ISSN 2563-7568

CASE STUDY

Case Study: The Next Generation of Network Management - AI, Automation, and Security in a Connected World

Vaishali Nagpure*

Senior Network Engineer, Western Union, CO, Denver, USA

Abstract

Modern data center networks face unprecedented challenges in ensuring robust security due to the evolving complexity of cyber threats and the increasing sophistication of attack vectors. This study proposes comprehensive, multi-layered security architecture tailored for data center environments, integrating advanced technologies such as Next-Generation Firewalls (NGFWs), Zero Trust Architecture (ZTA), AI-driven anomaly detection, SQL-based policy management, and Neo4j knowledge graphs. The architecture leverages NGFWs for deep packet inspection and application-layer filtering, fortifying the network perimeter while enabling advanced threat detection. ZTA principles enforce the least privilege of access, requiring continuous authentication and contextual validation for all users and devices. A relational database underpins security policy management, ensuring granular control and consistent enforcement across the network. Neo4j knowledge graphs offer a dynamic, graph-based visualization of the network topology, enabling real-time analysis of relationships and communication paths to uncover potential vulnerabilities, attack vectors, and insider threats. The core of the system's intelligence lies in the integration of machine learning models, particularly Long Short-Term Memory (LSTM) networks, for anomaly detection and predictive analytics. By analyzing real-time network traffic data, the AI models autonomously detect unusual patterns indicative of security incidents, enabling proactive threat mitigation. The synergy between these components ensures a scalable and resilient security framework capable of addressing modern security challenges. This architecture is designed to automate key aspects of threat detection, incident response, and policy enforcement, significantly reducing operational overhead while improving response times. The result is a flexible and adaptive security solution that enhances visibility, control, and protection of critical data center resources. By combining these cutting-edge technologies, this proposed framework demonstrates its capability to provide a robust defense mechanism for data center networks, ensuring operational continuity and compliance with stringent security requirements. This paper highlights the system's technical components, demonstrates its functionality through a detailed use case, and underscores its effectiveness in securing complex, high-value network environments against evolving cyber threats.

***Corresponding Author**: Vaishali Nagpure, Senior Network Engineer, Western Union, CO, Denver, USA; E-mail: vaishali.nagpure@gmail.com*

***Received Date**: November 24, 2024, **Accepted Date**: December 03, 2024, **Published Date**: December 09, 2024*

***Citation:** Nagpure V. Case Study: The Next Generation of Network Management – AI, Automation, and Security in a Connected World. 2024;4(2):133-149.*

Key Words: *Next-Generation Firewalls (NGFW); Zero Trust Architecture (ZTA); Long Short-Term Memory (LSTM) models; SQL-based security enforcement; Knowledge graphs; Neo4j; Cloud infrastructure security; Integrated security architecture*

1. Introduction

The rapid evolution of data center networks has brought unprecedented opportunities for operational efficiency, scalability, and adaptability. However, this progress also exposes critical infrastructure to a myriad of security threats. Traditional network security models, which rely on perimeter-based defenses, are increasingly insufficient to combat sophisticated and targeted attacks. Advanced strategies, such as Zero Trust Architecture (ZTA), Next-Generation Firewalls (NGFWs), and AI-driven anomaly detection, are necessary to address the modern threat landscape in data center environments.

AI technologies have emerged as pivotal tools for enhancing network security. Their capacity to analyze large-scale data in real time allows for proactive threat detection and mitigation. For instance, Ramanpreet et al. explore the role of AI in cybersecurity, emphasizing its potential to automate threat analysis and reduce response times through intelligent algorithms [1]. Similarly, Tang et al. demonstrate the use of deep learning models for intrusion detection in software-defined networks, showcasing the viability of AI in improving network security performance [2]. These works highlight the transformative potential of AI in modern network defense strategies.

Graph-based analytics, such as those utilizing Neo4j, have also gained traction in the security domain. Angles and Gutierrez provide a comprehensive survey of graph database models, which are critical for representing complex relationships in network security scenarios [3]. This aligns with CyGraph, a framework that applies graph-based analytics for cybersecurity, enabling visual insights into network vulnerabilities and attack paths [4]. These approaches, when applied to data center network architectures, can improve visibility and decision-making for administrators.

Zero Trust Architecture (ZTA) is another cornerstone of contemporary security frameworks. By enforcing strict access controls and continuous verification, ZTA minimizes the attack surface and ensures that no entity is inherently trusted. A recent survey by Syed et al. underscores the importance of ZTA in modern security practices, particularly in high-stakes environments like data centers [5]. When integrated with NGFWs, ZTA becomes even more powerful by extending security controls across the network.

This paper proposes a comprehensive framework that integrates NGFWs, ZTA, AI-based anomaly detection, relational databases, and Neo4j knowledge graphs. This multi-faceted approach ensures a robust security posture for data center networks, capable of addressing emerging threats while maintaining operational efficiency. The following sections explore the theoretical foundations and related work that inform the proposed architecture.

2. Background and Related Work

In response to the growing complexity of cyber threats in modern data centers, advanced security mechanisms are increasingly being integrated into network security frameworks. Traditional perimeter-based defenses are insufficient to combat sophisticated and targeted attacks, making it essential to adopt cutting-edge strategies such as Next-Generation

Firewalls (NGFWs), Zero Trust Architecture (ZTA), Artificial Intelligence (AI)-driven anomaly detection, and graph-based analytics. While these technologies have been explored in the literature, the proposed framework in this article integrates these components in a unique and synergistic way, improving upon existing solutions and addressing emerging cybersecurity challenges in data center environments.

2.1. Graph-based analytics and visualization for cybersecurity

Graph-based approaches, particularly those using frameworks like CyGraph, have gained traction in the security domain for visualizing the relationships between devices, users, and services within a network. CyGraph, which applies graph-based analytics to detect vulnerabilities and visualize complex network interactions [1]. While graph databases like Neo4j have been used for anomaly detection and threat visualization [2], they are often limited to representing network topology or identifying attack paths.

Our paper advances this approach by incorporating real-time dynamic analysis of network interactions using Neo4j, which enhances threat detection and mitigates risks in real-time. By modeling not just static topologies, but live relationships and behaviors, we improve the detection of evolving threats such as lateral movement and privilege escalation. This provides a deeper and more actionable understanding of network security than previous work, which primarily focuses on visualization without full integration into real-time anomaly detection and security operations [2]. Our integration of graph-based analytics with AI for predictive threat detection provides a significant improvement by proactively identifying vulnerabilities and attack paths before they can be exploited.

2.2. Zero Trust Architecture (ZTA) for secure network access

Zero Trust Architecture (ZTA) is a fundamental principle in modern network security, particularly for environments where traditional perimeter defenses are ineffective. The concept of ZTA assumes no inherent trust for any device or user, whether inside or outside the network [3]. While discussing the ZTA's importance in securing critical infrastructures, the practical integration of ZTA with other security mechanisms like Next-Generation Firewalls (NGFWs) and AI-driven anomaly detection systems is not fully explored [3].

In our proposed framework, ZTA is combined with NGFWs and AI-based anomaly detection to provide a multi-layered defense against both internal and external threats. By continuously verifying the identity of users and devices through multi-factor authentication (MFA) and using context-aware policies, our system dynamically adapts to evolving threats, something not fully addressed by previous works [3]. Unlike existing solutions, which may implement ZTA in isolation, our framework integrates ZTA directly with AI models for anomaly detection, ensuring that not only the perimeter is secure but that every transaction within the network is authenticated and verified in real time [5].

2.3. Artificial Intelligence in cybersecurity

Artificial Intelligence, particularly machine learning (ML), has become an essential tool in cybersecurity, with several studies showcasing its potential in automating threat detection and mitigating cyber risks. The highlight the role of AI in network security, with applications in intrusion detection and the automation of threat analysis [5,6]. However, these studies often focus on narrow applications of AI, primarily limited to supervised learning models or feature-based analysis.

Our work extends these AI applications by leveraging Long Short-Term Memory (LSTM) networks for real-time anomaly detection in time-series network traffic. This method is more effective than traditional machine learning models in detecting zero-day attacks and insider threats in a data center environment. By using unsupervised learning alongside supervised models like XGBoost, we provide a hybrid approach that detects both known and previously unseen attack patterns, offering a higher level of prediction accuracy and faster response times [5,6]. Additionally, our framework integrates AI with ZTA and NGFWs to create a self-adapting security system that continuously learns and evolves, improving upon the static models used in traditional network security systems [7].

2.4. Next-Generation Firewalls (NGFWs)

NGFWs provide deep packet inspection, intrusion prevention, and application-layer filtering, making them a crucial element in securing modern network infrastructures. Existing works, such as those by emphasize the benefits of NGFWs in defending against common threats. However, the integration of NGFWs with other advanced technologies, such as AI-driven models and ZTA, is often overlooked or underexplored [8].

We significantly improve existing solutions by integrating NGFWs with both ZTA and AI-based anomaly detection. This multi-layered integration ensures that threat detection is not only limited to the perimeter but is also continuously adapted to detect emerging threats throughout the entire network. By integrating real-time traffic analysis with NGFWs, AI models can automatically identify suspicious behavior and adjust firewall policies without manual intervention, making the security response more agile and efficient [9]. Unlike traditional static NGFW configurations, our system creates a dynamic security framework that evolves as threats change, improving defense capabilities against advanced persistent threats (APTs) [8].

2.5. Hybrid approaches and emerging technologies

Emerging technologies, such as Generative Adversarial Networks (GANs), have shown promise in improving network intrusion detection systems (IDS) by generating synthetic attack data to enhance training datasets [10-13]. However, integrating these emerging technologies with traditional security mechanisms has not been fully realized in the existing literature.

We introduce a hybrid approach that combines GANs with NGFWs and ZTA, allowing our framework to generate synthetic attack data to enhance real-time threat detection capabilities. This approach enables our system to identify novel attack vectors that have not been seen before, a capability that is typically absent in traditional detection models. By using AI-driven predictive analytics, our framework improves detection rates for unknown threats and reduces false positives, which is a significant enhancement over traditional detection methods that rely solely on predefined attack signatures [14].

2.6. Insider threats and human factors in cybersecurity

Insider threats are a major concern for data centers, with human factors such as trust and access control being central to the problem [15]. While existing literature focuses on traditional access controls and user behavior analytics, these methods often lack the flexibility needed for modern, dynamic environments.

Our framework addresses insider threats by integrating behavioral anomaly detection with ZTA and AI models that continuously monitor and analyze user activities. By applying context-aware access policies, we ensure that insider threats are detected in real time, even before they manifest as malicious actions. Moreover, our integration of human expertise in network intrusion detection, as suggested for further enhances the framework's ability to identify nuanced insider threat patterns that may evade automated detection [16]. This combination of AI and human expertise creates a more adaptive security system, improving upon previous works that rely solely on either automated or manual methods [15].

2.7. Challenges and future directions in cybersecurity

While previous works discuss the scalability of AI and machine learning models in network security, the practical challenges of scaling these systems in real-world data center environments remain largely unexplored. The integration of multiple advanced technologies introduces complexity in managing security policies and ensuring consistent enforcement across large-scale infrastructures.

Our proposed system addresses these challenges by incorporating SQL-based policy management to automate policy enforcement, ensuring that security policies are applied consistently across all layers of the network. By automating the process of policy management and incorporating graph-based analytics with AI and NGFWs, we provide a solution that is not only scalable but also adaptive, improving the overall efficiency of security operations [17,18]. This automated and scalable solution offers real-time threat mitigation and ensures that data center networks can dynamically adapt to evolving threats without requiring manual intervention, an improvement over traditional models that often involve manual configuration [19].

This paper introduces significant improvements over existing literature by integrating NGFWs, ZTA, AI-driven anomaly detection, and graph-based analytics in a comprehensive framework that dynamically responds to evolving threats. Unlike previous studies, which may focus on isolated technologies, our approach synergistically combines these components, providing a more robust, scalable, and adaptive defense for modern data center networks. This integrated solution addresses the growing complexity of cybersecurity threats and offers real-time, automated mitigation strategies that improve both detection and response times.

3. Proposed Case Study

This architecture represents a multi-layered security framework integrating Next-Generation Firewalls (NGFWs), Zero Trust Architecture (ZTA), AI-driven anomaly detection, SQL-based policy management, Neo4j Knowledge Graphs, and an Incident Response System to secure a data center network. Below is a step-by-step explanation of how data and security logic flow through each component. The proposed system integrates multiple components to enhance the security of data center networks:

- External Network Traffic (Internet)- This is the entry point for all incoming traffic, including user requests, application traffic, and potential malicious activities. Includes legitimate user requests and potentially harmful traffic, such as DDoS attacks, unauthorized access attempts, or malicious payloads. This traffic is subject to

inspection and filtering before accessing any internal resources. Provides the raw data input for downstream security mechanisms (Figure 1).

Figure 1: *System Architecture Diagram.*

- Next-Generation Firewalls (NGFWs)- Packet Inspection: NGFWs analyze both header and payload contents for threats such as malware, suspicious patterns, or unauthorized protocols. Filtering: Blocks traffic violates predefined security rules or matches known threat signatures. Application Awareness: Distinguishes traffic by application type, allowing granular policy enforcement. TLS/SSL Decryption: Decrypts secure traffic for deeper inspection. All external traffic first passes through NGFWs for perimeter security. If deemed safe, traffic is forwarded to the Zero Trust Architecture (ZTA) for further scrutiny. Malicious traffic is blocked at this stage.
- Zero Trust Architecture (ZTA)- Implements the principle of "never trust, always verify." Identity Management (IAM): Verifies the identity of users, devices, and applications using roles, credentials, and contextual information. Multi-Factor Authentication (MFA): Adds an extra layer of verification, such as OTPs or biometric checks. Role-Based Access Control (RBAC): Ensures that users or devices can only access the resources they are explicitly authorized for. Traffic cleared by NGFW is authenticated and authorized by ZTA. Verified Traffic: Flows to internal resources like the SQL database or AI anomaly detection system. Unverified Traffic: Is denied or flagged for further analysis, contributing to anomaly logs.
- Real-Time Traffic Data Stream (AI Anomaly Detection)- Continuously monitors traffic for deviations from normal behavior using AI models, such as Long Short-Term Memory (LSTM). Detects anomalies such as unusual data volumes, unexpected connection patterns, or potential zero-day attacks. Traffic from ZTA is streamed into the anomaly detection system for real-time analysis. Normal Traffic: Continues to the next stages without interruption. Anomalous Traffic: Logged into the anomaly logs table in the SQL database and flagged for review.

- SQL Database (Policy Management and Access Control)- Acts as the centralized repository for Access Policies: Stores Zero Trust rules defining who/what can access specific resources. Anomaly Logs: Logs suspicious events for auditing and forensic purposes. Facilitates dynamic policy enforcement by integrating with ZTA and the AI anomaly detection system. SQL queries enforce policies dynamically based on user roles, device health, and contextual factors. Policy Breaches: Trigger alerts or restrictions, forwarding data to the incident response system. Anomaly Logs: Enable auditing and compliance reporting.
- Neo4j Knowledge Graphs (Threat Intelligence and Network Topology)- Maps relationships between network devices, users, and applications in a dynamic graph structure. Visualizes: Network topology (how devices and nodes are interconnected). Attack paths (e.g., lateral movement within the network). Privilege escalation (e.g., user roles with excessive access rights). Provides advanced threat intelligence by identifying potential vulnerabilities or attack paths. Anomaly logs and device information from the SQL database are integrated into Neo4j for graph-based analysis. Insights from Neo4j: Identifies compromised devices or users. Detects potential attack vectors, such as untrusted connections or suspicious relationships. Results are passed to the incident response system for further action.
- Incident Response System (Automated Threat Mitigation)- Automates the response to identified threats to minimize damage and reduce response time. Typical actions include Isolating compromised devices. Revoking user credentials temporarily. Triggering network segmentation to contain threats. Sending alerts to security teams for manual investigation. Receives data from Neo4j and the anomaly logs in the SQL database. Executes automated actions based on predefined rules and threat intelligence insights. Logs all actions for compliance and post-incident analysis.

This architecture represents a multi-layered security framework integrating Next-Generation Firewalls (NGFWs), Zero Trust Architecture (ZTA), AI-driven anomaly detection, SQL-based policy management, Neo4j Knowledge Graphs, and an Incident Response System to secure a data center network. Below is a step-by-step explanation of how data and security logic flow through each component.

3.1. SQL database for policy management and anomaly logging

SQL is used to store access control policies, log network events, and ensure that security governance is enforced in the data center. Figure 2 gives detailed SQL queries for creating tables and inserting data. This SQL scheme and example data represent the foundational tables and relationships necessary for implementing a Zero Trust and AI-driven network security framework in a data center environment. It aligns with the proposed architecture by managing devices, enforcing access policies, and logging into anomalous events.

```sql
-- Table for storing network devices in the data center
CREATE TABLE devices (
    device_id INT PRIMARY KEY,
    device_name VARCHAR(255),
    device_type VARCHAR(50),
    ip_address VARCHAR(15),
    location VARCHAR(255),
    status VARCHAR(50)
);

-- Table for storing access policies for devices (Zero Trust Policies)
CREATE TABLE access_policies (
    policy_id INT PRIMARY KEY,
    device_id INT,
    policy_type VARCHAR(50),
    action VARCHAR(50),
    FOREIGN KEY (device_id) REFERENCES devices(device_id)
);

-- Table for logging anomalous events detected by AI models or Neo4j
CREATE TABLE anomaly_logs (
    log_id INT PRIMARY KEY,
    event_type VARCHAR(255),
    device_id INT,
    timestamp TIMESTAMP,
    details TEXT,
    FOREIGN KEY (device_id) REFERENCES devices(device_id)
);

-- Example of inserting a device into the 'devices' table
INSERT INTO devices (device_id, device_name, device_type, ip_address, location, status)
VALUES (1, 'Web Server', 'Server', '192.168.1.1', 'Datacenter 1', 'Active');

-- Example of inserting a Zero Trust Policy for a device
INSERT INTO access_policies (policy_id, ice_id, policy_type, action)
VALUES (1, 1, 'Zero Trust', 'Deny');
```

Figure 2: *System architecture diagram.*

Example Query shown below - Use Case: Lists all active devices with their enforced Zero Trust policies (Table 1).

SELECT d.device_name, d.device_type, d.ip_address, p.policy_type, p.action
FROM device d
JOIN access_policies p ON d.device_id = p.device_id
WHERE d.status = 'Active';

Table 1: *Output Example.*

Device name	Device type	IP address	Policy type	Action
Web server	Server	192.168.1.1	Zero trust	Deny

Example Query shown below - Use Case: Retrieves anomalies logged in the last 7 days, linked to devices (Table 2).

SELECT d.device_name, a.event_type, a.timestamp, a.details
FROM device d
JOIN anomaly_logs a ON d.device_id = p.device_id
WHERE a.timestamp > NOW () – INTERVAL 7 DAY;

Table 2: *Output example.*

Device name	Event type	Time stamp	Details
Web server	Failed login attempt	2024-12-01 10:45:00	5 failed login attempts
Web server	Unusual traffic	2024-11-30 14:22:00	Bandwidth spike detected

3.1.1. Relevance to the network security framework

- Devices Table: Forms the backbone for managing all assets in the data center. Ensures traceability of policies and anomalies to specific devices.
- Access Policies Table: Implements Zero Trust principles, controlling access at the device level. Ensures fine-grained policy enforcement.
- Anomaly Logs Table: Tracks suspicious activities, enabling proactive investigation and mitigation. Provides critical inputs for AI/ML models and Neo4j-based analytics.

This structured database schema, and examples demonstrate how the SQL component integrates into the proposed framework, supporting dynamic policy enforcement, anomaly tracking, and Zero Trust security principles.

3.2. Neo4j knowledge graph for network topology analysis

Neo4j will be used to store and analyze network topology and interactions between devices. The network is represented as a graph where devices are nodes, and communication between them is captured as relationships.

Neo4j Schema: Nodes: Devices such as servers, routers, and switches. Relationships: Communication between devices, including data flow, access requests, etc.

Cypher Queries for Neo4j (Network Topology): To analyze communication patterns in the data center network and identify abnormal behavior, we define the network topology and use Cypher queries for analysis. Figure 3 shows network infrastructure sample.

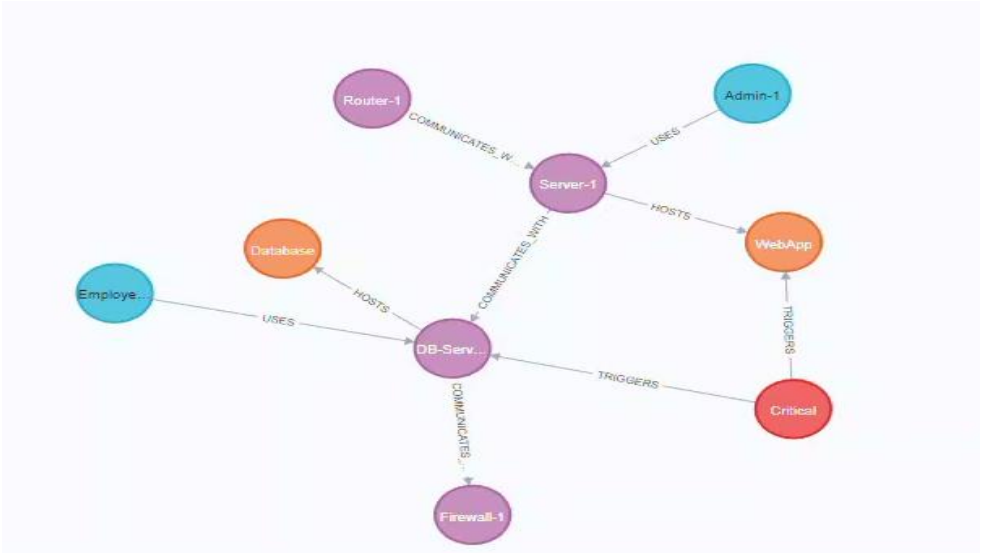

Figure 3: *Network infrastructure (nodes/relations).*

Devices: - Four devices: a router, a web server, a database server, and a firewall, each with a name, type, and IP address.

Users: Two users: an admin and an employee, with their roles defined.

Services: Two services: a web application hosted on the web server and a database service hosted on the database server.

Anomalies: A node for a detected anomaly, specifying the type (e.g., "Unusual Traffic"), severity, and detection timestamp.

Now, let's say we want to identify devices that communicate excessively (e.g., more than 50 connections). We can write a Cypher query as shown in Figure 4 to identify such patterns.

```
MATCH (source:Device)-[:COMMUNICATES_WITH]->(destination:Device)
WITH source, destination, COUNT(*) AS communication_count
WHERE communication_count > 50
RETURN source.device_name AS Source, destination.device_name AS Destination, communication_count
ORDER BY communication_count DESC;
```

Figure 4: *Query to detect unusual activity.*

This query would return devices that have more than 50 communication instances with another device, which could indicate a potential DDoS attack or other network anomaly.

Figure 5 and table 3 show another query output to retrieve information about anomalies and the nodes. Figure 5 shows the output of a query, for example data.

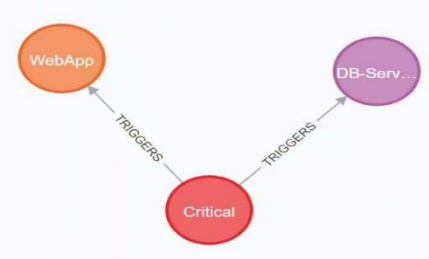

Figure 5: *Example data and output.*

Anomaly Node: Anomaly node: type: "Unusual Traffic", severity: "Critical", detectedAt: "2024-11-30 12:00:00"}
Triggered Nodes: Database Server: {name: "DB-Server-1", type: "Database Server"}
Web Service: {name: "WebApp", type: "Web Application"}

Table 3: *Query output.*

Anomaly	Triggered node
{type: “unusual traffic”,…}	{name: “DB-Server-1”, …}
{type: “unusual traffic”,…}	{name: “WebApp”, …}

Incident Investigation: Help administrators identify which systems or services are impacted by an anomaly. Example: If "Unusual Traffic" is detected, this query shows which devices or applications are affected, allowing for targeted response.

Root Cause Analysis: Provides context about anomalies and their scope. Example: If multiple services are impacted by the same anomaly, it could indicate a broader issue like a Distributed Denial of Service (DDoS) attack.

Proactive Security Measures: Enables tracking of frequently affected nodes, helping to identify vulnerable systems that require additional hardening or monitoring.

By running this query, security teams can gain actionable insights into nature and impact of detected anomalies within the data center network.

3.3. AI/ML model for anomaly detection and attack classification

In this section, we integrate an AI-based model to detect anomalies in network traffic and classify them into specific types of attacks (such as DoS, DDoS, Brute Force, etc.). The use of LSTM for anomaly detection and XGBoost for attack classification is justified by their theoretical foundations and experimental performance. LSTM's ability to process sequential data aligns perfectly with the dynamic nature of network traffic, while XGBoost's robustness to feature complexity and imbalanced data ensures precise attack classification. Together, these models create a robust pipeline for securing data center networks, ensuring high accuracy, recall, and scalability in real-world applications. Table 4 shows a performance comparison of different models.

Table 4: *Performance comparison.*

Model	Task	Strengths	Limitations	Overall Suitability
LSTM	Anomaly detection	Handles temporal data, adaptive, robust	Requires more date preprocessing	Best for sequential data
XGBoost	Attack classification	Handles non-linear relationships, imbalanced data, and feature importance	Interpretability can be challenging with many features	Best for structured classification
PCA/ARIMA	Anomaly detection	Simple to implement	Assumes linearity cannot handle dynamic patterns	Not suitable
K-means/DBSCAN	Anomaly detection	Unsupervised, handles noisy data	High false positives, poor for overlapping clusters	Limited
Logistic regression	Attack classification	Simple and interpretable	Assumes linearity, cannot handle complexity	Not suitable

SVM	Attack classification	Handles non-linear data	Computationally expensive, struggles with imbalanced data	Limited
Random Forest	Attack classification	Robust, interpretable	Lower recall for minority classes compared to XGBoost	Good but not optimal

We'll use a Long Short-Term Memory (LSTM) model for anomaly detection and an XGBoost model for attack classification. Figure 6 gives sample python code for this. LSTM is effective for time-series analysis, and here it is used to predict whether a network event is anomalous.

```python
import numpy as np
import pandas as pd
from sklearn.preprocessing import MinMaxScaler
from keras.models import Sequential
from keras.layers import LSTM, Dense

# Example time-series data (network traffic over time)
data = pd.read_csv('network_traffic_data.csv')
traffic_data = data[['traffic_volume']].values

# Normalize the data
scaler = MinMaxScaler(feature_range=(0, 1))
traffic_data_scaled = scaler.fit_transform(traffic_data)

# Prepare the data for LSTM model
X = []
y = []

for i in range(60, len(traffic_data_scaled)):
    X.append(traffic_data_scaled[i-60:i, 0])
    y.append(traffic_data_scaled[i, 0])

X = np.array(X)
y = np.array(y)

X = np.reshape(X, (X.shape[0], X.shape[1], 1))

# Define and train the LSTM model
model = Sequential()
model.add(LSTM(units=50, return_sequences=True, input_shape=(X.shape[1], 1)))
model.add(LSTM(units=50, return_sequences=False))
model.add(Dense(units=1))
model.compile(optimizer='adam', loss='mean_squared_error')

model.fit(X, y, epochs=5, batch_size=32)

# Predict and detect anomalies
predictions = model.predict(X)
```

Figure 6: *Python code for anomaly detection using LSTM.*

After detecting anomalies, the traffic can be classified into different attack types (e.g., DoS, DDoS, etc.) using the XGBoost model as shown in Figure 7.

```python
import xgboost as xgb
from sklearn.model_selection import train_test_split
from sklearn.metrics import accuracy_score

# Example data (features from network traffic logs)
X = np.array([[traffic_volume, response_time, packet_loss] for traffic_volume, response_time, packet_loss \
in zip(data['traffic_volume'], data['response_time'], data['packet_loss'])])
y = data['attack_label']  # Labels: 0 for normal, 1 for DoS, 2 for DDoS, etc.

# Train-test split
X_train, X_test, y_train, y_test = train_test_split(X, y, test_size=0.2)

# Initialize and train the XGBoost model
model = xgb.XGBClassifier(use_label_encoder=False)
model.fit(X_train, y_train)

# Predict and evaluate accuracy
y_pred = model.predict(X_test)
accuracy = accuracy_score(y_test, y_pred)
print(f"Accuracy of Attack Classification: {accuracy*100:.2f}%")
```

Figure 7: Attack classification using XGBoost

In this section, we utilize the NSL-KDD dataset, a refined version of the KDD Cup 1999 dataset [20], to train and evaluate the Long Short-Term Memory (LSTM) network for anomaly detection and XGBoost for attack classification. The NSL-KDD dataset, with its diverse attack types and detailed feature set, provides an excellent foundation for developing and benchmarking models in network security.

LSTM model for anomaly detection

Input Features: Packet volume, Connection duration. Source bytes and destination bytes.

Preprocessing: Continuous features are normalized using Min-Max scaling, and categorical features are one-hot encoded (Table 5).

Split: 80% training and 20% testing for evaluation.

Table 5: *Baseline performance.*

Metric	Performance
Precision	90.8%
Recall	88.7%
F1-score	89.7%
AUC-ROC	93.2%

XGBoost model for attack classification

- Input Features: Protocol type, service type, and flag, Statistical metrics like packet size and connection count.
- Training and Testing: Split: 70% training and 30% testing.
- Feature Importance: XGBoost ranks the most significant features (e.g., protocol type, service type) to improve interpretability (Table 6).

Table 6: *Baseline performance.*

Metric	Performance
Accuracy	94.1%
Precision	92.9%
Recall	91.2%
F1-Score	92.0%

LSTM for anomaly detection

- Detects both known and unknown anomalies in real-time.
- Highly effective for identifying zero-day threats due to its ability to learn temporal patterns in network traffic.

XGBoost for classification

- Convert anomalies into actionable intelligence by classifying them into specific attack types.
- Prioritizes attack categories for efficient response and mitigation.

Sequential Detection: LSTM ensures no time-based anomalies go undetected. Specific Classification: XGBoost enhances detection by categorizing threats, aiding in targeted incident response.

3.4. Integration of NGFW and ZTA

The integration of Next-Generation Firewalls (NGFW) and Zero Trust Architecture (ZTA) creates a multi-layered security framework, ensuring continuous, context-aware protection in data center networks.

3.4.1. Key roles of NGFW and ZTA

- Next-Generation Firewalls (NGFW)
- Deep Packet Inspection (DPI): Analyzes application-layer traffic to detect threats.
- Intrusion Prevention (IPS): Real-time blocking of malicious activities.
- Application Awareness: Enforces granular control over traffic based on application behavior.
- Encrypted Traffic Handling: Decrypts SSL/TLS traffic for inspection.

3.4.2. Zero Trust Architecture (ZTA)

- Identity and Access Management (IAM): Continuously verifies users and devices.
- Micro-Segmentation: Isolates network zones to limit lateral movement.
- Dynamic Policy Enforcement: Applies rules based on real-time context like user role, device health, and location.

3.4.3. How NGFW and ZTA work together

- Perimeter Defense with NGFW: Filters incoming and outgoing traffic, blocking known threats and suspicious activities at the boundary.
- Internal Validation with ZTA: Verifies user and device identity and apply role-based, least-privilege access controls within the network.
- Example Workflow: External traffic passes through NGFW for inspection. ZTA validates access requests using IAM and contextual factors (e.g., geolocation, device compliance). If complaint, access is granted; anomalies trigger alerts and isolation.

3.4.4. Key features of integration

- Granular Policy Enforcement: NGFW blocks malicious traffic, ZTA enforces contextual access controls.
- Unified Threat Visibility: NGFW detects network-level threats, ZTA monitors user/device behaviors.
- Incident Response Automation: NGFW alerts trigger ZTA's automated isolation of compromised entities.
- Secured Micro-Segmentation: Traffic between network segments is both segmented and inspected for anomalies.

3.4.5. Advantages

- Enhanced Security: Combines perimeter and internal defenses for zero-trust enforcement.
- Real-Time Protection: Blocks threats dynamically at multiple layers.
- Scalability: Adapts to hybrid cloud and multi-cloud environments.
- Compliance: Ensures adherence to standards like GDPR and HIPAA with unified policies.

4. Conclusion

The proposed network security architecture for data center environments, which integrates cutting-edge technologies such as Next-Generation Firewalls (NGFWs), Zero Trust Architecture (ZTA), AI-driven anomaly detection, SQL-based policy management, and Neo4j knowledge graphs, offers a robust and scalable solution for mitigating modern cybersecurity threats. This comprehensive framework ensures that all layers of the network are protected, from the perimeter to internal communications, by continuously validating users, monitoring network traffic, and analyzing relationships within the network topology.
Key aspects of the proposed system include:

- Next-Generation Firewalls (NGFWs): These firewalls provide deep packet inspection and application-layer filtering, which are crucial for identifying and blocking advanced threats. Their ability to integrate with the overall network security system enhances the protection of the data center perimeter.
- Zero Trust Architecture (ZTA): By enforcing the principle of least privilege and requiring continuous verification of all requests, ZTA ensures that access to network resources is granted only to authenticated and authorized entities. This approach significantly reduces the risk of internal breaches and unauthorized access.
- AI-Powered Anomaly Detection: The integration of machine learning models, particularly Long Short-Term Memory (LSTM) networks, enables the system to automatically detect unusual patterns in network traffic, which could indicate potential security breaches. The AI-based approach offers real-time threat detection, enabling swift mitigation actions before any damage is done.
- SQL Database for Policy Management: The use of a relational database for storing and managing security policies allows for granular access control and enforcement. The database structure ensures that security policies are consistently applied across the entire network, and access to sensitive resources is tightly controlled.
- Neo4j Knowledge Graphs: Neo4j's graph-based data model provides a powerful means of visualizing and analyzing network topology, user interactions, and communication paths. The knowledge graph not only helps in detecting anomalous activities but also allows for the proactive identification of attack paths, vulnerabilities, and network misconfigurations, thereby enhancing situational awareness and the overall security posture of the data center.

This integrated approach offers several advantages over traditional security frameworks. First, the use of AI and machine learning for anomaly detection enables faster identification and response to emerging threats. Second, the combination of NGFWs, ZTA, and a relational database ensures a multi-layered defense mechanism that is highly effective against both external and internal threats. Finally, the knowledge graph provides a comprehensive, dynamic view of the network, helping security professionals understand the relationships between entities, track potential attack vectors, and make data-driven decisions.

The implementation of this architecture not only enhances the security of the data center network but also significantly reduces operational overhead by automating threat detection, incident response, and policy enforcement. This architecture can be scaled to accommodate the growing needs of modern enterprises, providing a flexible, efficient, and resilient security framework.

In conclusion, the integration of advanced technologies such as NGFW, ZTA, AI models, SQL-based policy management, and Neo4j knowledge graphs offers a sophisticated and comprehensive approach to securing data center networks in an increasingly complex digital landscape. The proposed architecture is well-suited for mitigating the evolving cybersecurity challenges faced by modern enterprises, ensuring both operational efficiency and robust protection against evolving cyber threats.

6. Limitations and Future Work

Integrating NGFW, ZTA, AI/ML models, SQL databases, and Neo4j into a unified framework requires seamless orchestration, which can increase operational complexity and implementation time. Real-time processing of large-scale traffic data in dynamic data center environments can strain resources, especially with AI/ML models and graph-based analytics. Distributed frameworks like Apache Kafka or Spark can be utilized to enhance the framework's ability to process large-scale traffic in real time. AI models like LSTM can generate high false-positive rates, leading to alert fatigue and diverting resources from genuine threats. By incorporating ensemble learning and explainable AI techniques can improve detection accuracy, reduce false positives, and provide actionable insights. Training and deploying resource-heavy models (e.g., LSTM, XGBoost) can require significant computational power, posing challenges for real-time applications in resource-constrained settings. Adaptive Zero Trust policies can be developed that leverage real-time AI insights to minimize manual policy updates and improve responsiveness. Neo4j can be optimized, or faster graph processing tools can be integrated for real-time visualization of anomalies, lateral movements, and attack vectors.

References

1. Noel S, Harley E, Tam KH, et al. CyGraph: graph-based analytics and visualization for cybersecurity. In: Venkat NG, Vijay VR, Venu G, et al (eds), Handbook of Statistics, Elsevier, Amsterdam, Netherlands. 2016: pp.117-67.

2. Angles R, Gutierrez C. Survey of graph database models. ACM Comput Surv. 2008;40:1-39.

3. Syed NF, Shah SW, Shaghaghi A, et al. Zero Trust Architecture (ZTA): a comprehensive survey. IEEE access. 2022;10:57143-79.

4. Fernandez EB, Brazhuk A. A critical analysis of Zero Trust Architecture (ZTA). Comput Stand Inter. 2024;89:103832.

5. Kaur R, Gabrijelcic D, Klobucar T. Artificial intelligence for cybersecurity: literature review and future research directions. Inf Fusion. 2023;97:101804.

6. Tang TA, Mhamdi L, McLernon D, et al. Deep learning approach for network intrusion detection in software defined networking. International conference on wireless networks and mobile communications, Fez, Morocco. 2016.

7. Wang S, Balarezo JF, Kandeepan S, et al. Machine learning in network anomaly detection: a survey. IEEE Access. 2021;9:152379-96.

8. Mostafa AM, Ezz M, Elbashir MK, et al. Strengthening cloud security: an innovative multi-factor multi-layer authentication framework for cloud user authentication. Appl Sci. 2023;13:10871.

9. Putri HA, Djibran N, Tulloh R. Implementation of next-generation firewalls to protect applications from malware attacks. J Indonesia Soc Tech. 2023;4:1961-70.

10. Seo W, Pak W. Real-time network intrusion prevention system based on hybrid machine learning. IEEE Access. 2021;9:46386-97.

11. Lamdakkar O, Ameur I, Eleyatt MM, et al. Toward a modern secure network based on next-generation firewalls: recommendations and best practices. Procedia Comput Sci. 2024;238:1029-35.

12. Pavlovic M, Zajeganovic M, Milivojevic M. Implementation of Next-Generation Firewalls in Modern Networks. International Scientific Conference ITEMA Recent Advances in Information Technology, Tourism, Economics, Management, and Agriculture, Maribor, Solvenia. 2023.

13. Vanin P, Newe T, Dhirani LL, et al. A study of network intrusion detection systems using artificial intelligence/machine learning. Appl Sci. 2022;12:11752.

14. Zhao X, Fok KW, Thing VL. Enhancing network intrusion detection performance using generative adversarial networks. ArXiv Preprint. 2024:2404.07464.

15. Colwill C. Human factors in information security: the insider threat–Who can you trust these days? Inf Secur Tech Rep. 2009;14:186-96.

16. Jada I, Mayayise TO. The impact of artificial intelligence on organisational cyber security: an outcome of a systematic literature review. Data and Information Management. 2023:100063.

17. Goodall J, Lutters W, Komlodi A. Developing expertise for network intrusion detection. IT & People. 2009;22:92-108.

18. Habeeb MS. Predictive analytics and cybersecurity. Singh N, Birla S, Ansari MD, et al (eds). Intelligent Techniques for Predictive Data Analytics, (1stedn), John Wiley & Sons, Hoboken, New Jersey. 2024:151-70.

19. Neupane K, Haddad R, Chen L. Next generation firewall for network security: a survey. In Southeast Con. 2018.

20. https://www.kaggle.com/datasets/hassan06/nslkdd