Global Journal of Researches in Engineering: F
Electrical and Electronics Engineering
Volume 25 Issue 1 Version 1.0 Year 2025
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals
Online ISSN: 2249-4596 & Print ISSN: 0975-5861

Modern Network Security Threats and Defense Mechanisms: A Comparative Study of Intrusion Detection and Prevention Systems

By Dr. Osama Amin Marie
Al Quds Open University

Abstract- In today's fast-changing digital world, network security has become a critical issue due to the growing frequency and sophistication of cyberattacks [1], [2]. This study provides a detailed analysis of modern network threats and evaluates how defense mechanisms—especially Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS)—can help mitigate these risks. The paper explores current attack vectors, including Distributed Denial-of-Service (DDoS), Man-in-the-Middle (MitM), phishing, and threats that specifically target Internet of Things (IoT) environments [3].

A comparative overview of signature-based and anomaly-based IDS/IPS techniques is presented, with special emphasis on the role of artificial intelligence and machine learning in improving detection accuracy and accelerating response times [4]. Real-world case studies involving widely adopted tools such as Snort and Suricata are examined to illustrate their effectiveness.

Keywords: *network security, intrusion detection systems, cyber threats, zero trust architecture, ransomware, advanced persistent threats, machine learning, data encryption, phishing, firewalls.*

GJRE-F Classification: *ACM: B.8.1, UDC: 004.415*

Strictly as per the compliance and regulations of:

Modern Network Security Threats and Defense Mechanisms: A Comparative Study of Intrusion Detection and Prevention Systems

Dr. Osama Amin Marie

Abstract- In today's fast-changing digital world, network security has become a critical issue due to the growing frequency and sophistication of cyberattacks [1], [2]. This study provides a detailed analysis of modern network threats and evaluates how defense mechanisms—especially Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS)—can help mitigate these risks. The paper explores current attack vectors, including Distributed Denial-of-Service (DDoS), Man-in-the-Middle (MitM), phishing, and threats that specifically target Internet of Things (IoT) environments [3].

A comparative overview of signature-based and anomaly-based IDS/IPS techniques is presented, with special emphasis on the role of artificial intelligence and machine learning in improving detection accuracy and accelerating response times [4]. Real-world case studies involving widely adopted tools such as Snort and Suricata are examined to illustrate their effectiveness. The findings suggest that hybrid detection systems, when aligned with Zero Trust Architecture (ZTA), offer a proactive and resilient framework for defending modern networks.

Keywords: network security, intrusion detection systems, cyber threats, zero trust architecture, ransomware, advanced persistent threats, machine learning, data encryption, phishing, firewalls.

I. Introduction

The proliferation of interconnected systems, cloud computing platforms, and Internet of Things (IoT) devices has significantly expanded the digital attack surface, making network security a critical priority. As organizations increasingly rely on complex network infrastructures, protecting the confidentiality, integrity, and availability of data has become central to cybersecurity strategies [5], [6].

Despite significant advancements in encryption, authentication, and access control mechanisms, networks remain vulnerable to a wide range of cyberattacks. These include Distributed Denial-of-Service (DDoS), Man-in-the-Middle (MitM), spoofing, and insider threats, which continue to challenge both public and private institutions [5], [6].

To address these evolving risks, cybersecurity professionals employ various defense mechanisms. Among the most essential are Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS). IDS solutions monitor and analyze network traffic to detect malicious behavior, whereas IPS technologies go a step further by actively blocking threats in real time [7].

These systems have evolved beyond traditional signature-based detection models, incorporating behavior-based techniques and artificial intelligence (AI) to identify advanced threats such as zero-day exploits and polymorphic malware [8]. However, no single approach is sufficient on its own. The complexity of today's network environments necessitates hybrid security frameworks that integrate multiple technologies and align with principles such as Zero Trust Architecture (ZTA) [9].

This paper presents a structured comparison of IDS and IPS technologies, explores their respective roles in modern network security, and analyzes real-world implementations involving tools like Snort, Suricata, and Zeek.

II. Overview of Network Security

Network security encompasses a collection of technologies, strategies, and administrative controls aimed at safeguarding the confidentiality, integrity, and availability of information transmitted across digital networks. As the backbone of modern infrastructure, networks are exposed to an array of threats originating both internally and externally, ranging from phishing and malware to highly sophisticated nation-state cyberattacks [10].

Traditional network defenses relied heavily on perimeter-based models that assumed internal systems were inherently trustworthy. However, with the rise of cloud computing, mobile devices, and bring-your-own-device (BYOD) practices, this assumption has become obsolete [12]. Modern organizations must now adopt adaptive, multi-layered security frameworks capable of addressing complex and distributed threat landscapes.

Fundamental security components include firewalls, which act as a primary control by filtering traffic based on defined rules. IDS and IPS technologies provide additional layers of protection by detecting and responding to suspicious activity. Virtual Private Networks (VPNs) ensure the confidentiality of data in transit, especially in remote work scenarios and cloud environments [11]. Other technologies—such as

Author: Assistant Professor, Computer Information System Department, Al Quds Open University. e-mail: omarie@qou.edu

antivirus software, network access control (NAC), data loss prevention (DLP), and multi-factor authentication (MFA)—further reinforce organizational security.

To meet evolving threats, many organizations are shifting toward Zero Trust Architecture (ZTA), which rejects the assumption of implicit trust and requires continuous verification of every user and device, regardless of their location within the network [13].

In recent years, artificial intelligence (AI) and machine learning (ML) have been increasingly integrated into network security systems. These tools enable automated detection of anomalies by learning normal network behavior and identifying deviations that may indicate potential threats [14]. For instance, anomaly-based IDS can recognize zero-day exploits that traditional signature-based methods might miss.

Moreover, Security Information and Event Management (SIEM) systems now play a central role by aggregating data from multiple sources, enabling centralized monitoring and real-time threat correlation. As workloads migrate to public and hybrid clouds, traditional perimeter tools lose effectiveness, prompting cloud providers to offer integrated solutions such as AWS Shield, Microsoft Defender for Cloud, and Google Chronicle [15].

Despite technological advancements, several challenges persist. Encrypted traffic limits the visibility of deep packet inspection tools. Advanced Persistent Threats (APTs) can evade detection for extended periods, and the ongoing shortage of skilled cybersecurity professionals continues to hinder the maintenance of effective defenses.

In summary, network security has evolved from static, perimeter-based models to intelligent, adaptive architectures that require continuous innovation to keep pace with emerging threats and technologies.

III. Modern Network Threats

The contemporary digital environment is fraught with a wide range of evolving threats that challenge the integrity, confidentiality, and availability of computer networks. These threats have grown not only in volume but also in sophistication, exploiting both technical vulnerabilities and human error. This section outlines the most prevalent network security threats, their mechanisms, and their impact on organizational systems.

a) Distributed Denial-of-Service (DDoS) Attacks

Today's digital environment faces an escalating array of sophisticated cyber threats that undermine the confidentiality, integrity, and availability of networked systems. These threats exploit both technological weaknesses and human vulnerabilities, evolving constantly in form and scale. This section highlights the most common modern network threats, their operational mechanisms, and their potential impact on organizations.

b) Distributed Denial-of-Service (DDoS) Attacks

DDoS attacks aim to disrupt normal operations by overwhelming a network or server with excessive traffic. Typically executed using botnets—networks of compromised devices—these attacks generate massive data floods that exceed the system's capacity to respond to legitimate requests. Advanced variations, such as amplification and application-layer attacks, are designed to inflict maximum disruption with minimal effort [16].

c) Man-in-the-Middle (MitM) Attacks

MitM attacks involve an unauthorized entity intercepting or manipulating communication between two legitimate parties. These attacks are especially dangerous on unsecured or poorly configured networks. Techniques such as SSL stripping and ARP spoofing allow attackers to impersonate endpoints, potentially accessing sensitive information without detection [17].

d) Phishing and Social Engineering

Phishing attacks deceive users into providing confidential information by impersonating trusted sources through fake emails, websites, or messages. These attacks are becoming increasingly targeted, employing tactics like spear-phishing and Business Email Compromise (BEC) to infiltrate organizations through personalized deception [18].

e) Insider Threats

Insider threats originate from individuals within the organization—such as employees, contractors, or vendors—who intentionally or unintentionally misuse their access privileges. Because these actors are already trusted, detecting anomalous behavior is challenging without continuous monitoring and behavior analytics [19].

f) IoT-based Attacks

The rapid expansion of Internet of Things (IoT) devices has created new vulnerabilities stemming from poor security practices, outdated firmware, and weak authentication. Compromised IoT devices can be harnessed into large-scale botnets or used as entry points into more secure areas of the network [20].

Table 1: Summary of Major Modern Network Threats

Threat Type	Target	Technique	Impact	Detection Difficulty
DDoS	Servers & Networks	Botnets, Amplification	Service disruption	Medium
Man-in-the-Middle	Communication Channels	ARP spoofing, SSL stripping	Data theft, session hijack	High
Phishing	End Users	Fake emails, malicious links	Credential compromise	Low (if trained)
Insider Threat	Internal Systems	Privilege misuse, sabotage	Data leakage, system damage	High
IoT Attacks	Connected Devices	Firmware flaws, open ports	Lateral movement, botnets	Medium–High

g) Advanced Persistent Threats (APTs)

APTs are coordinated and prolonged cyberattacks typically executed by well-funded adversaries such as nation-state actors. They use stealth, multi-stage infiltration, and persistence mechanisms to gain long-term access and exfiltrate sensitive data while evading conventional detection methods [21].

h) Ransomware in Networked Environments

Ransomware attacks encrypt critical data and demand payment for decryption keys. In networked environments, such malware can spread laterally across file shares and backup systems. Increasingly, attackers adopt double-extortion tactics—encrypting data and threatening to publish it—to pressure victims into compliance [22].

IV. Intrusion Detection Systems (IDS) vs. Intrusion Prevention Systems (IPS)

With the growing sophistication of cyberattacks, organizations increasingly depend on proactive tools to defend their digital assets. Among the most critical are Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS), which serve complementary but distinct functions.

a) Intrusion Detection Systems (IDS)

IDS are passive security solutions that monitor network traffic and alert administrators upon detecting unusual or potentially malicious activity. These systems fall into two main categories:

- *Signature-Based IDS* rely on predefined patterns or known attack signatures to identify threats. While efficient at detecting previously identified attacks, they struggle to recognize novel or zero-day exploits.
- *Anomaly-Based IDS*, on the other hand, use statistical modeling or machine learning algorithms to establish a baseline of normal behavior. Any significant deviation from this baseline is flagged as suspicious [23].

IDS tools are frequently integrated with Security Information and Event Management (SIEM) platforms to enable contextual threat analysis and post-incident investigation. However, their passive nature means they cannot actively block attacks in real time.

b) Intrusion Prevention Systems (IPS)

In contrast, IPS technologies operate inline with network traffic, allowing them to intercept and neutralize threats as they occur. Like IDS, IPS solutions can use either signature-based or anomaly-based detection models [24].

Advanced IPS capabilities include:

- Dropping malicious packets.
- Resetting compromised connections.
- Dynamically updating firewall rules in response to detected threats [24].

These systems are often deployed at network gateways to enforce policy controls before malicious traffic reaches critical systems.

c) Deployment Architecture

IDS can be implemented in two forms:

- *Network-Based IDS (NIDS),* which inspect traffic across entire network segments.
- *Host-Based IDS (HIDS),* which reside on individual machines and provide localized monitoring.

In contrast, IPS solutions are typically deployed as *Network-Based IPS (NIPS),* positioned inline to analyze and block traffic in real-time [25].

Table 2: Comparison between IDS and IPS

Feature	IDS	IPS
Primary Function	Monitor and alert	Monitor, alert, and block
Placement	Out-of-band (passive)	Inline (active)
Response Time	After-the-fact	Real-time
Blocking Capability	✕ No	✓ Yes
False Positives	Logged for review	May block legitimate traffic
Complexity	Moderate	High (requires tuning and maintenance)
Resource Usage	Lower	Higher (due to inline inspection)
Use Case	Forensic analysis, alerting	Automated response and prevention

d) Emerging Trends in IDS/IPS Technologies

Modern IDS and IPS tools are increasingly adopting machine learning to enhance detection accuracy and reduce false positives. Algorithms such as Support Vector Machines (SVM), decision trees, and neural networks are used to dynamically classify threats [26], [27].

Open-source solutions like Snort, Suricata, and Zeek have gained popularity due to their flexibility, extensibility, and strong community support [28]. These platforms support modular rule-based detection, real-time alerting, and protocol-aware inspection.

Moreover, with the adoption of Software-Defined Networking (SDN) and cloud-native infrastructure, IDS/IPS components are being embedded into programmable firewalls and orchestration layers (e.g., AWS WAF, Azure NSGs) [29].

V. Case Studies and Industry Applications

To assess the practical effectiveness of IDS and IPS technologies, this section presents a set of real-world case studies from diverse industries. Each scenario illustrates how organizations have leveraged detection and prevention systems to address specific cybersecurity challenges.

a) Telecommunications: Real-Time IPS against DDoS Attacks

A major European telecom provider experienced repeated volumetric and application-layer DDoS attacks that disrupted its VoIP infrastructure. Conventional firewalls failed to distinguish between legitimate and malicious traffic. To resolve this, the company implemented a hybrid IPS with deep packet inspection (DPI) and anomaly detection capabilities. Within one month, the IPS identified and blocked several attack campaigns, resulting in a significant reduction in downtime. Moreover, firewall policies were dynamically updated to protect backend services in real time [30].

b) Banking Sector: Enhancing Internal Monitoring with HIDS

A global financial institution deployed host-based IDS (HIDS) across its internal systems to detect unauthorized access, monitor file integrity, and observe privileged user activities. Tools like OSSEC and Wazuh enabled fine-grained visibility into endpoint behavior. In one notable incident, the HIDS detected a privilege escalation attempt triggered by a misconfigured script. The security team responded immediately, revised access policies, and prevented what could have been a major breach [31].

c) Healthcare: AI-Powered IDS Mitigates Ransomware Threat

A hospital network in North America faced a ransomware infection that targeted its electronic health records via a phishing email. Despite failing to detect the payload at the endpoint level, the organization's AI-enhanced IDS flagged anomalous encryption behavior across the network. This early warning allowed security personnel to isolate affected systems and restore data from backups within 24 hours, minimizing operational impact and safeguarding patient care [32].

d) Academic Institutions: Layered IDS Deployment for Open Networks

University networks are particularly vulnerable due to open-access policies and large user bases. A large public university deployed both Suricata and Zeek across its data centers and student access points. This layered architecture enabled detection of port scanning, brute-force login attempts, and DNS anomalies. Zeek's scripting engine allowed custom monitoring of certificate usage and suspicious domain queries. Weekly threat reports generated from IDS logs were also used to train IT staff and raise cybersecurity awareness among students [33].

e) Cloud Environments: IPS Integration in Microservices

A SaaS provider operating on Kubernetes adopted container-aware IPS (e.g., Aqua Security and Trend Micro Deep Security) as part of its DevSecOps pipeline. These IPS tools monitored east-west traffic between microservices and enforced runtime policies. The system detected unusual activity patterns like cryptocurrency mining in compromised containers. By integrating IPS into CI/CD workflows, the company ensured that container images were scanned before deployment and that runtime protections were active post-deployment [34].

VI. Discussion and Future Trends

The comparative evaluation of intrusion detection and prevention technologies reveals both the capabilities and limitations of current solutions. Signature-based systems continue to provide reliable protection against known threats, offering high accuracy and low false positive rates. However, their effectiveness diminishes when dealing with sophisticated or previously unseen attacks such as zero-day exploits and polymorphic malware [35].

Anomaly-based systems have emerged as a promising alternative, capable of identifying unknown threats through behavioral analysis and statistical modeling. Nevertheless, they are prone to generating a high volume of false alerts, which can overwhelm security teams and delay incident response [35].

Performance optimization also remains a significant concern. Inline IPS systems, although highly effective in real-time mitigation, may introduce latency or block legitimate traffic if not properly tuned. This makes policy configuration and system calibration essential,

particularly in time-sensitive sectors like finance and healthcare [36].

From an architectural standpoint, the traditional centralized monitoring approach is gradually being replaced by distributed, intelligence-driven models. As networks become more dynamic—due to mobile users, cloud services, and remote work—the perimeter becomes increasingly irrelevant. This shift supports the adoption of Zero Trust Architecture (ZTA), which applies continuous verification and least-privilege access controls throughout the network [37].

Artificial intelligence and machine learning are reshaping the field of intrusion detection. Advanced models can analyze large volumes of network traffic to uncover hidden patterns associated with malicious activity. Deep learning techniques, such as convolutional neural networks (CNNs) and recurrent neural networks (RNNs), have demonstrated potential in identifying sequence-based attack behaviors [38]. However, issues such as explainability, class imbalance, and vulnerability to adversarial inputs continue to challenge their widespread deployment.

Encrypted traffic also presents a double-edged sword. While it improves privacy, it restricts the effectiveness of traditional deep packet inspection (DPI) tools. Emerging methods like TLS fingerprinting, encrypted traffic analytics (ETA), and metadata analysis aim to bridge this gap without compromising confidentiality [39].

In cloud-native environments, micro-segmentation and container-aware security practices are becoming standard. Integrating security measures into development pipelines—known as "security-as-code"—enables earlier threat detection and minimizes exposure in production environments [40].

The emergence of AI-driven offensive techniques, such as automated exploit generation, deepfake phishing, and autonomous malware, necessitates a shift in defensive strategies. Collaborative threat intelligence sharing, behavior baselining, and continuous adaptation will be vital for building resilient, self-healing security systems.

In conclusion, the future of network security lies in adopting intelligent, adaptable, and context-aware systems. IDS and IPS will remain integral components, but their continued relevance depends on integration with automated analytics, distributed architecture, and Zero Trust principles.

VII. Conclusion

In light of increasingly complex cyber threats, securing digital infrastructure has become an essential objective for both public and private organizations. This study offered an in-depth analysis of modern network threats and assessed the capabilities of Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) in responding to these challenges.

While signature-based approaches remain reliable for identifying known attack vectors, they are inherently limited in detecting sophisticated or novel threats, such as zero-day exploits [35]. In contrast, anomaly-based systems extend the detection range but often suffer from false positives that can hinder operational efficiency [35]. The integration of artificial intelligence and machine learning within IDS/IPS frameworks improves their adaptability by enabling faster, context-aware threat recognition and response [36].

Case studies across various sectors—including telecommunications, healthcare, finance, and academia—demonstrated that organizations deploying hybrid detection models benefit from enhanced threat visibility and reduced response time. When combined with the principles of Zero Trust Architecture (ZTA), these models contribute to a more proactive and resilient cybersecurity posture [37].

Moving forward, the next generation of defense mechanisms must incorporate intelligent automation, distributed enforcement, and context-aware access control. However, challenges such as the inspection of encrypted traffic, adversarial machine learning, and workforce shortages must also be addressed [38], [39].

Ultimately, IDS and IPS will remain essential components of modern cybersecurity strategies. Their ongoing relevance will depend not only on technical sophistication but also on their integration into dynamic, self-adaptive, and policy-driven security architectures [40].

References Références Referencias

1. S. Axelsson, "Intrusion detection systems: A survey and taxonomy," Technical Report, Chalmers University of Technology, 2000.
2. T. A. El-Darymli, P. G. Sant, and D. N. Serpanos, "A survey of intrusion detection systems in cloud computing," *Computer Communications*, vol. 95, pp. 85–105, Dec. 2016.
3. R. Roesch, "Snort—lightweight intrusion detection for networks," in *Proc. 13th USENIX Conf. Syst. Admin.*, 1999, pp. 229–238.
4. J. Kindervag, "Build security into your network's DNA: The Zero Trust Network Architecture," Forrester Research, Tech. Rep., 2010.
5. R. Sommer and V. Paxson, "Outside the closed world: On using machine learning for network intrusion detection," in *Proc. IEEE Symp. Security and Privacy*, 2010, pp. 305–316.
6. S. Al-Qahtani, A. Mahmood, and T. A. Alghamdi, "A survey on cyber security threats and detection techniques in network intrusion detection system," *IEEE Access*, vol. 9, pp. 56610–56636, 2021.

7. R. Roesch, "Snort—lightweight intrusion detection for networks," in *Proc. 13th USENIX Conf. Syst. Admin.*, 1999, pp. 238–242.
8. L. Buczak and E. Guven, "A survey of data mining and machine learning methods for cyber security intrusion detection," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 2, pp. 1153–1176, 2016.
9. J. Kindervag, "No more chewy centers: Introducing the Zero Trust Model of information security," Forrester Research, 2010.
10. P. Kumar and S. Agarwal, "Network security threats and solutions for organizations," *International Journal of Computer Applications*, vol. 165, no. 9, pp. 1–6, May 2017.
11. W. Stallings, *Network Security Essentials: Applications and Standards*, 6th ed., Pearson, 2017.
12. D. Shackleford, "The future of network security: Perimeterless architectures," *SANS Institute White Paper*, 2018.
13. J. Kindervag, "No more chewy centers: Introducing the Zero Trust Model of information security," Forrester Research, 2010.
14. L. Buczak and E. Guven, "A survey of data mining and machine learning methods for cyber security intrusion detection," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 2, pp. 1153–1176, 2016.
15. M. H. Sqalli and M. Alenezi, "Cloud security: A comprehensive guide to secure cloud computing," *Future Internet*, vol. 13, no. 2, p. 35, 2021.
16. Douligeris and D. N. Serpanos, "Network security: Current status and future directions," *Computers & Electrical Engineering*, vol. 30, no. 1, pp. 1–12, 2004.
17. Y. Liu, Y. Xia, and M. Zhang, "A survey on man-in-the-middle attacks," *Security and Communication Networks*, vol. 2021, Article ID 6637049, 2021.
18. Jain and B. Gupta, "A survey of phishing attack techniques, defenses and their implications," *Computers & Security*, vol. 86, pp. 70–90, 2019.
19. Greitzer and D. Frincke, "Combining traditional cyber security audit data with psychosocial data: Towards predictive modeling for insider threat mitigation," *Insider Threats in Cyber Security*, pp. 85–113, Springer, 2010.
20. J. Chen, S. Park, and J. Kim, "IoT security issues and challenges," *Journal of Information Processing Systems*, vol. 14, no. 2, pp. 353–362, 2018.
21. B. K. Sahu and S. Mohapatra, "Advanced persistent threat detection and mitigation techniques: A review," *IEEE Access*, vol. 9, pp. 123345–123364, 2021.
22. Kharraz et al., "Cutting the Gordian knot: A look under the hood of ransomware attacks," in *Proc. DIMVA*, Springer, 2015, pp. 3–24.
23. Patcha and J. M. Park, "An overview of anomaly detection techniques: Existing solutions and latest technological trends," *Computer Networks*, vol. 51, no. 12, pp. 3448–3470, 2007.
24. R. Bace and P. Mell, "Intrusion Detection Systems," NIST Special Publication 800-31, 2001.
25. S. Kumar and E. H. Spafford, "A pattern matching model for misuse intrusion detection," in *Proc. IEEE Symposium on Security and Privacy*, 1994, pp. 11–21.
26. L. Buczak and E. Guven, "A survey of data mining and machine learning methods for cyber security intrusion detection," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 2, pp. 1153–1176, 2016.
27. Sharafaldin, A. H. Lashkari, and A. A. Ghorbani, "Toward generating a new intrusion detection dataset and intrusion traffic characterization," in *Proc. ICISSP*, 2018, pp. 108–116.
28. M. Roesch, "Snort – Lightweight intrusion detection for networks," in *Proc. 13th USENIX Conf. Syst. Admin.*, 1999, pp. 229–238.
29. M. Alshamrani et al., "A survey on advanced persistent threats: Techniques, solutions, challenges, and research opportunities," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 2, pp. 1851–1877, 2019.
30. L. Chen, S. Sharma, and K. Ramakrishnan, "Real-time detection of DDoS attacks using adaptive filters," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 1, pp. 83–97, 2019.
31. OSSEC, "Open Source Host-based Intrusion Detection System," [Online]. Available: https://www.ossec.net
32. H. Lashkari, M. Saad, and A. A. Ghorbani, "Towards a robust ransomware detection system based on machine learning," in *Proc. ICISSP*, 2020, pp. 47–58.
33. T. Dreibholz and S. Rathgeb, "Network intrusion detection in campus environments: Combining Suricata and Zeek," *Journal of Cybersecurity and Privacy*, vol. 2, no. 3, pp. 456–470, 2022.
34. Modi, D. Patel, B. Borisaniya, H. Patel, and A. Rajarajan, "A survey on security issues and solutions at different layers of Cloud computing," *Journal of Supercomputing*, vol. 63, no. 2, pp. 561–592, 2013.
35. L. Buczak and E. Guven, "A survey of data mining and machine learning methods for cyber security intrusion detection," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 2, pp. 1153–1176, 2016.
36. R. Bace and P. Mell, "Intrusion Detection Systems," NIST Special Publication 800-31, 2001.
37. J. Kindervag, "No more chewy centers: Introducing the Zero Trust Model of information security," Forrester Research, 2010.

38. Sharafaldin, A. H. Lashkari, and A. A. Ghorbani, “Toward generating a new intrusion detection dataset and intrusion traffic characterization,” in *Proc. ICISSP*, 2018, pp. 108–116.
39. Cisco Systems, “Encrypted Traffic Analytics: Threat Visibility in the Age of Encryption,” White Paper, 2019. [Online]. Available: https://www.cisco.com
40. Modi et al., “A survey on security issues and solutions at different layers of cloud computing,” *Journal of Supercomputing*, vol. 63, no. 2, pp. 561–592, 2013.