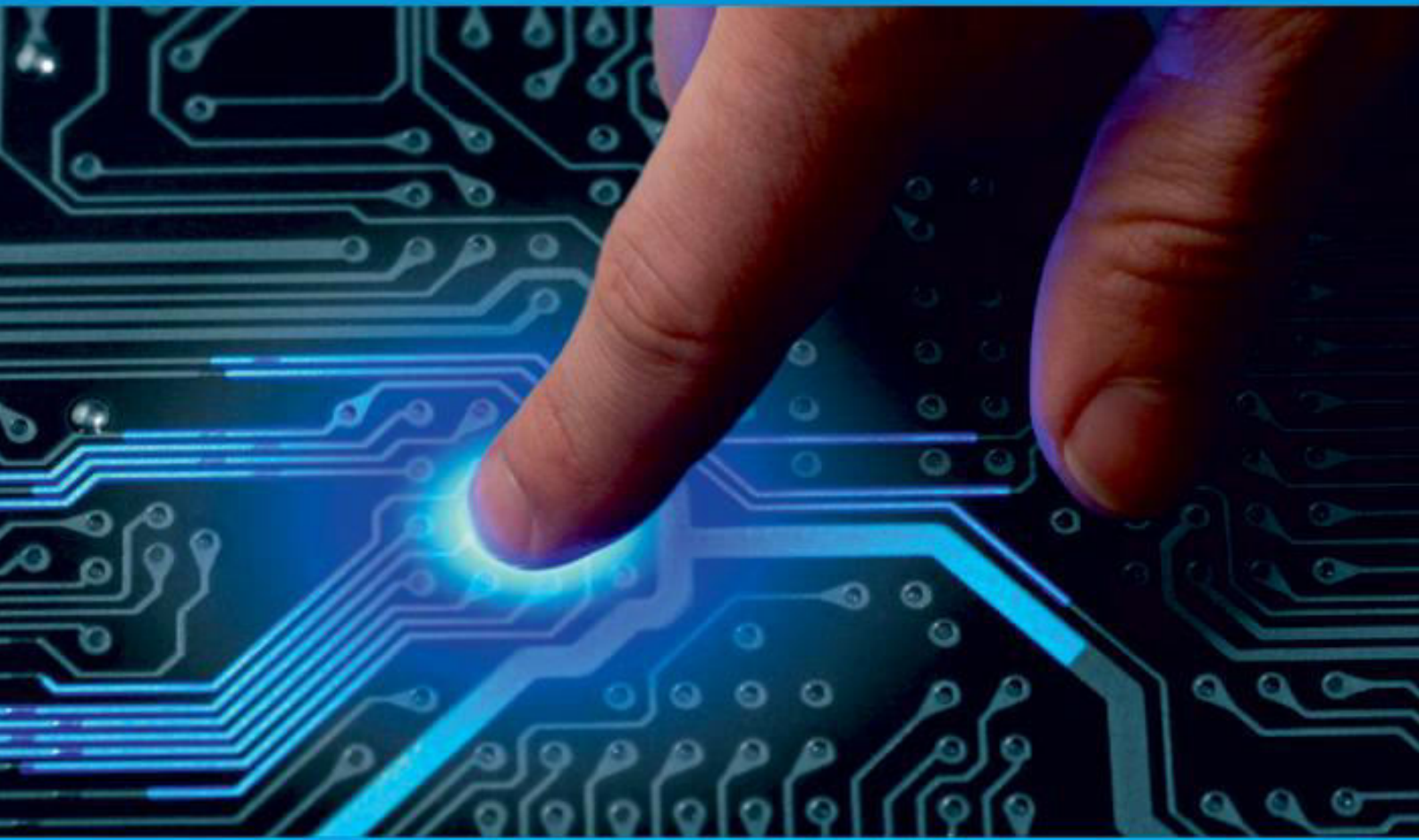




**IJIRCCCE**

e-ISSN: 2320-9801 | p-ISSN: 2320-9798



# INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH


IN COMPUTER & COMMUNICATION ENGINEERING

**Volume 9, Issue 11, November 2021**

**ISSN** INTERNATIONAL  
STANDARD  
SERIAL  
NUMBER  
INDIA

**Impact Factor: 7.542**

 9940 572 462

 6381 907 438

 [ijircce@gmail.com](mailto:ijircce@gmail.com)

 [www.ijircce.com](http://www.ijircce.com)

# A Study on Networking in Cloud Security

Anjali<sup>1</sup>, Sonu Velgeker<sup>2</sup>, Nitin Kamble<sup>3</sup>

U.G Student, School of Engineering, Ajeenkya DY Patil University, Pune, India<sup>1,2</sup>

Professor, School of Engineering, Ajeenkya DY Patil University, Pune, India<sup>3</sup>

**ABSTRACT:** A central element of managing pitfalls in cloud computing is to understand the nature of security pitfalls. The relevance of security concerns is evidenced by the efforts from both the technological organizations and academic community like ENISA, CSA and NIST, to probe security threats and vulnerabilities related to cloud systems. Provisioning secure virtual networks (SVNs) in a multi-tenant environment is an elemental aspect to insure trust in public cloud systems and to encourage their adoption. Still, comparing being SVN-oriented results is a tough task due to the lack of studies briefing the main enterprises of network virtualization and furnishing a comprehensive list of threats those results should cover. To address this issue, this paper presents a threat category for cloud networking, describing threat classes and attack scenarios that should be taken into account when designing, comparing or classifying results. The classification is grounded on the CSA trouble report, erecting upon studies and checks from the technical literature in order to extend list of threats and gives detailed analysis of cloud network virtualization issues.

**KEYWORDS:** Cloud security, Security threat, Security Taxonomy

## I. INTRODUCTION

The current concept of cloud computing evolved from technologies such as distributed computing and resource virtualization, enabling the shared computing infrastructures for delivering platforms, infrastructures and software's to different customers over the Internet. Nevertheless, cloud computing has other particular requirements such as [12]: on-demand provision of the computing resources; broad network access to configure and request computing capabilities; resources are pooled to be used by multiple customers in a multitenant model; the resources should be elastically provisioned and released; and delivered services should be transparently measured for managing and billing purposes. This new model of delivering computing power takes advantage of economies of scale, allowing cloud providers to deliver services for a reasonable cost to several institutions and companies. It also brings advantages to customers, who can pay only for what they consume instead of obliging them to purchase, install and maintain their own equipment.

Unfortunately, the advantages brought by the cloud also includes threats and security vulnerabilities which unable the full adoption by many companies. Public cloud systems utilize a multi-tenant architecture where customers should sees the cloud resources assigned to them, as if they were the sole user of the infrastructure.

Virtualization technologies play a pivotal part in administering this insulation, given that they're the main structure block in provisioning the guests' structure, including virtual machines (VMs) and virtual networks (VNs). Also, a virtualization result must insure not only that the VMs operate with insulated coffers, but also allow network business monitoring and the creation of secure network disciplines. For the same, enabling SVN in the pall computing is presently a subject of violent exploration [18]. Numerous of the being proffers calculate on open network virtualization results like Open vSwitch for defining virtualized network infrastructures with security features [10,5], fitting security modules inside VMs and virtual switches [2,1], or creating hypervisor grounded network regulators [11].

Nonetheless, identifying all of the dangers and weaknesses addressed by the various network virtualization solutions can be difficult. Indeed, number of issues can be targeted including address spoofing, preventing sniffer and traffic isolation, as well as detecting and mitigating Distributed-/Denial-of-Service (DoS/DDoS) and man-in-the-middle attacks [10,2,1,5,11]. The majority of the time, solutions presented in the literature expressly examines their (in) ability to cope with or prevent each of the existing risks.

This paper presents a threat classification for SVNs, describing threat classes and attack scenarios that should be taken into account when designing, comparing, categorizing, or evaluating solutions, in order to address this lack of uniformity in the treatment of network virtualization security proposals. This classification is based on technical reports from cloud standardization organizations such as the European Network and Information Security Agency [8], the Cloud Security Alliance [7], and the National Institute of Standards and Technology [15], as well as scientific papers [4, 16] that looked into the same issues. These reports' security difficulties do not (intentionally) provide a framework for evaluating security vulnerabilities linked to network virtualization in the cloud. As a result, the classification

presented here seeks to cover those gaps by concentrating on technological challenges connected to virtual networking in the cloud.

## II. CLOUD SECURITY ISSUES

As the demand for cloud-based systems grew, a lot of work went into identifying and categorizing security vulnerabilities in this context. ENISA [3, 8], the CSA [7], and NIST [15] have all issued security guidelines for cloud computing.

In the CSA report [7], which identifies important threats that may occur accidentally or intentionally in cloud systems, is of particular interest: it provides a clear view of the most relevant security threats when deploying and consuming cloud services, ranked by industry perspective. This research emphasizes security issues that will help cloud providers to maintain trust in their services. It's worth noting, though, that [7] is meant to be a general guideline of key security considerations, not a networking-specific guideline. Nonetheless, given its importance, it can be used as a jumping-off point for identifying important cloud networking concerns, which is exactly the strategy taken in this publication. On the basis of the CSA categorization for cloud security risks we have classified the technique for identifying security hazards in cloud networking.

## III. THREAT CLASSIFICATION

Below mentioned reports in the reference section (given in reference number: 7, 6,8,15, 9) are valuable resources for learning about cloud security issues. Their primary purpose, however, is to provide a high-level overview of potential difficulties rather than a detailed examination of how each of the numerous dangers identified applies to specific scenarios (e.g., virtual networking). On the other hand, certain works in the literature (given in the below reference link [4, 17, 14]), look into SVNs in greater depth. Unfortunately, they fail to provide a reusable taxonomy of the virtual networking hazards outlined, despite the fact that their purpose is to assess solutions and identify issues in the field. Given the importance of threat modeling in identifying security requirements [13], such works are not suited for comparing and assessing alternative virtual networking security proposals or directing the construction of complete solutions for the most significant dangers. To close the gap, we leverage the CSA's report to derive finer-grained threat classification for SVNs [7].

### 3.1 EXTENDING CURRENT CLASSIFICATIONS

The following general groups emerged from the aggregate of the detected threats according to their criteria. It's worth noting that achieving the correct level of abstraction while attempting to construct a complete perspective of virtual networking vulnerabilities in the cloud is a significant difficulty. Our proposed classification aims to be both concise and comprehensive, with two main requirements: (1) threats must have a detailed enough description to effectively guide the development of innovative solutions, and (2) the number of threat groups must be small enough to allow the classification to be applied to the analysis and comparison of common solutions. These requirements have an evident trade-off: having a big number of threat classes may result in an overly comprehensive categorization, whereas less number of threats may result in a high-level description i.e. imprecise and less valuable for comparison research. As a result, our taxonomy suggests fewer categories while still addressing significant elements of virtual networking [5,].

We analyzed many attack scenarios in the cloud platform, including who the attacker is and who is being attacked. We then aim to identify the distinct threat classes in each scenario to represent the issues that have previously been raised in the literature.

### 3.2 Cloud VN Threat Categories

We identified five virtual networking security threats, which are listed below, using the method and requirements mentioned in Section 3.1. We also show the CSA-related risks and virtual networking attacks discovered during the decomposition procedure outlined in Section 3.1 for each class. However, we should emphasize that the addition of additional threat classes to this classification should be considered a work in progress, as new discoveries in the field of cloud security are made [7,8]:

- Isolation on physical level: it will cover all vulnerabilities relating to the underlying network infrastructure's physical resources that are being shared between tenants. The majority of attacks in this category involve gathering and

analyzing data collected from shared resources, although they can also include the exhaustion of shared hardware resource [7]

- Logical Isolation: This category includes those vulnerabilities that are directly related to instances where logical resources (such as vCPUs, vLANs, and vSwitches) are not effectively isolated; allowing tenants to access each other's networking capabilities. This type of attack can take advantage of flaws in cloud virtualized network operations and network management modules [9].
- APIs that aren't secure: All hazards connected to API failures, malfunctions, and vulnerabilities in the cloud system are covered. This type of attack tries to take advantage of unsecured interfaces to gain access to or tamper with services run by other tenants or cloud administrative tools. This could result in data loss or leakage, as well as the inability to access services.
- Verification: it covers all those vulnerabilities which is caused by insufficient authentication, which allow attackers to conceal their true identities. This can be done by abusing authentication methods, collecting data traffic to get credentials and/or key materials, or via password recovery techniques.
- Authorization: This section covers all vulnerabilities linked to authorization issues, such as the ability to grant or scale rights, permissions, or credentials to or from an unauthorized user. To get privileged rights, the attacker can use a weakness in the cloud platform authorization modules, or even in the victim machine, to establish or update the victim's credentials. Authorization risks, like assaults that exploit authentication threats, can result in the disclosure of confidential data and access to management modules [7, 8].

#### IV. CLASSIFICATION ANALYSIS

This section correlates the threat scenarios with the classification proposed in Section 3.2. Threat scenario can be seen in 2 ways; the first is the Cloud Provider Network (which includes the entire cloud provider private network that allows the cloud service provisioning) and the second is the Public Network (which consist of public Internet that allows users to access the cloud services). On the basis of different entities of the cloud we can identify 3 attack scenarios:

- Tenant-to-provider
- Provider-to-tenant
- Tenant-to-Tenant

In this we will be presenting threat examples for each proposed category in both Tenant-to-Tenant and Tenant-to-Provider scenarios [8].

##### 4.1 Physical Isolation

If the attacker's VM shares the same host machine or physical network node as the victim's VM, such attacks can be carried out. In this situation, the attacker could employ a side-channel attack to crypto analyze secret traffic; use DoS/DDoS assaults to exhaust or knock down physical network resources; or acquire information about the services operating on the target machine. Sniffing is one of the most frequent attacks, in which attackers read packets passing via physical NICs in order to gain access to information from other tenants or the cloud provider network [9, 11].

Tenant-to-Tenant Scenario Threat Examples-

- 1) Side channel: it occurs when a tenant's encryption method is vulnerable to cryptanalysis using timed attacks.
- 2) Guest hopping: The attacker installs a virtual machine on the victim's host in order to take advantage of shared network components in subsequent attacks.
- 3) DoS/DDoS: Network resources shared by tenants on the same host are depleted.

Examples of threats in the Tenant-to-Provider Scenario-

- 1) Sniffing: An attacker can intercept provider management data by monitoring physical network interfaces.
- 2) Side channel: A provider's encryption scheme is vulnerable to cryptanalysis based on timing attacks.
- 3) DoS: Inside-the-cloud amplification attacks, maybe paired with address spoofing, can flood provider network infrastructure [9, 12].

##### 1.2 Logical Isolation

The cloud provider should provide resource isolation among its clients, which includes virtualized network components that make up the cloud logical network and the virtual networks of the tenants. Tenant-to-tenant attacks allow a hostile tenant to gain access to the victim's resources by breaking this logical isolation. This type of assault can result in data loss, malicious usage of other tenants' resources, and/or network service disruption.

A malevolent tenant might also exploit the cloud infrastructure to perform DoS attacks against the cloud infrastructure, its tenants, or any external targets.

Examples of Threats in a Tenant-to-Tenant Situation-

1) Open ports and running services in other tenant VMs are scanned by the attackers. 2) Network reconnaissance: Network configuration and identification protocols can be used to discover other tenants' virtual networks and/or network topologies (e.g., using ARP requests) Due to the absence of separation between virtual networks, sniffing and/or man-in-the-middle attacks are possible. 4) Malware (worm): has the ability to replicate itself between and within tenant virtual networks. 5) Botnets: Use the cloud infrastructure to set up botnets, which are groups of virtual machines (VMs) that run malicious software and attack other tenants and shared network resources.

Examples of Threats in the Tenant-to-Provider Scenario-

1) Use network reconnaissance tools to find different network topologies, virtual networks, and services. 2) Malware: it can replicate itself from a compromised tenant virtual network across the provider network architecture. 3) Botnets: Deploy botnets using cloud architecture, focusing on shared network resources and network controller nodes. 4) Replay attack: the replication of control messages, which can cause network and cloud operations to suffer (e.g., instantiating duplicated VMs) [10, 12]

### 1.3 Authentication

Tenant-to-Tenant and Tenant-to-Provider attacks that exploit authentication weaknesses are both possible. In both circumstances, the attacker may use compromised-key and/or password-based assaults to exploit the authentication protocols (example: dictionary and brute force attacks). Force authentication attacks can also be used against the authentication and identity management modules. The attacker wants to obtain access to the victim's virtual networks in a Tenant-to-Tenant scenario. The attacker may acquire access to the entire network services and/or controlling modules in a Tenant-to-Provider scenario, affecting the entire cloud [12].

Examples of Threats in a Tenant-to-Tenant Situation-

1) Credential replay: when user's credential is captured and replayed. 2) Spoofing: it is done when the hostile tenant impersonates another tenant and gains unauthorized access to resources by manipulating data.

Examples of threat on Tenant-to-Provider Scenario-

1) Credential replay: a user's credential replay might allow impersonation of a cloud administrator. 2) Spoofing: The malicious tenant performs a DNS spoofing attack, inserting bogus data into a DNS name server cache database and causing the name server to return an incorrect IP address [13,15].

### 1.4 Authorization

In this situation, the attackers are attempting to increase their system privileges. Because network privileges in the cloud are usually only relevant to the cloud provider, authorization attacks are only feasible in the Tenant-to-Provider scenario. For example, a malevolent user may impersonate them in order to obtain administrative positions, authorization to other customers' services, or access to services that are not covered by their contract [7].

Examples of Threats in the Tenant-to-Provider Scenario- 1) Network Reconnaissance: A lawful tenant can extend its privileges to execute network reconnaissance scripts in the cloud network architecture, allowing them to identify the cloud provider's network topology and use this information to launch more precise attacks against network resources. 2) Cloud Exploit Kits (Malware-as-a-Service): Malicious software that is housed inside the cloud provider's infrastructure and made available to other tenants in order to attack the provider's services via its network resources. 3) Network Programmability: The attackers attempt to increase their privileges in order to gain access to program APIs of the network devices (e.g., OpenFlow API) [12, 14].

### 1.5 Insecure APIs

API attacks can impact a wide range of cloud modules, including those in charge of resource allocation, authentication and identity management, storage, and accounting. The controller, compute, and network nodes, as well as the network modules deployed in VMs, are typically distributed across the cloud architecture. Attacks based on code injection techniques, for example, may take advantage of computer mistakes produced by processing improper input, putting cloud services and databases at risk. This type of attack could be directed at either Tenants or Providers.

Examples of threats in a Tenant-to-Tenant situation: 1) Code injection: in this attacker uses a network controller API (e.g., Neutron) to perform SQL injection in order to delete tenant data from the cloud network configuration database. Threat Examples in the Tenant-to-Provider Scenario: 1) SQL injection: The attacker uses a network controller API (e.g., Neutron) to perform SQL injection to edit (parts of) the network configuration database [13, 14].

## V. CONCLUSION & FUTURE WORK

Because of the wide range of dangers associated with cloud computing network virtualization, it's difficult to compare or categories existing virtual network security solutions. A threat classification for cloud virtual networks is mentioned in CSA report [7]. Furthermore, the taxonomy offered here provides more in-depth look at the network hazards discussed in the cloud computing literature. This finer-grained approach simplifies the analysis and design of security solutions by making it easier to identify the technologies that could be utilized to solve various security challenges in cloud networking.

We want to use this threat classification in a literature analysis of cloud networking security solutions in the future. The desired outcome is a thorough literature review that allows for not only comparing existing solutions, but also identifying gaps and issues in cloud networking security [17, 18].

## REFERENCES

- [1] Barjatiya, S. and Saripalli, P. (2012). BlueShield: A Layer 2 Appliance for Enhanced Isolation and Security Hardening among Multi-tenant Cloud Workloads. *IEEE Int. Conf. on Utility and Cloud Comp.*, pages 195–198.
- [2] Basak, D., Toshniwal, R., Maskalik, S., and Sequeira, A. (2010). Virtualizing networking and security in the cloud. *SIGOPS Oper. Syst. Rev.*, 44(4):86–94.
- [3] Catteddu, D. (2010). Cloud computing: Benefits, risks and recommendations for information security. In Serrao, C., Aguilera D'iaz, V., and Cerullo, F., editors, *Web Application Security*, volume 72 of CCIS, page 17.
- [4] Chowdhury, N. and Boutaba, R. (2010). A survey of network virtualization. *Comput. Netw.*, 54(5):862–876.
- [5] Cohen, R., Barabash, K., Rochwerger, B., Schour, L., Crisan, D., Birke, R., Minkenberg, C., Gusat, M., Recio, R., and Jain, V. (2013). An intent-based approach for network virtualization. In *IFIP/IEEE INM'13*.
- [6] CSA (2011). Security Guidance for Critical Areas of Focus in Cloud Computing V3.0. Technical report, CSA.
- [7] CSA (2013). The Notorious Nine Cloud Computing Top Threats in 2013. Technical report, CSA.
- [8] ENISA (2013). Threat landscape 2013-overview of current and emerging cyber-threats. Technical report, ENISA.
- [9] Gonzalez, N., Miers, C., Red'igolo, F., Jr. Simplicio, M., Carvalho, T., Naslund, M., and Pourzandi, M. (2012). "A quantitative analysis of current security concerns and solutions for cloud computing. *JCC*, 1(1):1–18.
- [10] Hao, F., Lakshman, T. V., Mukherjee, S., and Song, H. (2010). Secure Cloud Computing with a Virtualized Network Infrastructure. In *Proc. of the USENIX*.
- [11] Mattos, L. F. D. and Duarte, O. C. M. B. (2013). A Mechanism for Secure Virtual Network Isolation Using to Hybrid Approach Xen and OpenFlow. In *SBSeg'2013*.
- [12] Mell, P. and Grance, T. (2011). The NIST definition of cloud computing (draft). Technical report, NIST.
- [13] Myagmar, S., Lee, A., and Yurcik, W. (2005). Threat modeling as a basis for security requirements. In *SREIS*.
- [14] Natarajan, S. and Wolf, T. (2012). Security issues in network virtualization for the future internet. In *ICNC. ClassifyingSecurityThreatsinCloudNetworking* 219
- [15] NIST (2011). Guide to Security for Full Virtualization Technologies. Technical report, NIST.
- [16] Pearce, M., Zeadally, S., and Hunt, R. (2013). Virtualization: Issues, security threats, and solutions. *ACM Computing Surveys (CSUR)*, 45(2):17.
- [17] Schoo, P., Fusenig, V., Souza, V., Melo, M., Murray, P., Debar, H., Medhioub, H., and Zeghlache, D. (2011). Challenges for cloud networking security. In *MNM*.
- [18] Sun, Q. and Hu, Z. (2012). Security for networks virtual access of cloud computing. In *MINES'2012*.



**INNO**  **SPACE**  
SJIF Scientific Journal Impact Factor  
**Impact Factor: 7.542**



**ISSN** INTERNATIONAL  
STANDARD  
SERIAL  
NUMBER  
**INDIA**



# INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

 **9940 572 462**  **6381 907 438**  **ijircce@gmail.com**



[www.ijircce.com](http://www.ijircce.com)

Scan to save the contact details