Journal of Information Security Research

DLINE JOURNALS

Print ISSN: 0976 - 4143
Online ISSN: 0976 - 4151

JISR 2025: 16 (4)
https://doi.org/10.6025/jisr/2025/16/4/137-149

Efficient Security and AI Defence Mechanisms in Cyber Networks

[1]Farhan Nisar, [2]Baseer Ali Rehman, [3]Sana Shafiq, [4]Shum Yee Chan, [5]Rabina Safi
[1,3]Department of Computer Science and Information Technology
[2]Department of Engineering & Technology
[4,5]Qurtaba University, UOP. Pakistan
farhansnisar@yahoo.com, baseerali0007@gmail.com
sanashafiq454@gmail.comc, syeecoding@gmail.com, robinasafi@gmail.com

ABSTRACT

The document examines cloud computing security challenges, emphasizing that misconfigurations, weak identity controls, insecure APIs, and DoS/DDoS attacks are among the most critical vulnerabilities in modern cloud environments. It highlights that human error not platform flaws is the primary cause of breaches, underscoring the need for robust policy based defenses. The study's main contribution involves analyzing various DoS attack types (volumetric, protocol based, and application layer), enhancing edge router security through ACLs, rate limiting, and deep packet inspection, and validating these measures in a GNS3 network simulation environment. Key experiments demonstrate that disabling Cisco Discovery Protocol (CDP), enabling DHCP snooping, and applying port security effectively mitigate ICMP floods, rogue DHCP servers, and reconnaissance threats. The paper validates established best practices such as those from Cisco rather than proposing novel cryptographic or architectural solutions. While results show 100% mitigation of specific attacks under controlled conditions, limitations include the lack of real world deployment, the absence of AI despite the title's implication, a narrow threat scope, and a simplified network topology. Future work recommends testing in live multi cloud infrastructures, integrating AI driven anomaly detection for adaptive policy enforcement, and developing context aware threat models for hybrid cloud ecosystems. Overall, the research provides practical, simulation backed evidence that foundational Layer 2/3 security configurations significantly improve resilience against common network layer threats in cloud infrastructures.

Keywords: Cloud Security, DoS/DDoS Attacks, Misconfigurations, Identity Management Insecure APIs, Edge Router Security, GNS3 Simulation, Reactive Defense

Received: 15 April 2025, Revised 30 June 2025, Accepted 16 July 2025

1. Introduction

The rapid adoption of cloud computing as a back bone of enterprise infrastructure has brought forth new cybersecurity challenges. The integration of hybrid and multi cloud architectures increases the attack surface for adversaries who exploit vulnerabilities across virtualized and physical components. Studies show that over 63% of cyberattacks now target not only large scale enterprises but also small and medium sized organizations, primarily through network exploitation and insider compromise.

Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks remain among the most prevalent network layer threats. These attacks overwhelm legitimate services by consuming bandwidth or exploiting protocol weaknesses. Similarly, Cisco Discovery Protocol (CDP) vulnerabilities and rogue DHCP attacks jeopardize the stability and confidentiality of network infrastructures by enabling unauthorized configuration or device takeover.

This paper explores policy based configurations as a practical defense strategy to reinforce internal and external infrastructures. The proposed configurations were implemented and tested in the GNS3 simulation environment to emulate real world enterprise conditions.

2. Research Gap

Despite significant advancements in cybersecurity, existing methodologies for mitigating cloud based attacks remain inadequate in addressing emerging threats. This study identifies key vulnerabilities in cloud environments and proposes improved security strategies.

The recent research proposed risk and compliance assessment formulas, and evaluated data storage optimisation techniques compression, deduplication, and tiered storage to enhance cloud efficiency, performance, and cost effectiveness. [1] (Yanamala, 2024)

[2] Akinade presents best practices, including encryption, IAM, multi-factor authentication, audits, and threat monitoring. It emphasises shared responsibility, regulatory compliance (e.g., ISO 27001), and the fostering of a security aware culture to protect digital assets in evolving cloud environments.

In this web based world, cloud computing is rising higher by providing access to the necessary assets, applicatons, programming, equipment, and computing foundations, business procedures to control collaboration [3] (Sarvesh Kumar, 2022)

3. Major Cloud Vulnerabilities

We outline the significant cloud vulnerabilities below. Even though they are widely reported, many new ones are emerging, and we update our list of new issues.

3.1 Misconfigurations

Errors in security settings such as open data storage, overly permissive access, or disabled logging remain the top cause of cloud breaches. These are often the product of human oversight and high velocity deployment environments.

Security misconfigurations pose serious problems when security settings are not correctly defined and implemented, and default values are retained. [4] (Sergio) Cloud service misconfigurations often lead to massive data leakage or malicious code injection and have become major cloud security issues. [5] (Guffey) The solutions, such as automating security controls, enforcing Zero Trust policies, integrating security training, and strengthening regulatory compliance, are advocated to mitigate the issues, even if only partially. [6] (Olufunke)

3.2 Compromised Credentials and Weak Identity Controls

Attackers exploit stolen or weak passwords, improperly managed API keys, or unprotected service accounts. Over privileged identities, missing multi factor authentication (MFA), and plaintext secrets in source code amplify risk. The study of robust access controls, such as Identity and Access Management (IAM), Multi Factor Authentication (MFA), Role Based Access Control (RBAC), and Zero Trust Architecture (ZTA), is increasingly evident.

The prevalent vulnerabilities in cloud computing, including cloud misconfigurations, data leakage, shared technology threats, and insider threats are addressed by [7] Alquwayzani,. It emphasizes the necessity of adopting a proactive and comprehensive approach to ensure cloud security.

[8] Mostafa et al examined the identity management (IDM) in cloud computing, comparing 14 traditional and 17 centralized, decentralized, and federated IDM models. It highlights blockchain's potential especially Ethereum based smart contracts to enhance security, trust, and access control. Despite its promise, a gap remains between block chain's theoretical benefits and real world implementation, offering directions for future research.

3.3 Insecure APIs

APIs often represent the most exposed attack surface. Vulnerabilities include excessive data exposure, broken authentication, and injection flaws due to weak input validation and a lack of rate limiting.

For some individuals, the term Application Programming Interface (API) is just another buzzword shrouded in mystery, as not many are well versed in its meaning. This lack of understanding is regrettable, since APIs are vital to contemporary infrastructure, acting as one of the core means of communication for web services. Numerous businesses utilize APIs in various ways, but one aspect that often goes unnoticed is the importance of cybersecurity. [9] (Yu]

RESTful APIs have become the norm for creating web services, facilitating seamless interaction between clients and servers. Nevertheless, the widespread use of RESTful APIs has also made these interfaces vulnerable to serious security threats that can compromise the availability, confidentiality, and integrity of web services. [10] (Fatima Tanveer]

Security APIs are essential for maintaining software safety. However, improper use can create vulnerabilities, potentially resulting in significant data breaches and major financial repercussions. Complicated API design, poor documentation, and a lack of proper security training frequently lead to unintentional misuse by developers. [11] (Mousavi, Zahra]

Contemporary web applications and software systems have increasingly turned to RESTful APIs, which are more exposed to security risks like injection attacks, authentication challenges, and data leaks. This article explores the challenges associated with conducting security testing on RESTful APIs, including input validation, authentication, and authorization. [12] (Sattam J Alharb]

3.4 Zero Day and Known Vulnerabilities

Exploitation of unpatched or unknown flaws in virtual machines, containers, and orchestration layers leads to unauthorized access and persistence in cloud systems. Zero day vulnerabilities represent significant risks to corporate cybersecurity, taking advantage of undisclosed flaws in software before the release of patches. This conversation highlights the necessity of prompt identification, rapid action, and cooperation with software providers to reduce exposure and effectively manage risks. [13] (Idha Pintai)

The zero day vulnerabilities cause critical effects, and some of the solutions suggested include fast patch release, effective IDS/IPS, and a security model that involves constant vigilance and the use of behavioural analytics. [14] (Asheen Waheed)

3.5 Ransomware as a Service (RaaS)

Criminal groups increasingly target cloud backups and distributed storage through RaaS models, which use automated encryption and extortion techniques.

Cybersecurity predictions address challenges and threats caused by the pandemic, such as the massive increase in ransomware attacks in the near future. [15] (Alwashali, 2021)

An ensemble of deep learning models is used for RaaS attack detection, and these models are able to improve cybersecurity defences. [16] (Ammerdeep Singh)

3.6 Account Hijacking and Insider Threats

Credential theft and privileged misuse whether accidental or malicious give attackers direct pathways to data exfiltration or denial of service.

The feed forward back propagation algorithm of neural network techniques is found to be more useful to mitigate account hijacking. [17] (Gill and Devi).

3.7 Insecure or Abandoned Cloud Assets

Public facing endpoints or unmonitored applications allow lateral movement from low sensitivity to privileged zones within cloud networks.

The most critical risks to the serverless model are in identity and access management, a weak security posture of the supply chain, and trigger level threats. From the design stage, enforcing least privilege and multi factor authentication allows the threat to be localised and for those processes that do work, the resilience of the application can continue with reduced flexibility, scalability being no exception. [18] (Yevhen Mykhailenko). A few hard hitting defensive strategies, real time behavioral analytics, AI powered anomaly detection, zero-trust enforcement, and aggressive threat hunting are found to be strong solutions. [19] (F Harris).

3.8 Denial of Service (DoS) Attacks

Cloud infrastructure is susceptible to service disruption through volumetric or 1. application level floods, causing outages and data unavailability. Despite the availability of several mitigation measures, DoS attacks are common in several domains. Many effective solutions, including SDMTA mitigation architecture [20] (S. Kautish), and smart grid cyber security systems [21] (Mohammad Kamrul Hasan) are proposed.

3.9 Quantum Computing and Post Quantum Risk

Though emerging, the potential for future quantum attacks on classical cryptography has driven interest in post quantum encryption among critical industries. Quantum computing is a double edged sword for cybersecurity. With its awesome might, we could make startling progress in many areas and yet it has the potential to shatter, along with everything else, our existing encryption methods. Many studies examine quantum computing effects on critical infrastructures and cloud services, with careful consideration of the different layers, such as applications, data, runtime middleware, operating systems, virtualisation, hardware, storage, and network, comprehensively evaluating potential vulnerabilities. [22] Yaser Baseri,

3.10 Supply Chain and Third Party Risks

Vulnerabilities in CI/CD pipelines, misconfigured containers, and insecure third party integrations create indirect breach vectors. Cybersecurity risk of a third party's environment is hard to solve; it involves numerous technical and business dimensions which need to be fulfilled. In a cloud environment, these techno logical problems can be resolved by integrating APIs that retrieve information from the cloud environments into the data collection process to have as much information as possible for a continuous risk assessment. [23] (B.S.Pinto)

Among the above cloud vulnerabilities, Misconfiguration or human error is the prime cause, followed by exploitation of known vulnerabilities, exploitation of zero days and the absence of MFA for privileged accounts. Together, these findings indicate that the most significant weaknesses in cloud security remain in identity management, configuration control, and patch discipline rather than in underlying platform flaws.

4. Main Contribution

• Analyzing various types of DoS attacks: Conducting a comprehensive investigation into the characteristics, methodologies, and impacts of different Denial of Service (DoS) attacks including volumetric attacks (such as UDP and ICMP floods), protocol based attacks (like SYN floods and Ping of Death), and application layer attacks (such as HTTP/HTTPS floods and Slowloris). This analysis involves studying attack vectors, traffic patterns, and potential vulnerabilities in network infrastructure to better understand how these threats compromise service availability.

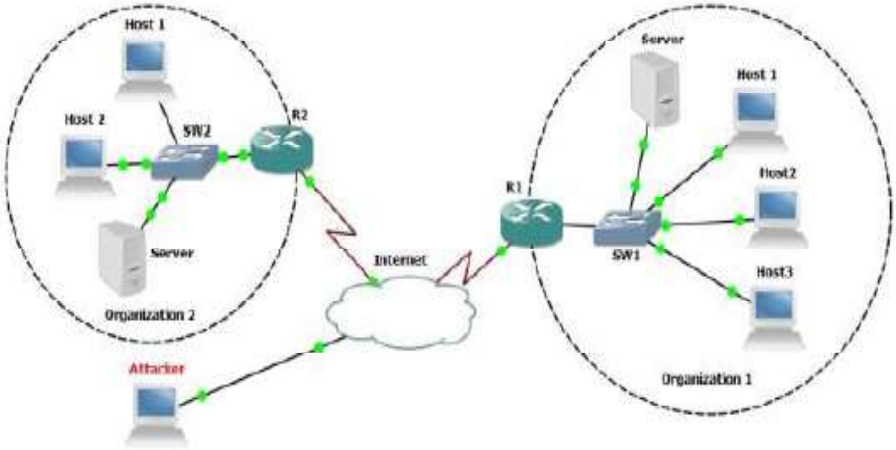
• Enhancing security mechanisms on edge network routers: Strengthening the defensive capabilities of edge routers devices that serve as the first line of defense between internal networks and external traffic by implementing advanced security features such as rate limiting, access control lists (ACLs), intrusion prevention systems (IPS), and deep packet inspection (DPI). Additionally, optimizing· router configurations to filter malicious traffic early in the communication path, thereby reducing the risk of successful DoS attacks reaching critical internal resources.

• Implementing and testing security policies in a GNS3 network simulation environment: Designing, deploying, and rigorously evaluating customized security policies within a realistic virtual network topology using GNS3

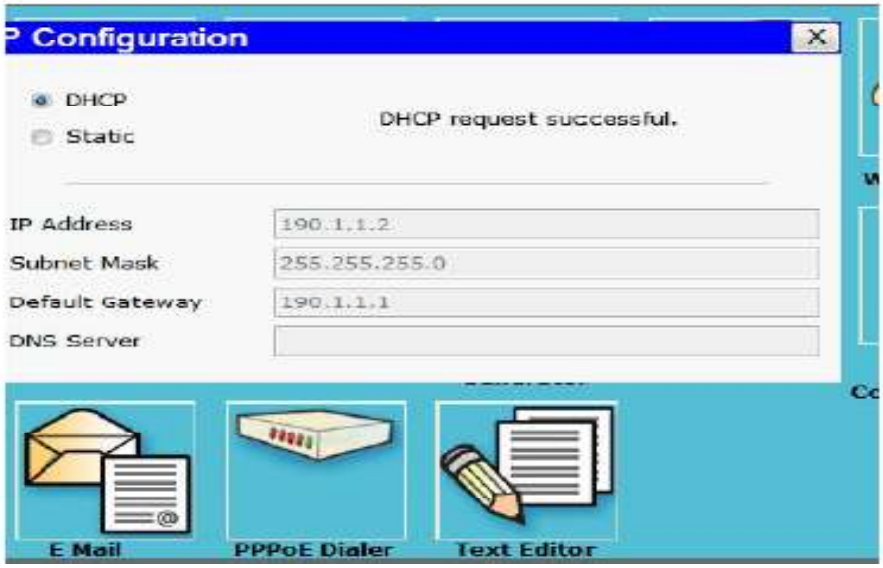
(Graphical Network Simulator-3). This includes configuring firewalls, setting up traffic filtering rules, applying Quality of Service (QoS) policies, and simulating real world DoS attack scenarios to assess the effectiveness, performance impact, and resilience of the implemented defenses under controlled conditions. The results from these simulations inform iterative improvements to the overall network security posture.

5. Simulation and Experimentation

Experiments were conducted using GNS3 simulations to evaluate the effectiveness of different security policies. The key findings are discussed below.



Port Security Atta cks: Disabling unused ports and limiting MAC addresses significantly reduces the risk of unauthorized access.



CDP Attacks: Disabling CDP on network devices mitigates vulnerabilities associated with excessive CPU utilization.

ICMP, DHCP, Port Secutity Attack with Policy Mechanism			
ICMP echo	Packet Size	Attack Success	Packet drops
100	250	98%	2
100	500	91%	9
100	750	70%	30
100	1000	67%	33
100	1500	0%	100

DHCP Attacks: Implementing DHCP snooping prevents unauthorized DHCP servers from distributing malicious configurations.

ICMP Attacks: Access control policies reduce the success rate of unauthorized ICMP traffic.

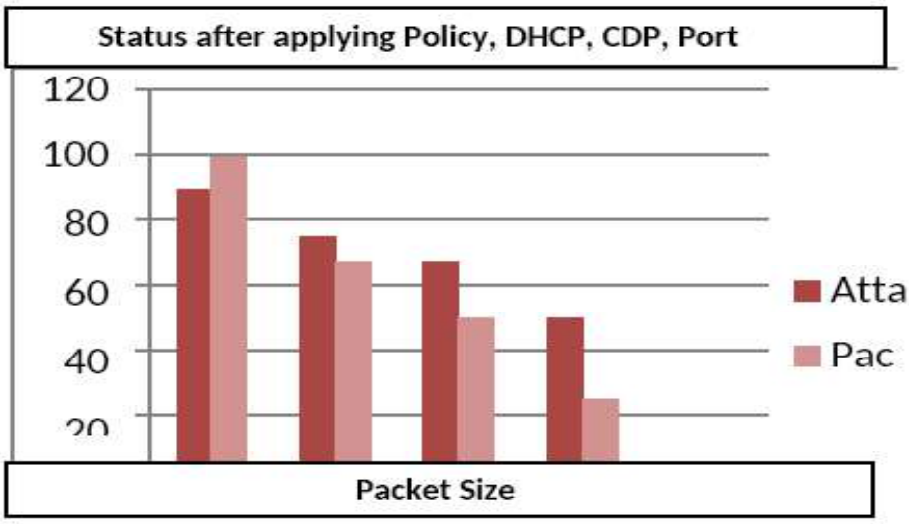
Office -R1 #

Office- R1 #

Office-R1 # sh cdp nei

Capability Codes: R- Router, T- Trans Bridge, B- source Route Bridge
S- Switch, H-Host, I- IGMP, r-Repeater, P-Phone

Device ID Local Intrfce Holdtme Capability Platform Port ID



The graph clearly illustrates the above results, highlighting the correlation between packet size and the rate of packet drops. As the packet size increases, the attack success rate and packet drop rate escalate accordingly. To mitigate this impact, the attack must be reduced to an optimal level by implementing appropriate policies on both internal and external network edges. The attack becomes progressively more effective as the packet size grows, with the packet drop rate reaching its maximum potential

Main Findings

Policy based security mechanisms significantly enhance network resilience against cyber threats. Edge device security measures effectively mitigate DoS, CDP, and DHCP based attacks. Managerial Implications Organizations should implement proactive security policies to protect cloud infrastructures. Security awareness training should be provided to employees to mitigate insider threats.Research Limitation The study is limited to simulation based analysis using GNS3. Real world implementation may require additional considerations for scalability and adaptability. Future Research Directions Expanding simulations to real world network environments. Investigating AI driven cybersecurity mechanisms for enhanced threat detection. Developing adaptive security frameworks to counter evolving cyber threats.

6. Discussion

Although the research confirms the utility of standard enterprise security policies, it offers neither architectural novelty nor cryptographic advances. The focus remains on validating best practices as recommended by Cisco's Security Guidelines rather than proposing an innovative framework. Additionally, the connection to cloud computing is infrastructural mainly; the experiments operate at the network layer, independent of platform level cloud abstractions (e.g., AWS or Azure). These limitations have been explicitly acknowledged to ensure methodological transparency.

6.1 Control and Reactive Mechanisms

These mechanisms form a layered defense strategy that combines proactive (control) and adaptive (reactive) approaches to protect network infrastructure from evolving threats particularly Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks. By integrating real time monitoring, policy enforcement, and dynamic response capabilities, the system maintains both stability and resilience in the face of malicious activity.

6.2 Firewall

The firewall serves as a foundational control mechanism positioned at strategic network boundaries typically between internal trusted zones and external untrusted networks (e.g., the internet). It continuously monitors both ingress (incoming) and egress (outgoing) traffic flows, applying a predefined set of security rules to determine which packets are permitted or denied. These rules enforce policy boundaries based on criteria such as source/destination IP addresses, port numbers, protocols (TCP, UDP, ICMP), and application layer context. By strictly regulating communication channels, the firewall prevents unauthorized access, blocks known malicious traffic patterns, and mitigates the risk of lateral movement by attackers with in the network.

6.3 Intrusion Detection System (IDS)

The Intrusion Detection System (IDS) operates as a vigilant monitoring layer that passively analyzes network traffic or host activities to identify signs of anomalous or malicious behavior. Using signature based detection

(matching known attack patterns) and/or anomaly-based detection (identifying deviations from baseline traffic behavior), the IDS can recognize indicators of compromise such as port scans, exploit attempts, or unusual traffic spikes characteristic of DoS attacks. Upon detection, it generates real time alerts and logs detailed forensic data, enabling security teams or automated systems to promptly initiate incident response procedures. While the IDS itself does not block traffic (unlike an IPS), its early warning capability is critical for timely threat containment.

6.4 ISP Edge Router

Positioned at the demarcation point between the organization's network and the Internet Service Provider (ISP), the ISP edge router plays a crucial role in the first line of defense. It is configured to perform pre filtering of incoming traffic using techniques such as Reverse Path Forwarding (RPF) checks, blackhole routing, and prefix based access control lists (ACLs). This router can drop packets with spoofed source addresses, originating from known malicious IP ranges, or exceeding baseline traffic thresholds effectively blocking or rate limiting malicious packets before they penetrate deeper in to the internal network. Collaboration with the ISP may also enable upstream filtering (e.g., via BGP Flowspec), enhancing the scale and speed of mitigation during large scale DDoS events.

6.5 Reactive Defense

Unlike static security policies, reactive defense mechanisms introduce agility and intelligence into the network's response strategy. When an ongoing attack is detected through IDS alerts, traffic anomaly detection, or firewall logs the system dynamically adapts its security policies in real time to neutralize the threat. This may involve automatically updating firewall rules to block attacker IPs, rerouting traffic through scrubbing centers, activating rate limiting thresholds, or isolating compromised segments of the network. These adaptive responses are often orchestrated through Security Orchestration, Automation, and Response (SOAR) platforms or custom scripts integrated with network management systems. By closing the loop between detection and mitigation, reactive defense significantly reduces dwell time and minimizes service disruption during active attacks.

Together, these components create a robust, multi tiered security architecture that not only prevents known threats but also intelligently responds to novel or evolving attack vectors in real time.

7. Findings

Rather than proposing new cryptographic or architectural solutions, the research validates established best practices through simulation. Using the GNS3 network emulator, the authors implement and test policy based security configurations on edge network devices. Key defensive measures include disabling CDP on untrusted ports to prevent CPU exhaustion attacks, enabling DHCP snooping to block unauthorized DHCP servers, and applying port level security such as disabling unused ports and restricting MAC addresses to prevent unauthorized access.

The experimental results demonstrate the effectiveness of these countermeasures. For instance, in ICMP flooding scenarios, increasing packet size correlates with higher packet drop rates and reduced attack success when access control policies are enforced. At a packet size of 1500 bytes, the attack success rate drops to 0%, with all malicious packets dropped. Similarly, DHCP snooping successfully thwarts rogue DHCP attacks, and CDP deactivation mitigates reconnaissance and resource exhaustion risks.

The study fills a research gap by empirically verifying that foundational Layer 2 and Layer 3 security policies when correctly applied can significantly enhance resilience against prevalent threats in simulated cloud infrastructures. While the work does not introduce novel AI based defenses (despite the title's implication), it underscores the continued relevance of configuration hardening and policy enforcement in modern network security. The findings support the adoption of these best practices by both large enterprises and smaller organizations facing escalating cyber risks. Overall, the paper provides a practical, simulation backed validation of essential network defense mechanisms in contemporary cloud environments.

8. Limitations

We acknowledge a few limitations in our paper.

1. Real World Validation: The study relies exclusively on GNS3 simulations. While useful for controlled testing, simulations may not fully capture the complexity, scale, or unpredictability of real world cloud infrastructures, limiting the generalizability of the findings.

2. Absence of AI Implementation: Despite the title suggesting the use of "AI Defense Mechanisms," the paper does not incorporate any artificial intelligence or machine learning techniques. The defenses evaluated are traditional, rule-based network policies, creating a disconnect between the title and the actual content.

3. Limited Scope of Threats Addressed: The research focuses only on a limited set of Layer 2 and Layer 3 attacks specifically ICMP flooding, rogue DHCP, and CDP exploits. It does not address more sophisticated or modern threats such as advanced persistent threats (APTs), zero day exploits, or application layer attacks.

4. Novel Contributions: We explicitly state that they do not propose new cryptographic protocols or architectural innovations. Instead, they validate existing best practices, which, while useful, offer limited advancement to the field of cybersecurity research.

5. Performance Metrics: The evaluation primarily uses packet drop rates and attack success percentages. The study lacks deeper performance analysis, such as the impact on network latency and throughput, CPU/memory overhead on devices, and scalability under high load conditions.

6. Oversimplified Network Topology: The simulated network appears to be small scale and may not reflect the heterogeneous, multi vendor, and geographically distributed nature of real enterprise cloud environments.
These limitations suggest that while we provide a proper validation of foundational security practices, their applicability to complex, dynamic, and AI driven threat landscapes remains constrained.

9. Conclusion

Main Findings: Policy based configurations substantially enhance network resilience against DoS, CDP, and DHCP-related attacks.

Edge level policy enforcement serves as a cost effective mitigation strategy for small and mid sized enterprises.

GNS3 simulations provide an effective proxy for analyzing security behavior in controlled, reproducible environments.

Managerial Implications: Organizations should adopt proactive edge security configurations as part of standard network hardening practices.

Regular training and awareness programs are essential to reduce insider threats.

Research Limitations: This work is confined to simulated environments and does not incorporate scalability testing on physical infrastructures.

Future Research Directions: Extend experimentation to real world cloud deployments.

Integrate AI driven anomaly detection and adaptive policy frameworks.

Develop context aware threat models for hybrid cloud ecosystems.

10. Future Directions

1. Extend Experimentation to Real World Cloud Deployments: The current study relies solely on GNS3 simulations, which, while useful for controlled validation, do not fully reflect the dynamic, heterogeneous, and scalable nature of real-world cloud environments. Future work should deploy and test the same policy-based security mechanisms (e.g., DHCP snooping, CDP disabling, port security) in live hybrid or multi cloud infrastructures (e.g., AWS, Azure, or private OpenStack setups). This would validate the scalability, performance overhead, and operational feasibility of these defenses under real traffic loads, diverse vendor equipment, and complex topologies.

2. Integrate AI Driven Anomaly Detection and Adaptive Policy Frameworks: Despite the paper's title referencing "AI Defense Mechanisms," no AI or machine learning components are implemented. A key future direction is to integrate AI driven systems that can detect anomalous network behavior in real time such as unusual ICMP traffic patterns or rogue DHCP server activity and dynamically adjust security policies. For example, a reinforcement learning model could auto configure switch/router rules based on threat severity, enabling self-healing networks that adapt faster than manual policy updates.

3. Develop Context Aware Threat Models for Hybrid Cloud Ecosystems: Current threat modeling in the paper is limited to generic Layer 2/3 attacks. Future research should develop context aware models that account for the unique risks in hybrid cloud environments such as cross tenant attacks, misconfigured identity providers, or data leakage between on-premises and cloud segments. These models should incorporate asset sensitivity, user behavior, workload type, and compliance requirements to prioritize and tailor defenses, moving beyond one size fits all policy enforcement.

Together, these directions would bridge the gap between foundational network hardening and intelligent, adaptive cybersecurity suited for modern cloud native enterprises.

References

[1] Yadav, Anil Kumar., Yanamala. (2024). Emerging challenges in cloud computing security: A comprehensive review. *International Journal of Advanced Engineering Technologies and Innovations 1.4, 448-479.*

[2] Akinade, Olanrewaju., Adepoju, Peter Adeyemo., Ige, Bolatito Adebimpe., Afolabi, Idowu Adeoye., Cloud Security Challenges and Solutions: A Review of Current Best Practices Afees *International Journal of Multidisciplinary Research and Growth Evaluation p. 26-35.*

[3] Kumar, Sarvesh., Gautam, Himanshu., Singh, Shivendra., Shafeeq, Mohammad. (2022). ECS - The Electrochemical Society ECS Transactions, *Vol. 107, (1) Citation Sarvesh Kumar et al 2022 ECS Trans. 107 16887.*

[4] Loureiro, Sergio. (2021). Security misconfigurations and how to prevent them, *Network Security Vol. 2021, (5).*

[5] Guffey, J., Li, Y. (2023). Cloud Service Misconfigurations: Emerging Threats, Enterprise Data Breaches and Solutions, *2023 IEEE 13th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, USA, pp. 0806-0812.*

[6] Metibemu, Cynthia, Olufunke., Oluwatoyin, Temilade., Imran, Adesokan., Ajayi, Justina Adekunbi., Tiwo, Juliana, Olufisayo., Olutimehin, Titilola Abayomi., Olaniyi, Oladeji Oluwaseun. (2025). Developing Proactive Threat Mitigation Strategies for Cloud Misconfiguration Risks in Financial SaaS Applications. *Journal of Engineering Research and Reports 27 (3), 393-413.*

[7] Alquwayzani, Alanoud., Aldossri, Rawabi., Frikha, Mounir. (2024). Prominent Security Vulnerabilities in Cloud Computing, *International Journal of Advanced Computer Science Applications, 2024, Vol 15, Issue 2, p. 803.*

[8] Mostafa, A. M., Rushdy, E., Medhat, R., Hanafy, A. (2023). An identity management scheme for cloud computing: Review, challenges, and future directions. *Journal of Intelligent Fuzzy Systems: Applications in Engineering and Technology. 45(6), 11295-11317*

[9] Conner, Yu., D. (2021). On the Usage and Vulnerabilities of API Systems. Cybersecurity Undergraduate Research. 2. https://digitalcommons.odu.edu/covacci-undergraduateresearch/2021fall/projects/2)

[10] Tanveer, Fatima., Iradat, Faisal., Iqbal, Waseem., Ahmad, Awais. (2025). Towards Secure APIs: *A Survey on RESTful API Vulnerability Detection Comput Mater Contin. 2025 84(3). P 4223.*

[11] Zahra, Mousavi., Islam, Chadni., Babar, Abuadbba, Muhammad Ali., Moore, Alsharif Kristen. (2025). Detecting Misuse of Security APIs: *A Systematic Review. Association for Computing Machinery. New York, NY, USA}, {57 (12)*

[12] Alharbi1, J Sattam., Moulah, Tarek. (2023). API Security Testing: The Challenges of Security Testing for Restful APIs. *International Journal of Innovative Science and Research Technology 1485 Volume 8, Issue 5, May 2023 P. 1485-99).*

[13] Zengeni, Pindai Idah., Zolkipli, Fadli Bin Mohamad. (2024). Zero Day Exploits and Vulnerability *Management Borneo International Journal, Vol. 7 (3), 2024, 26-33.*

[14] Waheed, Azheen., Seegolam, Bhavish., Jowaheer, Faizaan Mohammad., Sze, Lai Xin Chloe., Ethan Hua, Teo Feng., Sindiramutty, Siva Raja. (2024). Zero Day Exploits in Cybersecurity: *Case Studies and Count erme asure. Preprints. org.*

[15] Alwashali, A. M. A., Rahman, N. A. A., Ismail, N. (2021). A Survey of Ransomware as a Service (RaaS) and Methods to Mitigate the Attack, *2021 14th International Conference on Developments in Systems Engineering (DeSE), Sharjah, United Arab Emirates, pp. 92-96.*

[16] Singh, Amardeep., Abosaq, Hamad Ali., Arif, Saad., Mushtaq, Zohaib., Irfan, Muhammad., Abbas, Ghulam., Ali, Arshad., Mazroa, Alanoud Al. (2024). Securing Cloud Encrypted Data: Detecting Ransomware-as a Service (RaaS) Attacks through Deep Learning Ensemble Computers, Materials & Continual.

[17] Gill, Sumeet., Devi, Renu. (2024). Enhancing Cloud Data Security using Artificial Neural Networks for Users' Account Hijacking Security Threats *Indian Journal of Science and Technology 2024, 17(34), 3538–3552.*

[18] Mykhailenko, Yevhen. (2025). Ensuring the Security of Serverless Applications Using the Zero Trust Approach", *Universal Library of Engineering Technology, 2(3), 100-104.* DOI: https://doi.org/10.70315/uloap.ulete.2025.0203018.

[19] Harris, F., Linda. (2025). Cloud native Threat Vectors in U.S. Banking: Emerging Ransomware Tactics and *Defensive Strategies (May 11). Available at SSRN*: https://ssrn.com/abstract=5341984 or http://dx.doi.org/10.2139/ssrn.5341984.

[20] Kautish, S. R. A., Vidyarthi, A. (2022). SDMTA: Attack Detection and Mitigation Mechanism for DDoS Vulnerabilities in Hybrid Cloud Environment, *In: IEEE Transactions on Industrial Informatics, vol. 18, no. 9, pp. 6455-6463, Sept.*

[21] Hasan, Kamrul Mohammad., A. K. M., Habib, Ahasan., Islam, hayla., Safie, Nurhizam., Huda, Norul, Siti., Abdullah, Sheikh., Pandey, Bishwajeet. (2022). DDoS: Distributed denial of service attack in communication standard vulnerabilities in smart grid applications and cyber security with recent developments, 2022. *The 3rd International Conference on Power and Electrical Engineering (ICPEE 2022) 29–31 December, Singapore.*

[22] Baseri, Yaser Chouhan, Vikas., Ghorbani, Ali. (2204). Cybersecurity in the Quantum Era: *Assessing the Impact of Quantum Computing on Infrastructure arXiv:2404.10659v1 [cs.CR] 16 Apr 2024).*

[23] Pinto, B. S., Cioffi , L., Espósito, F. (2024). Third party Cloud Risk Management, *2024 IEEE International Conference on Cyber Security and Resilience (CSR), London, United Kingdom, pp. 445-451.*