest further information. The attacker's capabilities in such a scenario are almost limitless and this inherently implies that

IPR2025-01083
Orca Security EX1011 Page 6

hypervisors in a virtualized cloud environment represent a single point of failure and this is not surprising considering that cloud computing technology is centered around virtualization [18]. Since VM running under virtualization are oblivious of the underlying hypervisor, it is difficult to handle this attacker from a client's end especially if the attack action thereof is passive.

B. Honest but Curious Server

The honest-but-curious server breaches security by violating the fundamental need-to-know principle of security. This is actualized by the need-to-know attack [27] where a party does not adhere to system security policies by collecting information which is not relevant to its operation. The attack in general is based on breaking the trust relationship between a server and an entity whose data is being handled by the server. This constitutes a breach against confidentiality of the CIA tenets. In this case, the party violating the need-to-know principle is a server in the cloud and it's apparent from here that such an attack originates from within the cloud itself. Furthermore, this attack spans across all the three cloud layers discussed earlier. A virtual server on the second layer can implement this attack to cloud SaaS users desiring access on the application layer and likewise a virtual server can collect more than necessary information from a client VM. A physical sever in the same manner can effectuate this attack on the data it processes as well as data that is stored locally. A malicious insider or even outsider who's aware of a server capable of launching a need-to-know attack could leverage this capability to breach clients' confidentiality. Unlike routers which tend to only process header information of the packet being routed, a honest-but-curious server on the other hand processes the actual information and however encrypted the client data might be, it is more often than not decrypted before processing in the cloud thereby exposing the client's data to the need-to-know attack. Since it is very difficult for a cloud user to monitor this attack as the mostly likely perpetrator is the provider, mitigation of this attacker tends to be costly, e.g. homomorphic encryption [28] which seeks to conceal information that the server is processing from itself.

C. Link Aggregation Attack

This is a DOS-type of attack [25] targeting VMs running in a virtualized environment, the cloud. It leverages data center networks under-provisioning in a shared infrastructure such as the cloud environment. Since a typical network setup involves a broadcast domain of cloud VMs in a specific subnet, access to other VMs in other subnets is facilitated by a stub router with a failover in cases where redundancy is implemented. The router could be either a physical router or a virtual router at the virtual layer connection to a virtual or physical switch spanning multiple collision domains. The maximum uplink capacity of the router is usually less than the cumulative uplink capacity of all the hosts in a subnet. The attacker in this cases only needs to saturate the uplink of the router to denial accessibility of other host. The attacker seeks to find where there is a bottleneck in the network to launch the attack. It is therefore imperative to interpret the network topology since switches span multiple collision domains thereby supporting a 100% throughput. Alternatively, the attacker could get hold of the host which creates VMs in the subnet or personally launch multiple VMs depending on their access permission to the cloud. In a targeted attack, the attack would need to attain critical mass from the target domain by launching many VMs in order to make unavailable a service or application in that domain. Using UDP datagrams is particularly effective in that TCP datagrams tend to institute back-off mechanisms during congestion, hence the denial of service. In so doing, the attacker could render unavailable a client application and this is particularly cumbersome to mitigate by the application owner since they don't own the cloud.

D. Side Channel Attack

Side channel attacks [23] take advantage of colocation to breach confidentiality of the neighbor VM. This attack is based on the premise that under virtualization, co-resident VMs share the same CPU and memory of the physical machine. The attacker thus initiates surveillance on the neighbor VM to monitor and subsequently acquired targeted information. It is therefore imperative that the attacker establishes co-residency with the targeted host. To achieve this, the attacker launches multiple VMs and checks whether the resultant VM is co-resident with the target. Side channels attacks are only feasible when two VMs reside on the same physical machine. The attacker can probe for co-residency by using traceroute requests. Since the hypervisor will report itself as the next host for VMs on a local machine (assuming the typical configuration), tracerouting the next hop IP address can be used to probe co-residency. The attacker can likewise use ping echo request and monitor the round trip time with shorter times suggesting co-residency. If ICMP requests are blocked in the target environment and a cloud tenant is not assured of exclusive use of hardware, the attacker can launch VMs by chance hoping one will be co-resident with the target VM or resort to other techniques like cloud cartography [29]. Once the attacker is co-resident with the target VM, he initiates a technique to monitor the activities of the shared CPU, cache and memory. In so doing, the attacker can obtain valuable data such as usernames, passwords, cryptographic keys etc all across cloud tenant boundaries. Which tenet of CIA will be breached further depends on the type of information acquired but one thing for sure is that confidentiality is inadvertently breached foremost.

E. VM Migration Attack

The philosophy of cloud computing emphasizes efficiency in the use of resource by VMs and this entails that in events of resource saturation, VMs tend to be stopped, started, restarted and eventually moved to prevent overload. Depending on the setup, one physical machine running a couple of VMs in a domain might be getting overburdened and in order to implement the elasticity property of cloud computing, some VMs might

IPR2025-01083
Orca Security EX1011 Page 7

need to be moved to another physical machine. Since the VMs need to cross the network as they are being copied, they are exposed to other VMs residing in the network they traverse in order to reach the destination location. The VM migration attack [30] centers on eavesdropping valuable information from a VM traversing the network to another location. It's worth noting that the attacker's NIC need to be in promiscuous mode in order to capture traffic no destined to itself. Though this attack has a limitation in that the targeted VM might not be moved when desired, the attacker could induce other tactics like link aggregation DOS or resource freeing attack which might in turn initiate the migration of the desired VM. So the attacker monitors the cloud network and once a migration is detected, he collects packets of the migrating VM and filters them for valuable information such as cryptographic keys, certificates, credentials etc which he can use further to access the migrated VM once it's started or use such information to access other VMs where applicable. This attack evidently breaches confidentiality but logically seen can escalate to integrity and availability. Clearly this attacks spans both the virtual and physical layers considering that the key nodes of the attack are from the two layers.

F. VM Escape

The VM escape attack [31] is based on the notion that even though the VM is unaware that it's running on top of another host, misconfigurations and vulnerabilities can enable the constrained user to break off the jail and escape to the host OS or the hypervisor. Since the host machine usually has root privileges, an attacker escaping the jail constraint imposed by virtualization consequently elevates his level of privilege in the cloud and this implies that his attack surface span across all VMs under the compromised OS or hypervisor. In this type of attack, the attacker's VM needs to reside on the machine with the vulnerable or misconfigured OS or hypervisor to reach the target VM. This could be a VM the attacker has legitimate access to or if not, the attacker could launch multiple VMs until one launches on the target machine. The attacker can the initiate the escape via applicable means and if successful, he can attack the intended VM. If the target VM's machine is not vulnerable or not misconfigured, the attacker could user credentials of the compromised hypervisor to access the hypervisor or OS where the target VM lies. Since the hypervisor manages all the VMs under its domain, the attacker can likewise breach the confidentiality and or the integrity of the targeted VMs. He can also launch a DOS attack against any VM by simply stopping it or more crudely by deleting it. The source of this attack evidently is the network outside the cloud, i.e. Internet but it can as well originate from a malicious insider who has access to VMs.

G. MITC Attack

A Man-In-The-Cloud attack [32] is a typical cloud attack that happens on the application layer. Unlike other attacks which only affect client data on the cloud, a MITC attack is able to inversely attack client data via synchronization services offered by most cloud service providers. The attack targets cloud users utilizing the cloud synchronization service implemented using the OAuth framework. The attacker indirectly enters the cloud by attacking the bearer token used in the OAuth framework. This attack is possible because the client synchronization application trying to synchronize with the cloud does not verify the authenticity of the synchronization token. Therefore the attacker swaps the client's synchronization token with his on the client's machine and the client's cloud synchronization application ends up synchronizing with the attacker's account. This implies that whatever modifications the client makes will be synchronized with the attacker. The attacker can in turn add malicious code to the synchronization folder and it will replicate unto the client. In so doing the attacker can run arbitrary code remotely and harvest a lot of information from the victim. This attacker is largely reflected in SaaS and PaaS is seen to directly breach both the confidentiality and integrity aspect of the CIA. As can be seen, the source of this attack is outside the cloud and thus postulate it to be the Internet.

H. XML - HTTP DOS

This type of attack [33] of attack takes advantage of the delivery mode of web request in the cloud to attain a denial of service state. Clearly this attack is confined to the application layer in the realms of SaaS and PaaS though the server serving web request could be running on a physical server. The attack is twofold in that it denies legitimate users from accessing an authorized service and any PaaS clients hosting such a service will not be able to serve their customers. This attack incorporates common web resources such as XML and HTTP due to their universality and ease of implementation. The attack can come as one based either on XML (X-DOS) or HTTP (H-DOS) or even as an integration of both. Further the attack can be metamorphosised into a distributed denial of service (DDOS) by leveraging the availability of vulnerable host on the Internet. In a typical X-DOS, Coercive Parsing for example, the attacker floods malicious XML messages to the server with the intent of having it to malfunction via manipulation of the Simple Object Access Protocol (SOAP) requests to make application content inaccessible. The attacker achieves this by streaming a continuous sequence of open tags thereby making the server's CPU so busy and thus inaccessible. To transform X-DOS into distributed X-DOS (DX-DOS), the attacker engages other hosts to send the XML messages. These hosts could be compromised VM hosts from within the cloud or a botnet of zombies from the Internet. In the case of using cloud VMs in DX-DOS, the attacker launches multiple VMs and further launches multiple XML applications, e.g. browsers which in turn generate and flood XML messages to the targeted server thereby overwhelming it in the end, hence DX-DOS.

In like manner, H-DOS uses the concepts of volumetric flooding the victim with messages, only this time seemingly legitimate HTTP POST or GET requests

IPR2025-01083
Orca Security EX1011 Page 8

executing in a loop-like structure. In so doing, the attack can quickly cripple a server because not only does it consume resources from the TCP/IP stack but from the server as well. The challenge in mitigating this attack is that it's difficult to practically distinguish and filter legitimate HTTP requests in DH-DOS attack in a public domain.

I. Resource Freeing Attacks

Resource Freeing Attacks (RFA) [34] seek to modify the workload of the target VM to an extent that it's starved of services. Typically this is a case of denial of service and is constrained to the virtual layer. This attack targets the main principle of cloud computing of multiplexing tenant workloads unto a single machine which share access to the same host's memory, CPU, cache and network resources. It's apparent that this attack can only be actualized if the attacker is co-resident with the victim and we suppose this is achieved by earlier discussed means. RFA employs the concept of a beneficiary - which is the entity that benefits from the attack, and the helper – an entity collaborating with the attacker to launch the RFA. The beneficiary and helper increase the workload of the victim by increasing the time spent on one resource thereby freeing up other resources. The goal is to ensure that the victim reaches saturation and induce a bottleneck with regards one resource so that the victim can no longer consume any other resource. Since raising the victim to a bottleneck just prevents additional usage and not really free up resources, the attacker shifts the victim's resource usage spent on the bottleneck so that the victim spends a greater fraction of his time on the bottleneck. In so doing the victim is forced to spend less on the other resource.

J. SDN Attacks

Software Defined Networking (SDN) is a new networking paradigm which fits well in the basic principles of cloud computing. As a new technology, SDN has vulnerabilities [35] which it introduces when integrated into the cloud. SDN incorporates the use of virtual devices which are special purpose virtual machines for managing networking in the cloud environment. Depending on the prevailing design pattern, these special purpose VMs could exhibit colocation with the guest's VM OS on the same hypervisor or it could be incorporated within the HV. In the former case, the attacker is in the same domain with the target VM and if not, he would establish co-residency via earlier discussed methodologies. The attacker thus is able to get hold of the underlying HV by means such as VM escape, Hyperjacking or other applicable means to further gather valuable information such as decryption keys, credentials, discover network architecture etc from the host's RAM. Armed with such information, the attacker is able to modify virtual switch and virtual router configurations such as routing tables which inadvertently affects the routing process of packets traversing the cloud network. The attackers promiscuously listens to and monitors the network for interesting inbound and outbound network traffic. He can now not only eavesdrop but intercept packets for MITM attacks and so on. Being able to modify SDN devices avails the attacker to launch other forms of attacks such as DOS by simply redirecting network traffic or induce ARP poisoning. Though this attacks lurks the virtual layer, its effects span both the application and physical layers. If the SDN devices are integrated into the underlying HV, the attacker needs to compromise the HV in the manner discussed earlier.

V. ILLUSTRATIVE RESULTS

Having elaborated the threat model and attack path formulations, we endeavor to generate and characterize the attack paths resulting from a series of exploited vulnerabilities. We apply the attack model to the cloud diagram in figure 4 by specifying a known attack (as illustrated in the preceding section) against a specific vulnerability for each attack action. In our exposition, the attacker is a cloud user with an active VM. This is typically acquired via legitimate means in a PaaS or IaaS subscription. Following from this, the attack source is the cloud itself. So the attacker first finds vulnerabilities via a reconnaissance attack by surveilling the applicable network environment using tools like Armitage, Nessus, Nmap etc. The discovered vulnerabilities that make the previously discussed attacks possible are shown in Table I below.

Table 1. Attack Characteristics

Attack Name	Attack Category	Cloud Layer	Pivot Nodes	Exploited Vulnerability	Base Score Prob
Venom	Intra-Layer	Virtual Layer	VM, SDN	CVE-2015-3456	0.77
VM Escape	Inter-Layer	Virtual Layer	Hyper visor	CVE-2015-3456	0.77
Side Channel	Intra-Layer	Application, Virtual	VM	CVE-2017-5681	0.75
Link Aggr. DDos	Inter-Layer	All	VM, SDN	CVE-2017-0181	0.76
Source Infiltration	-	Virtual	-	-	0.90

We get the base score probability from the CVE value of the vulnerability exhibited in the node. This is an intrinsic value denoting the nature of the vulnerability immune to perturbation with time and we assign it to a node exhibiting such a vulnerability. Thus, we calculate the base score probability as:

$$Pr(n_i \mid \forall\, c \in R_i) = {}^{BS_i}/_{10} \tag{8}$$

where BS_i is the base score from the NVD database, c are the conditions necessary for exploitation of the vulnerability from the base score parameter set. Using the attack graph from the attack model in figure 3, the subjective source infiltration by the attacker on node n_0 is 0.90. The attack exploits the Venom vulnerability at node

IPR2025-01083
Orca Security EX1011 Page 9

n_1 with a probability of success of 0.77. This enables him to completely take over the VM. Since this VM is a pivot node, the attacker as an option of launching an intra-layer multi-stage attack against node n_2 by exploiting CVE-2017-5681 with a probability of 0.75. This results in a side channel attack where the attacker acquires further credentials to reach hosts on another layer. In this case, the attack breaches confidentiality of client data as was witnessed in the Dropbox attack in 2015 [36]. Since the attacker now has credentials to node n_3, he can exploit the vulnerability on node n_3 to effectuate a VM escape attack with a probability of 0.77. With this attack in perspective, the attacker gets hold of the hypervisor and is able to breach all the CIA tenets at node n_3. This constitutes an inter-layer multi-stage attack. This enables him to launch multiple VM and exploit CVE-2017-0181 with a probability of 0.76 causing a DDOS attack on node n_4. This particular action is an attack against availability of both the network where node n_4 lies and accessibility to the servers therein.

On the other hand, if the attacker while at node n_2 decides to reach node n_3, that would constitute an inter-layer attack. In this case, he has to find a vulnerability on node n_3 that will enable him to traverse across the layers. If such a condition is not met, the attacker is forced to first launch an intra-layer attack on n_2 which would subsequently elevate his capabilities of reaching node n_3 from node n_2. Given the above attack scenarios, we generate the following attack paths representative of both intra-layer and inter-layer multi-stage attacks:

$$\begin{aligned} P(1)&: n_0 \rightarrow n_1 \rightarrow n_2 \\ P(2)&: n_0 \rightarrow n_1 \rightarrow n_3 \\ P(3)&: n_0 \rightarrow n_1 \rightarrow n_2 \rightarrow n_3 \\ P(4)&: n_0 \rightarrow n_1 \rightarrow n_3 \rightarrow n_4 \\ P(3)&: n_0 \rightarrow n_1 \rightarrow n_2 \rightarrow n_3 \rightarrow n_4 \end{aligned} \tag{9}$$

It's vivid from the attack graph that attack path $P(1)$ is the only exclusive intra-layer multi-stage attack. This happens in Layer I. Conversely, attack path $P(2)$ is the only exclusive inter-layer multi-stage attack. Attack path $P(3)$ is an inter-layer multi-stage attack comprising one intra-layer multi-stage attack in Layer I. As opposed to attack path $P(3)$, attack path $P(4)$ is an inter-layer multi-stage attack comprising an intra-layer attack in Layer II and not Layer I, i.e. the order of the sub multi-stage attacks is reversed. Attack path $P(5)$ is an inter-layer multi-stage comprising two intra-layer multi-stage attacks one in layer I and another one in layer II.

Since each attack action in the paths $P(1) - P(5)$ is independent one from the other and do occur sequentially and not at the same time, we can express the overall likelihood of reaching a given target as probability of mutually exclusive events. Therefore to find this likelihood given the base score probabilities, we find the product as:

$$\mathbb{P}(P_{ij}) = \prod_{i,j=0}^{m} P_n(P_{ij}) \tag{10}$$

where P_{ij} is an attack path originating from source i to target j and $P_n(P_{ij})$ is base score probability at the node n_i exploited from a parent node n_j. Applying Equation (10) and using Equations (2) – (7) for the above attacks paths $P(1) - P(5)$, the resultant probabilities $\mathbb{P}(P_{ij})$ are:

$$\begin{aligned} \mathbb{P}(P_1) &= 0.518 \\ \mathbb{P}(P_2) &= 0.533 \\ \mathbb{P}(P_3) &= 0.400 \\ \mathbb{P}(P_4) &= 0.405 \\ \mathbb{P}(P_5) &= 0.304 \end{aligned}$$

From the attack paths in Equation (9), we deduce a parametric value k to denote the number of atomic attack steps required to compromise a target. This is equivalent to the number of attack actions in a given attack path.

$$k_i = n + 1 \tag{11}$$

where n is the position of the target node in the attack graph. It's worth noting that we always a one to the position of the node in the graph to get the k parametric value because the attack source infiltration step is not shown in the graph though it's a step present in each attack path as the initial action of the active attack phase of a given attack.

Since the base score probability is intrinsic and thus remains constant with time, and such intrinsic probabilities in a given attack path are independent one from the other, we can model attack actions in a given attack path as Poisson variables obeying the Erlang distribution. These satisfy the Erlang function with respect to time t:

$$F(t: \lambda, k) = 1 - \sum_{n=0}^{k-1} \frac{(\lambda t)^n \cdot e^{-\lambda t}}{n!} \tag{12}$$

where k is the number of attack steps in a given path and the parametric value λ is the mean of the attack path indicative of the success rate of the whole attack process. Therefore, λ is calculated as:

$$\lambda = \frac{1}{k} \cdot \prod_{i,j=0}^{m} P_n(P_{ij}) \tag{13}$$

Using Equation (11) and (13), we have the following k *and* λ parametric values for each path:

$$\begin{aligned} (P_1)&: \quad k = 3;\ \lambda = 0.172 \\ (P_2)&: \quad k = 3;\ \lambda = 0.176 \\ (P_3)&: \quad k = 4;\ \lambda = 0.100 \\ (P_4)&: \quad k = 4;\ \lambda = 0.102 \\ (P_5)&: \quad k = 5;\ \lambda = 0.061 \end{aligned} \tag{14}$$

To generate the probability density curves with respect to time, we apply Equation (14) parametric values to Equation (12) to produce the density curves depicted in figure 5 below.

IPR2025-01083
Orca Security EX1011 Page 10

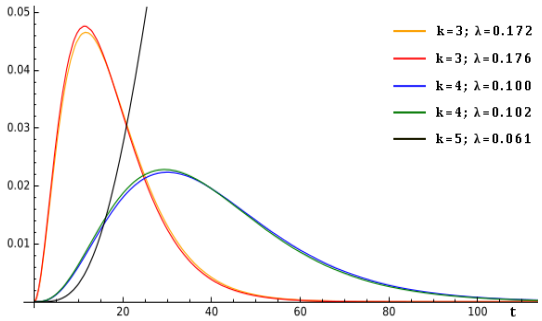

Fig.5. Probability Density Curves for Paths $P(1) - P(5)$

It's visible from the graph that the width of the distribution is greatly influenced by the k parameter. Nonetheless, a higher k parameter doesn't necessarily imply a higher modal frequency. This evidenced from the graph of $P(1)$ and $P(2)$ which have lower k parametric values as compared to those of $P(3)$ and $P(4)$ yet with higher modal frequencies but still less than that of path $P(5)$ which has a higher k parameter as well as a modal frequency than those of both $P(1)$ and $P(2)$. It can be observed from the graphs that the further the target is from the attack source, the wider the distribution. The graphs are all right skewed entailing the mutual exclusiveness of the attack events in a given path. This means that the probability of reaching a target located further in the attack network reduces with an increase in atomic attack steps. This in itself strongly suggests that observance of an attack at an end node as a result of an exploited vulnerability is a strong Indicator of Compromise (IOC) in the cloud network. IOCs entail a higher likelihood of intra-layer and inter-layer multi-stage attacks. Critical pivot nodes in an attack path ought to be prioritized in security mitigation, i.e. the critical nodes should be sought to be turned into failure nodes. This inherently thwarts the attack. Further, the hierarchy for eliminating vulnerabilities, e.g. via security patches, should start with nodes closet to the source and the critical node. Such an approach eliminates beforehand the propagation of the attack through the cloud network.

VI. Conclusion

In this paper, we have shown that the existence of vulnerabilities in cloud computing components can be leveraged to effectuate cyber-attacks resulting into intra-layer and inter-layer multistage attacks. Inter-layer multi-stage cyber-attacks harbor a subset of intra-layer multi-stage cyber-attacks. Using base score probabilities, we have shown that the resultant probability density curves depend on the k parametric values. The higher the k parametric value, the wider the distribution. However, the maximum of the graph, denoting the modal frequency of the attack pattern is in addition influenced by the λ parametric value. The resultant probability density curves are right-skewed entail that the larger mass of the attack activity is concentrated near the attack source. This means that the likelihood of reach the target with an increment in attack action reduces. This means that observance of a breach at a node located far away from the attack source or critical node is a strong IOC. Security mitigation priority should first be given to the critical node owing to the fact that it reflects the isthmus of the underlying attack graph and its mitigation thwarts the attack under consideration. Thus, the security administrator should seek to turn the critical node into a failure node. The security mitigation hierarchy should start with securing those nodes closest to the critical node and the attack source since the mass of the observed density curves is concentrated to the left.

References

[1] Sumit Goyal,"Public vs Private vs Hybrid vs Community - Cloud Computing: A Critical Review", IJCNIS, vol.6, no.3, pp.20-29, 2014. DOI:10.5815/ijcnis.2014.03.03

[2] Fatemeh shieh, Mostafa Ghobaei Arani, Mahboubeh Shamsi,"An Extended Approach for Efficient Data Storage in Cloud Computing Environment", IJCNIS, vol.7, no.8, pp.30-38, 2015.DOI:10.5815/ijcnis.2015.08.04

[3] S. Srinivasan. "Cloud Computing Basics." Springer Briefs in Electrical and Computer Engineering. 2014.

[4] H. Tianfield. "Security issues in cloud computing." In Systems, Man, and Cybernetics (SMC), 2012 IEEE International Conference on, pp. 1082-1089. IEEE, 2012.

[5] K.M. Khan and Q. Malluhi. "Establishing trust in cloud computing." IEEE IT professional 12, no. 5, pp. 20-27. 2010.

[6] A. Vance. "Flow based analysis of Advanced Persistent Threats detecting targeted attacks in cloud computing." In Problems of Infocommunications Science and Technology, 2014 First International Scientific-Practical Conference, pp. 173-176. IEEE, 2014.

[7] M. Jensen, J. Schwenk, N. Gruschka and L. L. Iacono. "On technical security issues in cloud computing." In Cloud Computing, 2009. CLOUD'09. IEEE International Conference on, pp. 109-116. IEEE, 2009.

[8] N. Gruschka and J. Meiko. "Attack surfaces: A taxonomy for attacks on cloud services." In Cloud Computing (CLOUD), 2010 IEEE 3rd International Conference on, pp. 276-279. IEEE, 2010.

[9] C. Tankard. "Advanced persistent threats and how to monitor and deter them." Network Security no. 8, Elsevier Publishing , pp.16-19. 2011.

[10] P. Mell and T. Grance, "The NIST Definition of Cloud Computing." NIST, 2011.

[11] P. Mell, K. Scarfone and S. Romanosky, "Common Vulnerability Scoring System v3.0: Specification Document" Jun. 2011, [Online]. Available: https://www.first.org/cvss/user-guide. [Accessed: 9-Sept-2017].

[12] P. Mell, K.A. Kent, and S.Romanosky. "The common vulnerability scoring system (CVSS) and its applicability to federal agency systems." US Department of Commerce, National Institute of Standards and Technology (NIST), 2007.

[13] M.K.A.MAlnazir, A. Babiker, N. Mustafa, A.A. Hamid, and A.O. Yousif. "Performance analysis of Cloud Computing for distributed data center using cloud-sim." In Communication, Control, Computing and Electronics Engineering (ICCCCEE), 2017 International Conference on, pp. 1-6. IEEE, 2017.

[14] T. Clark. "Designing Storage Area Networks: A Practical Reference for Implementing Storage Area Networks." Addison-Wesley Longman Publishing Co., Inc., 2003.

Copyright © 2018 MECS

IPR2025-01083
Orca Security EX1011 Page 11

[15] G.A. Gibson and R.V. Meter. "Network attached storage architecture." Communications of the ACM 43, no. 11, pp.37-45. ACM 2000.
[16] P.M. Chen, E.K. Lee, G.A. Gibson, R.H. Katz, and D. A. Patterson. "RAID: High-performance, reliable secondary storage." ACM Computing Surveys (CSUR) 26, no. 2, pp.145-185. ACM 1994.
[17] B.P. Tholeti "Hypervisors, Virtualization and the Cloud." 23rd September 2011, IBM. [Online] Available: https://www.ibm.com/developerworks/cloud/library/cl-hypervisorcompare/ [Accessed 14th September 2017]
[18] F. Lombardi and R.D. Pietro. "Secure virtualization for cloud computing." Journal of Network and Computer Applications 34, no. 4, pp. 1113-1122. Elsevier 2011.
[19] C. Cachin and M. Schunter. "A cloud you can trust." IEEE Spectrum 48, no. 12, pp. 28-51. IEEE 2011.
[20] D. McCullagh, 20th June 2011. "Dropbox confirms security glitch--no password required." [Online]. Available: http://www.cnet.com/news/dropbox-confirms-security-glitch-no-password-required/ [Accessed 29th August 2017]
[21] J. Homer, S, Zhang, X. Ou, D. Schmidt, Y. Du, S. Raj Rajagopalan, and A. Singhal. "Aggregating vulnerability metrics in enterprise networks using attack graphs." Journal of Computer Security 21, no. 4 (2013): 561-597.
[22] V. Shandilya, C. B. Simmons, and S. Shiva. "Use of attack graphs in security systems." Journal of Computer Networks and Communications 2014 (2014).
[23] T. Ristenpart, E.Tromer, H. Shacham, and S. Savage. "Hey, you, get off of my cloud: exploring information leakage in third-party compute clouds." In Proceedings of the 16th ACM conference on Computer and communications security, pp. 199-212. ACM, 2009.
[24] M. Aamir and M. Arif. "Study and performance evaluation on recent DDoS trends of attack & defense." International Journal of Information Technology and Computer Science (IJITCS). Mecs-Press Publishers, 2013 Jul 1;Vol. 5No. (8):pp.54-65.
[25] L. Huan. "A new form of DOS attack in a cloud and its avoidance mechanism." In Proceedings of the 2010 ACM workshop on Cloud computing security workshop, pp. 65-76. ACM, 2010.
[26] Y.L. Huang, C. Borting , W.S. Ming, and Y.L. Chien. "Security impacts of virtualization on a network testbed." In Software Security and Reliability (SERE), 2012 IEEE Sixth International Conference on, pp. 71-77. IEEE, 2012.
[27] L.E. Olson, M.J. Rosulek, and M.Winslett. "Harvesting credentials in trust negotiation as an honest-but-curious adversary." In Proceedings of the 2007 ACM workshop on Privacy in electronic society, pp. 64-67. ACM, 2007.
[28] B. Wang, W. Song, W. Lou, and Y. T. Hou. "Inverted index based multi-keyword public-key searchable encryption with strong privacy guarantee." In Computer Communications (INFOCOM), 2015 IEEE Conference on, pp. 2092-2100. IEEE, 2015.
[29] T. Ristenpart, E.Tromer, H. Shacham, and S. Savage. "Hey, you, get off of my cloud: exploring information leakage in third-party compute clouds." In Proceedings of the 16th ACM conference on Computer and communications security, pp. 199-212. ACM, 2009.
[30] M.I. Gofman, R. Luo, P. Yang, and K. Gopalan. "Sparc: a security and privacy aware virtual machinecheckpointing mechanism." In Proceedings of the 10th annual ACM workshop on Privacy in the electronic society, pp. 115-124. ACM, 2011.
[31] J. Sahoo, S. Mohapatra, and R. Lath. "Virtualization: A survey on concepts, taxonomy and associated security issues." In Computer and Network Technology (ICCNT), 2010 Second International Conference on, pp. 222-226. IEEE, 2010.
[32] C.H. Kao, J.H. Dai, R.K , Y.T. Kuang, C.P. Lai, and C.H. Mao. "MITC Viz: Visual Analytics for Man-in-the-Cloud Threats Awareness." In Computer Symposium (ICS), 2016 International, pp. 306-311. IEEE, 2016.
[33] A. Chonka, X. Yang, W. Zhou, and A. Bonti. "Cloud security defence to protect cloud computing against HTTP-DoS and XML-DoS attacks." Journal of Network and Computer Applications 34, no. 4, pp. 1097-1107. 2011.
[34] V. Varadarajan, T. Kooburat, B. Farley, T. Ristenpart, and M. M. Swift. "Resource-freeing attacks: improve your cloud performance (at your neighbor's expense)." In Proceedings of the 2012 ACM conference on Computer and communications security, pp. 281-292. ACM, 2012.
[35] J. Fortes, "Cloud Computing Security: What Changes with Software-Defined Networking?," presented at the ARO Workshop on Cloud Security, Mar 11, 2013.
[36] S.J. Stolfo, M.B. Salem, and A. D. Keromytis. "Fog computing: Mitigating insider data theft attacks in the cloud." In Security and Privacy Workshops (SPW), 2012 IEEE Symposium on, pp. 125-128. IEEE, 2012.

Authors' Profiles

Aaron Zimba is currently a PhD candidate at the University of Science and Technology Beijing in the Department of Computer Science and Technology. He received his Master and Bachelor of Science degree from the St Petersburg Electrotechnical University in St Petersburg in 2009 and 2007 respectively. He is also a member of the IEEE and his main research interests include Network and Information Security, Cloud Computing Security and Network Security Models.

Victoria Chama is currently a Staff Development Fellow (SDF) in the Department of Computer Science and Information Technology at Mulungushi University. She holds a Bachelor's Degree in Computer Science with a distinction from Mulungushi University obtained in 2016. She has experience in Spring Java, PHP, Oracle, SQL Databases and has participated in a number of consultancy projects. Her current research interests include Software Engineering, Interface Design and Information and Communications Security.

How to cite this paper: Aaron Zimba, Victoria Chama," Cyber Attacks in Cloud Computing: Modelling Multi-stage Attacks using Probability Density Curves", International Journal of Computer Network and Information Security(IJCNIS), Vol.10, No.3, pp.25-36, 2018.DOI: 10.5815/ijcnis.2018.03.04

Copyright © 2018 MECS

IPR2025-01083
Orca Security EX1011 Page 12