Naif Arab University for Security Sciences
Journal of Information Security and Cybercrimes Research
مجلة بحوث أمن المعلومات والجرائم السيبرانية
https://journals.nauss.edu.sa/index.php/JISCR
JISCR

Quantitative Comparative Analysis of Traditional, Virtualized, and Cloud-Based DMZ Architectures for Securing Local Area Networks

Roger Kasongo[1]* and Justin Nduhura Munga[2]

[1]Department of Mathematics, Statistics and Computer Science, University of Kinshasa, Kinshasa, Democratic Republic of the Congo.

[2]Department of Mathematics and Computer Science, University of Kinshasa, Kinshasa, Democratic Republic of the Congo.

Received 13 Jan. 2026; Accepted 31 Mar. 2026; Available Online 24 Jun. 2026

Abstract

Demilitarized Zone (DMZ) architectures are widely deployed to protect Internet-facing services in local area networks. However, their quantitative security effectiveness across physical, virtualized, and cloud-based environments remains insufficiently documented. This study presents a structured and reproducible quantitative comparison of these DMZ architectures using controlled and simulated cyberattack scenarios. Security performance was evaluated using measurable indicators including intrusion probability, recovery time, and service availability. The experimental analysis demonstrates that DMZ deployment significantly reduces successful intrusion probability and improves network resilience compared to non-segmented architectures. Physical DMZ architectures provide the highest isolation level, while virtualized and cloud-based environments DMZs offer improved scalability and faster recovery capabilities. The results contribute a quantitative evaluation framework to support secure network architecture design and provide insights for integrating DMZ with modern security paradigms such as Zero Trust.

I. Introduction

The rapid expansion of Internet-based services has profoundly transformed the design and operation of local area networks (LANs). Services such as web applications, mail servers, and remote access platforms are now commonly deployed within local infrastructures while remaining directly accessible from public networks. Although this connectivity improves service availability and operational efficiency, it also significantly increases exposure to cyber threats, including unauthorized access, denial-of-service (DoS) attacks, malware propagation, and lateral movement toward internal resources [1], [2].

To mitigate these risks, modern network security architectures rely heavily on segmentation and perimeter defense mechanisms that separate Internet-facing services from internal network resources [15]. Among these mechanisms, the Demilitarized Zone (DMZ) has become a fundamental architectural component for enhancing information and network security. A DMZ typically

Keywords: Cybersecurity, demilitarized zone (DMZ), intrusion probability, network security, network segmentation, risk modeling, service availability, zero trust.

Production and hosting by NAUSS

* Corresponding author: Roger Kasongo
Email: roger.kasongo@unikin.ac.cd

doi: 10.26735/LODJ7903

hosts public services within a dedicated network segment, isolated from the internal LAN by one or more security devices such as firewalls and intrusion detection systems. This architectural approach aims to reduce the attack surface and limit the impact of successful intrusions by containing them within controlled network boundaries [3].

Despite their widespread adoption, DMZ implementations vary considerably depending on organizational requirements, technological constraints, and deployment environments. Traditional DMZ architectures based on single-firewall or dual-firewall designs coexist with more recent approaches leveraging virtualization technologies and cloud infrastructures. Each of these implementations presents specific trade-offs in terms of security effectiveness, scalability, operational complexity, and service availability. Consequently, evaluating the effectiveness of DMZ architectures requires not only a qualitative discussion of design principles but also a quantitative assessment of their impact on network security and resilience [4].

Recent research has also emphasized the importance of automated security validation and quantitative approaches to network protection mechanisms to improve resilience against evolving cyber threats [18], [19].

This paper investigates the role of DMZ-based architectures in securing Internet-facing services deployed within local area networks. The primary objective is to analyze different DMZ deployment strategies and to assess their effectiveness using quantitative security indicators. Simulated yet realistic attack scenarios are employed to compare physical, virtual, and cloud-based DMZ implementations with respect to intrusion probability, recovery time, and service availability.

The remainder of this paper is organized as follows. Section II reviews related work on network security architectures and DMZ deployment strategies. Section III presents the problem statement and research hypothesis. Section IV describes the DMZ architectures and use cases considered in this study. Section V details the quantitative analysis methodology and risk modeling approach. Section VI discusses the experimental results and their implications for securing Internet services. Finally, Section VII concludes the paper and outlines directions for future research.

II. Related Work

A. Role of Demilitarized Zones in Network Security

The concept of the Demilitarized Zone (DMZ) has long been recognized as a foundational mechanism for protecting Local Area Networks (LANs) against external threats. Originally derived from military terminology, the DMZ concept was adapted to network security to create a controlled buffer zone between untrusted external networks and sensitive internal resources [8], [11]. In modern LAN environments, DMZs are widely deployed to host publicly accessible services such as web servers, mail servers, and DNS servers, thereby reducing direct exposure of internal systems to the Internet [1], [4].

Several studies emphasize that the primary security benefit of a DMZ lies in its ability to limit lateral movement following a compromise. By isolating exposed services within a dedicated network segment, attackers who successfully exploit a public-facing service are constrained within the DMZ and prevented from directly accessing internal resources [5], [6]. This architectural separation significantly reduces the overall attack surface and supports defense-in-depth strategies.

B. DMZ Deployment Strategies and Best Practices

The effectiveness of a DMZ is highly dependent on its design and deployment strategy. Industry guidelines and academic studies consistently highlight the importance of strict network segmentation, well-defined access control rules, and comprehensive traffic filtering policies [2], [3]. Firewalls play a central role in enforcing security boundaries between the Internet, the DMZ, and the internal LAN.

Traditional deployment strategies typically rely on either single-firewall or dual-firewall architectures. Single-firewall DMZs offer a basic level of protection and are relatively easy to deploy, but they introduce a single point of failure and are highly sensitive to configuration errors. In contrast, dual-firewall architectures enforce independent

security policies at each boundary, providing stronger isolation and improved resilience against misconfiguration or device compromise [3].

C. Security Benefits and Operational Impact of DMZ Architectures

Numerous studies report that the implementation of a DMZ leads to measurable improvements in network security posture [10]. These benefits include enhanced protection of sensitive resources, improved monitoring of inbound and outbound traffic, and increased effectiveness of intrusion detection and response mechanisms [4], [9].

By centralizing security controls at strategic network boundaries, DMZ-based architectures facilitate better visibility into attack attempts targeting public services. This visibility enables faster incident response and supports proactive threat mitigation, particularly when combined with intrusion detection systems (IDS) and continuous log analysis [7].

D. Quantitative Approaches to DMZ Security Evaluation

While qualitative discussions of DMZ benefits are abundant, recent research increasingly emphasizes the need for quantitative evaluation of DMZ effectiveness. Quantitative approaches typically focus on indicators such as attack frequency, intrusion probability, recovery time, and service availability to assess the real impact of DMZ deployment [6], [13].

Simulation-based models and estimated risk analyses are commonly used to evaluate different architectural configurations under controlled attack scenarios. These models provide valuable insights into how various DMZ designs influence security outcomes and help identify trade-offs between protection level, performance, and operational complexity.

E. DMZ in Virtualized and Cloud-Based Environments

The evolution of network infrastructures toward virtualization and cloud computing has led to the adaptation of traditional DMZ concepts to new deployment environments. Virtual DMZs leverage hypervisors and software-defined networking to achieve flexible segmentation, while cloud-based DMZs rely on provider-managed security services to isolate Internet-facing workloads [4].

Research indicates that cloud and virtual DMZs offer advantages in scalability and deployment flexibility, but they also introduce challenges related to visibility, shared responsibility models, and dependency on external providers [9], [17]. To address these challenges, modern DMZ implementations increasingly integrate identity-based access control, continuous monitoring, and policy automation mechanisms.

F. Challenges and Limitations Identified in Existing Studies

Despite their effectiveness, DMZ architectures are not without limitations. Common challenges reported in the literature include configuration complexity, maintenance overhead, and the risk of misconfiguration leading to unintended exposure of internal resources [3], [4]. Additionally, static perimeter-based models may be insufficient to address modern threats such as insider attacks and advanced persistent threats.

These limitations highlight the need for evolving DMZ designs that incorporate emerging security paradigms such as Zero Trust architectures [12], [20], automated security validation, and advanced threat modeling techniques. Recent research highlights the importance of quantitative evaluation and formal modeling in network segmentation and DMZ architectures [18], [19].

G. Positioning Summary

This review demonstrates that, while DMZ architectures remain a cornerstone of LAN security, existing work either focuses on qualitative design principles or lacks comprehensive quantitative comparison across modern deployment models. The present study builds upon these foundations by providing a quantitative, comparative analysis of traditional, virtual, and cloud-based DMZ architectures using realistic attack scenarios.

III. Problem Statement and Research Hypothesis

A. Problem Statement

The increasing exposure of local area networks to Internet-based services has significantly amplified the complexity of securing internal resources against external threats. While Demilitarized Zones (DMZs) are widely recognized as an effective architectural solution for isolating public-facing services, their real-world effectiveness varies considerably depending on deployment strategies, technological environments, and security configurations.

Existing studies on DMZ architectures predominantly emphasize qualitative design principles and best practices. Although these contributions provide valuable guidance for network design, they often lack quantitative evidence that clearly demonstrates how different DMZ implementations influence security outcomes such as intrusion probability, recovery time, and service availability. Furthermore, the evolution of network infrastructures toward virtualization and cloud computing has introduced new DMZ deployment models whose security implications are not yet sufficiently quantified or compared with traditional physical architectures.

As a result, network designers and administrators face challenges when selecting appropriate DMZ architectures, as decisions are frequently based on conceptual arguments rather than measurable security indicators. This lack of quantitative comparison limits the ability to objectively assess the trade-offs between security effectiveness, operational complexity, and resilience across different DMZ deployment models.

B. Research Objectives

To address the aforementioned challenges, this study aims to provide a systematic and quantitative evaluation of DMZ architectures used to secure Internet-facing services in local area networks. The specific objectives of this research are as follows:

1) To analyze and classify traditional, virtualized, and cloud-based DMZ architectures commonly deployed in modern network environments.
2) To evaluate the security effectiveness of these architectures using quantitative indicators, including intrusion probability, recovery time, and service availability.
3) To compare the resilience and operational impact of different DMZ deployment models under simulated yet realistic attack scenarios.
4) To identify architectural design choices that significantly influence network security and service continuity.

C. Research Hypothesis

Based on the analysis of existing literature and the architectural principles underlying DMZ deployment, this study formulates the following hypothesis:

H1: Properly designed DMZ architectures significantly reduce the probability of successful intrusions and improve network resilience and service availability compared to non-segmented or weakly segmented network architectures.

In addition, the study explores the assumption that advanced DMZ implementations, particularly those based on virtualization and cloud infrastructures, can offer enhanced scalability and recovery capabilities while maintaining an acceptable level of security when appropriate controls are applied.

D. Scope of the Study

This research focuses on the evaluation of DMZ architectures deployed to protect Internet-facing services within local area networks. The analysis is limited to simulated environments designed to reflect realistic operational conditions and attack scenarios. While the results provide meaningful insights into architectural effectiveness and comparative performance, they are intended to support architectural decision-making rather than replace comprehensive security audits in production environments.

E. Threat Model and Security Assumptions

To ensure a structured and realistic security evaluation, this study defines an explicit threat model describing attacker capabilities, attack

vectors, and system assumptions.

The attacker is assumed to be an external entity located on the public Internet with no prior authorized access to the internal network. The attacker can perform common cyberattack techniques targeting Internet-facing services, including Distributed Denial of Service (DDoS), port scanning, SQL injection, phishing, and malware injection.

The attacker's objective is to compromise services hosted in the DMZ and potentially gain unauthorized access to internal network resources.

- The firewall and intrusion detection systems are correctly configured and operational.
- The DMZ enforces network segmentation between external and internal networks.
- Internal network systems are not directly accessible from the Internet.
- Security monitoring systems generate accurate event logs.

This threat model provides a realistic and controlled framework for evaluating the effectiveness of different DMZ architectures under comparable attack conditions.

The following section presents the DMZ architectures and use cases considered in this study. It details the structural characteristics of traditional, virtualized, and cloud-based DMZ implementations that form the basis for the quantitative analysis.

IV. DMZ Architectures and Use Cases

This section describes the Demilitarized Zone (DMZ) architectures considered in this study and defines the use cases on which the quantitative analysis is based. The selected architectures represent commonly deployed security models in enterprise and institutional local area networks and reflect both traditional and modern deployment environments.

A. Overview of DMZ-Based Network Segmentation

1) Conceptual Model of Quantitative DMZ Security Evaluation: This study is based on a conceptual security evaluation model designed to quantitatively assess the effectiveness of different DMZ architectures under controlled attack scenarios. The model consists of four main components: the external attacker, the DMZ security layer, the protected internal network, and the security monitoring and analysis module.

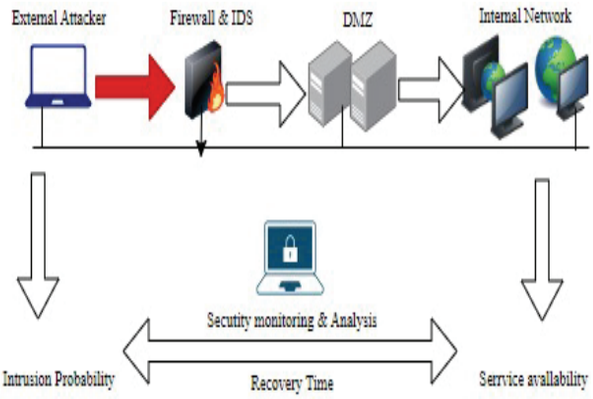

Fig. 1. Conceptual model.

The attacker generates cyberattack attempts targeting Internet-facing services hosted in the DMZ. The firewall and intrusion detection systems enforce security policies and record security events. These events are analyzed to compute quantitative security metrics, including intrusion probability, recovery time, and service availability.

This conceptual model establishes the relationship between network architecture, attack scenarios, and measurable security outcomes, providing a structured framework for comparative security evaluation. Fig. 1 illustrates the conceptual model for quantitative evaluation of DMZ security architectures.

A Demilitarized Zone is a dedicated network segment designed to host Internet-facing services while maintaining strict isolation from the internal local area network. The DMZ acts as an intermediate security zone between untrusted external networks and trusted internal resources. Communication between these zones is governed by security devices such as firewalls and intrusion detection systems, which enforce predefined access control and traffic filtering policies.

In the context of this study, the DMZ hosts public services that are directly accessible from the Internet, while the internal LAN contains critical resources that must be protected from unauthorized access. This segmentation principle forms the

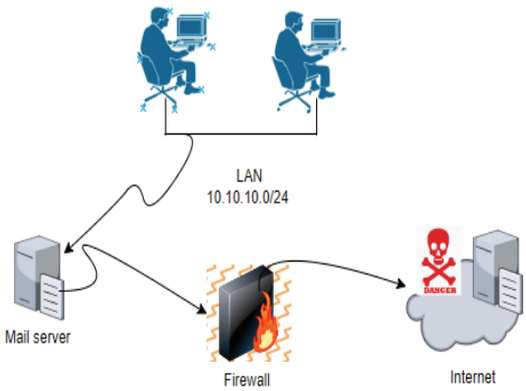

Fig. 2. DMZ-less architecture.

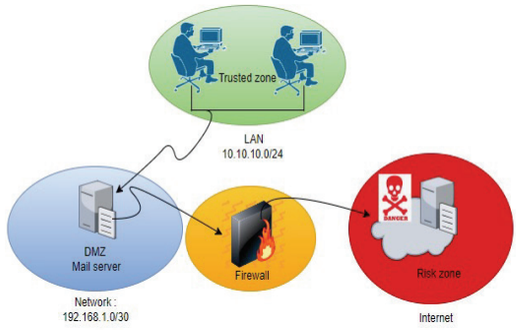

Fig. 3. Traditional DMZ architecture with a single firewall.

basis for all architectural configurations analyzed in the following subsections.

B. Security Risks of DMZ-less Architectures

Network infrastructures without a DMZ are particularly vulnerable to a wide range of cyber threats. Common risks include rapid propagation of malware, unauthorized access to sensitive systems, ineffective intrusion detection, and limited control over inbound and outbound traffic flows [3].

In such environments, a successful compromise of a public-facing service can directly impact the entire LAN, as no isolation mechanism exists to contain the attack. This scenario highlights the limitations of flat network architectures and underscores the necessity of segmentation as a fundamental security principle.

Fig. 2 illustrates a traditional network architecture without a demilitarized zone, where Internet-facing services are directly connected to the internal local area network.

C. Traditional Physical DMZ Architectures

1) Single-Firewall DMZ Architecture : The single-firewall DMZ architecture is one of the earliest and most widely adopted DMZ deployment models. In this configuration, a single firewall device is equipped with multiple network interfaces, each corresponding to a specific security zone: the external network (Internet), the DMZ, and the internal LAN.

Traffic between these zones is controlled through firewall rules that permit only explicitly authorized communications. While this architecture is relatively simple to deploy and manage, it introduces a single point of failure and requires careful configuration to prevent unintended access paths. As a result, its effectiveness is strongly dependent on the correctness and consistency of security policies [2].

Fig. 3 presents a network architecture incorporating a demilitarized zone using a single-firewall configuration.

a) Limitation of Single-Firewall DMZ Architectures: Although single-firewall DMZ configurations offer improved security compared to DMZ-less architectures, they remain vulnerable to misconfiguration and single points of failure. A compromised or improperly configured firewall may allow unauthorized access to internal resources, thereby undermining the intended isolation between network zones [3].

2) Dual-Firewall DMZ Architecture: In the dual-firewall DMZ architecture, two independent firewall devices are used to separate the Internet from the DMZ and the DMZ from the internal LAN. The first firewall controls inbound and outbound traffic between the Internet and the DMZ, while the second firewall enforces isolation between the DMZ and internal resources.

This layered approach provides stronger security guarantees by applying defense-in-depth principles and reducing the impact of misconfiguration or compromise of a single device. Dual-firewall DMZs are commonly deployed in

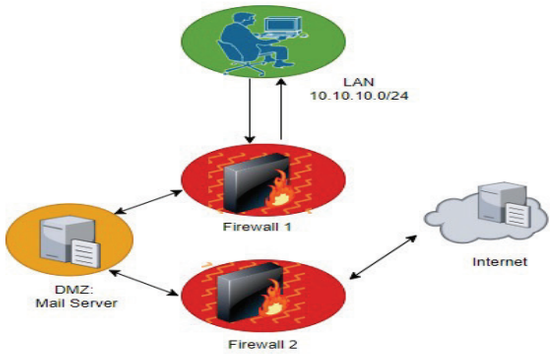

Fig. 4. DMZ with dual firewalls

environments hosting critical services that require enhanced protection and higher fault tolerance.

Fig. 4 illustrates a dual-firewall DMZ architecture providing enhanced isolation between external networks, the DMZ, and internal resources.

3) Security Benefits of Dual-Firewall DMZ Designs: Empirical studies and attack simulations demonstrate that dual-firewall architectures reduce intrusion success rates and improve recovery times compared to single-firewall designs. By enforcing independent security policies, dual-firewall DMZs provide higher resilience against both external and internal threats, directly supporting Hypotheses H1 [7].

D. Virtualized DMZ Architectures

Virtualized DMZ architectures extend the traditional DMZ concept by leveraging virtualization technologies to implement network segmentation within shared physical infrastructures. In this model, DMZ services are deployed as virtual machines or containers, and isolation is enforced through virtual switches, virtual firewalls, and software-defined networking mechanisms.

Virtual DMZs offer increased flexibility and scalability, enabling rapid deployment and dynamic reconfiguration of security policies. However, they also introduce additional dependencies on hypervisor security and require effective monitoring to maintain visibility across virtualized network layers.

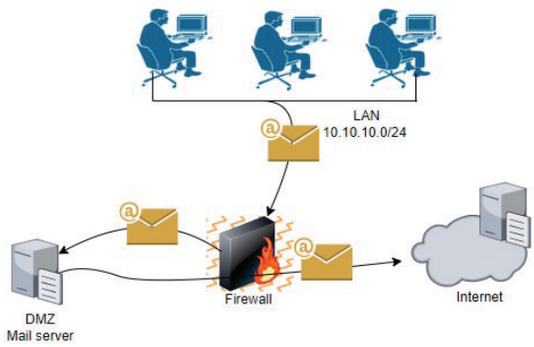

Fig. 5. Simulation of email communication through a DMZ.

E. Email Communication Simulation in DMZ Environments

To illustrate the practical impact of DMZ architectures on traffic control, an email communication scenario is considered. In this simulation, internal users send and receive emails through a mail server deployed within the DMZ. Communication between the LAN and the mail server is restricted to specific protocols, such as SMTP for sending emails and IMAP or POP3 for retrieval. The firewall enforces strict protocol and port-based filtering, ensuring that the mail server cannot initiate arbitrary connections to internal systems. This controlled communication flow demonstrates how DMZ deployment effectively limits attack vectors while maintaining service availability [2].

Fig. 5 depicts the simulated mail communication flow through the DMZ.

F. Comparative Analysis of Architectures with and Without DMZ

A comparative evaluation of network architectures with and without DMZ deployment highlights the security advantages of segmented designs. DMZ-based architectures significantly reduce intrusion probability, improve containment of compromised services, and enhance overall network resilience.

These observations provide a qualitative foundation for the quantitative analysis presented in Section 5, where simulated attack data are used to measure intrusion frequency, response

effectiveness, and recovery time across different DMZ configurations.

G. Cloud-Based DMZ Architectures

Cloud-based DMZ architectures adapt DMZ principles to public or hybrid cloud environments. Internet-facing services are hosted within isolated cloud network segments and protected by cloud-native security mechanisms such as virtual firewalls, security groups, and access control lists.

These architectures provide high scalability and availability through automated resource management and built-in redundancy. At the same time, they operate under shared responsibility models, where security obligations are divided between the cloud service provider and the customer. Proper configuration and continuous monitoring are therefore essential to maintain adequate security levels [12].

H. Use Cases and Service Deployment Scenarios

To ensure consistency in the comparative analysis, all DMZ architectures are evaluated using identical service deployment scenarios. The DMZ hosts common Internet-facing services, such as web and application servers, representing typical exposure points for external attacks.

The internal LAN contains protected resources that are not directly accessible from external networks. Communication between the DMZ and the internal LAN is restricted to explicitly authorized flows required for service operation. These standardized use cases provide a controlled basis for evaluating the security effectiveness and resilience of each DMZ architecture.

I. Architectural Basis for Quantitative Evaluation

The DMZ architectures presented in this section form the structural foundation for the quantitative analysis conducted in the next section. Each architecture is subjected to the same attack scenarios and evaluated using identical security indicators to ensure fair comparison. This approach enables objective assessment of how architectural design choices influence intrusion probability, recovery time, and service availability.

The following section presents the quantitative analysis methodology and risk modeling approach used to evaluate the DMZ architectures described above.

V. Statistical Analysis of Threats and Attacks Against the DMZ

To statistically analyze threats and attacks targeting the Demilitarized Zone (DMZ), a structured data collection and analysis process was conducted based on security events recorded at the network perimeter. The objective of this analysis is to obtain a representative dataset enabling the characterization of attack types, their frequency, temporal behavior, and the effectiveness of the deployed DMZ protection mechanisms.

The dataset was derived from simulated yet realistic security logs generated by perimeter defense components, including firewalls and intrusion detection/prevention systems (IDS/IPS), as well as application and system logs from servers hosted within the DMZ. Each recorded security event was characterized using operational attributes such as timestamp, source IP address, targeted service or port, applied action (allowed or blocked), and attack category.

A. Simulation Environment and Experimental Setup

This study was conducted using a controlled and reproducible simulation environment designed to evaluate the security effectiveness of different DMZ architectures. The experimental platform was implemented using virtualized network infrastructure, including virtual machines, firewall systems, and intrusion detection components deployed in isolated network segments. Three network architectures were simulated: a flat network without DMZ, a traditional physical DMZ architecture, and a cloud-based DMZ architecture. Each architecture hosted identical Internet-facing services, including web and email servers, to ensure fair comparison.

Attack scenarios were generated using controlled and predefined cyberattack models representing common real-world threats, including Distributed Denial of Service (DDoS), port scanning,

TABLE I
SUMMARY OF COLLECTED SECURITY DATA

Date	Attack Type	Frequency	DMZ Response
2025-01-20	DDoS	50	Blocked
2025-01-21	SQL injection	20	Blocked
2025-01-22	Port Scanning	30	Monitored
2025-01-23	Phishing	15	Blocked
2025-01-24	Malware	25	Blocked

SQL injection, phishing, and malware propagation. A total of 140 simulated attack attempts were executed across multiple experimental runs. Security logs were collected from firewall and intrusion detection systems and recorded parameters such as attack type, timestamp, response action, and success or failure outcome. The intrusion probability is calculated based on the ratio of successful attacks to total attempts, as formally defined in Equation (2).

This setup ensures reproducibility and provides a quantitative basis for comparing the security effectiveness of different DMZ architectures.

Table I summarizes the observation period, attack types, estimated frequencies, and DMZ responses.

B. Data Collection Framework and Observation Dataset

The Date column indicates the day on which each attack was recorded. The observation dataset covers a five-day period, from January 20 to January 24, 2025, allowing the identification of short-term trends and variations in malicious activity targeting DMZ-exposed services.

The Attack Type column specifies the category of simulated attacks, selected to reflect realistic threat vectors commonly observed in operational environments. These include distributed denial-of-service (DDoS) attacks, SQL injection attempts, port scanning activities, phishing campaigns, and malware propagation.

The Frequency column represents the estimated number of occurrences associated with each attack type during the defined observation period. Finally, the DMZ Response column presents the security actions applied by the DMZ protection mechanisms, such as traffic blocking or monitoring, based on predefined filtering rules and detection policies.

Although the dataset is based on controlled simulation scenarios, the attack models and security responses were designed to reflect realistic operational conditions observed in enterprise network environments.

C. Statistical Typology of Observed Threats

Based on the dataset summarized in Table I, a statistical classification of the observed threats was conducted in order to identify the dominant attack categories targeting the Demilitarized Zone (DMZ). The analysis reveals that distributed denial-of-service (DDoS) attacks represent the most frequent threat, followed by port scanning activities, which indicate systematic reconnaissance attempts against publicly exposed services.

Other attack types, including SQL injection, phishing, and malware-related activities, occur with lower frequency but remain critical due to their potential impact on application integrity, user credentials, and overall system security. Despite their relatively lower occurrence, these attacks often target specific vulnerabilities and can lead to severe

security breaches if not properly mitigated.

The observed diversity of attack vectors highlights the necessity of deploying layered security mechanisms within the DMZ. High-frequency attacks such as DDoS require robust traffic filtering and rate-limiting controls, while targeted attacks demand deep packet inspection, application-layer protections, and continuous monitoring capabilities.

Based on the dataset summarized in Table I, Fig. 6 illustrates the temporal analysis of attacks blocked by the DMZ over the observation period, highlighting variations in attack frequency across different dates.

Fig. 6. Temporal analysis of attacks blocked by the DMZ.

As shown in Figure 6, the number of blocked

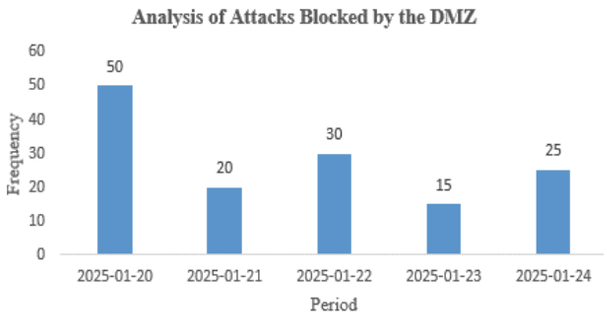

Fig. 6. Temporal analysis of attacks blocked by the DMZ.

attacks varies across the observation period. A pronounced peak is observed on January 20, followed by fluctuations on subsequent days. These variations indicate non-uniform attack patterns and emphasize the importance of continuous monitoring and adaptive security policies within the DMZ to effectively respond to changing threat dynamics.

D. Comparison Between Physical, Virtual, and Cloud-Based DMZ Architectures

A comparative analysis was conducted to evaluate the effectiveness of physical, virtual, and cloud-based DMZ architectures in terms of cost, performance, and security efficiency. This comparison aims to highlight the trade-offs associated with each deployment model and to support informed architectural decision-making.

Physical DMZ architectures provide strong isolation and stable performance through dedicated hardware and network segmentation. However, they typically involve higher deployment and maintenance costs. Virtual DMZs leverage resource virtualization to improve flexibility and cost efficiency, while maintaining acceptable levels of security and performance. Cloud-based DMZs offer high scalability and reduced infrastructure costs, but may introduce higher latency and dependency on external service providers.

The results presented in Table II indicate that physical DMZ architectures achieve the highest level of security effectiveness, albeit at a higher cost. Virtual DMZs provide a balanced trade-off between cost reduction and acceptable performance, while cloud-based DMZs offer the most cost-effective solution with increased scalability. However, the latter may introduce additional latency and reliance on external infrastructure providers.

TABLE II
COMPARISON OF PHYSICAL, VIRTUAL, AND CLOUD-BASED DMZ ARCHITECTURES

DMZ Type	Annual Cost ($)	Latency	Efficiency (%)
Physical	50000	5	95
Virtual	3000	8	92
Cloud-based	2000	10	90

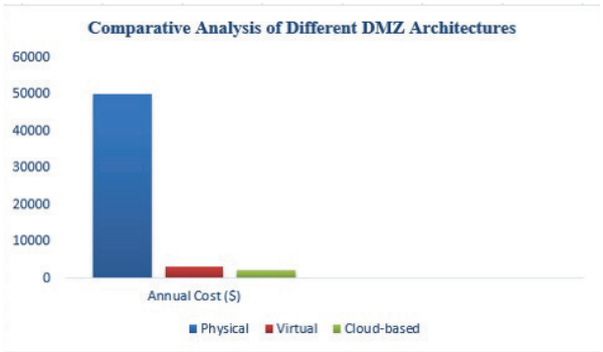

Fig. 7. Comparison of physical, virtual, and cloud-based DMZ performance metrics.

Based on the comparative data presented in Table II, Fig. 7 provides a visual comparison of physical, virtual, and cloud-based DMZ architectures in terms of cost, latency, and effectiveness.

The visual comparison shown in Fig. 7 confirms that physical DMZs achieve higher security effectiveness at increased cost, while virtual and cloud-based DMZs offer a trade-off between scalability, cost efficiency, and acceptable security performance. These findings highlight the importance of selecting DMZ architectures based on organizational constraints and security requirements.

E. Risk Modeling

Risk modeling was conducted to evaluate and compare the security levels of network architectures deployed with and without a Demilitarized Zone (DMZ).

To provide a quantitative evaluation of security risk, a formal risk model was defined based on intrusion probability and impact severity.

The overall Security risk is expressed as:

$$R = P * I \quad (1)$$

Where:

R = Security risk level

P = Intrusion probability

I = Impact severity factor

Intrusion probability is calculated as:

$$P = Ns / Nt \quad (2)$$

Where:

Ns = Number of successful intrusions

Nt = Total number of attack attempts

Service availability is calculated as:

$$Availability\ (\%) = (Ttotal - Tdown) / Ttotal \times 100$$

Where:

Ttotal = Total observation time

Tdown = Total service downtime

These equations provide a quantitative framework for comparing the effectiveness of DMZ architectures under identical attack conditions.

The analysis focuses on two key indicators: intrusion probability and recovery time, which together provide insight into the effectiveness of DMZ deployment in reducing risk and improving network resilience.

F. Risk Modeling with and without DMZ

The comparative risk analysis examines three deployment scenarios: a network architecture without a DMZ, a network protected by a traditional DMZ, and a network incorporating a cloud-based DMZ. These scenarios were evaluated using quantitatively measured risk indicators derived from controlled and repeatable simulated attack conditions.

Without a DMZ, Internet-facing services are directly exposed to external threats, resulting in a high probability of successful intrusion and prolonged recovery time following security incidents. In contrast, the deployment of a DMZ introduces an isolation layer that significantly reduces exposure and limits the impact of attacks on internal resources.

TABLE III
RISK MODELING FOR NETWORK ARCHITECTURES WITH AND WITHOUT DMZ

Scenario	Intrusion Probability (%)	Recovery Time (h)
Without DMZ	80	48
With Traditional DMZ	20	12
With Cloud DMZ	10	6

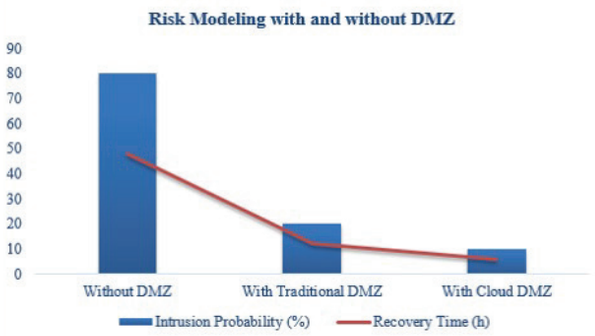

Fig. 8. Risk modeling comparison with and without DMZ.

Table III summarizes the estimated risk levels associated with different network deployment scenarios.

The data presented in Table III clearly demonstrate the impact of DMZ deployment on risk reduction. Architectures without a DMZ exhibit significantly higher intrusion probability and longer recovery time due to the absence of segmentation between public services and internal resources. The introduction of a traditional DMZ substantially lowers both indicators, while cloud-based DMZs show the lowest estimated risk levels, reflecting improved recovery capabilities and enhanced scalability.

Fig. 8 illustrates the comparative risk levels for network architectures deployed with and without DMZ protection.

As illustrated in Fig. 8, networks deployed without a DMZ present the highest risk profile, while DMZ-protected architectures significantly improve security posture by reducing intrusion probability and accelerating recovery. These findings confirm the critical role of DMZ deployment in enhancing network resilience against external threats.

TABLE IV
ESTIMATED EFFECTIVENESS OF DMZ SECURITY BEST PRACTICES

Security	Measures Effectiveness(%)	Ease of Implementation
Port and Protocol filtering	90	Medium
Advanced network segmentation	85	Difficult
Monitoring and log management	95	Easy
Multi-factor authentication	98	Medium
Regular update of security rules	92	Easy

G. Best Practices

In the context of securing a Demilitarized Zone (DMZ), several essential best practices are recommended to strengthen the protection of Internet-facing services and to reduce the overall attack surface [14]. These practices aim to enhance both preventive and detective security controls while maintaining operational feasibility.

Key measures include port and protocol filtering, advanced network segmentation, continuous monitoring and log management, multi-factor authentication, and regular updates of security rules. Each practice contributes differently to the security posture of the DMZ, depending on its effectiveness and ease of implementation.

Table IV presents an estimated evaluation of the effectiveness and ease of implementation of key DMZ security best practices.

Port and protocol filtering demonstrates a high level of effectiveness (90%) by limiting unnecessary exposure of services, although it requires careful rule configuration. Advanced network segmentation provides strong isolation benefits but is more difficult to implement due to architectural constraints and operational complexity.

Monitoring and log management emerge as highly effective (95%) and relatively easy to implement, enabling real-time detection of security events and improved incident traceability. Multi-factor authentication offers the highest effectiveness (98%) by strengthening access control mechanisms, though it introduces moderate

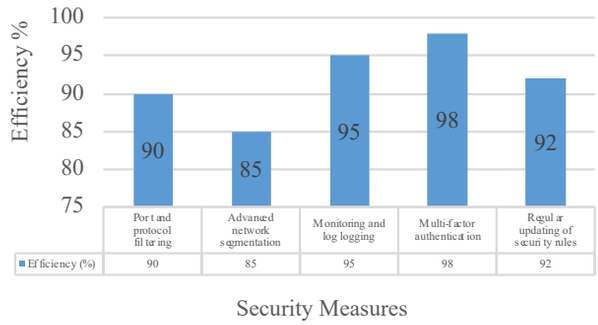

Fig. 9. Best practices for securing a DMZ.

implementation complexity. Regular updates of security rules also contribute significantly to security enhancement (92%) and are generally easy to deploy, ensuring continuous adaptation to evolving threats.

Fig. 9 provides a visual synthesis of the relative effectiveness of the identified DMZ security best practices.

The estimated results highlight the importance of achieving a balance between security effectiveness and implementation feasibility when securing a DMZ. Combining highly effective measures with manageable deployment complexity enables organizations to enhance protection while maintaining operational efficiency.

H. Statistical Validation and Uncertainty Analysis

To improve the reliability and scientific validity of the results, statistical analysis was performed on the observed and simulated security data. The objective was to evaluate the variability and uncertainty associated with intrusion probability, recovery time, and service availability measurements.

The mean value of each security metric was calculated as:

$$\mu = (1/n) \times \sum xi \quad (4)$$

Where:

μ = mean value

xi= observed value

n = number of observations

The standard deviation was calculated as:

$$\sigma = \sqrt{\frac{1}{n}\sum(x_i - \mu)^2} \quad (5)$$

This parameter quantifies the variability of the measured security indicators.

In addition, confidence analysis was used to ensure the consistency of comparative results between DMZ architectures. The use of repeated simulated attack scenarios and averaged measurements reduces experimental uncertainty and improves the reliability of the quantitative evaluation.

These statistical validation methods confirm that the observed differences between DMZ architectures are consistent and support the validity of the proposed quantitative security evaluation framework.

VI. Results and Discussion

This section presents and discusses the results obtained from the statistical analysis of threats and attacks targeting the Demilitarized Zone (DMZ), as well as the comparative evaluation of different DMZ architectures. The discussion focuses on the implications of these results for network security, resilience, and architectural decision-making.

A. Analysis of Observed Threat Patterns

The statistical analysis presented in Table I and Figure 6 highlights the diversity and non-uniform distribution of attacks targeting DMZ-exposed services. Distributed denial-of-service (DDoS) attacks constitute the most frequent threat, reflecting common attempts to disrupt service availability. Port scanning activities also appear prominently, indicating systematic reconnaissance behavior aimed at identifying potential vulnerabilities.

Although less frequent, attacks such as SQL injection, phishing, and malware propagation remain highly critical due to their potential impact on application integrity and data confidentiality. These results confirm that DMZ environments must be designed to address both high-volume attacks and targeted intrusion attempts through layered and adaptive security mechanisms.

B. Effectiveness of DMZ Architectures

The comparative results presented in Table II and illustrated in Fig. 7 demonstrate that different DMZ deployment models offer varying levels of effectiveness, cost efficiency, and performance. Physical DMZ architectures achieve the highest security effectiveness due to strong isolation and dedicated resources, but at the expense of higher deployment and maintenance costs.

Virtual DMZ architectures provide a balanced solution by reducing costs while maintaining acceptable levels of security and performance. Cloud-based DMZs offer the greatest scalability and cost efficiency; however, they introduce increased latency and dependency on external service providers. These findings indicate that organizational constraints, service criticality, and acceptable risk levels should guide the selection of a DMZ architecture.

These differences in performance can be directly explained by architectural design characteristics. Physical DMZ architectures provide stronger isolation because they rely on dedicated hardware and physically separated network segments, reducing the attack surface and limiting lateral movement. Virtualized DMZs offer improved flexibility and faster recovery due to dynamic resource allocation, but may introduce additional attack vectors related to hypervisor security. Cloud-based DMZ architectures benefit from built-in redundancy, automated scaling, and distributed infrastructure, which significantly reduces recovery time and improves service availability. However, their security effectiveness may depend on correct configuration and shared responsibility with the cloud provider.

These results demonstrate that architectural design directly influences measurable security outcomes and confirm the importance of segmentation and layered security mechanisms.

C. Impact of DMZ Deployment on Risk Reduction

The risk modeling results presented in Table III and Figure 8 clearly demonstrate the benefits of deploying a DMZ. Architectures without a DMZ exhibit significantly higher intrusion probability and longer recovery times due to the lack of segmentation between public-facing services and

internal resources.

The introduction of a traditional DMZ substantially reduces both intrusion probability and recovery time, confirming the effectiveness of network segmentation as a defensive strategy. Cloud-based DMZ architectures further reduce estimated risk levels by enabling faster recovery and improved scalability, although these benefits must be balanced against potential limitations in control and visibility.

The observed reduction in intrusion probability is directly related to the presence of an intermediate security layer that filters and monitors traffic before it reaches internal resources. The DMZ acts as a containment zone, preventing attackers from directly accessing critical systems.

In addition, faster recovery times observed in virtual and cloud-based DMZ architectures are explained by automated recovery mechanisms, resource elasticity, and system redundancy. These characteristics improve system resilience and reduce operational downtime following cyber incidents.

D. Implications of Security Best Practices

The evaluation of security best practices summarized in Table IV and visualized in Figure 9 underscores the importance of combining multiple protective measures to enhance DMZ security. Monitoring and log management, multi-factor authentication, and regular updates of security rules emerge as highly effective measures that can be implemented with relatively manageable complexity.

Advanced network segmentation, while more difficult to deploy, provides significant security benefits by reinforcing isolation between network zones. These results emphasize that effective DMZ security relies not on a single control, but on a coordinated set of practices that balance effectiveness and operational feasibility.

E. Discussion and Practical Implications

Overall, the results confirm that properly designed and managed DMZ architectures significantly enhance network security and resilience. The statistical and comparative analyses demonstrate that DMZ deployment reduces intrusion probability, shortens recovery time, and improves service availability under attack conditions.

From a practical perspective, these findings provide network designers and administrators with quantitative insights to support architectural choices and security policy optimization. The results also highlight the importance of aligning DMZ design with organizational requirements, technological environments, and evolving threat landscapes.

The following section concludes the paper by summarizing the main findings and outlining directions for future research.

VII. Conclusion and Future Work

This paper investigated the role of Demilitarized Zone (DMZ) architectures in securing Internet-facing services deployed within local area networks. Through a structured statistical analysis of threats and attacks, combined with a comparative evaluation of physical, virtual, and cloud-based DMZ deployments, the study provided quantitative insights into the effectiveness of DMZ-based security architectures.

The results demonstrate that the deployment of a DMZ significantly reduces intrusion probability and recovery time when compared to network architectures without segmentation. Physical DMZs offer the highest level of security effectiveness due to strong isolation, albeit at higher cost. Virtual DMZs provide a balanced trade-off between cost efficiency and acceptable performance, while cloud-based DMZs offer scalability and reduced operational costs with slightly increased latency and dependency on external providers. These findings confirm that DMZ architectures remain a fundamental component of network security strategies, particularly when combined with appropriate security best practices.

The statistical typology of observed threats highlighted the prevalence of high-frequency attacks such as distributed denial-of-service and reconnaissance activities, as well as the continued relevance of targeted attacks including SQL

injection, phishing, and malware propagation. The analysis of security best practices further emphasized the importance of layered defenses, continuous monitoring, strong access control mechanisms, and regular policy updates in enhancing DMZ protection.

Despite these contributions, this study is subject to certain limitations. The analysis is based on estimated and simulated datasets designed to reflect realistic attack scenarios. While the simulation approach enables controlled comparison and reproducibility, real-world network environments may introduce additional operational variability. However, the proposed methodology provides a valid and reproducible framework for comparative DMZ security evaluation.

Future work will focus on extending this research by incorporating real-world datasets and more advanced analytical models. In particular, the integration of automation, intelligent threat detection techniques, and adaptive security policies represents a promising direction for enhancing DMZ effectiveness. Additionally, exploring the convergence of DMZ architectures with emerging security paradigms, such as Zero Trust and identity-centric access control, may further improve resilience against sophisticated and evolving cyber threats.

This study provides a reproducible and quantitative framework for evaluating DMZ security architectures and contributes to evidence-based design of secure network infrastructures.

Funding

This article did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

Conflict of Interest

Authors declare that they have no conflict of interest.

References

[1] B. Schneier, Network Security: Protecting Data in the Age of Cyber Threats. Hoboken, NJ, USA: Wiley, 2011.

[2] Fortinet, “What is a DMZ and why would you use one?” Fortinet Documentation, 2023. [Online]. Available: https://www.fortinet.com/resources/cyberglossary/what-is-dmz. [Accessed: May 20, 2026].

[3] M. Gallo and W. Hancock, Networking and Security Fundamentals: DMZ and Firewall Design. Boston, MA, USA: Pearson Education, 2016.

[4] P. Morris, “The evolution of DMZ in virtualized and cloud environments,” International Journal of Network Security, vol. 14, no. 3, pp. 178–192, 2022.

[5] Y. Kobayashi and H. Lee, The Evolution of Security Zones: From Geopolitical to Cybersecurity Applications. Cham, Switzerland: Springer, 2014.

[6] K. Salhi, “Segmentation and segregation mechanisms and models to secure industrial control systems,” Ph.D. dissertation, Dept. Computer Science, University of Lorraine, Nancy, France, 2019.

[7] B. Scanlon and L. Rocco, “Securing network architectures: A case study of DMZ in critical infrastructure,” J. Cybersecurity Res., vol. 6, no. 2, pp. 88–97, 2018.

[8] A. Essaidi, V. Boistuaud, and N. Diop, “Conception of a demilitarized zone (DMZ),” Tech. Rep., Université de Marne-la-Vallée, Marne-la-Vallée, France, 2019.

[9] C. Chen and Z. Zhang, Optimizing Network Security with DMZ: A Case Study in Enterprise Environments. Amsterdam, Netherlands: Elsevier, 2020.

[10] B. Liskov and R. Smith, “The role of DMZ in cybersecurity risk mitigation,” in Proc. Int. Conf. Network Security Management, Paris, France, 2020, pp. 45–62.

[11] J. Norris, The Concept of DMZ in Network Security: From Military Strategy to Cyber Defense. Cham, Switzerland: Springer, 2017.

[12] A. T. Tunggal, What Is Zero Trust? A Model for More Effective Security, 2021.

[13] Y. Shen and X. Wang, “Integrating artificial intelligence into DMZ-based security architectures,” Cybersecurity and AI Applications Journal, vol. 5, no. 1, pp. 112–127, 2020.

[14] Cisco Systems, “Best practices for implementing DMZ in LAN security,” Cisco White Paper, 2023. [Online]. Available: https://www.cisco.com/. [Accessed: May 20, 2026].

[15] M. Baker, Modern Approaches to LAN Security: DMZ and Beyond. Cham, Switzerland: Springer, 2023.

[16] Tufin, “Understanding DMZ Networks and Improving

Enterprise Security," 2025. [Online]. Available: https://www.tufin.com/. [Accessed: May 20, 2026].

[17] University of Quebec, "Cloud Security: DMZ and Segmentation for Securing Web Services in the Cloud," Tech. Rep., Quebec, QC, Canada, 2020.

[18] M. Alabbad, N. Mhaskar, and R. Khedri, "Hardening of network segmentation using automated referential penetration testing," J. Netw. Comput. Appl., vol. 235, Art. no. 103861, 2024.

[19] A. Palma and S. Bonomi, "Vulnerable network generator for experimental evaluation of attack graph scalability," Comput. Secur., vol. 145, Art. no. 103952, 2025.

[20] S. Rose, O. Borchert, S. Mitchell, and S. Connelly, "Zero Trust Architecture," Nat. Inst. Stand. Technol., Gaithersburg, MD, USA, NIST SP 800-207, Aug. 2020.