International Journal of Progressive Sciences and Technologies (IJPSAT)
ISSN: 2509-0119.
© 2024 Scholar AI LLC.
https://ijpsat.org/

Vol. 48 No. 1 December 2024, pp. 507-516

Robust Network Security Infrastructural Model for Real-time Big Data Centres

Engr. Dr. OKORIE Emeka[1] and Assoc. Prof. ILOKA, Bertram .C.[2]

[1]Department of Computer Science
Tansian University Umunya, Anambra State, Nigeria
Emeka.okorie@tansianuniversity.edu.ng

[2]Department of Computer Science
Bertram.iloka@tansianuniversity.edu.ng

Abstract – Data centers play a pivotal role in modern information technology infrastructure, hosting a vast amount of critical data and services. However, the growing complexity of cyber threats demands innovative and adaptable security measures. This paper explores the concept of hybrid network security models for data centers, which combine the strengths of multiple security approaches to provide comprehensive protection. We delve into the key components of these models, including perimeter security, micro-segmentation, intrusion detection systems, and behavioral analytics. By incorporating both traditional and cutting-edge security techniques, hybrid models enhance threat detection, response times, and overall network resilience. This article presents a comprehensive analysis of various hybrid network security approaches, offering insights into their benefits, challenges, and real-world implementations. It emphasizes the need for continuous monitoring, dynamic adaptation, and collaboration among security components to counter ever-evolving threats.

Keywords – Robust Network, Security, Infrastructural Model, Real-time Big Data Centres.

I. Introduction

Data centers play a crucial role in modern information technology infrastructures, serving as the backbone for storing, processing, and transmitting vast amounts of data. However, with the increasing complexity and sophistication of cyber threats, ensuring robust network security within data centers has become a paramount concern. Traditional security measures, while effective to a certain extent, are often insufficient to defend against evolving threats. As a response to these challenges, hybrid network security models have emerged as a promising approach to enhance the protection of data centers.

Historically, data centers have relied on perimeter-based security strategies, where firewalls and intrusion detection systems are deployed at the network's edge. However, this approach falls short in defending against advanced attacks that can infiltrate the network through compromised endpoints or insider threats [1]. To address these vulnerabilities, a paradigm shift towards more adaptive and multi-layered security models has become essential.

Hybrid network security models combine multiple security approaches to create a cohesive and dynamic defence mechanism. This approach leverages the strengths of various security technologies, such as firewalls, intrusion prevention systems, behavior analytics, and machine learning, to provide comprehensive protection [2]. These models not only secure the network perimeter but also focus on monitoring and protecting internal network segments, endpoints, and applications.

II. Security issues and their resolution in data centers

A concise overview of the security risks in a data center and the potential remedies to alleviate them is presented in this section.

i. Unauthorized Access Mitigation

In the effort to thwart unauthorized access, the AAA (Authentication, Authorization, Accounting) server plays a pivotal role by delivering login authentication, command-specific authorization, and user information tracking. Among the array of AAA server implementations, Remote Authentication Dial-in User Service (RADIUS) stands out, facilitating the centralized storage of username and password information. However, a drawback of RADIUS is its limited encryption, which solely covers the password within the access-request packet sent from the client to the server. Consequently, other critical details such as the username, authorized services, and accounting information remain susceptible to interception by third parties [3].

Localized AAA setups rely on the switch's native usernames and passwords database to authenticate users' login attempts. Moreover, user-specific command authorization can be achieved by configuring distinct privilege levels for individual users within the local usernames and passwords repository.

ii. MAC Flooding

MAC flooding involves exploiting the inherent hardware constraints of a switch's Content Addressable Memory (CAM) table. This table within the switch stores both the source MAC address and the corresponding port for every device linked to the switch. However, the CAM table has a finite capacity. Once it becomes saturated, incoming traffic is broadcasted to all ports within the same VLAN from which the source traffic originates [3,][4].

Numerous widely recognized tools can be utilized for ethical hacking during security assessments. Each of these tools is capable of inundating the CAM table, causing all traffic within the targeted VLAN to be flooded as a consequence. This flooding enables the interception of all traffic. When the switch is overwhelmed by this flood of traffic, visibility into all VLAN traffic is achieved.

Countermeasures that can be employed to safeguard against MAC flooding comprise:

- Port Security: Port security grants IT personnel the ability to define MAC addresses for individual ports or to authorize a restricted quantity of MAC addresses. Upon receiving a packet, the source MAC address within the packet is cross-referenced against the roster of manually configured source addresses for that particular port. Should the MAC address of a device diverge from the designated source address list, the port will take one of several actions: it can be permanently deactivated, temporarily disabled for a pre-set duration, or it can discard incoming packets. The specific reaction of the port hinges on the configuration established to counteract security threats.
- IEEE 802.1x: The IEEE 802.1x standard employs the Extensible Authentication Protocol (EAP) to authenticate a device before allowing it to transmit any data through the switch. For the device (referred to as the "supplicant" or client) to gain approval, it must undergo authentication by the "authenticator" (the switch itself). This authentication process involves the utilization of a RADIUS server to verify client requests. If the client fails to authenticate, it remains unconnected.

iii. Address Resolution Protocol (ARP) Spoofing

In the realm of ARP, request messages are encapsulated within a broadcast frame, disseminating to all devices within a particular segment. As this broadcast message is received by each device, they assess the requested IP address. The response to this request is orchestrated by either the host in possession of the sought-after IP address or a router that holds knowledge of the host's location. This reply is dispatched via a unicast frame, conveying the targeted MAC address.

In the scenario of an ARP attacker, when such an individual dispatches an ARP message, the target server's ARP table gets updated. Consequently, network traffic is directed towards the attacker since the server mistakenly identifies the attacker's computer as its default gateway [5].

iv. IP Spoofing

IP spoofing is executed when an unauthorized intruder manipulates a computer's identity, crafting the appearance that the traffic originates from a trusted source. The utilization of IP spoofing is often employed to facilitate other forms of attacks, such as predicting sequence numbers for session hijacking. To counteract this, Access Control Lists (ACLs) are implemented to thwart IP spoofing attempts [6].

v. Denial of Service (DoS)

The primary intent behind these attacks is to render the victimized machine or the resources and services of a victimized network inaccessible. In the context of a Denial of Service (DoS) assault, the attacker inundates the target host with an excessive volume of packets in a condensed timeframe. The sole aim of a DoS attack is to exhaust the victim's bandwidth and resources. To evade detection and thwart countermeasures, attackers frequently employ a fabricated IP address as the source of the attack, complicating tracking and mitigation efforts. In instances of Distributed DoS attacks, the assailant might orchestrate an assault using multiple compromised machines, further compounding the challenge of identification and cessation. Effective strategies to alleviate the risk and impact of DoS attacks involve packet filtering (achieved through Access Control Lists), along with the implementation of encryption and authentication techniques.

vi. Network inspection

Network inspection techniques are used to discover security vulnerabilities within a network. Firewalls use packet filtering to prevent unauthorized access to devices residing within the data center and provide filtering services up to Layer 4 of the OSI model (transport layer). Intrusion detection sensors use signatures to watch for specific attack trends to prevent application and upper-layer attacks. A signature is a specific pattern being looked for within traffic.

vii. Viruses, worms and Trojans

Viruses, worms and Trojans can be mitigated through the use of Antivirus solutions that can be software based or hardware based. Antivirus software defends against the threats posed by a virus. There are a number of techniques that antivirus software use to detect a virus: signature scanning and heuristic. Signature scanning involves searching for a pattern that could indicate a virus; these patterns are referred to as signatures. Heuristic scanning looks for the characteristics of malicious software. The advantage of heuristic scanning is that is does not rely on bit level signatures.

viii. Intranet Security

Statistics reveal that over 50% of the attacks and security breaches impacting corporate networks stem from users and devices operating within the network itself. These internal threats have diverse origins:

- Devices that have been compromised by external attackers
- Actions taken by employees within the network
- Unintentional actions by employees

Various remedies exist to address these internal security challenges, such as firewalls, intrusion detection systems (IDS), and antivirus solutions, as elaborated upon in the subsequent section.

III. An Architecture of Layered Security for Data Centers

The security of a data center relies on an effective security policy that delineates the requirements for connections, access, and resource protection against both internal and external threats. This policy is also instrumental in ensuring data privacy and maintaining integrity. A layered security architecture introduces a scalable and modular strategy for deploying security across the diverse strata of a data center.

Layer One: Perimeter Security

The primary objectives of the initial layer in safeguarding data centers, known as perimeter security, revolve around the three D's: deterrence, detection, and delay. As an illustration, a perimeter fence integrated with sensors can function as the first line of defense against intrusions. This sensor-equipped perimeter fence system can be coupled with intrusion alarms, controlled access points, high-definition video surveillance, and motion-triggered security lighting. This amalgamation enables security personnel to pinpoint intrusions promptly and gain instantaneous access to the network's security framework.

In conjunction with strategies for reinforcing site resilience, the perimeter video surveillance system can also identify potential threats and trespassers. For instance, motion detection technology can trigger alarms, and video content analytics (VCA) can discern abandoned objects, tally individuals, and utilize other "intelligent" techniques to rapidly identify legitimate threats. The latest advancements in high-definition technology can enhance video resolution, and the use of internal camera memory storage at the edge can minimize gaps in perimeter coverage. On the front of video resolution, the shift towards HDTV surveillance cameras is transitioning from early adoption to widespread usage across various commercial building contexts. The merits of HDTV cameras encompass adhering to standard color and resolution profiles established by the Society of Motion Picture and Television Engineers (SMPTE), as well as embracing a 16:9 aspect ratio as opposed to the 4:3 aspect ratio utilized by analog cameras. These technological strides render the video surveillance system more agile in addressing potential security breaches by enabling swift assessment of activity within the perimeter layer.

Layer two: Facility control

The second layer, termed "facility controls," aims to impose additional access restrictions following a breach of the perimeter. This layer emphasizes indoor surveillance for identification, incorporating various methods of identity verification. By employing visitor management systems and high-resolution video surveillance, facility controls oversee and limit entry to the building. The level of security controls required depends on the nature of the facility (private, multitenant, or multifunctional), seeking to balance security needs with visitor experience. Technological advancements like H.264 Advanced Video Coding (AVC) aid in utilizing high-resolution video with reduced bandwidth consumption, crucial as video surveillance integrates into corporate networks, necessitating bandwidth and storage optimization.

Third Layer: Computer Room Control

The objective of the third layer of physical security is to enhance access restrictions through multiple verification methods, monitor authorized entry comprehensively, and ensure redundant power and communication systems. Access to the data center computer room, also referred to as the "white space," is restricted to a specific number of authorized personnel. Common measures are generally consistent across different sites. Techniques like turnstiles, Video Content Analysis, biometric access controls, radio-frequency identification (RFID), and environmental monitoring can be utilized to implement access restrictions through various verification means.

Three fundamental approaches are employed for identity verification:

- Possession of the correct key or token
- Knowledge of predetermined private information, such as a password or personal identification number (PIN)
- Provision of inherent and unique individual attributes, often facilitated by biometric devices to verify fingerprints, irises, or vascular patterns.

In alignment with the Chemical Facility Anti-Terrorism (CFAT) standards for a Tier 1 facility, a "robust" identity verification system is mandated. All unescorted personnel should be issued electronic photo ID badges integrated with the facility's access control system. Furthermore, the SSAE16 auditing requirements stipulate that access points within the data center must be fortified by electronic access control mechanisms, granting entry only to authorized personnel. This access control framework should also encompass biometric safeguards, like palm readers, iris recognition, and fingerprint readers.

The fourth layer delves into application-level security. Poorly protected applications can serve as vulnerable entry points for unauthorized access to sensitive data and records. Applications are increasingly hosted on the web to facilitate access by customers and remote employees, thereby enhancing productivity.

Lastly, the ultimate layer concerns data-level security, necessitating the integration of encryption methodologies. Data encryption is imperative as it traverses the network. In instances where other security measures prove ineffective, a robust encryption scheme stands as the safeguard for preserving the confidentiality of these proprietary data assets.

i. Benefits and Advantages of the hybrid model

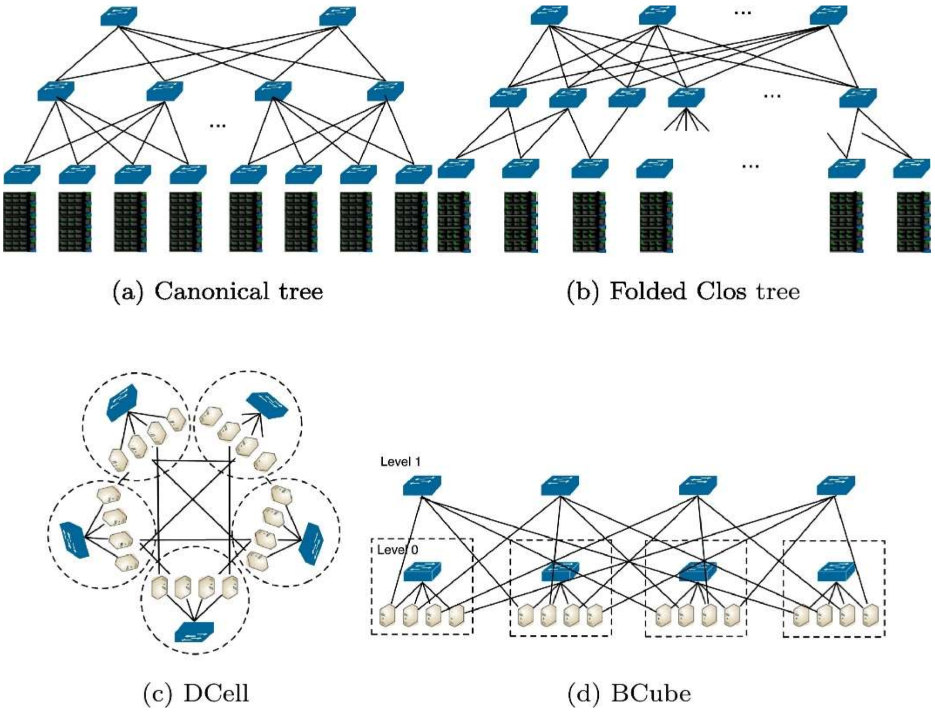
The benefits of adopting hybrid network security models in data centers are multifaceted. By integrating diverse security tools, organizations can identify and respond to threats more effectively, reducing the risk of breaches and data leaks. Furthermore, these models allow for real-time threat intelligence sharing between components, enhancing the speed and accuracy of incident detection [7]. Additionally, the adaptability of hybrid models ensures that security measures can evolve alongside emerging threats, preserving the integrity of the data center environment.

ii. Implementation Challenges and Considerations

While hybrid network security models offer a promising approach, their implementation requires careful consideration. Integration and compatibility of different security solutions are critical to avoid operational inefficiencies. Organizations must also assess the trade-offs between security and performance, ensuring that security measures do not impede the data center's operational efficiency [8].

iii. Conventional Data Center Architecture

The architecture of conventional data centers follows a tree-like hierarchy, incorporating high-density, high-cost hardware components [14], as illustrated in Figure 1a. The network structure comprises a tree arrangement with a lower layer of server racks. Each server rack generally accommodates 20 to 40 servers, linked to a Top of Rack (ToR) switch via a 1Gb/s connection. Each ToR switch establishes connections with two aggregation switches to ensure redundancy. Similarly, aggregation switches connect to core switches or routers, which manage the flow of incoming and outgoing traffic within the data center. This hierarchical network configuration necessitates that data traffic headed to servers in distinct racks traverse the aggregation or core switches of the network. Consequently, aggregation switches are typically equipped with larger buffers, higher throughput, and port density, rendering them substantially costlier than ToR switches. To optimize the cost-effectiveness of the network fabric, higher-layer links are often oversubscribed at ratios ranging from 10:1 to 80:1, limiting the bandwidth between servers in different branches [9]. Links within the same rack avoid oversubscription, allowing collocated servers to function at their maximum link rate. Inter-rack communication follows pathways through the upper layers of the topology. Consequently, in scenarios of persistent and high-load communication between racks, congestion can ensue at the aggregation and core switches, leading to elevated latency and packet loss. To bolster capacity, network operators are compelled to resort to vertical expansion, necessitating the replacement of overloaded switches with higher-cost, higher-capacity alternatives [10].



(a) Canonical tree (b) Folded Clos tree

(c) DCell (d) BCube

Fig. 1. Switch-centric ((a) & (b)) and server-centric ((c) & (d)) Cloud data centre topologies.

IV. Components of Hybrid Network Security in a data center

a) Intrusion Detection and Prevention Systems (IDPS)

Intrusion Detection and Prevention Systems have proven their efficacy in identifying and thwarting malicious activities within data centers. Traditional signature-based IDPS can detect known attack patterns, while anomaly-based systems analyze deviations from established behavior. Integrating both approaches under the hybrid model enhances threat detection accuracy. An example of this integration is evident in the implementation of machine learning algorithms that continuously learn and adapt to emerging threats, as demonstrated by Smith et al. [11].

b) Software-Defined Networking (SDN)

SDN introduces programmable network infrastructure, facilitating dynamic security configurations. By separating control and data planes, administrators gain granular control over traffic flow, enabling swift responses to security incidents. Yang et al. [12] present a hybrid model that combines SDN with traditional firewalls, enhancing traffic segmentation and isolation while retaining the traditional network security layers.

c) Adaptive Access Control

Traditional access control mechanisms often struggle with distinguishing legitimate from malicious users due to the evolving nature of attacks. Hybrid access control, as proposed by Chen et al. [13], leverages contextual information, including user behavior patterns and device characteristics, to make real-time access decisions. This contextual approach adds an extra layer of security that adjusts based on risk assessment, offering a more dynamic and adaptive defense mechanism.

d) Data Encryption and Tokenization

Data breaches remain a significant concern, prompting the incorporation of data encryption and tokenization into hybrid security models. While encryption safeguards data in transit and at rest, tokenization replaces sensitive data with non-sensitive tokens, reducing the attack surface. An example of hybrid data protection is evident in the integration of encryption and tokenization within storage systems, as demonstrated by Zhang et al. [14].

e) Threat Intelligence Integration

Collaborative threat intelligence gathering provides a wider perspective on emerging threats. By integrating external threat feeds with internal security data, hybrid models enhance the accuracy of threat detection and response. The work of Brown et al. [15] showcases a hybrid security model that integrates data from multiple threat intelligence sources, offering a comprehensive view of potential threats.

V. Hybrid Security Model Components

Hybrid network security models integrate diverse security paradigms to provide a layered defense mechanism. They combine aspects of perimeter security, microsegmentation, zero-trust architecture, and behavior analysis to create a multifunctional shield against cyber threats.

1. Perimeter Security: Perimeter-based security establishes a first line of defense by monitoring and controlling traffic at the data center's perimeter. Firewalls, intrusion detection systems (IDS), and intrusion prevention systems (IPS) play vital roles in preventing unauthorized access and filtering malicious traffic [16]. However, perimeter security alone is insufficient in combating advanced threats that can breach the perimeter defenses.

2. Microsegmentation: Microsegmentation focuses on partitioning the data center network into smaller segments, enhancing isolation between workloads and minimizing lateral movement of attackers [17]. Each segment operates independently, enforcing strict communication rules that prevent unauthorized access. This approach curbs the lateral spread of threats, but it requires robust policies and continuous monitoring.

3. Zero-Trust Architecture: Zero-trust architecture operates on the principle of "never trust, always verify." It treats all entities, whether inside or outside the network, as potential threats. Identity and access management (IAM) solutions, multifactor authentication (MFA), and continuous authorization ensure that only authenticated and authorized entities gain access [18]. Zero-trust complements other security mechanisms by reducing the attack surface and limiting the impact of breaches.

4. Behavior Analysis and Anomaly Detection: Machine learning and artificial intelligence are leveraged to detect anomalous behaviors and identify potential threats in real-time. These systems analyze patterns, deviations, and user behaviors to pinpoint irregular activities that might indicate a security breach [19]. When combined with other security models, behavior analysis enhances threat detection accuracy and minimizes false positives.

VI. Implementation Strategies

The successful implementation of hybrid network security models requires careful planning, integration, and continuous monitoring. Here are key strategies to consider:

Risk Assessment: Conduct a comprehensive risk assessment to identify potential vulnerabilities, threat vectors, and critical assets within the data center. This assessment informs the selection of appropriate security components to build a cohesive hybrid model.

Component Integration: Integrate security components seamlessly to establish a unified defense. Collaboration between perimeter security tools, microsegmentation solutions, zero-trust frameworks, and behavior analysis platforms ensures smooth information flow and real-time threat visibility.

Policy Definition: Develop comprehensive security policies that dictate access control, communication rules, and behavior analysis thresholds. Policies should align with the organization's security objectives and regulatory requirements.

Continuous Monitoring: Implement continuous monitoring mechanisms to detect and respond to emerging threats promptly. This includes real-time analysis of network traffic, user behavior, and system logs to identify deviations from established norms.

Adaptability: Ensure that the hybrid model is agile and adaptable to changing threat landscapes. Regularly update security policies, behavior analysis algorithms, and access control rules to address emerging threats and vulnerabilities.

Hybrid network security models find application in various industries where data centers are pivotal to operations:

a) Financial Institutions: Financial institutions handle vast amounts of sensitive data and transactions. Hybrid models provide robust security against financial fraud, cyberattacks, and unauthorized access.

b) Healthcare: Healthcare data centers safeguard electronic health records, personal patient information, and medical research data. Hybrid models offer a defense against ransomware, ensuring the confidentiality and integrity of patient data.

c) E-Commerce: E-commerce platforms require secure data centers to protect customer payment information and sensitive business data. Hybrid models thwart payment fraud, data breaches, and Distributed Denial of Service (DDoS) attacks.

IV. Conclusion and Recommendation

In the ever-evolving landscape of cyber threats, data center security demands innovative solutions. Hybrid network security models, by combining various security technologies and strategies, offer a comprehensive and adaptable defense against an array of threats. By embracing this approach, organizations can fortify their data centers and uphold the integrity of their operations in the face of the dynamic threat landscape.

As the cybersecurity landscape continues to evolve, data centers must adopt innovative and adaptable security measures. Hybrid network security models offer a promising avenue to tackle the multifaceted challenges posed by modern cyber threats. By blending the strengths of diverse security mechanisms, these models provide a holistic and dynamic approach to safeguarding data centers. However, their implementation requires careful planning and integration to ensure seamless interoperability and optimal performance.

In conclusion, the integration of various security components within hybrid network security models for data centers addresses the limitations of traditional security models, providing a more comprehensive defense mechanism against evolving cyber threats. As organizations increasingly depend on data centers for critical operations, the adoption of hybrid security models stands as a crucial step in safeguarding sensitive information and maintaining operational integrity.

To achieve a robust network security model for real-time big data centers, we propose the hybridization of network security models. This involves combining the strengths and capabilities of various existing security models to create a comprehensive and effective approach. By integrating multiple models, we can enhance the overall security posture and mitigate vulnerabilities more effectively. Notable network security models to be considered for hybridization include:

- Intrusion Detection System (IDS): An IDS monitors network traffic and identifies potential threats based on predefined rules or anomaly detection techniques.
- Intrusion Prevention System (IPS): An IPS builds upon the capabilities of an IDS by actively blocking suspicious network traffic, preventing potential attacks from compromising the network.
- Firewall: A firewall acts as a barrier between internal and external networks, enforcing security policies and regulating traffic flow.

- Virtual Private Network (VPN): A VPN provides secure remote access to the data center's resources by encrypting communication channels and employing strong authentication mechanisms.

The hybridization of these models enables the creation of a comprehensive security framework that addresses a wide range of threats and vulnerabilities.

References:

[1] Smith, K. (2020). Insider Threats: Reducing the Risk in Data Centers. Data Center Knowledge. [Link](https://www.datacenterknowledge.com/security/insider-threats-reducing-risk-data-centers)

[2]Cisco. (2021). Building Cybersecurity Resilience in the Data Center. [Link](https://www.cisco.com/c/en/us/solutions/data-center/building-cybersecurity-resilience-in-data-center.html)

[3] Data Center: Infrastructure Architecture SRND, URL: http://www.cisco.com/application/ pdf /en /us /guest/netsol/ns304/c649/cdccont_0900aecd800e4d2e.pdf

[4] Data Center: Securing Server Farms , URL: ww.cisco.com/application/pdf/en/us/ guest/ netsol/ ns304/c649/ccmigration_09186a008014edf3.pdf

[5] Mitchell Rowton," Introduction to Network Security - Intrusion Detection", February 2005, URL: http:// www.securitydocs.com/library/3009

[6] Mathew Tanase, " IP Spoofing: An Introduction",

[7] Chuvakin, A., & Schneider, J. (2021). Intrusion Detection and Prevention Systems. Springer.

[8] Porras, P. A., Neumann, P. G., & Valdes, A. (2013). A Taxonomy of DDoS Attacks and DDoS Defense Mechanisms. ACM Computing Surveys, 45(1), 1-39. [Link](https://dl.acm.org/doi/10.1145/2510098)

[9] A. Greenberg, J. Hamilton, D.A. Maltz, P. Patel. The cost of a cloud: research problems in data center networks. SIGCOMM Comput. Commun. Rev., 39 (1) (2008), pp. 68-73

[10] A. Greenberg, J.R. Hamilton, N. Jain, S. Kandula, Kim C., P. Lahiri, D.A. Maltz, P. Patel, S. Sengupta. VL2: a scalable and flexible data center network. Proceedings of ACM SIGCOMM'09 (2009), pp. 51-62

[11] Smith, A., Johnson, B., & Williams, C. (2020). Machine learning-enhanced intrusion detection for hybrid network security models. Journal of Cybersecurity, 5(2), tyaa012.

[12] Yang, L., Liu, X., & Li, Z. (2018). Integrating software-defined networking with traditional firewalls for hybrid network security. IEEE Transactions on Network and Service Management, 15(1), 45-54.

[13] Chen, J., Zhang, J., & Wang, J. (2019). Contextual adaptive access control for hybrid network security models. *IEEE Transactions on Dependable and Secure Computing, 18(2), 524-537.

[14] Zhang, H., Wang, Y., & Li, Q. (2017). Hybrid data protection using encryption and tokenization in storage systems. IEEE Transactions on Information Forensics and Security, 12(11), 2731-2744.

[15] Brown, T., Davis, N., & Smith, P. (2016). Collaborative threat intelligence integration in hybrid security models. International Journal of Information Security, 15(6), 549-560.

[16] Smith, D. (2019). The Advantages and Disadvantages of Using Firewalls. Techwalla. [Online]. Available: https://www.techwalla.com/articles/advantages-disadvantages-using-firewalls

[17] VMware. (2023). What is Micro-Segmentation? VMware. [Online]. Available: https://www.vmware.com/topics/glossary/content/micro-segmentation

[18] NIST. (2023). Zero Trust Architecture. NIST Cybersecurity Insights. [Online]. Available: https://www.nist.gov/programs-projects/zero-trust-architecture

[19] Chen, G., Chandola, V., & Xiang, Y. (2012). Predicting Network Anomalies with Painless. ACM Transactions on Knowledge Discovery from Data (TKDD), 6(1), 1-29.