Computer and Telecommunication Engineering 2025, 3(2), 3072
https://doi.org/10.54517/cte3072

Article

An efficient security framework, vulnerabilities, and defense mechanisms in LoraWAN

Farhan Nisar[1,*], Baseer Ali Rehman[2,*]

[1] Department of Computer Science and Information Technology, Qurtaba University, Peshawar 25000, Pakistan
[2] Department of Engineering & Technology, University of Engineering & Technology, Peshawar 25000, Pakistan
*** Corresponding authors:** Farhan Nisar, farhansnisar@yahoo.com; Baseer Ali Rehman, baseerali0007@gmail.com

CITATION

Nisar F, Rehman BA. An efficient security framework, vulnerabilities, and defense mechanisms in LoraWAN. Computer and Telecommunication Engineering. 2025; 3(2): 3072. https://doi.org/10.54517/cte3072

ARTICLE INFO

Received: 16 November 2024
Accepted: 13 March 2025
Available online: 1 April 2025

Abstract: The rapid expansion of cloud computing within business environments, along with the increasing complexity of organizational deployments, has led to a surge in cloud-based attacks on computer networks. These attacks exploit security vulnerabilities and systemic breaches. This study explores robust defense mechanisms by leveraging policy-based configurations and rule enforcement on edge network devices. These mechanisms were tested using GNS3 simulations to strengthen internal and external infrastructures against critical threats such as ICMP, CDP, and port security attacks.

Keywords: exploits; cybersecurity; infrastructure; denial-of-service (DoS); Internet control message protocol (ICMP); cisco discovery protocol (CDP); port-level safeguarding

1. Introduction

The exponential growth in network utilization for data storage and exchange has resulted in a significant rise in cyber threats targeting computer networks. Among these, insider attacks have become more prevalent. According to an annual cybersecurity survey, 63% of attacks target not only large enterprises but also small businesses. Denial-of-Service (DoS) attacks, where adversaries masquerade as legitimate users to exploit services, are becoming increasingly common. These attacks can originate from a single machine or as part of Distributed Denial-of-Service (DDoS) campaigns, overwhelming systems and disrupting services. Cisco Discovery Protocol (CDP) attacks pose severe risks by compromising network devices, potentially causing connectivity loss and data breaches. Encryption, decryption, and policy reinforcement strategies are commonly employed to mitigate these threats and ensure data integrity [1]. Additionally, memory allocation and advanced cryptographic algorithms are used to bolster security mechanisms. While data mining techniques have been explored for cybersecurity, they remain insufficient in fully addressing these challenges.

1.1. 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.

1.2. Research goal

This study aims to analyze and enhance security mechanisms for mitigating cyber threats in cloud environments using policy-based configurations and edge device security implementations.

1.3. Research questions

1) What are the primary security threats facing cloud-based infrastructures?
2) How effective are policy-based configurations in mitigating these threats?
3) What security improvements can be implemented to enhance cloud resilience against cyberattacks?

2. Related work

A review of existing literature on cybersecurity measures highlights previous research on DoS mitigation techniques, encryption methodologies, and security policies. Prior work has focused on firewall implementations and intrusion detection systems (IDS) to mitigate network threats. However, emerging threats necessitate a more dynamic and adaptive security framework, which this study aims to develop.

Research hypotheses

H1: Policy-based security mechanisms significantly reduce the impact of cyberattacks on cloud infrastructures. H2: Edge network security measures enhance the resilience of cloud environments against DoS and insider attacks. H3: Simulated policy enforcement in GNS3 provides a reliable model for evaluating real-world cybersecurity defenses.

3. Research methodology

This study employs a simulation-based approach using GNS3 to evaluate the effectiveness of various security policies. The methodology consists of:

1) Identifying key vulnerabilities in cloud infrastructures.
2) Implementing policy-based security configurations on edge devices.
3) Conducting simulation experiments to analyze attack mitigation effectiveness.
4) Evaluating the impact of different security policies on network performance.

3.1. Types of attacks

3.1.1. Cyber attacks

These attacks target online [2] applications such as banking, e-commerce, and trading platforms. A single host or an entire network can be affected.

3.1.2. Insider attacks

These originate from trusted individuals within an organization who exploit their knowledge of network policies and security measures to misuse confidential information.

3.1.3. Active attacks

These originated from a single compromised device and spread across the internet, affecting systems with weak security.

3.1.4. Close-in attacks

Attackers analyze network traffic, often using social engineering tactics such as phishing emails, to obtain confidential information.

3.1.5. Denial-of-Service (DoS) attacks

DoS attacks aim to overwhelm a network service by exploiting vulnerabilities, leading to service disruptions.

3.2. Types of DoS attacks

3.2.1. Port security attacks

These exploits leverage ICMP vulnerabilities to overwhelm network resources with excessive echo messages [3].

3.2.2. ICMP attacks

Attackers flood networks with ICMP_ECHO_Reply packets, consuming bandwidth and disrupting network operations.

3.2.3. CDP attacks

CDP flooding overwhelms network switches, increasing CPU utilization and degrading performance.

3.2.4. DHCP attacks

Rogue DHCP servers (**Figure 1**) assign malicious configurations to users, enabling man-in-the-middle attacks.

4. Main contribution of our work

1) Analyze different types of security as:
2) Studying different types of DoS attacks;
3) Enhance different type of security mechanism on edge network router;
4) GNS3 network to protect our network like
5) CDP, DHCP, ICMP, and port security attacks.

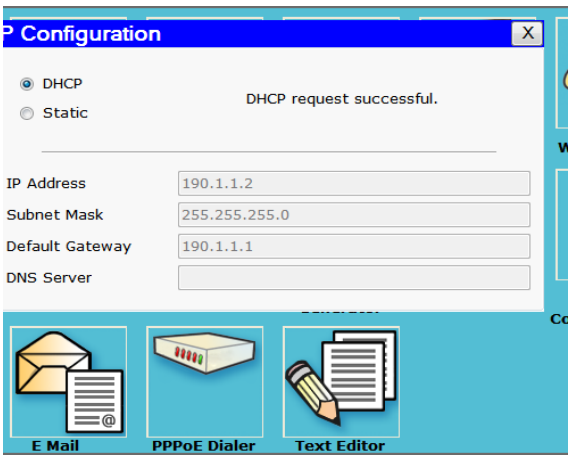

Figure 1. DHCP server.

5. Simulation and experimentation

i) For the port, from the network port security is used for inside organization security because the attack ratio will be random and communication from source to destination will be random. It is necessary that when any attacker or intruder connects the port, it will disconnect the interface automatically by using this command [4,5].

The results above provide a clearer depiction of the packet drop status. As the volume of packets increases, the rate of packet drops correspondingly escalates, necessitating a reduction in the intensity of the attack to maintain an optimal operational threshold. We apply policies on all router edges and switch off all interfaces when not in use and also disable the ping command.

6. Control mechanisms

6.1. Firewall

Monitors and controls network traffic, preventing unauthorized access.

6.2. Intrusion detection system (IDS)

Detects and alerts network administrators about suspicious activities.

6.3. ISP edge router

Monitors and filters incoming and outgoing traffic to prevent attacks.

6.4. Reactive mechanisms

Immediately respond to threats, reducing the impact of ongoing attacks.

7. Main contribution

Analyzing various types of DoS attacks. Enhancing security mechanisms on edge network routers. Implementing and testing security policies in a GNS3 network simulation environment.

8. Simulation and experimentation

Experiments were conducted using GNS3 simulations to evaluate the effectiveness of different security policies (**Figure 2**). Key findings include:

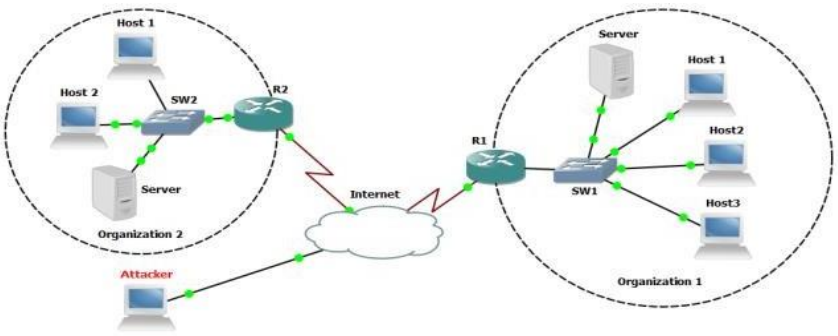

Figure 2. GNS simulator.

Port security attack

Disabling unused ports and limiting MAC addresses (**Figure 3**) significantly reduces the risk of unauthorized access.

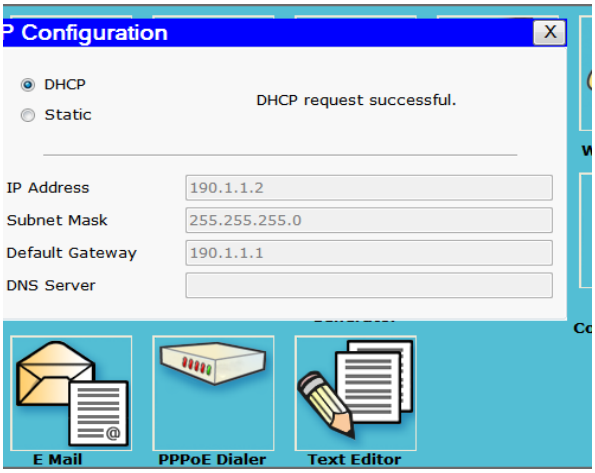

Figure 3. DHCP request.

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

Table 1. ICMP, DHCP, port security 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 (**Figure 4**). ICMP Attacks: Access control policies reduce the success rate of unauthorized ICMP traffic (see **Table 1**).

```
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
```

Figure 4. GNS simulator.

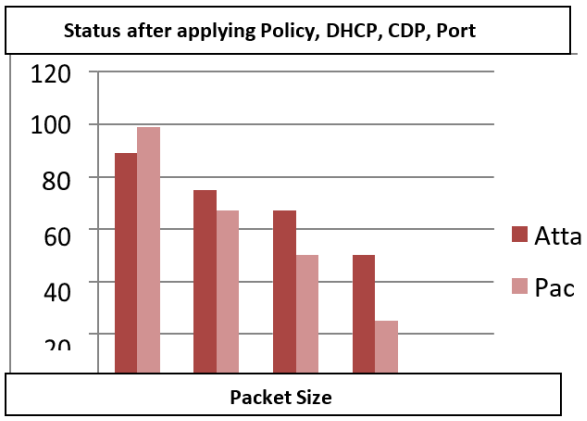

Figure 5. Attacks control.

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 (**Figure 5**). 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.

9. Conclusions

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.

Author contributions: Conceptualization, FN and BAR; methodology, FN; software, FN; validation, FN and BAR; formal analysis, FR; investigation, BAR; resources, BAR; data curation, FN; writing—original draft preparation, BAR; writing—review and editing, FN; visualization, BAR; supervision, BAR; project administration BAR; funding acquisition, FN. All authors have read and agreed to the published version of the manuscript.

Institutional review board statement: Not applicable.

Informed consent statement: Not applicable.

Conflict of interest: The authors declare no conflict of interest.

References

1. National Institute of Standards and Technology. NIST Cybersecurity Framework 2.0. Available online: https://en.wikipedia.org/wiki/NIST_Cybersecurity_Framework (accessed on 2 November 2024).
2. Goodin D. An AWS Configuration Issue Could Expose Thousands of Web Apps. Available online: https://www.wired.com/story/aws-application-load-balancer-implementation-compromise (accessed on 2 November 2024).
3. Sanger M. Dozens of Former Officials Chart Course for Next Administration's Cyber Policies. Available online: https://www.politico.com/news/2024/10/22/former-officials-next-administration-cyber-policies-00184854 (accessed on 2 November 2024).
4. Telford T. Quantum Chips Pose Huge Threat to Data Encryption. Available online: https://www.theaustralian.com.au/business/qanapi-boss-trent-telford-says-quantum-computing-could-blow-apart-current-data-encryption/news-story/c9e2b014fefb298d902f7516744d39fb (accessed on 2 November 2024).
5. Smith J. Battle Begins to Stop Quantum Computers Smashing Cyber Defences. Available online: https://www.thetimes.co.uk/article/battle-begins-to-stop-quantum-computers-smashing-cyber-defences-rzmlwqw7f (accessed on 2 November 2024).