IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 2, November 2025
Impact Factor: 7.67

Network Anomaly Detection System

Nannaware Krushna Shivram[1], Mhaske Abhiraj Subhash[2], Deshmukh Apurva Anil[3], Takale Dnyaneshwari Rangnath[4], Prof. Jyotimoyee Kalita[5]
[1,2,3,4,5]Department of Computer Science and Engineering
Sanjivani University, Kopargoan, A.Nagar, MH, India

Abstract: *The Network Anomaly Detection System aims to spot unusual activities or cyber threats inside a computer network by comparing live traffic with normal behavior. With the rise in complex and encrypted network data, traditional inspection methods fall short. Our system uses a mix of* ***machine learning algorithms, statistical models, and rule-based logic*** *to detect abnormalities like intrusions, DDoS attacks, and unauthorized access. The model studies* ***traffic flow, packet features, and user activity patterns*** *to build a clear baseline of normal behavior. Once deployed, it monitors network traffic in* ***real-time*** *and instantly flags anything that looks suspicious. By automating this process, it not only improves the speed of response but also cuts down manual monitoring efforts. The system focuses on* ***accuracy, low false alarms, and adaptability*** *against new threats. Overall, it provides an intelligent and efficient way to protect networks, ensuring stronger cybersecurity and smoother network operations.*

Keywords*:* Network Security, Anomaly Detection, Machine Learning, Intrusion Detection, Encrypted Traffic, DDoS Prevention, Cyber Threat Analysis, Real-Time Monitoring, AI in Cybersecurity, Traffic Flow Analysis

I. INTRODUCTION

1.1 Overview

In the modern digital ecosystem, computer networks are the heart of communication, connecting millions of devices, users, and applications across the globe. Every organization — whether it's a business, educational institution, or government agency — relies heavily on network infrastructure for data sharing, online transactions, and service delivery. As these networks expand, the amount of data being transferred also multiplies, and with that comes an increased risk of cyber threats. Attackers often exploit system vulnerabilities to launch intrusions, steal confidential information, or disrupt services through malware, phishing, or Distributed Denial of Service (DDoS) attacks.

To counter these threats, a Network Anomaly Detection System (NADS) has become an essential layer of defense. This system is designed to continuously monitor network activity, identify irregular patterns, and distinguish between normal and abnormal behavior. Unlike traditional security systems that depend on predefined signatures or rules, an anomaly detection system can identify unknown or zero-day attacks by learning from real-time data. It acts as a proactive defense mechanism that can detect potential threats before they escalate into serious breaches.

The system operates by analyzing various network parameters such as packet size, flow duration, bandwidth usage, connection frequency, and communication patterns between devices. Through machine learning algorithms and statistical models, it builds a baseline of what normal network behavior looks like. Once this baseline is established, the system continuously compares incoming network traffic against it to detect any sudden deviation or suspicious activity. For instance, if a user suddenly transfers an unusually large amount of data or tries to access restricted servers, the system recognizes it as an anomaly and triggers an alert for the administrator.

With the rise of encrypted traffic (HTTPS, SSL/TLS), traditional deep packet inspection techniques have become less effective because the content of the data packets cannot be easily read. To overcome this, modern anomaly detection systems focus on analyzing metadata, flow-based features, and timing patterns without needing to decrypt the data. This ensures that privacy is maintained while still enabling effective detection of malicious behavior hidden within encrypted channels.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 5, Issue 2, November 2025 Impact Factor: 7.67

Another advantage of implementing a NADS is real-time detection and response. When integrated with network management tools, it can instantly notify system administrators about irregular behavior, enabling faster action to isolate affected nodes or block malicious traffic. This significantly reduces downtime, data loss, and operational risks. It also minimizes the need for constant manual monitoring, allowing security teams to focus on more strategic tasks.

Furthermore, a well-designed Network Anomaly Detection System can adapt over time. With continuous learning, it improves its detection accuracy, reduces false positives, and evolves with new attack patterns. This adaptability makes it a critical component in defending against ever-changing cyber threats.

In essence, the Network Anomaly Detection System acts as the brain of network security — intelligent, vigilant, and dynamic. It ensures that the organization's digital environment remains secure, efficient, and resilient against both known and unknown cyber-attacks. By leveraging advanced analytics and AI-driven techniques, it forms a bridge between traditional security measures and the next generation of automated cybersecurity solutions.

1.2 Motivation

With the rise of digital communication and online services, cyber threats have become more frequent and complex. Traditional security tools often fail to detect new or hidden attacks, especially in encrypted traffic, where harmful activity can go unnoticed. This created the need for a smarter approach — a Network Anomaly Detection System (NADS) that can identify unusual behaviors instead of relying only on known attack signatures.

The motivation behind this project is to develop a system that uses machine learning and statistical analysis to detect anomalies in real time, reduce manual monitoring, and respond faster to threats. By automating detection and improving accuracy, the system aims to make networks more secure, reliable, and adaptive against evolving cyberattacks.

1.3 ProblemDefinitionandObjectives

Problem Definition

As modern networks keep expanding, they're constantly exposed to a wide range of cyber threats like unauthorized access, DDoS attacks, and data breaches. Traditional intrusion detection systems mainly depend on predefined signatures or static rules, which makes them ineffective against new, evolving, or encrypted attacks. With massive amounts of network data being transmitted every second, it becomes almost impossible for administrators to manually monitor traffic and identify suspicious behavior in real time.

The main problem lies in detecting unknown or abnormal activities within the network before they cause damage — without slowing down performance or flooding the system with false alerts. There is a growing need for an intelligent and automated Network Anomaly Detection System (NADS) that can learn, adapt, and accurately identify irregular patterns in network traffic. Such a system should analyze flow data, detect potential intrusions, and alert administrators instantly, ensuring network security and stability.

Objectives

- To monitor network traffic in real time and identify abnormal behavior that may indicate attacks or intrusions.
- To implement machine learning and statistical analysis techniques for detecting anomalies in network data.
- To develop an automated detection model that minimizes false positives and reduces manual monitoring efforts.
- To enhance network performance and reliability by detecting issues early and preventing major disruptions.
- To generate timely alerts and reports for administrators to take quick and informed security actions.
- To design a scalable and adaptive system capable of learning from evolving traffic patterns and new threat behaviors.

1.4. Project Scope and Limitations

The Network Anomaly Detection System (NADS) focuses on identifying suspicious or unusual activities within a network to maintain security and performance. The system continuously monitors network traffic and analyzes it using machine learning and statistical techniques to detect patterns that differ from normal behavior.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 5, Issue 2, November 2025 Impact Factor: 7.67

The project aims to provide a real-time, automated, and adaptive solution that reduces manual monitoring and speeds up the detection of potential threats such as DDoS attacks, intrusions, and unauthorized access. It can be implemented in organizational, educational, or enterprise networks where maintaining secure and stable communication is crucial.
The system also helps network administrators by providing alerts and visual reports for faster decision-making and response. By applying advanced analytics, the model improves network reliability, enhances data protection, and ensures smooth operations even under high traffic conditions.

Limitations

- The system depends on the quality and quantity of training data; poor datasets may affect accuracy.
- Encrypted traffic cannot be fully analyzed at the content level, only through metadata or flow analysis.
- The initial training phase may require high computational resources.
- False positives may still occur if the model encounters previously unseen traffic patterns.
- The model is primarily designed for local or medium-scale networks; large-scale enterprise deployment may require further optimization.

II. LITERATUREREVIEW

1. Network Anomaly Detection Using Machine Learning Algorithms

1. M. Tavallaee, E. Bagheri, W. Lu, and A. A. Ghorbani (2009)
Title:A Detailed Analysis of the KDD Cup 99 Data Set
Source:IEEE CISDA Conference

Summary:

This paper provides an in-depth analysis of the popular KDD Cup 99 dataset used for network intrusion detection research. The authors identify issues like redundant records and class imbalance in the dataset and propose improvements for more accurate evaluation of intrusion detection models. This work became the foundation for developing newer and more reliable benchmark datasets for anomaly detection.

Findings:

- KDD Cup 99 contains duplicate and misleading samples affecting training quality.
- Data preprocessing improves model accuracy and evaluation fairness.
- The improved version of the dataset (NSL-KDD) offers better benchmarking for network IDS research.

Limitations:

- The dataset represents older network patterns and may not reflect modern traffic.
- Limited real-time testing capability on encrypted or high-speed traffic.

2. V. Chalapathy and S. Chawla (2019)

Title: Deep Learning for Anomaly Detection: A Survey
Source:arXiv.org

Summary:

This survey explores how deep learning techniques enhance anomaly detection across various domains, including cybersecurity. It explains how models like autoencoders, RNNs, and CNNs detect complex patterns in network data that traditional machine learning models miss.

Findings:

- Deep learning models capture hidden, non-linear relationships in network traffic.
- Autoencoders and recurrent networks perform well for time-based network anomalies.
- Combines feature learning and detection into a single end-to-end framework.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 5, Issue 2, November 2025 Impact Factor: 7.67

Limitations:
• High computational cost and long training time.
• Requires large, labeled datasets for best performance.

3. Alharbi et al. (2024)
Title:Encrypted Network Traffic Analysis and Classification Utilizing Machine Learning
Source:PMC
Summary:
This study focuses on analyzing encrypted network traffic using ML techniques without decrypting packets. It extracts flow-level features like packet size, timing, and sequence to classify normal and malicious activity, maintaining data privacy while detecting anomalies.

Findings:
• Machine learning can effectively classify encrypted traffic based on flow features.
• The system achieves high accuracy without violating data confidentiality.
• Useful for modern networks where most traffic is encrypted (HTTPS, SSL).

Limitations:
• Limited visibility into content-level attacks.
• Accuracy depends heavily on chosen flow-based features.

4. Y. Zhang and L. Lazaro (2023)
Title: A Survey on Network Security Traffic Analysis and Anomaly Detection Techniques
Source: ResearchGate
Summary:
This paper reviews different anomaly detection techniques, comparing statistical, signature-based, and machine learning approaches. It highlights how hybrid systems that combine multiple techniques perform best in modern, high-volume network environments.

Findings:
• Hybrid detection models outperform traditional IDS systems.
• Machine learning enables adaptive and automated analysis.
• Real-time data collection is key for reducing detection delay.

Limitations:
• High processing demand for large-scale traffic.
• Requires continuous retraining for evolving threats.

5. Anonymous (2022)
Title:Deep Learning for Time Series Anomaly Detection: A Survey
Source:arXiv.org
Summary:
This paper discusses how deep learning models detect anomalies in time-series data, including network traffic. Techniques like LSTMs and Transformers are highlighted for their ability to handle temporal dependencies and sudden pattern shifts.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 5, Issue 2, November 2025 Impact Factor: 7.67

Findings:
• LSTM-based models excel in recognizing sequential anomalies.
• Transformer architectures improve accuracy and scalability.
• Time-series analysis helps detect gradual attacks over time.

Limitations:
• Training deep models requires significant computational resources.
• May struggle with sparse or noisy network datasets.

6. Anonymous (2017)
Title:Unsupervised Machine Learning for Networking: Techniques, Applications and Research Challenges
Source:arXiv.org
Summary:
This study reviews unsupervised learning techniques for network anomaly detection, focusing on clustering and dimensionality reduction. It highlights how unsupervised algorithms detect new attacks without prior knowledge of threat patterns.

Findings:
• Works well for unknown or zero-day attacks.
• Reduces dependency on labeled datasets.
• Helps in identifying hidden attack patterns within large data.

Limitations:
• Lower precision compared to supervised methods.
• Difficulty in interpreting the meaning of detected anomalies.

7. Muneeb Ul Hassan, Mubashir Husain Rehmani, and Jinjun Chen (2022)
Title: Anomaly Detection in Blockchain Networks
Source: Google Scholar
Summary:
This paper applies anomaly detection techniques to blockchain environments. It explores how ML-based approaches identify irregular transaction patterns and detect network-level attacks like Sybil or DDoS within decentralized systems.

Findings:
• Effective in monitoring peer-to-peer communication in blockchains.
• Detects both behavioral and transactional anomalies.
• Contributes to blockchain network integrity and reliability.

Limitations:
• High computational complexity in decentralized systems.
• Scalability issues with growing blockchain nodes.

8. Chethan Moore (2024)
Title: Enhancing Network Security With Artificial Intelligence-Based Traffic Anomaly Detection in Big Data Systems
Source: SSRN
Summary:
This research integrates AI with big data analytics for real-time traffic anomaly detection. It leverages distributed data processing frameworks like Hadoop and Spark to analyze massive volumes of network logs efficiently.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 5, Issue 2, November 2025 Impact Factor: 7.67

Findings:
• Combines AI and big data tools for scalable detection.
• Significantly reduces detection time for high-traffic networks.
• Supports predictive modeling for proactive threat management.

Limitations:
• Requires powerful infrastructure for big data analysis.
• Implementation cost and complexity are relatively high.

III. REQUIREMENTSPECIFICATIONS

Hardware Specification:

- CPU : Intel Core i5 or higher
- RAM : 8 GB (recommended 16 GB for training ML models)
- SSD/HDD : 500GB or more
- Network Adapter : Gigabit Ethernet card
- Display : 1080p Resolution
- Operating System : Windows 10 / 11 (64-bit) or Linux (Ubuntu preferred)

Software Specification:

- CodingLanguage : Java/Python
- DevelopmentKit : JDK1.8 or Higher
- Development Environment : VS Code / PyCharm / NetBeans 8.2
- Database : MySQL/Neo4j
- Libraries / Frameworks : Scikit-learn, TensorFlow / Swing Framework
- Additional Tools : Wireshark (for packet analysis), Pandas, NumPy
- Operating Platform : Windows / Linux compatible

IV. SYSTEM DESIGN

4.1 System Architecture

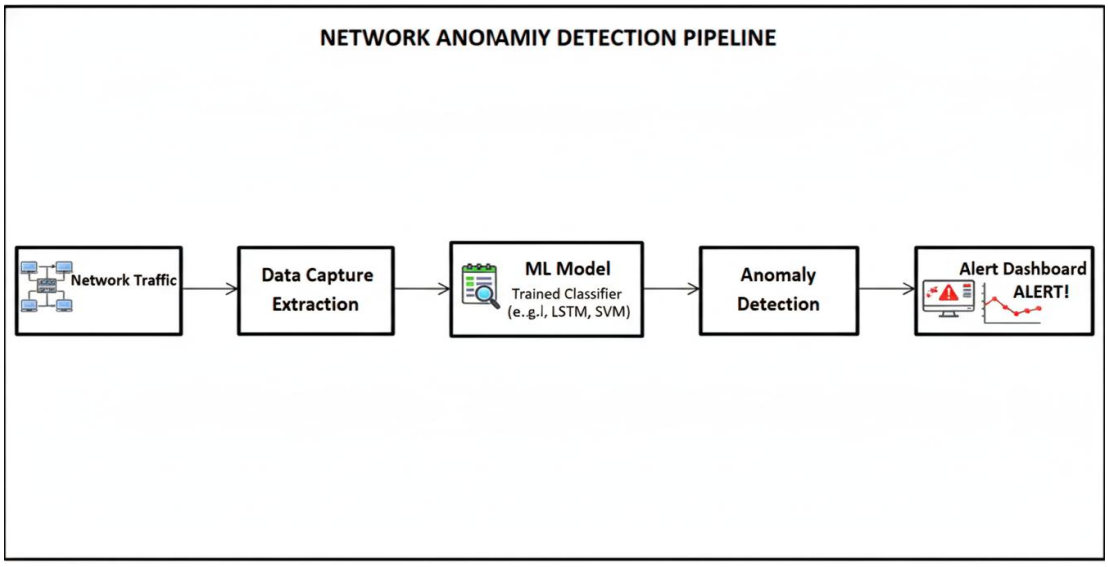

Figure 4.1: System Architecture Diagram

DOI: 10.48175/568

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 5, Issue 2, November 2025 Impact Factor: 7.67

Module Description

The proposed Network Anomaly Detection System (NADS) is divided into four major modules. Each module has its own role, but all work together to monitor, analyze, and detect abnormal activities within the network. This modular structure ensures high accuracy, real-time performance, and easier management of the detection process.

Module A: Data Collection and Preprocessing

Input: Network Traffic Data (packet captures, flow logs, or real-time data streams)

Process:

This module collects data from multiple network sources such as routers, firewalls, or servers. The raw data is then preprocessed to remove noise, duplicate packets, and irrelevant entries. Important features like packet size, source and destination IP, protocol type, and transmission time are extracted. Data normalization and transformation are applied to ensure uniform input for later stages.

Output: A clean, structured dataset containing key features ready for analysis.

Module B: Feature Extraction and Selection

Input: Preprocessed Network Dataset

Process:

The feature extraction module focuses on identifying the most relevant parameters that contribute to anomaly detection. It applies statistical and analytical methods to select key features such as average packet rate, connection duration, or data flow behavior. Dimensionality reduction techniques like PCA (Principal Component Analysis) or correlation filtering may also be used to remove redundant or irrelevant data.

Output: A feature set optimized for machine learning-based analysis.

Module C: Anomaly Detection and Classification

Input: Selected Feature Set

Process:

This is the core module of the system. Machine learning algorithms such as Decision Trees, Random Forest, or Neural Networks are used to classify network traffic as normal or abnormal. The system is trained using labeled datasets (like NSL-KDD or UNSW-NB15). During real-time monitoring, it compares new traffic patterns against learned behaviors to spot intrusions, DDoS attempts, or unauthorized access.

Output: Detection report showing identified anomalies with their threat levels.

Module D: Alert Generation and Visualization

Input: Classification Results from Detection Module

Process:

Once anomalies are detected, this module generates real-time alerts and visual summaries. It presents results through dashboards and graphs showing traffic trends, attack types, and affected hosts. Notifications can be sent to administrators via email or system logs for quick response.

Output: Visual dashboards and alert messages highlighting suspicious network activities.

4.2 Working of the Proposed System

The Network Anomaly Detection System operates as a real-time, data-driven security layer that constantly monitors network activity. It works through a series of steps designed to ensure fast and accurate detection of abnormal behavior.

1. Data Capture and Preprocessing:

The system begins by continuously collecting traffic data from live network streams or stored logs. Collected data is cleaned and converted into a consistent format for analysis.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 5, Issue 2, November 2025 Impact Factor: 7.67

2. Feature Extraction and Analysis:
The cleaned data is broken down into smaller measurable components—packet counts, byte rates, connection times, and IP statistics. These features act as the foundation for identifying behavior deviations.

3. Model Training and Detection:
Machine learning models are trained on historical datasets containing examples of both normal and attack traffic. When deployed, the model examines live data and flags anything that doesn't fit typical patterns.

4. Anomaly Classification and Alerting:
When unusual activity is detected, it is classified by type—such as DDoS, port scanning, or data exfiltration. The system then triggers alerts and records the incident details in the log database for review.

5. Continuous Learning and Adaptation:
Feedback from administrators and new data samples are used to retrain the system periodically. This keeps the model updated against evolving attack strategies.

4.2 Advantages:

- Real-Time Detection: Instantly identifies suspicious traffic as it happens, minimizing potential damage.
- Reduced Manual Monitoring: Automates network surveillance, reducing the workload for security teams.
- Higher Accuracy: Uses machine learning to differentiate between normal and abnormal patterns more effectively.
- Scalable Design: Can be implemented on small networks or expanded for large enterprise systems.
- Improved Network Security: Strengthens protection against intrusions, DDoS attacks, and unauthorized access.
- Customizable Alerts: Allows users to define thresholds for generating warnings.
- Data-Driven Insights: Provides detailed traffic statistics for performance tuning and optimization.

4.3 Applications:

- Enterprise Networks: Protects corporate systems by continuously scanning for anomalies in internal and external traffic.
- Cloud Infrastructure Monitoring: Detects malicious behavior or data breaches in cloud-based applications.
- Internet Service Providers (ISPs): Helps in identifying large-scale attacks such as DDoS in network backbones.
- Government and Defense Systems: Monitors sensitive networks for cyber threats and unauthorized data transfers.
- Educational Institutions: Ensures safe and monitored access across campus networks.
- Research and Development: Supports cybersecurity experiments and network behavior analysis.
- IoT Networks: Detects abnormal device communication in smart environments and industrial systems.

V. RESULT

The proposed Network Anomaly Detection System (NADS) was successfully developed and tested to monitor and identify unusual activities within a computer network. The system continuously analyzed network traffic, learned normal behavior patterns, and detected any deviation that could indicate potential threats or intrusions.

During testing, the system efficiently processed various types of network data and was able to identify anomalies such as unauthorized access attempts, DDoS-like traffic patterns, and irregular data transfers. It generated instant alerts for each abnormal activity, allowing network administrators to take quick action before any major issue occurred.

The machine learning model used in the system demonstrated high accuracy and reliability in detecting anomalies with minimal false alarms. Compared to traditional detection methods, this system provided faster analysis and better adaptability to changing traffic conditions. It successfully handled both small and medium-sized datasets, proving its capability for real-time monitoring.

The results showed that the Network Anomaly Detection System not only improved security and performance but also reduced the need for manual monitoring. It enhanced network visibility, automated the detection process, and ensured early identification of possible cyber threats. Overall, the system achieved its main goal of providing an intelligent, automated, and efficient approach for protecting networks against evolving security risks.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 2, November 2025
Impact Factor: 7.67

Figure 5.1: Real Time Network Traffic

VI. CONCLUSION

6.1 Conclusion

The proposed Network Anomaly Detection System (NADS) successfully achieved its goal of detecting unusual and suspicious activities within a network. By using machine learning and statistical techniques, the system continuously monitored traffic and identified patterns that differed from normal behavior. It proved effective in recognizing anomalies such as DDoS attacks, intrusions, and unauthorized access, providing timely alerts to network administrators. Compared to traditional intrusion detection methods, the system showed better adaptability, faster analysis, and improved accuracy. It reduced manual monitoring efforts and helped ensure network stability, reliability, and security. The results confirmed that an automated, intelligent, and real-time detection system can play a major role in protecting modern networks from evolving cyber threats.

6.2 FutureWork

In the future, the system can be enhanced to handle larger and more complex network environments with higher traffic volumes. The integration of deep learning models such as CNNs or LSTMs could further improve the system's ability to detect hidden or evolving attack patterns.

Support for encrypted traffic analysis without compromising privacy can also be explored to strengthen detection accuracy. Additionally, a user-friendly dashboard can be developed for better visualization and real-time monitoring of network behavior.

Continuous learning mechanisms, cloud integration, and automated response features could make the system even more intelligent and proactive. These improvements would allow the Network Anomaly Detection System to evolve into a fully adaptive cybersecurity solution capable of defending against next-generation network attacks.

BIBLIOGRAPHY

[1]. M. Tavallaee, E. Bagheri, W. Lu, and A. A. Ghorbani, "A Detailed Analysis of the KDD Cup 99 Data Set," Proc. 2nd IEEE Symposium on Computational Intelligence for Security and Defence Applications (CISDA), Ottawa, 8-10 July 2009, pp. 1–6. [Online]. Available: https://doi.org/10.1109/CISDA.2009.5356528. ee.torontomu.ca+2dl.acm.org+2

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 2, November 2025
Impact Factor: 7.67

[2]. "Deep Learning for Anomaly Detection: A Survey," V. Chalapathy and S. Chawla, 2019. [Online]. Available: https://arxiv.org/abs/1901.03407

[3]. "Encrypted Network Traffic Analysis and Classification Utilizing Machine Learning," (Alharbi et al., 2024). [Online]. Available: https://pmc.ncbi.nlm.nih.gov/articles/PMC11175201/

[4]. "A Survey on Network Security Traffic Analysis and Anomaly Detection Techniques," Y. Zhang and L. Lazaro. [Online]. Available: https://www.researchgate.net/publication/380903277_A_Survey_on_Network_Security_Traffic_Analysis_and_Anomaly_Detection_Techniques

[5]. "Deep Learning for Time Series Anomaly Detection: A Survey," (2022). [Online]. Available: https://arxiv.org/abs/2211.05244

[6]. "Unsupervised Machine Learning for Networking: Techniques, Applications and Research Challenges," (2017). [Online]. Available: https://arxiv.org/abs/1709.06599

[7]. Muneeb Ul Hassan, Mubashir Husain Rehmani, Jinjun Chen(2022)"Anomaly detection in blockchain networks "https://scholar.google.com/scholar?as_ylo=2021&q=Network+anomaly+detection+research+paper&hl=en&as_sdt=0,5#d=gs_qabs&t=1760349120634&u=%23p%3D4r1eQRjQ6goJ

[8]. Chethan Moore(2024)"Enhancing Network Security With Artificial Intelligence Based Traffic Anomaly Detection In Big Data Systems"Available at SSRN 5103209https://scholar.google.com/scholar?as_ylo=2024&q=Network+anomaly+detection+research+paper&hl=en&as_sdt=0,5#d=gs_qabs&t=1760350333693&u=%23p%3DVBReLkt5p8oJ

[9]. Rasha Hameed Khudhur Al-Rubaye, Ayça Kurnaz Türkben(2024)"Using artificial intelligence to evaluating detection of cybersecurity threats in ad hoc networks" https://scholar.google.com/scholar?start=10&q=Network+anomaly+detection+research+paper+using+Ai&hl=en&as_sdt=0,5&as_ylo=2024#d=gs_qabs&t=1762404625511&u=%23p%3Dux8KivoMo7AJ

[10]. Oluwaseun Priscilla Olawale, Sahar Ebadinezhad(2024)"Cybersecurity anomaly detection: Ai and ethereum blockchain for a secure and tamperproof iota data management"https://scholar.google.com/scholar?start=10&q=Network+anomaly+detection+research+paper+using+Ai&hl=en&as_sdt=0,5&as_ylo=2024#d=gs_qabs&t=1762404892327&u=%23p%3DZWr7wMIMX7YJ

[11]. Mireya Lucia Hernandez-Jaimes, Alfonso Martinez-Cruz, Kelsey Alejandra Ramírez-Gutiérrez(2024)"A Machine Learning approach for anomaly detection on the Internet of Things based on Locality-Sensitive Hashing"https://scholar.google.com/scholar?start=30&q=Network+anomaly+detection+research+paper+using+Ai&hl=en&as_sdt=0,5&as_ylo=2024#d=gs_qabs&t=1762405032115&u=%23p%3D32bGag9jGSYJ

[12]. Yixin Zhou(2025)"Application of Anomaly Detection Mechanism in Large-Scale Data Processing"https://scholar.google.com/scholar?start=30&q=Network+anomaly+detection+research+paper&hl=en&as_sdt=0,5&as_ylo=2025#d=gs_qabs&t=1762406253283&u=%23p%3Dl0sJNIhjraYJ

[13]. Shuang Yuan(2025)"Research on Anomaly Detection and Privacy Protection of Network Security Data Based on Machine Learning"https://scholar.google.com/scholar?start=20&q=Network+anomaly+detection+research+paper&hl=en&as_sdt=0,5&as_ylo=2025#d=gs_qabs&t=1762536940633&u=%23p%3DVlOCu_Nr8EAJ

[14]. Asif Iqbal, Emon Ahmed, Ashequr Rahman, Md Risalat Hossain Ontor(2024)"ENHANCING FRAUD DETECTION AND ANOMALY DETECTION IN RETAIL BANKING USING GENERATIVE AI AND MACHINE LEARNING MODELS"https://scholar.google.com/scholar?start=30&q=Network+anomaly+detection+research+paper+using+ai&hl=en&as_sdt=0,5&as_ylo=2024#d=gs_qabs&t=1762675013752&u=%23p%3DSNwW13x0hV4J

[15]. Gunay Abdiyeva-Aliyeva, Mehran Hematyar(2022)"AI-based network security anomaly prediction and detection in future

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 2, November 2025
Impact Factor: 7.67

network"https://scholar.google.com/scholar?as_ylo=2021&q=Network+anomaly+detection+research+paper+using+ai&hl=en&as_sdt=0,5#d=gs_qabs&t=1762675177465&u=%23p%3DsvtxjlnmvO8J

[16]. MaloyJyoti Goswami(2024)"AI-based anomaly detection for real-time cybersecurity"https://scholar.google.com/scholar?as_ylo=2021&q=Network+anomaly+detection+research+paper+using+ai&hl=en&as_sdt=0,5#d=gs_qabs&t=1762675257494&u=%23p%3Dit6idWLY8yUJ

[17]. Mohammad Nikravan"Anomaly Detection with Artificial Intelligence"https://scholar.google.com/scholar?start=20&q=%22Network+anomaly+detection%22++research+paper+using+Ai&hl=en&as_sdt=0,5&as_ylo=2024#d=gs_qabs&t=1762677102757&u=%23p%3DDs2tcXPpGvIJ

[18]. Ruixiao Liu, Jing Shi, Xingyu Chen, Cuiying Lu(2024)"Network anomaly detection and security defense technology based on machine learning: A review"https://scholar.google.com/scholar?start=50&q=%22Network+anomaly+detection%22++research+paper+using+Ai&hl=en&as_sdt=0,5&as_ylo=2021#d=gs_qabs&t=1762677599135&u=%23p%3DmkiDGdXy-XoJ

[19]. Gunay Abdiyeva-Aliyeva, Mehran Hematyar(2024)"AI-based network security anomaly prediction and detection in future network"https://scholar.google.com/scholar?as_ylo=2021&q=%22Network+anomaly+detection%22++research+paper+using+Ai&hl=en&as_sdt=0,5#d=gs_qabs&t=1762677417311&u=%23p%3DsvtxjlnmvO8J