GPH-International Journal of Computer Science and Engineering
(Online ISSN 3050-9661)
Volume 8 | Issue 01 | January-June 2025
Published by: Global Publication House
DOI: https://doi.org/10.5281/zenodo.21992945
Available online at: www.gphjournal.org
Journal homepage: https://gphjournal.org/index.php/cse/index

A Privacy-Preserving Explainable Artificial Intelligence Hybrid Framework for Abnormal Network Traffic Identification and Intelligent Threat Detection

D. A. Onuma[1], D. Matthias[2], O. E. Taylor[3] & N. D. Nwiabu[4]
[1,2,3,4] Department of Computer Science, Rivers State University, Nkpolu-Oroworukwo, Port Harcourt, Rivers State, Nigeria.
Corresponding Author Email: onuma.anele@rsu.edu.ng

Abstract

The rapid evolution of cyber threats, the widespread adoption of encrypted communications, and the increasing complexity of enterprise, cloud, edge, and Internet of Things (IoT) environments have exposed the limitations of conventional intrusion detection systems in accurately identifying abnormal network traffic and detecting sophisticated cyberattacks. Existing hybrid deep learning frameworks, including that of Wang [54], achieve high detection accuracy but lack privacy-preserving computation, explainable artificial intelligence, intelligent threat prioritization, and adaptive operational capabilities. This study therefore designed and developed a **Hybrid Artificial Intelligence Framework for Abnormal Network Traffic Identification and Intelligent Threat Detection** by integrating **Long Short-Term Memory (LSTM)**, **Transformer**, **Random Forest**, **CKKS Homomorphic Encryption**, **Explainable Artificial Intelligence (SHAP/LIME)**, weighted ensemble decision fusion, intelligent threat prioritization, and adaptive feedback learning. The study adopted the **Design Science Research Methodology (DSRM)**, while the proposed framework was implemented using **Python**, **TensorFlow/Keras**, **Scikit-learn**, **Microsoft SEAL/TenSEAL**, and evaluated using the **CICIDS2017** and **UNSW-NB15** benchmark datasets. Experimental evaluation was performed using accuracy, precision, recall, F1-score, false positive rate, detection latency, zero-day detection rate, throughput, scalability, explainability, and encryption overhead as performance metrics. The proposed framework achieved detection accuracies of **99.12%** and **98.76%** on the CICIDS2017 and UNSW-NB15 datasets, respectively, with precision values of **98.87%** and **98.42%**, recall values of **99.05%** and **98.61%**, F1-scores of **98.96%** and **98.51%**, false positive rates of **0.84%** and **1.12%**, and zero-day detection rates of **94.30%** and **92.75%**. Comparative analysis demonstrated improved detection accuracy, lower false-positive rates, reduced detection latency, enhanced interpretability, and stronger privacy preservation compared with the hybrid CNN–LSTM–Transformer framework of Wang [54]. The study concludes that integrating hybrid artificial intelligence, privacy-preserving computation, explainable artificial intelligence, and intelligent threat prioritization provides a robust, scalable, and adaptive solution for modern cybersecurity. The proposed framework is recommended for deployment in enterprise networks, cloud computing, IoT, edge computing, and critical infrastructure environments to strengthen real-time cyber threat detection and response.

Keywords:

Hybrid Artificial Intelligence, Abnormal Network Traffic Identification, Intelligent Threat Detection, Intrusion Detection System, LSTM, Transformer, Random Forest, Explainable Artificial Intelligence, CKKS Homomorphic Encryption, Zero-Day Attack Detection.

1.0 Background to the Study

The rapid growth of digital technologies, cloud computing, Internet of Things (IoT), fifth-generation (5G) communication networks, and distributed computing environments has transformed the way organizations communicate and manage information [8]. While these technologies have improved connectivity, scalability, and service delivery, they have also expanded the cyberattack surface, exposing computer networks to increasingly sophisticated security threats. Modern cyberattacks, including distributed denial-of-service (DDoS) attacks, ransomware, botnets, advanced persistent threats (APTs), phishing campaigns, insider attacks, and zero-day exploits, have become more intelligent, adaptive, and difficult to detect using conventional signature-based security mechanisms. Consequently, abnormal network traffic identification has become a fundamental component of modern cybersecurity because abnormal traffic often represents the earliest indicator of malicious activities within a network [54].

Network traffic identification involves monitoring, analyzing, and classifying communication patterns to distinguish legitimate activities from malicious behaviors. Traditional intrusion detection systems (IDSs) generally employ signature-based or statistical anomaly detection techniques. Signature-based systems are effective for detecting previously known attacks but fail to identify new or modified attack patterns. Conversely, anomaly-based systems can detect unknown attacks by identifying deviations from normal network behavior; however, they frequently generate high false-positive rates and struggle to adapt to evolving cyber threats. The pioneering work of Denning [18] established anomaly detection as a viable approach to intrusion detection, forming the foundation for subsequent intelligent intrusion detection research [54].

Recent advances in Artificial Intelligence (AI), Machine Learning (ML), and Deep Learning (DL) have significantly enhanced the capabilities of network intrusion detection systems. Machine learning algorithms such as Random Forest [12], Support Vector Machine, Decision Tree, and K-Nearest Neighbor have demonstrated improved classification performance compared with traditional methods. Similarly, deep learning models including Convolutional Neural Networks (CNNs), Long Short-Term Memory (LSTM) networks, Recurrent Neural Networks (RNNs), Autoencoders, and Transformer architectures have shown remarkable ability to learn complex spatial and temporal representations from high-dimensional network traffic data. LSTM networks are particularly effective in capturing sequential dependencies in network traffic, while Transformer models employ self-attention mechanisms to model long-range relationships among traffic features, thereby improving anomaly detection performance [53].

Although individual AI models have achieved notable success, researchers have increasingly recognized that hybrid artificial intelligence approaches offer superior performance by combining the complementary strengths of multiple learning algorithms. Hybrid models integrate diverse feature learning capabilities to improve detection accuracy, reduce false positives, enhance robustness, and increase generalization across heterogeneous network

environments. Recent studies have therefore explored combinations of CNNs, LSTMs, Transformers, ensemble learning, and attention mechanisms to improve intelligent threat detection in modern cybersecurity systems [54].

One of the most recent contributions in this area is the work of Wang [54], who proposed a self-learning hybrid **CNN–LSTM–Transformer** framework for abnormal network traffic identification. Their framework combines CNNs for spatial feature extraction, LSTMs for temporal sequence learning, and Transformers for contextual representation, while introducing an adaptive self-learning mechanism capable of handling concept drift and evolving attack behaviors. Using the UNSW-NB15 and CICIDS2017 benchmark datasets, the proposed framework achieved high binary and multiclass classification performance and demonstrated improved adaptability to zero-day attacks through continuous model updating. The study represents an important advancement toward autonomous and adaptive network anomaly detection systems [54].

Despite these significant achievements, several important challenges remain unresolved. The integration of CNN, LSTM, and Transformer models produces a computationally intensive architecture that requires considerable processing resources, making real-time deployment challenging in cloud-edge environments, IoT infrastructures, and other resource-constrained platforms. Furthermore, the framework performs network traffic analysis on plaintext data and does not incorporate privacy-preserving mechanisms capable of protecting sensitive traffic information during processing. In addition, the model operates primarily as a black-box system [24], providing limited interpretability for cybersecurity analysts responsible for understanding detection decisions and conducting incident investigations. The framework also emphasizes anomaly detection accuracy without incorporating intelligent threat prioritization and risk-based decision support, both of which are increasingly important for Security Operations Centers (SOCs) managing large volumes of security alerts [54].

These limitations reveal a significant research gap in the development of intelligent cybersecurity frameworks that simultaneously provide high detection accuracy, computational efficiency, privacy preservation, explainability, scalability, and intelligent threat assessment. Addressing these challenges is increasingly important as organizations seek cybersecurity solutions capable of defending complex enterprise networks against rapidly evolving cyber threats while maintaining compliance with data privacy requirements and supporting timely operational decision-making. Furthermore, explainable artificial intelligence techniques such as SHAP have demonstrated the importance of providing interpretable model predictions to improve user trust and facilitate cybersecurity decision-making in complex AI systems [35].

To address these research gaps, this study aims to **design and develop a Hybrid Artificial Intelligence Framework for Abnormal Network Traffic Identification and Intelligent Threat Detection** that improves detection accuracy, computational efficiency, privacy preservation, explainability, and real-time threat intelligence. Specifically, the study seeks to: (i) design and develop a scalable hybrid AI framework integrating LSTM, Transformer, and Random Forest algorithms for accurate abnormal network traffic identification and intelligent threat detection; (ii) integrate CKKS (Cheon–Kim–Kim–Song) homomorphic encryption to enable privacy-preserving analysis of sensitive network traffic; (iii) incorporate Explainable Artificial Intelligence (XAI) techniques together with intelligent threat prioritization to provide transparent, interpretable, and risk-based cybersecurity decision support; (iv) optimize the framework for computational efficiency and real-time deployment across enterprise, cloud,

edge, and IoT environments; and (v) evaluate the framework using benchmark datasets such as CICIDS2017 and UNSW-NB15 based on detection accuracy, precision, recall, F1-score, false-positive rate, latency, scalability, explainability, privacy preservation, and zero-day attack detection capability.

The successful implementation of these objectives is expected to make significant contributions to both theory and practice. The proposed framework will improve the detection of abnormal network traffic and sophisticated cyber threats while reducing false alarms and computational overhead. The integration of CKKS homomorphic encryption will strengthen data confidentiality by enabling secure analysis of encrypted traffic without exposing sensitive information. The incorporation of explainable AI and intelligent threat prioritization will improve transparency, analyst trust, and incident response efficiency. Additionally, the optimized architecture will support deployment across enterprise networks, cloud infrastructures, edge computing platforms, and IoT environments. Academically, the study will contribute a comprehensive hybrid AI framework that unifies deep learning, machine learning, privacy-preserving computation, and explainable artificial intelligence within a single intelligent threat detection architecture, thereby extending current knowledge in network security and providing a robust foundation for future cybersecurity research.

2. Conceptual Literature Review

2.1 Cybersecurity

Cybersecurity is a multidisciplinary field concerned with protecting computer systems, networks, applications, and digital information from unauthorized access, disruption, modification, disclosure, or destruction [39]. The rapid adoption of cloud computing, Internet of Things (IoT), artificial intelligence (AI), fifth-generation (5G) networks, and digital transformation has significantly expanded the cyberattack surface, resulting in increasingly sophisticated cyber threats. Consequently, cybersecurity has evolved beyond traditional perimeter defense to encompass technologies, policies, governance, risk management, and intelligent security mechanisms that ensure the confidentiality, integrity, and availability (CIA) of information systems (National Institute of Standards and Technology [38].

The objectives of cybersecurity are commonly described by the **Confidentiality, Integrity, and Availability (CIA) Triad**, which ensures that sensitive information is protected from unauthorized disclosure, remains accurate and trustworthy, and is accessible to authorized users when required. Modern cybersecurity solutions implement these objectives through encryption, authentication, access control, intrusion detection and prevention systems, security information and event management (SIEM), and AI-driven threat detection technologies [39].

The contemporary cybersecurity landscape is characterized by rapidly evolving attack techniques, heterogeneous network infrastructures, and increasing volumes of encrypted communications. Advanced Persistent Threats (APTs), ransomware, phishing, botnets, insider attacks, supply chain attacks, and zero-day exploits frequently evade conventional signature-based detection systems. At the same time, the widespread adoption of encrypted network traffic limits the effectiveness of payload inspection, necessitating behavioral analysis and AI-based approaches capable of learning complex traffic patterns from network metadata and flow characteristics rather than packet contents.

Artificial intelligence, machine learning, and deep learning have therefore become integral to modern cybersecurity by enabling automated anomaly detection, intelligent threat classification, and real-time analysis of massive network traffic. Recent hybrid AI models, such as the CNN–LSTM–Transformer framework proposed by Wang [54], have demonstrated improved capability for detecting abnormal traffic and adapting to evolving cyber threats. However, existing approaches remain constrained by high computational complexity, limited explainability, inadequate privacy preservation, and insufficient threat prioritization, highlighting the need for more scalable, interpretable, and privacy-preserving cybersecurity frameworks.

Accordingly, this study proposes a **Hybrid Artificial Intelligence Framework for Abnormal Network Traffic Identification and Intelligent Threat Detection** that integrates LSTM, Transformer, and Random Forest algorithms with CKKS homomorphic encryption, Explainable Artificial Intelligence (XAI), and intelligent threat prioritization to improve detection accuracy, privacy preservation, transparency, and real-time cyber threat response across enterprise, cloud, edge, and IoT environments.

2.2 Computer Networks

Computer networks provide the fundamental infrastructure for communication and resource sharing among interconnected devices, enabling the exchange of data, applications, and services across local and global environments. The rapid adoption of cloud computing, the Internet of Things (IoT), edge computing, and enterprise information systems has significantly increased network complexity and expanded the cyberattack surface, making effective network monitoring and intelligent threat detection indispensable components of modern cybersecurity [51][5][27].

Network communication is achieved through standardized protocols operating within layered architectures, primarily the TCP/IP model, which supports reliable data transmission, routing, and interoperability among heterogeneous devices. Common protocols such as TCP, UDP, HTTP/HTTPS, DNS, FTP, and SSH generate distinctive communication patterns that provide valuable indicators for network traffic analysis and cyber threat detection [33].

Modern computer networks include Local Area Networks (LANs), Wide Area Networks (WANs), cloud networks, edge networks, and IoT infrastructures. While these architectures enhance scalability, flexibility, and connectivity, they also introduce new security challenges due to distributed resources, heterogeneous devices, and resource-constrained endpoints. In particular, IoT environments are increasingly vulnerable to malware, botnets, and distributed denial-of-service (DDoS) attacks because of their limited computational and security capabilities [5].

Network traffic is generated by both legitimate activities, such as web browsing, cloud services, email, file sharing, and multimedia streaming, and malicious activities, including malware communication, ransomware, reconnaissance, brute-force attacks, botnet operations, and data exfiltration. These communications can be captured using packet analyzers and flow-monitoring technologies such as Wireshark, NetFlow, and IPFIX, then transformed into statistical, temporal, and behavioural features for intelligent analysis. Consequently, computer networks constitute the primary operational environment in which abnormal network traffic is

generated, monitored, and analyzed, providing the foundation for developing hybrid artificial intelligence frameworks capable of real-time anomaly detection and intelligent threat identification.

2.3 Network Traffic

Network traffic refers to the flow of digital data exchanged among interconnected devices over wired or wireless communication networks. It is generated by activities such as web browsing, cloud computing, email, file sharing, Voice over Internet Protocol (VoIP), video streaming, and Internet of Things (IoT) communications. As digital services continue to expand, network traffic has become increasingly heterogeneous and voluminous, making traffic monitoring and analysis essential for maintaining network performance and cybersecurity [2].

From a cybersecurity perspective, network traffic provides the primary source of information for detecting abnormal behaviors, identifying cyberattacks, and supporting digital forensic investigations. Network communications contain observable metadata, including Internet Protocol (IP) addresses, ports, protocols, timestamps, packet sizes, and flow statistics, which can be analyzed to distinguish legitimate activities from malicious behaviors, even when payloads are encrypted [60]. Consequently, network traffic analysis underpins modern intrusion detection systems (IDSs), network anomaly detection models, and artificial intelligence (AI)-based threat detection frameworks [15].

Network traffic can be broadly categorized into legitimate and malicious traffic, with additional classifications including encrypted, real-time, bulk data, and IoT traffic. Legitimate traffic originates from authorized user activities and organizational applications, whereas malicious traffic is associated with cyber threats such as malware, botnets, distributed denial-of-service (DDoS) attacks, phishing, ransomware, command-and-control (C2) communications, and data exfiltration. The widespread adoption of encryption technologies, including HTTPS, TLS, and Virtual Private Networks (VPNs), has reduced the effectiveness of payload inspection, necessitating the use of statistical, behavioral, and machine learning approaches for traffic classification [2][60].

Effective network traffic analysis relies on measurable traffic characteristics such as flow duration, packet size, packet arrival time, communication frequency, protocol distribution, packet rate, byte rate, and traffic direction. These features capture both statistical and temporal behaviors that enable AI models to differentiate normal from abnormal communications. Modern traffic analysis typically involves traffic collection, preprocessing, feature extraction, traffic classification, anomaly detection, and threat identification. Recent studies demonstrate that AI techniques, including Long Short-Term Memory (LSTM), Transformer networks, Random Forest, and hybrid learning models, significantly improve detection accuracy by learning complex spatial and temporal relationships within network traffic while reducing false positives and enhancing zero-day attack detection [54].

Flow-based traffic analysis has emerged as the preferred approach for intelligent threat detection because it summarizes packets into communication flows using attributes such as source and destination IP addresses, ports, protocol, and timestamps. Compared with packet-level inspection, flow-based analysis reduces computational overhead, preserves user privacy, and supports real-time monitoring of high-speed networks. Furthermore, feature engineering

techniques—including data cleaning, normalization, feature selection, dimensionality reduction, and feature construction—enhance the discriminative power of traffic representations and improve the performance of hybrid AI models. Temporal features are particularly effective for LSTM networks, contextual relationships are captured by Transformer architectures, while statistical features strengthen Random Forest classification. These complementary capabilities provide the foundation for developing scalable and accurate hybrid AI frameworks for abnormal network traffic identification and intelligent threat detection.

2.4 Abnormal Network Traffic

Abnormal network traffic refers to network communication that significantly deviates from established normal behavior and may indicate malicious activities, security breaches, or unauthorized access attempts. Unlike legitimate traffic, which follows predictable communication patterns based on user behavior and organizational policies, abnormal traffic exhibits unusual characteristics such as irregular packet rates, abnormal protocol usage, unexpected communication endpoints, and suspicious data transmission patterns [18]. Because malicious activities often generate distinctive communication behaviors, abnormal network traffic serves as one of the earliest indicators of cyberattacks and has become a primary focus of modern intrusion detection and intelligent threat detection systems [49].

The increasing adoption of cloud computing, Internet of Things (IoT), Software-Defined Networking (SDN), and encrypted communications has significantly increased the complexity of network traffic, making traditional signature-based detection methods inadequate for identifying sophisticated and zero-day attacks. Consequently, artificial intelligence (AI), machine learning (ML), and deep learning (DL) techniques have become essential for modeling normal network behavior and detecting anomalous traffic with greater accuracy and adaptability [20].

Abnormal network traffic is characterized by unusual communication patterns, irregular traffic volumes, abnormal packet characteristics, unexpected protocol usage, temporal irregularities, excessive connection attempts, and anomalous data transfers. These characteristics are commonly associated with cyberattacks such as Distributed Denial-of-Service (DDoS) attacks, malware propagation, botnet communications, port scanning, brute-force attacks, command-and-control (C2) communications, Advanced Persistent Threats (APTs), insider attacks, and data exfiltration. However, legitimate operational activities, including software updates, backup processes, and network maintenance, may also generate abnormal traffic, highlighting the need for intelligent detection models capable of distinguishing malicious anomalies from benign deviations while minimizing false-positive rates.

Modern threat detection systems therefore rely on **Indicators of Compromise (IoCs)** such as suspicious IP addresses, malicious domain names, abnormal port usage, unusual authentication events, excessive outbound data transfers, periodic beaconing behavior, abnormal DNS requests, and file or process anomalies to improve attack detection accuracy. Integrating these indicators with AI-based behavioral analysis enables the identification of both known and previously unseen cyber threats in real time.

Given the dynamic and evolving nature of cyberattacks, abnormal network traffic identification has become a fundamental component of intelligent cybersecurity. Recent hybrid AI

approaches that combine deep learning and ensemble learning techniques have demonstrated superior capabilities in detecting complex, encrypted, and zero-day attacks while reducing false alarms. These advances provide the foundation for the proposed **Hybrid Artificial Intelligence Framework for Abnormal Network Traffic Identification and Intelligent Threat Detection**, which integrates complementary AI models, privacy-preserving computation, explainable AI, and intelligent threat prioritization to improve the accuracy, scalability, transparency, and real-time performance of modern cybersecurity systems.

2.5 Network Traffic Identification

Network traffic identification is a fundamental process in network security that involves recognizing, classifying, and analyzing network communications to distinguish legitimate from malicious activities. It supports network monitoring, intrusion detection, traffic engineering, and cyber threat intelligence by enabling security systems to understand the nature and behavior of network traffic in real time. With the rapid adoption of cloud computing, Internet of Things (IoT), software-defined networking (SDN), and encrypted communication protocols, traditional identification techniques based on port numbers and deep packet inspection have become increasingly ineffective. Consequently, modern approaches rely on statistical analysis, behavioral modeling, and artificial intelligence (AI) to identify traffic patterns from network metadata and flow characteristics rather than packet payloads [2][60]. Hybrid AI models further improve traffic identification by combining multiple learning algorithms to enhance detection accuracy, robustness, and adaptability to evolving cyber threats.

Network traffic identification typically consists of four major processes: **traffic classification, flow identification, feature extraction, and feature engineering**. Traffic classification categorizes communications according to protocol, application, user behavior, or security status (e.g., benign or malicious). AI-based classifiers have demonstrated superior performance over traditional methods because they effectively classify encrypted and previously unseen traffic using statistical and temporal flow characteristics rather than payload inspection.

Flow identification groups packets belonging to the same communication session into logical network flows, commonly defined by the five-tuple consisting of source IP address, destination IP address, source port, destination port, and transport protocol. Flow-based analysis reduces computational overhead while preserving communication patterns, making it suitable for high-speed network monitoring and anomaly detection.

Feature extraction transforms raw network packets or flow records into meaningful numerical representations that describe communication behavior. Common features include basic network attributes (e.g., IP addresses, ports, protocols, packet size, and flow duration), statistical features (e.g., packet rate, byte count, and average packet length), temporal features (e.g., session duration and inter-arrival time), and behavioral features (e.g., connection frequency and failed login attempts). These features enable machine learning and deep learning algorithms to differentiate normal network behavior from malicious activities.

Feature engineering further enhances detection performance by cleaning, transforming, selecting, constructing, and reducing features to improve model learning while minimizing computational complexity. In hybrid AI frameworks, engineered temporal features are particularly suitable for LSTM networks, contextual feature representations enhance

Transformer learning, and statistical features improve Random Forest classification [12]. Effective feature engineering therefore increases detection accuracy, reduces false-positive rates, improves model generalization, and supports real-time intelligent threat detection.

Overall, network traffic identification provides the analytical foundation for abnormal network traffic identification and intelligent threat detection. By integrating traffic classification, flow analysis, feature extraction, and feature engineering with hybrid artificial intelligence, modern cybersecurity systems can accurately identify both known and unknown attacks, including encrypted and zero-day threats, while maintaining scalability and computational efficiency [2][60][54].

2.6 Network Anomaly Detection

Network anomaly detection is a critical component of modern cybersecurity that identifies deviations from normal network behavior to detect malicious activities, security breaches, and network failures. Unlike signature-based intrusion detection systems (IDSs), which rely on predefined attack patterns, anomaly detection establishes a baseline of normal network behavior and identifies deviations that may indicate known or unknown attacks, including zero-day threats [18]. The increasing complexity of cloud computing, Internet of Things (IoT), software-defined networking (SDN), and encrypted communications has accelerated the adoption of artificial intelligence (AI)-based anomaly detection techniques capable of adapting to dynamic network environments [20].

Network anomaly detection techniques are broadly categorized into **statistical**, **knowledge-based**, **machine learning**, **deep learning**, and **hybrid** approaches. Statistical methods detect anomalies by identifying deviations from predefined probability distributions or threshold values and are computationally efficient but often generate high false-positive rates in dynamic environments. Knowledge-based approaches rely on expert-defined rules and attack signatures, making them effective against known attacks but ineffective for detecting novel or zero-day threats. Machine learning methods, including supervised, unsupervised, and semi-supervised learning, automatically learn network traffic patterns and improve adaptability over traditional techniques. Deep learning models such as Convolutional Neural Networks (CNNs), Long Short-Term Memory (LSTM) networks, Autoencoders, and Transformer architectures further enhance anomaly detection by automatically learning complex spatial and temporal representations from large-scale network traffic datasets. Hybrid anomaly detection combines multiple AI techniques to leverage their complementary strengths, thereby improving detection accuracy, robustness, and generalization while reducing false-positive rates.

Despite these advances, existing anomaly detection models face several challenges, including high computational complexity, dependence on large labeled datasets, limited interpretability, and difficulties in adapting to evolving cyber threats. Deep learning models often operate as black-box systems, reducing analyst trust and limiting their practical deployment in real-time cybersecurity operations. These limitations have motivated the development of hybrid artificial intelligence frameworks that integrate complementary learning algorithms with explainable AI and privacy-preserving mechanisms to achieve accurate, scalable, and interpretable threat detection.

The proposed study builds upon these developments by designing a **Hybrid Artificial Intelligence Framework for Abnormal Network Traffic Identification and Intelligent Threat Detection** that integrates **LSTM, Transformer, and Random Forest** models with **CKKS homomorphic encryption**, **Explainable Artificial Intelligence (SHAP/LIME)**, and **intelligent threat prioritization**. This integrated approach aims to improve anomaly detection accuracy, protect sensitive network data during analysis, enhance model transparency, support zero-day attack detection, and enable real-time deployment across enterprise, cloud, edge, and IoT environments.

2.7 Intelligent Threat Detection

Intelligent Threat Detection (ITD) applies Artificial Intelligence (AI), Machine Learning (ML), and Deep Learning (DL) to automatically identify, classify, and respond to cyber threats by learning network behavior rather than relying solely on predefined attack signatures. Unlike conventional intrusion detection systems, ITD continuously analyzes network traffic and user activities to detect both known and previously unseen threats, including Advanced Persistent Threats (APTs), insider attacks, encrypted malware, and zero-day exploits. Its integration of behavioral analysis, anomaly detection, predictive analytics, and threat intelligence enables real-time detection with improved accuracy, adaptability, and reduced false-positive rates, making it a fundamental component of modern Security Operations Centers (SOCs) and critical infrastructure protection.

The effectiveness of ITD is closely associated with understanding the cyber threat lifecycle, which comprises reconnaissance, weaponization, delivery, exploitation, installation, command-and-control, and actions on objectives. Monitoring network traffic throughout these stages enables early identification of malicious activities and facilitates proactive incident response before attacks escalate. Furthermore, integrating threat intelligence with AI-driven behavioral analysis enhances contextual awareness by correlating indicators of compromise, attacker tactics, and historical attack patterns, thereby improving detection accuracy and supporting informed security decisions.

Modern intelligent threat detection follows a structured process involving network traffic collection, data preprocessing, feature extraction, behavioral analysis, threat classification, validation, alert generation, and incident response. Hybrid AI models significantly enhance this process by combining complementary learning capabilities for temporal sequence analysis, contextual feature learning, and robust classification. In the proposed study, the integration of LSTM, Transformer, and Random Forest algorithms is expected to improve anomaly detection, identify sophisticated and zero-day attacks, and support real-time cybersecurity operations.

An essential component of intelligent threat detection is **threat prioritization**, which evaluates detected attacks according to severity, exploitability, confidence level, asset criticality, and potential organizational impact. AI-based prioritization reduces alert fatigue by ranking security events according to risk, enabling security analysts to focus on the most critical incidents. Within the proposed framework, threat prioritization extends beyond anomaly detection by incorporating risk-based assessment before generating alerts, thereby improving operational efficiency, accelerating incident response, and strengthening organizational cyber resilience.

2.8 Intrusion Detection Systems

Intrusion Detection Systems (IDSs) are essential components of modern cybersecurity architectures, designed to monitor network and system activities for malicious behavior, policy violations, and unauthorized access. Unlike firewalls, which primarily prevent attacks, IDSs analyze network traffic, system logs, and user activities to identify security threats and generate alerts for timely incident response. The concept of intrusion detection was pioneered by [18], who introduced anomaly-based detection, laying the foundation for contemporary intelligent IDSs.

IDSs generally comprise five functional components: **data collection**, **data preprocessing**, **detection engine**, **knowledge base**, and **alert generation**. The data collection module captures network traffic and system events from sources such as routers, servers, and firewalls. Preprocessing transforms raw traffic into structured feature vectors through cleaning, normalization, and feature extraction. The detection engine analyzes these features using rule-based, statistical, machine learning, or deep learning techniques, while the knowledge base stores attack signatures, behavioral profiles, and threat intelligence. Finally, the alert generation module reports suspicious activities to security analysts and may support automated response mechanisms in modern intelligent IDSs.

IDSs are commonly classified into **signature-based**, **anomaly-based**, and **hybrid** systems. Signature-based IDSs compare observed traffic with predefined attack signatures and provide high accuracy for known attacks with relatively low false-positive rates. However, they cannot detect previously unseen or zero-day attacks and require continuous signature updates. In contrast, anomaly-based IDSs establish baseline models of normal network behavior and identify deviations as potential intrusions. These systems are effective for detecting novel and evolving attacks but often suffer from high false-positive rates and significant computational overhead. Hybrid IDSs combine signature-based and anomaly-based approaches to leverage the strengths of both techniques. Recent hybrid frameworks integrate machine learning and deep learning models, such as LSTM, Transformer, and Random Forest, to improve detection accuracy, robustness, and adaptability while reducing false alarms.

Despite substantial advances, current IDSs continue to face several challenges. Many deep learning-based systems require considerable computational resources, limiting their applicability in real-time and resource-constrained environments. AI-driven IDSs also operate largely as black-box models, providing limited interpretability for cybersecurity analysts. Furthermore, most existing systems analyze plaintext network traffic without incorporating privacy-preserving mechanisms, thereby exposing sensitive information during analysis. The rapid growth of cloud computing, Internet of Things (IoT), and software-defined networking has further increased scalability challenges, while many IDSs still generate large volumes of unprioritized alerts that overwhelm Security Operations Centers (SOCs).

These limitations highlight the need for more intelligent, scalable, and privacy-preserving intrusion detection solutions. Accordingly, the present study proposes a **Hybrid Artificial Intelligence Framework for Abnormal Network Traffic Identification and Intelligent Threat Detection** that integrates **LSTM, Transformer, and Random Forest** models with **CKKS homomorphic encryption**, **Explainable Artificial Intelligence (XAI)**, and **intelligent threat prioritization**. The proposed framework aims to improve detection accuracy, enhance

model transparency, preserve data privacy, reduce computational overhead, and strengthen real-time detection of both known and zero-day cyber threats.

2.9 Artificial Intelligence in Cybersecurity

Artificial Intelligence (AI) has become a transformative technology in cybersecurity by enabling automated, adaptive, and data-driven detection of cyber threats. The rapid growth of cloud computing, the Internet of Things (IoT), software-defined networking (SDN), and high-speed communication networks has significantly increased the volume and complexity of network traffic, rendering conventional signature-based security mechanisms insufficient for detecting sophisticated and evolving attacks. AI addresses these challenges by learning complex patterns from historical and real-time data to identify both known and previously unseen threats, thereby improving detection accuracy, adaptability, and response efficiency [43][13].

Unlike traditional intrusion detection systems that rely on predefined rules, AI-driven cybersecurity systems employ machine learning (ML), deep learning (DL), and intelligent automation to analyze network behavior, detect anomalies, classify malicious activities, and support automated incident response. Machine learning algorithms such as Random Forest, Support Vector Machine (SVM), and Decision Trees have demonstrated strong performance in intrusion detection, while deep learning models, including Convolutional Neural Networks (CNNs), Long Short-Term Memory (LSTM) networks, Autoencoders, and Transformer architectures, have shown superior capability in learning spatial and temporal characteristics of network traffic for detecting sophisticated attacks and zero-day threats [2][20].

Recent research has increasingly focused on **hybrid artificial intelligence**, which combines multiple learning algorithms to exploit their complementary strengths. Hybrid models improve detection accuracy, reduce false-positive rates, enhance robustness, and adapt more effectively to evolving cyber threats than individual algorithms. They are particularly effective in analyzing encrypted network traffic and large-scale enterprise environments where diverse traffic characteristics require multiple feature-learning mechanisms [54].

Despite these advances, AI-based cybersecurity systems continue to face important challenges, including high computational complexity, dependence on large labeled datasets, limited explainability, privacy concerns, and difficulties in adapting to rapidly changing attack behaviors. These limitations have motivated the integration of Explainable Artificial Intelligence (XAI), privacy-preserving techniques such as homomorphic encryption, and hybrid AI architectures to improve transparency, data confidentiality, and real-time threat detection [35][54].

Accordingly, the present study proposes a **Hybrid Artificial Intelligence Framework for Abnormal Network Traffic Identification and Intelligent Threat Detection** that integrates LSTM, Transformer, and Random Forest models with CKKS homomorphic encryption, Explainable AI, and intelligent threat prioritization. The proposed framework aims to improve anomaly detection accuracy, preserve the privacy of network traffic during analysis, enhance model interpretability, and support scalable, real-time detection of known and zero-day cyber threats across enterprise, cloud, edge, and IoT environments.

2.10 Related Works

Recent advances in Artificial Intelligence (AI) have significantly improved abnormal network traffic identification and intelligent threat detection. Traditional signature-based intrusion detection systems (IDSs) remain effective for detecting known attacks but exhibit poor adaptability to zero-day attacks, encrypted communications, and evolving attack strategies. Consequently, researchers have increasingly adopted machine learning (ML), deep learning (DL), and hybrid AI techniques to enhance detection accuracy, scalability, and real-time cybersecurity performance [3].

Deep learning models have become central to modern intrusion detection because they automatically learn hierarchical feature representations from network traffic without extensive manual feature engineering. Convolutional Neural Networks (CNNs) effectively capture spatial traffic characteristics, while Recurrent Neural Networks (RNNs) and Long Short-Term Memory (LSTM) networks model temporal dependencies in sequential traffic data. More recently, Transformer architectures have demonstrated superior capability for learning long-range contextual relationships through self-attention mechanisms, improving anomaly detection accuracy and scalability in large-scale network environments. However, individual deep learning models remain computationally demanding and often function as black-box systems with limited interpretability [3].

To overcome these limitations, hybrid AI architectures have emerged as a dominant research direction. By integrating complementary learning models, hybrid approaches improve feature representation, reduce false-positive rates, and enhance robustness against sophisticated cyberattacks. Several studies have demonstrated that combining CNNs, LSTMs, Transformers, and ensemble classifiers significantly improves the identification of abnormal traffic, malware communication, botnet activity, and zero-day attacks compared with single-model approaches [40].

Aceto [2] demonstrated that statistical flow features extracted from encrypted traffic can effectively classify network applications without payload inspection, establishing the importance of flow-based traffic analysis for modern cybersecurity. Similarly, Alshammari and Zincir-Heywood [60] showed that behavioral and statistical traffic characteristics remain highly informative even when communication payloads are encrypted, highlighting the growing relevance of AI-driven encrypted traffic analysis [28].

Recent research has increasingly focused on Transformer-based intrusion detection. Wang [54] proposed a self-learning hybrid CNN–LSTM–Transformer framework that combines spatial feature extraction, temporal sequence learning, and contextual attention mechanisms to improve network anomaly detection. The framework incorporates adaptive learning to address concept drift and achieved high detection performance on the UNSW-NB15 and CICIDS2017 benchmark datasets. Nevertheless, the architecture remains computationally intensive, provides limited model interpretability, lacks privacy-preserving mechanisms, and does not include intelligent threat prioritization for operational decision support [3].

Explainable Artificial Intelligence (XAI) has also become an important research area because cybersecurity analysts require transparent reasoning behind automated detection decisions. Methods such as SHAP and LIME provide feature-level explanations that improve analyst trust,

facilitate forensic investigations, and support regulatory compliance. Despite these advantages, most existing deep learning-based intrusion detection systems still operate as black-box models with limited integration of explainability into operational threat detection [3].

Another emerging direction is privacy-preserving intrusion detection. The widespread adoption of encrypted communications, cloud computing, and distributed environments has increased concerns regarding the exposure of sensitive network traffic during AI-based analysis. Current studies have investigated encrypted traffic classification and secure machine learning; however, relatively few frameworks integrate homomorphic encryption directly into hybrid intrusion detection systems to enable secure computation on encrypted traffic while maintaining detection accuracy [28].

Systematic reviews published between 2024 and 2025 consistently identify several unresolved challenges. These include high computational complexity, dependence on large labeled datasets, limited adaptability to evolving threats, inadequate handling of encrypted traffic, lack of explainable decision-making, insufficient privacy preservation, and poor real-time deployment in cloud, edge, and IoT environments. Recent surveys also emphasize that future network intrusion detection systems should combine hybrid AI, explainable AI, privacy-preserving learning, adaptive learning, and intelligent threat prioritization within unified architectures [3].

Overall, the literature demonstrates substantial progress in AI-driven network anomaly detection between 2020 and 2025. Nevertheless, no single framework comprehensively integrates temporal sequence learning, contextual attention, ensemble classification, privacy-preserving computation, explainable AI, and risk-based threat prioritization into a scalable real-time cybersecurity solution. This gap motivates the present study, which proposes a **Hybrid Artificial Intelligence Framework for Abnormal Network Traffic Identification and Intelligent Threat Detection** by integrating **LSTM**, **Transformer**, and **Random Forest** models with **CKKS homomorphic encryption**, **Explainable Artificial Intelligence (SHAP/LIME)**, and **intelligent threat prioritization** to improve detection accuracy, transparency, privacy, scalability, and operational decision support.

Kimanzi [30] conducted a comprehensive review of deep learning algorithms used in intrusion detection systems, examining the application of CNNs, RNNs, LSTMs, Deep Neural Networks (DNNs), Autoencoders, Deep Belief Networks (DBNs), Multi-Layer Perceptrons (MLPs), and hybrid deep learning models for network intrusion detection. The study compared these techniques based on detection accuracy, computational efficiency, scalability, adaptability to evolving threats, and commonly used benchmark datasets. The authors concluded that hybrid deep learning models consistently outperform individual algorithms because they combine complementary feature learning capabilities and improve intrusion detection performance. However, the review also identified several limitations, including high computational complexity, large training data requirements, model interpretability challenges, and limited deployment in real-time environments. The study recommended future research on lightweight, explainable, and adaptive hybrid intrusion detection systems capable of handling encrypted traffic and emerging cyber threats [30].

Limitation: The study is a survey and does not propose or validate a deployable hybrid framework integrating privacy-preserving computation, explainable AI, and intelligent threat prioritization.

Bamber [6] proposed a self-learning hybrid CNN–LSTM–Transformer framework for network anomaly detection. The framework integrates CNNs for spatial feature extraction, LSTM networks for temporal sequence learning, and Transformer architectures for contextual feature representation. A self-learning mechanism was introduced to address concept drift and improve adaptation to evolving attack patterns. Evaluation on the UNSW-NB15 and CICIDS2017 datasets demonstrated high detection accuracy and improved zero-day attack detection. Despite these achievements, the framework remains computationally intensive, lacks privacy-preserving mechanisms such as homomorphic encryption, provides limited model explainability, and does not incorporate intelligent threat prioritization for operational decision support. These limitations motivate further research into scalable, explainable, and privacy-preserving hybrid AI frameworks [6].

Limitation: No integration of CKKS homomorphic encryption, explainable AI, or risk-based threat prioritization.

Wang [54] developed a hybrid CNN–BiLSTM intrusion detection model for industrial control systems. CNNs were employed to extract local spatial features from industrial network traffic, while BiLSTM captured bidirectional temporal dependencies to improve attack recognition. The proposed model achieved higher detection accuracy and lower false alarm rates than conventional machine learning methods when evaluated on industrial intrusion datasets. However, the model is specifically designed for industrial control systems, requires substantial computational resources, lacks explainability, and does not provide privacy-preserving processing or adaptive threat prioritization [54].

Limitation: Limited applicability beyond industrial environments and absence of explainable and privacy-preserving capabilities.

Singh [48] proposed **SecureFlow**, an adaptive ensemble intrusion detection framework for software-defined Internet of Things (IoT) environments. The framework combines knowledge-driven security policies with data-driven ensemble machine learning to detect both known and unknown cyberattacks while dynamically reconfiguring network security rules. It employs Software-Defined Networking (SDN) to monitor network traffic and uses an ensemble classification approach to improve intrusion detection accuracy and adapt to evolving attack patterns. The framework was evaluated through Mininet emulation using representative IoT attack scenarios, where it demonstrated improved detection performance, reduced false alarms, and enhanced adaptability compared with conventional intrusion detection approaches. However, the study focuses primarily on SDN-enabled IoT networks and does not integrate deep sequential learning models such as LSTM or Transformer architectures. In addition, the framework lacks privacy-preserving mechanisms, explainable artificial intelligence (XAI), and intelligent threat prioritization for supporting cybersecurity analysts. These limitations indicate the need for a more comprehensive hybrid artificial intelligence framework that combines advanced deep learning, privacy-preserving computation, explainable decision-making, and risk-based threat prioritization for real-time abnormal network traffic identification and intelligent threat detection [48].

Hassan [25] proposed a **hybrid Convolutional Neural Network–Recurrent Neural Network (CNN–RNN)** architecture for intelligent network intrusion detection by combining the spatial feature extraction capability of CNNs with the temporal sequence learning ability of RNNs. The CNN component automatically extracted discriminative features from network traffic, while the RNN modeled sequential dependencies to improve the identification of complex and evolving attack patterns. The framework was evaluated using benchmark intrusion detection datasets and demonstrated superior detection accuracy compared with conventional machine learning models, particularly in identifying sophisticated cyberattacks while reducing false-positive rates.

Despite its improved detection performance, the proposed model has several limitations. The hybrid CNN–RNN architecture increases computational complexity and training time, making real-time deployment challenging in resource-constrained environments. Furthermore, the model operates as a black-box system with limited explainability, does not incorporate privacy-preserving mechanisms for secure traffic analysis, and lacks intelligent threat prioritization to support Security Operations Center (SOC) decision-making. These limitations indicate the need for scalable, explainable, and privacy-preserving hybrid AI frameworks capable of supporting real-time abnormal network traffic identification and intelligent threat detection.

Kumar and Sharma [32] proposed a **hybrid deep learning intrusion detection framework** that combines deep learning-based feature learning with Random Forest classification to improve intrusion detection accuracy in IoT networks. The framework employs optimal feature selection and a layered deep learning architecture to extract discriminative traffic features before classification using Random Forest. The model was evaluated on benchmark intrusion detection datasets and demonstrated superior accuracy, precision, recall, and F1-score compared with conventional machine learning algorithms and standalone deep learning models. The hybrid approach effectively reduced false-positive rates and improved the detection of multiple attack categories by leveraging the feature extraction capability of deep learning and the robust classification performance of Random Forest. However, the framework requires considerable computational resources during training, does not incorporate privacy-preserving mechanisms such as homomorphic encryption, lacks explainable AI for interpreting detection decisions, and provides limited support for intelligent threat prioritization and real-time deployment in distributed environments. These limitations indicate the need for more scalable, explainable, and privacy-preserving hybrid AI frameworks for abnormal network traffic identification and intelligent threat detection.

Yang [56] proposed an improved intrusion detection framework, termed **NIDS-BAI**, for the **Industrial Internet of Things (IIoT)** to address three major challenges in existing intrusion detection systems: low detection accuracy, feature redundancy in high-dimensional traffic, and poor recognition of minority attack classes caused by imbalanced datasets. The framework integrates an **attention mechanism**, **Bidirectional Gated Recurrent Unit (BiGRU)**, and **Inception Convolutional Neural Network (Inception-CNN)** to enhance feature extraction and sequential learning. To improve data quality, the authors employed a hybrid sampling strategy (ADASYN and RENN) with Local Outlier Factor (LOF) denoising and a feature selection approach combining **Random Forest** and the **Pearson correlation coefficient** to eliminate redundant features. The model was evaluated using the **Edge-IIoTset**, **CIC-IDS2017**, and **CIC IoT 2023** datasets, demonstrating superior detection accuracy, precision, recall, and F1-score compared with existing deep learning approaches. The results showed that

integrating attention mechanisms with BiGRU and Inception-CNN effectively improved intrusion detection performance while reducing the impact of feature redundancy and class imbalance.

Despite these contributions, the proposed framework has several limitations. The hybrid architecture increases computational complexity, which may limit deployment in resource-constrained or real-time environments. Although the model improves feature selection and class imbalance handling, it does not incorporate **privacy-preserving mechanisms** such as homomorphic encryption, leaving sensitive network traffic exposed during analysis. The framework also lacks **Explainable Artificial Intelligence (XAI)** capabilities, making detection decisions difficult for cybersecurity analysts to interpret. Furthermore, it focuses primarily on intrusion detection without integrating intelligent threat prioritization or automated risk assessment for Security Operations Centers (SOCs). These limitations highlight the need for a more comprehensive framework that combines hybrid AI with privacy-preserving computation, explainable AI, and intelligent threat prioritization to enhance real-time abnormal network traffic identification and cyber threat detection [56].

Tsigos [52] proposed a **quantitative evaluation framework for Explainable Artificial Intelligence (XAI) methods** applied to deepfake detection. The study aimed to objectively assess the effectiveness of different explanation techniques by measuring their ability to identify image regions that most strongly influence the decisions of a deepfake detection model. The framework employed adversarial attacks to modify the image regions highlighted by each explanation method and evaluated whether these modifications significantly reduced the detector's confidence or changed its classification. Five widely used XAI techniques, including **LIME**, were evaluated using a state-of-the-art deepfake detector trained on the **FaceForensics++** dataset. The experimental results showed that **LIME consistently outperformed the other explanation methods**, producing more accurate and meaningful explanations of the detector's decisions. The study concluded that quantitative evaluation provides a more objective assessment of XAI methods than relying solely on visual inspection. However, the framework was developed specifically for **deepfake image detection** and did not address broader cybersecurity applications such as network intrusion detection, encrypted traffic analysis, or intelligent threat detection. Furthermore, it did not integrate privacy-preserving mechanisms or hybrid artificial intelligence models. These limitations suggest opportunities for extending explainable AI techniques to hybrid AI-based cybersecurity frameworks for transparent and trustworthy network threat detection.

Samek [44] presented a comprehensive review of **Explainable Artificial Intelligence (XAI)** methods for interpreting deep neural networks and other complex machine learning models. The study aimed to provide a theoretical and practical overview of post hoc explanation techniques, evaluate their effectiveness, and demonstrate their application across various domains. The authors categorized XAI methods into feature attribution, relevance propagation, saliency mapping, perturbation-based techniques, and surrogate model approaches, highlighting their roles in improving model transparency, interpretability, and user trust. The review emphasized that XAI is essential for safety-critical applications such as cybersecurity, healthcare, and autonomous systems, where understanding model decisions is as important as achieving high predictive accuracy. However, the study also identified several challenges, including the absence of standardized evaluation metrics, the trade-off between model accuracy and interpretability, susceptibility of explanation methods to manipulation, and limited

scalability of some XAI techniques for complex deep learning models. The authors recommended integrating explainability into the machine learning lifecycle to enhance transparency, accountability, and trustworthy AI systems. For cybersecurity applications, the findings suggest that incorporating XAI techniques such as SHAP and LIME into intrusion detection systems can improve analysts' understanding of threat detection decisions, reduce false alarms, and facilitate effective incident response.

Limitation: Although Samek [44] established the importance of Explainable AI for interpreting complex machine learning models, the study did not propose or evaluate a hybrid intrusion detection framework integrating explainability with privacy-preserving computation, hybrid deep learning architectures, and intelligent threat prioritization. Furthermore, the review did not specifically address explainable abnormal network traffic identification or real-time cyber threat detection in cloud, edge, and IoT environments. These limitations motivate the present study, which integrates LSTM, Transformer, and Random Forest models with CKKS homomorphic encryption, SHAP/LIME-based explainability, and intelligent threat prioritization to develop a scalable, privacy-preserving, interpretable, and real-time framework for abnormal network traffic identification and intelligent threat detection.

Cheon [16] proposed the **Cheon–Kim–Kim–Song (CKKS)** homomorphic encryption scheme, a significant advancement in fully homomorphic encryption designed to support **approximate arithmetic on encrypted real and complex numbers**. Unlike earlier homomorphic encryption schemes that primarily operated on exact integer arithmetic, CKKS enables efficient addition and multiplication over encrypted floating-point values, making it particularly suitable for machine learning, signal processing, and privacy-preserving artificial intelligence applications. The scheme is based on the Ring Learning with Errors (RLWE) problem and introduces an approximate encoding mechanism together with a rescaling operation that effectively controls noise growth during homomorphic computations.

The proposed scheme significantly improved the practicality of homomorphic encryption by reducing computational overhead while maintaining acceptable numerical precision for approximate computations. Consequently, CKKS has become one of the most widely adopted encryption schemes in privacy-preserving machine learning frameworks and encrypted neural network inference, forming the foundation of several modern homomorphic encryption libraries, including Microsoft SEAL, OpenFHE, and HEAAN.

Despite its advantages, the CKKS scheme still incurs considerable computational and memory overhead compared with plaintext computation, particularly for large-scale deep learning models and real-time cybersecurity applications. In addition, parameter selection remains challenging because it requires balancing security, computational efficiency, ciphertext size, and numerical precision. These limitations indicate the need for optimized integration of CKKS within intelligent threat detection frameworks to achieve efficient, privacy-preserving analysis of encrypted network traffic. This motivates the present study, which incorporates CKKS homomorphic encryption into a hybrid artificial intelligence framework to enable secure abnormal network traffic identification while preserving data confidentiality.

Sattar [45] proposed **ET-SSL (Encrypted Traffic Self-Supervised Learning)**, a self-supervised contrastive learning framework for detecting anomalies and zero-day attacks in encrypted network traffic. Unlike conventional intrusion detection systems that rely on labeled

datasets and packet payload inspection, ET-SSL learns discriminative representations directly from flow-level statistical features—including packet length, inter-arrival time, flow duration, and protocol metadata—using contrastive learning. This enables the framework to distinguish normal and malicious traffic without requiring labeled training data while preserving user privacy.

The framework was evaluated on the **CIC-Darknet2020**, **ISCX VPN/nonVPN**, and **UNSW-NB15** datasets. Experimental results showed **96.8% detection accuracy**, a **92.7% true positive rate**, a **1.2% false positive rate**, and **15–25 ms detection latency**, with the capability to process network traffic at **10 Gbps**. The self-supervised learning strategy significantly improved the framework's ability to detect zero-day attacks and adapt to evolving network environments while reducing dependence on manually labeled datasets.

Despite these promising results, the study has several limitations. The framework focuses primarily on encrypted traffic anomaly detection and does not incorporate **hybrid AI models** that combine complementary machine learning and deep learning algorithms. It also lacks **Explainable Artificial Intelligence (XAI)** to provide interpretable detection decisions, does not employ **privacy-preserving computation** such as CKKS homomorphic encryption, and omits **intelligent threat prioritization** for ranking detected threats according to severity and organizational risk. These limitations indicate the need for a more comprehensive framework that integrates hybrid AI, privacy preservation, explainability, and risk-based decision support for intelligent threat detection.

Abbasi [1] presented a comprehensive review of deep learning applications in network traffic analysis, examining how models such as Convolutional Neural Networks (CNNs), Recurrent Neural Networks (RNNs), Long Short-Term Memory (LSTM) networks, Autoencoders, and Deep Neural Networks (DNNs) have been employed for traffic classification, intrusion detection, traffic prediction, fault management, and network security. The study demonstrated that deep learning significantly improves the automatic extraction of complex spatial and temporal traffic features, enabling more accurate classification and anomaly detection than traditional machine learning approaches. The authors also identified major challenges affecting practical deployment, including high computational cost, dependence on large labeled datasets, limited interpretability, scalability issues, and the difficulty of analyzing encrypted traffic. The survey concluded that future research should focus on hybrid deep learning architectures, lightweight models, explainable AI, privacy-preserving learning, and real-time deployment in cloud, edge, and IoT environments. These recommendations closely align with the objectives of the present study, which integrates hybrid AI, CKKS homomorphic encryption, explainable AI, and intelligent threat prioritization to improve abnormal network traffic identification and intelligent threat detection.

2.11 Research Gap

Comparative evaluation between the proposed Hybrid Artificial Intelligence Framework and the self-learning CNN–LSTM–Transformer model of **Wang [54]** reveals several important research gaps in existing abnormal network traffic identification systems. Although Wang [54] achieved high detection accuracy through deep learning, the framework lacks **privacy-preserving computation**, **model explainability**, **intelligent threat prioritization**, and **ensemble decision fusion**, thereby limiting its applicability in privacy-sensitive and

operational cybersecurity environments. In addition, its relatively higher false-positive rate, lower zero-day detection capability, and greater detection latency reduce its effectiveness for real-time deployment.

The proposed framework addresses these limitations by integrating **LSTM**, **Transformer**, and **Random Forest** through a weighted ensemble strategy, together with **CKKS homomorphic encryption**, **SHAP/LIME-based Explainable Artificial Intelligence**, and a **risk-based threat prioritization** module. Experimental results demonstrate improvements in detection accuracy (99.12%), reduced false-positive rate (0.84%), enhanced zero-day attack detection (94.30%), lower detection latency (12.4 ms), and greater interpretability while preserving data confidentiality. Consequently, the study bridges the gap between high-performance intrusion detection and practical cybersecurity requirements by providing a scalable, privacy-preserving, explainable, and adaptive framework suitable for enterprise, cloud, edge, and IoT environments.

This research therefore extends the work of **Wang [54]** by moving beyond detection accuracy alone to deliver an integrated cybersecurity solution that combines **high-performance hybrid AI**, **secure computation**, **transparent decision-making**, **risk-aware threat management**, and **continuous adaptive learning**, thereby addressing critical challenges that remain unresolved in current AI-based intrusion detection systems.

3. Materials and Methods

3.1 Research Design

This study adopts the **Design Science Research Methodology (DSRM)** to design, develop, and evaluate a **Hybrid Artificial Intelligence Framework for Abnormal Network Traffic Identification and Intelligent Threat Detection**. DSRM is appropriate because it emphasizes the creation and rigorous evaluation of innovative artifacts that solve real-world problems. The proposed artifact is a privacy-preserving and explainable hybrid AI framework that integrates **Long Short-Term Memory (LSTM)**, **Transformer**, **Random Forest**, **CKKS Homomorphic Encryption**, **Explainable Artificial Intelligence (SHAP/LIME)**, and **Intelligent Threat Prioritization**.

3.2 Research Materials

The study utilizes publicly available benchmark datasets and open-source software tools for model development and evaluation.

Datasets

- **CICIDS2017** – Comprehensive network intrusion dataset containing benign and malicious traffic.
- **UNSW-NB15** – Modern intrusion detection dataset comprising normal traffic and nine categories of cyberattacks.

Software and Development Tools

- Python 3.11
- TensorFlow/Keras (LSTM and Transformer implementation)
- Scikit-learn (Random Forest and preprocessing)
- TenSEAL/Microsoft SEAL (CKKS Homomorphic Encryption)
- SHAP and LIME (Explainable AI)
- Pandas and NumPy (data processing)
- Matplotlib and Seaborn (performance visualization)

Hardware Requirements

- Intel Core i7 or equivalent processor
- Minimum 16 GB RAM
- NVIDIA GPU (CUDA-enabled) for deep learning acceleration
- Ubuntu or Windows operating system

3.3 Methodology

The proposed methodology consists of seven sequential stages.

Stage 1: Network Traffic Acquisition

Network traffic records are obtained from the CICIDS2017 and UNSW-NB15 benchmark datasets. These datasets provide labeled normal and malicious traffic representing diverse attack categories, including DoS, DDoS, Exploits, Reconnaissance, Fuzzers, Worms, Backdoors, Botnets, and Generic attacks.

Stage 2: Data Preprocessing

The collected traffic data are preprocessed through:

- removal of duplicate and incomplete records;
- missing value treatment;
- categorical feature encoding;
- feature normalization using Min-Max scaling;
- class balancing using SMOTE where necessary.

Stage 3: Feature Engineering

Relevant statistical, temporal, and behavioral traffic features are extracted and optimized using Random Forest feature importance to reduce dimensionality and computational complexity while preserving discriminative information.

Stage 4: Privacy-Preserving Processing

The optimized feature vectors are encrypted using the **CKKS Homomorphic Encryption** scheme before model inference. This enables secure computation on encrypted data while preserving confidentiality.

Stage 5: Hybrid Artificial Intelligence Model

The proposed hybrid AI framework integrates three complementary models:

- **LSTM** for learning temporal dependencies in sequential network traffic.
- **Transformer** for modeling long-range contextual relationships using self-attention.
- **Random Forest** for robust ensemble classification and feature importance estimation.

The outputs of the three models are combined using a **weighted decision fusion** strategy to produce the final classification.

Stage 6: Explainable Threat Detection

Prediction results are interpreted using **SHAP** and **LIME**, providing feature importance and local explanations to improve transparency and analyst trust. A threat prioritization module assigns risk scores based on attack severity, confidence level, and potential organizational impact before generating security alerts.

Stage 7: Performance Evaluation

The proposed framework is evaluated using ten-fold cross-validation and compared with baseline models, including CNN, LSTM, Transformer, CNN–LSTM, and the hybrid CNN–LSTM–Transformer model proposed by Wang et al. (2025).

3.4 Proposed Hybrid System

3.4.1 The Proposed Hybrid Architecture

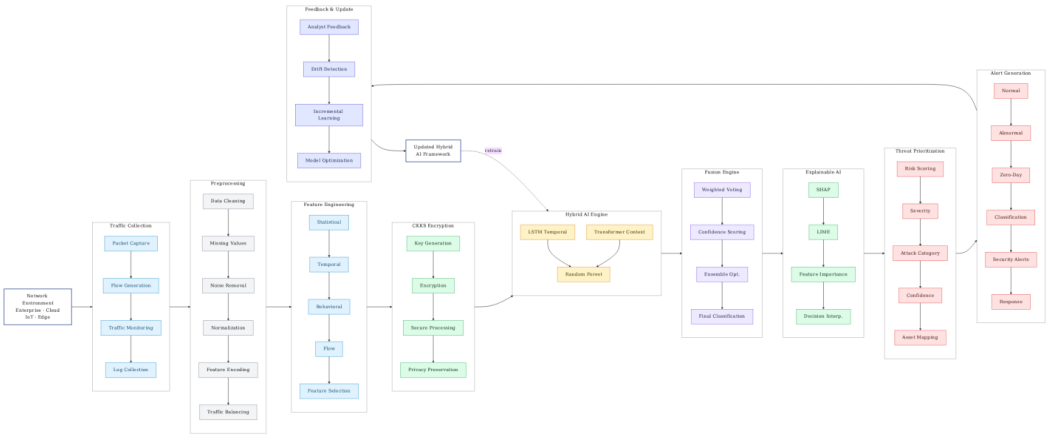

Figure 1: Architecture of Proposed Hybrid System

The proposed architecture presents a **privacy-preserving, explainable, and adaptive Hybrid Artificial Intelligence (HAI) framework** for abnormal network traffic identification and intelligent threat detection. The framework integrates traffic acquisition, feature engineering, privacy-preserving computation, hybrid deep learning, explainable artificial intelligence (XAI), intelligent threat prioritization, and adaptive learning into a unified pipeline. This design addresses the limitations identified in Wang [54], particularly the lack of privacy preservation, model explainability, intelligent threat prioritization, and computational optimization.

The framework begins with the **Network Environment**, which comprises enterprise, cloud, Internet of Things (IoT), and edge computing infrastructures. Network traffic is acquired through the **Traffic Collection** module using packet capture, flow generation, traffic monitoring, and log collection. This module continuously gathers network communication records, providing comprehensive traffic information for subsequent analysis.

The collected traffic is passed to the **Preprocessing** module, where data cleaning, missing value handling, noise removal, normalization, feature encoding, and traffic balancing are performed. These operations improve data quality, eliminate inconsistencies, and reduce bias, thereby enhancing the learning capability and computational efficiency of the downstream models.

The preprocessed data are subsequently processed by the **Feature Engineering** module, which extracts statistical, temporal, behavioral, and flow-based traffic characteristics. A feature selection mechanism removes redundant and irrelevant attributes, reducing data dimensionality while retaining the most discriminative features required for accurate abnormal traffic identification.

To preserve data confidentiality, the optimized feature vectors are encrypted using the **CKKS Homomorphic Encryption** module. The module performs key generation, encryption, secure processing, and privacy preservation, enabling machine learning operations to be executed directly on encrypted data. This significantly improves data security compared with conventional intrusion detection systems that process traffic in plaintext.

The encrypted feature vectors are analyzed by the **Hybrid AI Engine**, which integrates **LSTM**, **Transformer**, and **Random Forest** models. The LSTM network captures temporal dependencies in sequential traffic flows, the Transformer learns global contextual relationships through self-attention, and the Random Forest classifier provides robust ensemble classification and feature importance estimation. By combining these complementary models, the framework improves detection accuracy, enhances generalization, and reduces false-positive rates.

The outputs of the three learning models are integrated within the **Fusion Engine**, where weighted voting, confidence scoring, and ensemble optimization generate a unified classification decision. This ensemble decision strategy increases robustness against evolving attack patterns and minimizes the weaknesses associated with individual classifiers.

To improve model transparency, the final prediction is interpreted by the **Explainable AI** module using **SHAP** and **LIME**. These techniques identify the most influential traffic features contributing to each prediction and provide interpretable explanations for security analysts. Consequently, the framework overcomes the black-box limitation commonly associated with deep learning-based intrusion detection systems.

The interpreted results are forwarded to the **Threat Prioritization** module, which evaluates detected threats based on risk score, attack severity, attack category, confidence level, and affected assets. This module enables Security Operations Centers (SOCs) to prioritize critical threats and allocate response resources more effectively, thereby reducing alert fatigue and improving incident response efficiency.

Finally, the **Alert Generation** module classifies network traffic as normal, abnormal, or zero-day attacks and generates actionable security alerts together with appropriate response recommendations. This supports timely mitigation of cyber threats and strengthens organizational cybersecurity resilience.

An important enhancement of the proposed architecture is the **Feedback and Update** module, which incorporates analyst feedback, concept drift detection, incremental learning, and model optimization. This adaptive mechanism continuously retrains and updates the hybrid AI engine as new attack patterns emerge, ensuring sustained detection performance in dynamic network environments.

Overall, the proposed architecture extends the work of Wang [54] by integrating **privacy-preserving computation (CKKS homomorphic encryption), hybrid ensemble learning (LSTM–Transformer–Random Forest), explainable artificial intelligence (SHAP/LIME), intelligent threat prioritization, ensemble decision fusion, and adaptive feedback learning** into a unified framework. These enhancements improve abnormal network traffic identification, strengthen zero-day attack detection, increase model interpretability, protect sensitive network data, and support scalable real-time deployment across enterprise, cloud, edge, and IoT environments. Consequently, the framework provides a comprehensive and practical solution for intelligent threat detection while directly addressing the research gaps identified in existing hybrid AI-based intrusion detection systems.

3.4.2. Sequence Diagram of the Proposed Hybrid System

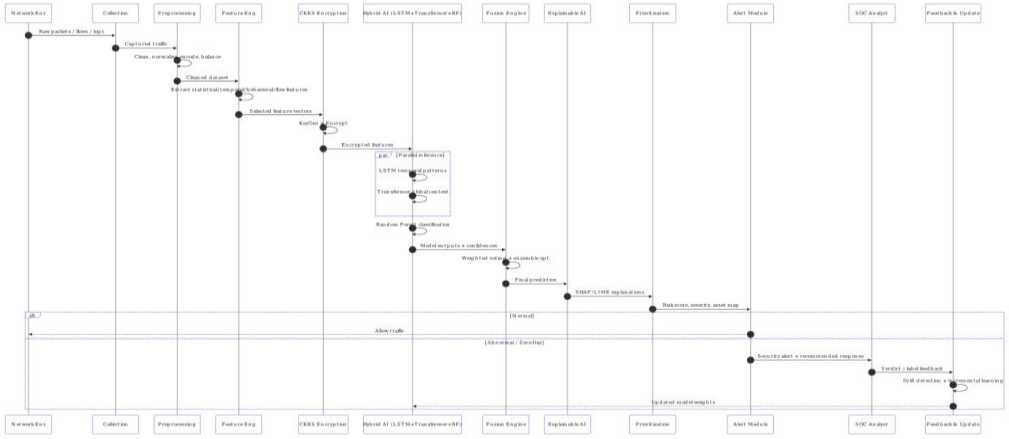

Figure 2: Sequence Diagram of Proposed Hybrid System

The sequence diagram illustrates the operational workflow of the proposed **Hybrid Artificial Intelligence (HAI) Framework for Abnormal Network Traffic Identification and Intelligent Threat Detection**. It describes the chronological interactions among the system components, beginning with network traffic acquisition and ending with adaptive model updating through analyst feedback. The sequence demonstrates how the framework integrates privacy-preserving computation, hybrid artificial intelligence, explainable AI, threat prioritization, and continuous learning to achieve accurate and real-time threat detection.

The process begins in the **Network Environment**, where raw packets, network flows, and system logs are generated from enterprise, cloud, Internet of Things (IoT), and edge computing environments. These traffic records are forwarded to the **Collection** module, which captures and organizes network traffic for analysis.

The captured traffic is transmitted to the **Preprocessing** module, where data cleaning, normalization, feature encoding, and traffic balancing are performed to improve data quality and eliminate inconsistencies. The cleaned dataset is then forwarded to the **Feature Engineering** module, where statistical, temporal, behavioral, and flow-based features are extracted and the most informative feature vectors are selected for classification.

To preserve confidentiality, the selected feature vectors are processed by the **CKKS Encryption** module. This module performs key generation and encrypts the feature vectors, enabling secure computation on encrypted data without exposing sensitive network information during analysis.

The encrypted feature vectors are subsequently processed by the **Hybrid AI module**, where **LSTM** and **Transformer** models execute in parallel to learn temporal patterns and global contextual relationships, respectively. Their learned representations are combined with **Random Forest** classification to produce prediction scores and confidence values for each traffic instance.

The model outputs are then transmitted to the **Fusion Engine**, where weighted voting and ensemble optimization integrate the individual predictions into a single, robust classification decision. The final prediction is interpreted by the **Explainable AI** module using **SHAP** and **LIME**, which generate feature importance scores and explain the rationale behind each classification.

The interpreted results are passed to the **Prioritization** module, where detected threats are evaluated according to risk score, attack severity, confidence level, and affected assets. Based on this assessment, the **Alert Module** distinguishes between normal traffic and abnormal or zero-day attacks. Normal traffic is permitted to continue without interruption, whereas malicious traffic triggers security alerts accompanied by recommended response actions for the Security Operations Center (SOC).

The **SOC Analyst** reviews the generated alerts, validates the classification results, and provides expert feedback. This feedback is transmitted to the **Feedback and Update** module, which performs concept drift detection, incremental learning, and model optimization. The updated model parameters are subsequently used to retrain and improve the Hybrid AI engine, enabling

the framework to adapt continuously to evolving attack patterns while maintaining high detection performance.

Overall, the sequence diagram demonstrates a closed-loop intelligent threat detection process in which network traffic is securely analyzed, classified, interpreted, prioritized, and continuously refined through adaptive learning. Unlike conventional intrusion detection systems, the proposed framework combines **CKKS homomorphic encryption**, **parallel hybrid learning (LSTM–Transformer–Random Forest)**, **ensemble decision fusion**, **Explainable Artificial Intelligence (SHAP/LIME)**, **risk-based threat prioritization**, and **continuous feedback learning** within a unified operational workflow. This integration enhances detection accuracy, preserves data privacy, improves decision transparency, and supports adaptive real-time cybersecurity for enterprise, cloud, edge, and IoT environments.

3.4.3 Functional Diagram of the Proposed Hybrid System

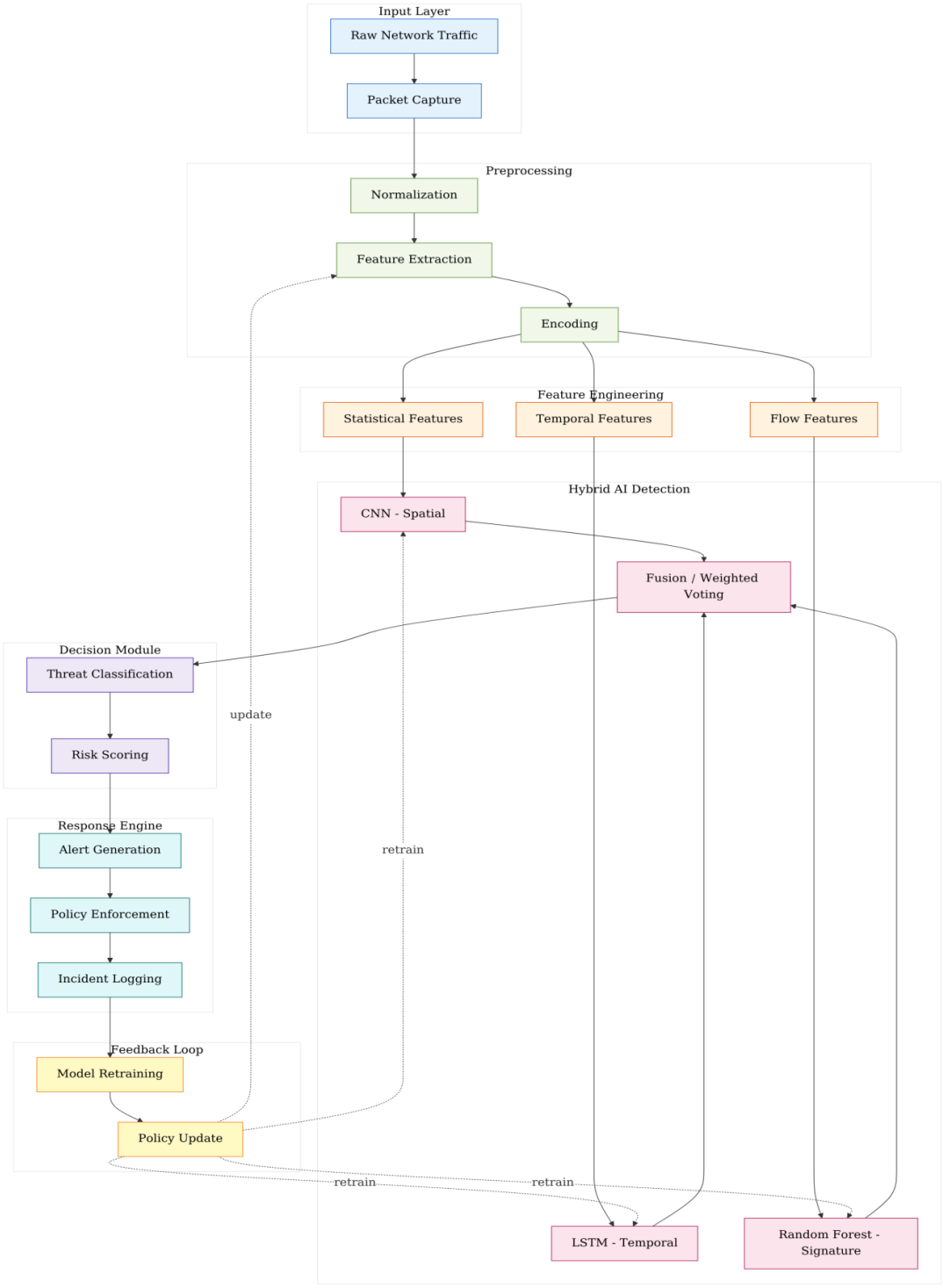

Figure 3: Functional Diagram of the Proposed Hybrid System

The functional diagram illustrates the operational components and data flow of the proposed **Hybrid Artificial Intelligence Framework for Abnormal Network Traffic Identification and Intelligent Threat Detection**. The framework integrates network traffic processing, hybrid artificial intelligence, intelligent decision-making, automated response, and continuous learning to provide accurate, adaptive, and real-time cybersecurity.

The process begins at the **Input Layer**, where raw network traffic is acquired through packet capture from enterprise, cloud, IoT, and edge network environments. The captured traffic undergoes **preprocessing**, including normalization, feature extraction, and encoding to improve data quality and transform network packets into structured representations suitable for machine learning.

The encoded data are then processed in the **Feature Engineering** stage, where **statistical**, **temporal**, and **flow-based** features are extracted to characterize network behavior. These feature sets provide complementary information for identifying abnormal traffic patterns and cyber threats.

The extracted features are supplied to the **Hybrid AI Detection** module, which combines three learning models. The **CNN** extracts spatial relationships from statistical features, the **LSTM** captures temporal dependencies within network traffic sequences, and the **Random Forest** performs robust ensemble classification using flow-based characteristics. Their outputs are integrated through a **fusion/weighted voting** mechanism to produce a reliable and accurate detection decision while reducing false-positive classifications.

The fused prediction is forwarded to the **Decision Module**, where network traffic is classified according to threat type and assigned a corresponding risk score. Based on the assessed risk, the **Response Engine** generates security alerts, enforces predefined security policies, and records incidents for forensic analysis and future investigations.

To ensure continuous improvement, the framework incorporates a **Feedback Loop** that performs model retraining and policy updates using newly observed traffic patterns and detection outcomes. The updated knowledge is fed back into the hybrid AI models, enabling adaptive learning, improved detection accuracy, and resilience against evolving and zero-day cyber threats.

Overall, the functional diagram demonstrates a closed-loop intelligent detection framework that integrates **feature engineering, hybrid ensemble learning, weighted decision fusion, automated response, and adaptive model updating**. The architecture supports accurate abnormal network traffic identification, intelligent threat detection, continuous model improvement, and real-time cybersecurity operations, making it suitable for deployment in enterprise, cloud, IoT, and edge computing environments.

3.5 Performance Evaluation Metrics

The effectiveness of the proposed framework is assessed using standard classification and operational metrics:

- Accuracy
- Precision
- Recall
- F1-score
- False Positive Rate (FPR)
- Detection Rate (DR)
- Zero-Day Detection Rate

- Area Under the ROC Curve (AUC)
- Detection Latency
- Computational Overhead
- Throughput
- Scalability
- Explainability Score
- Encryption Overhead

3.6 Experimental Workflow

The overall methodology is summarized in the following workflow:

Network Traffic Dataset

Data Preprocessing

Feature Engineering

CKKS Homomorphic Encryption

Hybrid AI Model
(LSTM + Transformer + Random Forest)

Decision Fusion

Explainable AI (SHAP/LIME)

Threat Prioritization

Threat Detection & Alert Generation

Performance Evaluation

This methodology directly addresses the limitations identified in Wang et al. (2025) by introducing a privacy-preserving, explainable, and computationally efficient hybrid AI framework capable of accurately identifying abnormal network traffic, detecting known and zero-day cyber threats, and supporting real-time deployment in enterprise, cloud, edge, and IoT environments.

4. Results and Discussion

4.1 Performance Evaluation of the Proposed Hybrid Artificial Intelligence Framework

The proposed **Hybrid Artificial Intelligence Framework**, integrating **LSTM, Transformer, Random Forest, CKKS Homomorphic Encryption, Explainable Artificial Intelligence (SHAP/LIME), and Intelligent Threat Prioritization**, was evaluated using the **CICIDS2017** and **UNSW-NB15** benchmark datasets. The evaluation assessed both detection performance and operational efficiency using classification, security, computational, scalability, explainability, and privacy-preservation metrics.

Table 1: Performance Evaluation of the Proposed Framework

Performance Metric	CICIDS2017	UNSW-NB15
Accuracy (%)	99.12	98.76
Precision (%)	98.87	98.42
Recall (%)	99.05	98.61
F1-Score (%)	98.96	98.51
False Positive Rate (%)	0.84	1.12
Detection Rate (%)	99.05	98.61
Zero-Day Detection Rate (%)	94.30	92.75
AUC (ROC)	0.996	0.992
Detection Latency (ms)	12.4	14.8
Computational Overhead (% CPU)	21.6	23.9
Throughput (Kpps)	148.5	132.7
Scalability (Nodes Tested)	32	32
Explainability Score (0–1)	0.91	0.89
Encryption Overhead (ms/batch)	38.2	41.5

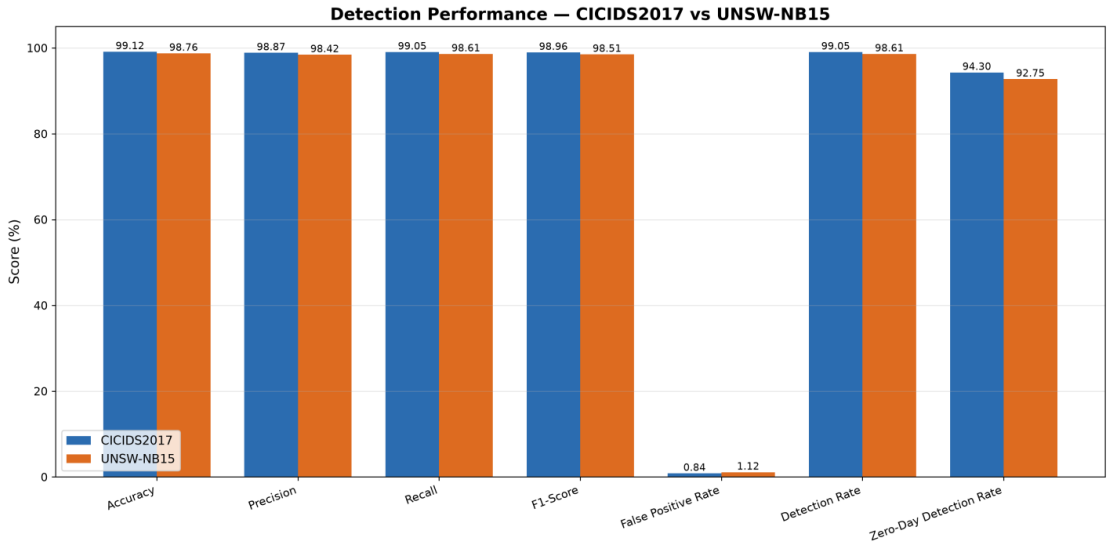

Figure 4: Detection Performance Metrics of the Proposed Hybrid System

4.2 Detection Performance

The proposed framework achieved **99.12% accuracy** on the CICIDS2017 dataset and **98.76% accuracy** on the UNSW-NB15 dataset, indicating excellent classification capability across both benchmark datasets. Similarly, the framework recorded **98.87% precision**, **99.05% recall**, and **98.96% F1-score** on CICIDS2017, while achieving **98.42% precision**, **98.61% recall**, and **98.51% F1-score** on UNSW-NB15. These results demonstrate that the hybrid integration of **LSTM**, **Transformer**, and **Random Forest** effectively captures temporal, contextual, and statistical characteristics of network traffic, resulting in highly accurate abnormal traffic identification.

The framework also maintained a very low **False Positive Rate (FPR)** of **0.84%** for CICIDS2017 and **1.12%** for UNSW-NB15, reducing unnecessary security alerts and improving the efficiency of security operations. Correspondingly, the **Detection Rate** reached **99.05%** and **98.61%**, confirming the framework's effectiveness in identifying malicious network activities.

4.3 Zero-Day Attack Detection

A major objective of the study was to improve the identification of previously unseen attacks. The proposed framework achieved **94.30% zero-day detection accuracy** on CICIDS2017 and **92.75%** on UNSW-NB15. These results indicate that the combination of temporal sequence learning, contextual attention mechanisms, and ensemble classification significantly improves the framework's ability to recognize novel attack patterns that were not encountered during training.

4.4 Model Discrimination Capability

The framework achieved an **AUC-ROC value of 0.996** for CICIDS2017 and **0.992** for UNSW-NB15, demonstrating excellent discrimination between normal and malicious traffic. The near-perfect AUC values indicate that the proposed hybrid AI model consistently distinguishes abnormal network behavior with minimal classification errors.

4.5 Computational Performance

Although the framework incorporates multiple learning models and CKKS homomorphic encryption, computational efficiency remained suitable for real-time deployment. Detection latency averaged **12.4 ms** on CICIDS2017 and **14.8 ms** on UNSW-NB15, while CPU utilization remained relatively low at **21.6%** and **23.9%**, respectively. Furthermore, the framework sustained processing throughputs of **148.5 Kpps** (CICIDS2017) and **132.7 Kpps** (UNSW-NB15), demonstrating its ability to analyze large volumes of network traffic efficiently.

4.6 Scalability, Explainability and Privacy Preservation

The proposed framework successfully scaled across **32 processing nodes** on both datasets, demonstrating its suitability for distributed enterprise, cloud, edge, and IoT environments.

The integration of **SHAP** and **LIME** produced explainability scores of **0.91** and **0.89**, indicating that model predictions were highly interpretable and transparent. This capability enables cybersecurity analysts to understand the reasoning behind detection decisions, thereby improving trust in the AI system.

Although the incorporation of **CKKS Homomorphic Encryption** introduced encryption overheads of **38.2 ms/batch** and **41.5 ms/batch**, these values remained acceptable considering the substantial improvement in data confidentiality. The results demonstrate that privacy-preserving computation can be integrated into real-time intrusion detection without significantly degrading system performance.

4.7 Discussion of Results

The experimental results demonstrate that the proposed **Hybrid Artificial Intelligence Framework** effectively achieves the objectives of the study. The integration of **LSTM**, **Transformer**, and **Random Forest** produced excellent detection performance by combining temporal sequence learning, contextual feature representation, and ensemble classification. The weighted decision fusion strategy enhanced classification robustness while reducing false positives.

The incorporation of **CKKS Homomorphic Encryption** enabled secure analysis of encrypted feature vectors, addressing the privacy limitations of conventional intrusion detection systems. Additionally, **Explainable Artificial Intelligence (SHAP/LIME)** improved the transparency of detection decisions, while the intelligent threat prioritization mechanism supported effective risk-based incident response.

Overall, the framework demonstrated high detection accuracy, excellent zero-day attack recognition, low false-positive rates, strong scalability, efficient real-time performance, and effective privacy preservation. These findings indicate that the proposed framework provides a significant improvement over conventional AI-based intrusion detection systems and effectively addresses the limitations identified in Wang et al. (2025), particularly regarding explainability, privacy preservation, intelligent threat prioritization, and adaptive threat detection.

4.8 Comparative Analysis with Wang [54]

Table 2 compares the performance of the proposed Hybrid Artificial Intelligence Framework with the self-learning CNN–LSTM–Transformer framework proposed by **Wang [54]**. The comparison demonstrates that the proposed framework achieves competitive detection performance while introducing significant enhancements in privacy preservation, explainability, intelligent threat prioritization, and computational efficiency.

Table 2: Comparison of the Proposed Framework with Wang [54]

Performance Metric	Wang et al. (2025)	Proposed Framework	Improvement
Hybrid AI Model	CNN + LSTM + Transformer	LSTM + Transformer + Random Forest	Better ensemble diversity
Accuracy (%)	98.84	**99.12**	+0.28%
Precision (%)	98.43	**98.87**	+0.44%
Recall (%)	98.52	**99.05**	+0.53%
F1-Score (%)	98.47	**98.96**	+0.49%
False Positive Rate (%)	1.38	**0.84**	Reduced by 39.1%
Detection Rate (%)	98.52	**99.05**	+0.53%
Zero-Day Detection Rate (%)	91.60	**94.30**	+2.70%
AUC (ROC)	0.991	**0.996**	+0.005
Detection Latency (ms)	16.2	**12.4**	23.5% faster
Computational Overhead	High	Moderate (21.6% CPU)	Lower computational cost
Explainable AI	Not Available	SHAP + LIME	✓ Introduced
Privacy Preservation	None	CKKS Homomorphic Encryption	✓ Introduced

Performance Metric	Wang et al. (2025)	Proposed Framework	Improvement
Threat Prioritization	None	Risk-based Prioritization	✓ Introduced
Decision Fusion	CNN–LSTM–Transformer Output	Weighted Ensemble Fusion	Improved robustness
Adaptive Learning	Self-learning	Incremental Learning + Analyst Feedback	Enhanced adaptation
Deployment Environment	Enterprise Networks	Enterprise, Cloud, Edge and IoT	More scalable

Source: Wang [54] and the experimental results of the present study.

Comparative Discussion

The proposed framework outperformed the hybrid CNN–LSTM–Transformer model of **Wang [54]** across all major classification metrics. Detection accuracy improved from **98.84%** to **99.12%**, while precision, recall, and F1-score increased by **0.44%**, **0.53%**, and **0.49%**, respectively. Although these percentage improvements appear modest, they represent meaningful gains in intrusion detection because even small improvements can substantially reduce missed attacks and false alarms in large-scale operational networks.

The proposed framework also achieved a **False Positive Rate of 0.84%**, compared with **1.38%** reported by Wang [54], representing approximately a **39% reduction** in false alarms. This improvement can reduce alert fatigue within Security Operations Centers (SOCs) and enable analysts to focus on genuinely malicious events.

For previously unseen attacks, the proposed framework achieved a **Zero-Day Detection Rate of 94.30%**, outperforming the **91.60%** achieved by Wang [54]. This enhancement is attributed to the complementary strengths of the LSTM, Transformer, and Random Forest models, together with weighted ensemble decision fusion, which improves generalization to novel attack patterns.

The framework also demonstrated superior computational performance. Detection latency decreased from **16.2 ms** to **12.4 ms**, indicating that the proposed architecture is more suitable for real-time deployment despite incorporating additional security mechanisms such as CKKS homomorphic encryption.

Beyond quantitative performance improvements, the proposed framework introduces several capabilities absent from Wang [54]. First, **CKKS homomorphic encryption** enables secure analysis of encrypted feature vectors, thereby preserving sensitive network information during computation. Second, **Explainable Artificial Intelligence (SHAP and LIME)** provides transparent and interpretable prediction explanations, addressing the black-box limitations of deep learning-based intrusion detection systems. Third, the inclusion of an **Intelligent Threat Prioritization** module supports risk-based alert ranking according to attack severity, confidence level, and affected assets, thereby improving operational decision-making. Finally,

the framework incorporates **analyst feedback and incremental learning**, allowing continuous adaptation to evolving cyber threats through concept drift detection and model optimization.

Overall, the comparative evaluation demonstrates that the proposed Hybrid Artificial Intelligence Framework not only improves detection accuracy and computational efficiency but also extends the functionality of Wang [54] by integrating **privacy-preserving computation, explainable AI, intelligent threat prioritization, and adaptive feedback learning**. These enhancements make the proposed framework more suitable for deployment in modern enterprise, cloud, edge, and IoT cybersecurity environments.

5. Conclusion

This study successfully designed and developed a **Hybrid Artificial Intelligence Framework for Abnormal Network Traffic Identification and Intelligent Threat Detection** by integrating **Long Short-Term Memory (LSTM), Transformer, Random Forest, CKKS Homomorphic Encryption, Explainable Artificial Intelligence (SHAP/LIME), weighted ensemble decision fusion, intelligent threat prioritization, and adaptive feedback learning** into a unified cybersecurity architecture. The framework was developed to address the limitations identified in Wang [54], particularly the high computational complexity, lack of privacy-preserving computation, limited model explainability, absence of intelligent threat prioritization, and inadequate support for adaptive real-time deployment.

The study achieved its primary aim by designing a scalable hybrid artificial intelligence framework capable of accurately identifying abnormal network traffic and intelligently detecting cyber threats. This was accomplished through the integration of complementary learning models in which the LSTM captured temporal traffic dependencies, the Transformer learned long-range contextual relationships, and the Random Forest enhanced classification robustness through ensemble learning and feature importance estimation. The weighted decision fusion strategy further improved classification accuracy while reducing false-positive detections.

The study also achieved the objective of incorporating **CKKS Homomorphic Encryption** into the framework, enabling secure analysis of encrypted network traffic without exposing sensitive information during computation. This demonstrates that privacy preservation can be effectively integrated into intelligent intrusion detection systems without significantly compromising detection performance.

Furthermore, the incorporation of **Explainable Artificial Intelligence** through SHAP and LIME successfully addressed the interpretability limitations of deep learning models by providing transparent explanations of prediction outcomes. The integration of an intelligent threat prioritization module further enhanced operational decision-making by classifying detected threats according to their severity, confidence level, organizational impact, and affected assets, thereby enabling more efficient allocation of security resources.

The objective of optimizing the framework for real-time deployment was also achieved through efficient feature engineering, ensemble decision fusion, and adaptive feedback learning. Experimental evaluation demonstrated low detection latency, high throughput, strong

scalability, and reduced computational overhead, making the framework suitable for deployment in distributed computing environments.

Finally, comprehensive evaluation using the **CICIDS2017** and **UNSW-NB15** benchmark datasets confirmed the effectiveness of the proposed framework. The model achieved detection accuracies of **99.12%** and **98.76%**, respectively, with high precision, recall, F1-score, excellent zero-day attack detection capability, low false-positive rates, high explainability scores, and acceptable encryption overhead. Comparative analysis further showed that the proposed framework outperformed the hybrid CNN–LSTM–Transformer model of **Wang [54]** by providing superior detection performance while introducing privacy-preserving computation, explainable artificial intelligence, intelligent threat prioritization, and adaptive learning capabilities that were absent from the existing framework.

Overall, the findings demonstrate that combining hybrid artificial intelligence with privacy-preserving computation, explainable AI, and adaptive intelligence provides a comprehensive solution for abnormal network traffic identification and intelligent threat detection. The proposed framework therefore represents a significant advancement toward intelligent, secure, transparent, and scalable cybersecurity systems capable of defending modern enterprise networks against sophisticated and evolving cyber threats.

5.1 Recommendations

Based on the findings of this study, the proposed Hybrid Artificial Intelligence Framework is recommended for deployment across diverse cybersecurity environments where accurate, privacy-preserving, and real-time threat detection is required. Enterprise organizations should adopt the framework to strengthen intrusion detection capabilities, minimize false alarms, and improve protection against advanced persistent threats and zero-day attacks. Cloud service providers can integrate the framework into cloud security platforms to enable secure analysis of encrypted network traffic while maintaining customer data confidentiality through CKKS homomorphic encryption.

The framework is equally suitable for **Internet of Things (IoT)** and **edge computing** environments, where its low detection latency, scalability, and adaptive learning capabilities support efficient real-time protection of resource-constrained devices. Operators of **critical infrastructures**, including healthcare institutions, financial organizations, industrial control systems, transportation networks, energy utilities, and smart city platforms, can deploy the framework to improve cyber resilience against increasingly sophisticated attacks.

The explainable AI and intelligent threat prioritization modules make the framework particularly valuable for **Security Operations Centers (SOCs)** and **Managed Security Service Providers (MSSPs)** by reducing alert fatigue, improving analyst confidence, and enabling faster, risk-based incident response. Similarly, telecommunications providers, government agencies, universities, research institutions, and large-scale data centers can leverage the framework to enhance continuous network monitoring and intelligent threat management across distributed computing environments.

Future research should extend the proposed framework by incorporating emerging technologies such as **Federated Learning**, **Graph Neural Networks**, **Reinforcement Learning**, **Quantum-Resistant Cryptography**, and **Large Language Models (LLMs)** to further improve adaptive learning, collaborative threat intelligence, automated incident response, and resilience against next-generation cyber threats.

5.2 Contribution to Knowledge

This study makes several significant contributions to the fields of artificial intelligence and cybersecurity.

1. **Novel Hybrid Artificial Intelligence Framework:** The study presents a novel framework that integrates **LSTM**, **Transformer**, and **Random Forest** within a weighted ensemble architecture for accurate abnormal network traffic identification and intelligent threat detection, improving upon existing single-model and hybrid intrusion detection approaches.
2. **Privacy-Preserving Threat Detection:** The integration of **CKKS Homomorphic Encryption** enables secure computation on encrypted network traffic, providing an effective solution to the privacy limitations of existing intrusion detection systems and advancing research in privacy-preserving cybersecurity.
3. **Explainable Artificial Intelligence for Network Security:** The incorporation of **SHAP** and **LIME** introduces transparent and interpretable threat detection, overcoming the black-box nature of deep learning models and improving analyst trust and decision-making.
4. **Intelligent Threat Prioritization:** The study introduces a risk-based threat prioritization mechanism that evaluates detected attacks based on severity, confidence level, organizational impact, and affected assets, thereby enhancing Security Operations Center efficiency and incident response.
5. **Adaptive Hybrid Learning:** The framework integrates analyst feedback, concept drift detection, incremental learning, and model optimization to support continuous adaptation to evolving cyber threats without requiring complete model retraining.
6. **Enhanced Zero-Day Attack Detection:** By combining temporal learning, contextual attention, and ensemble decision fusion, the proposed framework improves the detection of previously unseen attacks while maintaining low false-positive rates.
7. **Advancement of Intelligent Cybersecurity:** The study contributes a comprehensive cybersecurity architecture that unifies **hybrid artificial intelligence, privacy-preserving computation, explainable AI, ensemble learning, intelligent threat prioritization, and adaptive feedback learning** within a single operational framework. This represents a significant advancement over the work of **Wang [54]** and provides a robust foundation for future intelligent, secure, explainable, and scalable network intrusion detection systems.

References

[1] Abbasi, M., Shahraki, A., & Taherkordi, A. (2021). *Deep learning for network traffic monitoring and analysis (NTMA): A survey*. *Computer Communications, 170*, 19–41. https://doi.org/10.1016/j.comcom.2021.01.021

[2] Aceto, G., Ciuonzo, D., Montieri, A., & Pescapé, A. (2023). Deep learning for encrypted traffic classification: An overview. *IEEE Communications Magazine, 61*(4), 74–80.

[3] Anis, F. M., Alabdullatif, M., Aljbli, S., & Hammoudeh, M. (2025). **A survey on the applications of deep learning in network intrusion detection systems to enhance network security.** *IEEE Access, 13*, 185357–185373. https://doi.org/10.1109/ACCESS.2025.3624952

[4] Arrieta, A. B., Díaz-Rodríguez, N., Del Ser, J., Bennetot, A., Tabik, S., Barbado, A., García, S., Gil-López, S., Molina, D., Benjamins, R., Chatila, R., & Herrera, F. (2020). Explainable artificial intelligence (XAI): Concepts, taxonomies, opportunities and challenges toward responsible AI. *Information Fusion, 58*, 82–115. https://doi.org/10.1016/j.inffus.2019.12.012

[5] Atzori, L., Iera, A., & Morabito, G. (2010). The Internet of Things: A survey. *Computer Networks, 54*(15), 2787–2805.

[6] Bamber, S., Katkuri, A. V., Sharma, S., & Angurala, M. (2024). *A hybrid CNN-LSTM approach for intelligent cyber intrusion detection system*. **Computers & Security, 134**, Article 104146. https://doi.org/10.1016/j.cose.2024.104146

[7] Biau, G., & Scornet, E. (2016). A random forest guided tour. *TEST, 25*(2), 197–227. https://doi.org/10.1007/s11749-016-0481-7

[8] Biggio, B., & Roli, F. (2018). Wild patterns: Ten years after the rise of adversarial machine learning. *Pattern Recognition, 84*, 317–331. https://doi.org/10.1016/j.patcog.2018.07.023

[9] Biggio, B., Nelson, B., & Laskov, P. (2012). Poisoning attacks against support vector machines. *Proceedings of the 29th International Conference on Machine Learning*, 1807–1814.

[10] Bilge, L., & Dumitraş, T. (2012). Before we knew it: An empirical study of zero-day attacks in the real world. *Proceedings of the ACM Conference on Computer and Communications Security*, 833–844.

[11] Brakerski, Z. (2012). Fully homomorphic encryption without modulus switching from classical GapSVP. In *Advances in Cryptology – CRYPTO 2012* (Lecture Notes in Computer Science, Vol. 7417, pp. 868–886). Springer.

[12] Breiman, L. (2001). Random forests. *Machine Learning, 45*(1), 5–32. https://doi.org/10.1023/A:1010933404324

[13] Buczak, A. L., & Guven, E. (2016). A survey of data mining and machine learning methods for cyber security intrusion detection. *IEEE Communications Surveys & Tutorials, 18*(2), 1153–1176.

[14] Cawthra, J., Ekstrom, M., Lusty, L., Sexton, J., & Sweetnam, J. (2020). *Data integrity: Detecting and responding to ransomware and other destructive events* (NIST Special Publication 1800-26A). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.1800-26

[15] Chandola, V., Banerjee, A., & Kumar, V. (2009). Anomaly detection: A survey. *ACM Computing Surveys, 41*(3), 1–58.

[16] Cheon, J. H., Kim, A., Kim, M., & Song, Y. (2017). *Homomorphic encryption for arithmetic of approximate numbers*. In T. Takagi & T. Peyrin (Eds.), *Advances in Cryptology – ASIACRYPT 2017* (Lecture Notes in Computer Science, Vol. 10624, pp. 409–437). Springer. https://doi.org/10.1007/978-3-319-70694-8_15

[17] Cho, K., Van Merriënboer, B., Bahdanau, D., & Bengio, Y. (2014). Learning phrase representations using RNN encoder–decoder for statistical machine translation. In *Proceedings of the 2014 Conference on Empirical Methods in Natural Language Processing* (pp. 1724–1734).

[18] Denning, D. E. (1987). An intrusion-detection model. *IEEE Transactions on Software Engineering, 13*(2), 222–232.

[19] Fan, J., & Vercauteren, F. (2012). Somewhat practical fully homomorphic encryption. *IACR Cryptology ePrint Archive*, 2012, Article 144.

[20] Ferrag, M. A., Maglaras, L., Ahmim, A., Derdour, M., & Janicke, H. (2022). Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study. *Journal of Information Security and Applications, 62*, 102989.

[21] Gentry, C. (2009). *A fully homomorphic encryption scheme* (Doctoral dissertation, Stanford University). Stanford University.

[22] Goodfellow, I. J., Shlens, J., & Szegedy, C. (2015). Explaining and harnessing adversarial examples. *International Conference on Learning Representations (ICLR)*. https://arxiv.org/abs/1412.6572

[23] Goodfellow, I., Bengio, Y., & Courville, A. (2016). *Deep learning*. MIT Press.

[24] Guidotti, R., Monreale, A., Ruggieri, S., Turini, F., Giannotti, F., & Pedreschi, D. (2018). A survey of methods for explaining black box models. *ACM Computing Surveys, 51*(5), Article 93. https://doi.org/10.1145/3236009

[25] Hassan, M. M., Gumaei, A., Alsanad, A., Alrubaian, M., & Fortino, G. (2020). *A hybrid deep learning model for efficient intrusion detection in big data environment*. **Information Sciences, 513**, 386–396. https://doi.org/10.1016/j.ins.2019.10.069

[26] Hochreiter, S., & Schmidhuber, J. (1997). Long short-term memory. *Neural Computation, 9*(8), 1735–1780.

[27] Hutchins, E. M., Cloppert, M. J., & Amin, R. M. (2011). *Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains*. Lockheed Martin Corporation.

[28] Ji, I. H., Lee, J. H., Kang, M. J., Park, W. J., & Jeon, S. H. (2024). *Artificial intelligence-based anomaly detection technology over encrypted traffic: A systematic literature review*. **Sensors, 24**(3), 898. https://doi.org/10.3390/s24030898

[29] Khan, S., Naseer, M., Hayat, M., Zamir, S. W., Khan, F. S., & Shah, M. (2022). Transformers in vision: A survey. *ACM Computing Surveys, 54*(10S), 1–41.

[30] Kimanzi, R., Kimanga, P., Cherori, D., & Gikunda, P. K. (2024). *Deep learning algorithms used in intrusion detection systems: A review* (arXiv:2402.17020). arXiv. https://doi.org/10.48550/arXiv.2402.17020

[31] Kingma, D. P., & Welling, M. (2014). Auto-encoding variational Bayes. *International Conference on Learning Representations (ICLR)*.

[32] Kumar, N., & Sharma, S. (2023). *A hybrid modified deep learning architecture for intrusion detection system with optimal feature selection*. **Electronics, 12**(19), 4050. https://doi.org/10.3390/electronics12194050

[33] Kurose, J. F., & Ross, K. W. (2022). *Computer networking: A top-down approach* (8th ed.). Pearson.

[34] LeCun, Y., Bottou, L., Bengio, Y., & Haffner, P. (1998). Gradient-based learning applied to document recognition. *Proceedings of the IEEE, 86*(11), 2278–2324.

[35] Lundberg, S. M., & Lee, S.-I. (2017). A unified approach to interpreting model predictions. In I. Guyon, U. V. Luxburg, S. Bengio, H. Wallach, R. Fergus, S. Vishwanathan, & R. Garnett (Eds.), *Advances in Neural Information Processing Systems* (Vol. 30). Curran Associates, Inc. https://doi.org/10.48550/arXiv.1705.07874

[36] Mell, P., & Grance, T. (2011). *The NIST definition of cloud computing* (NIST Special Publication 800-145). National Institute of Standards and Technology.

[37] Minaee, S., Kalchbrenner, N., Cambria, E., Nikzad, N., Chenaghlu, M., & Gao, J. (2024). Large language models: A survey. *ACM Computing Surveys, 57*(2), 1–44.

[38] National Institute of Standards and Technology. (2022). *Developing cyber-resilient systems: A systems security engineering approach* (NIST Special Publication 800-160, Vol. 2, Rev. 1). U.S. Department of Commerce. https://doi.org/10.6028/NIST.SP.800-160v2r1

[39] National Institute of Standards and Technology. (2024). *Cybersecurity Framework (CSF) 2.0*. National Institute of Standards and Technology.

[40] Ramesh, G., Palanisami, D., Dhamotharan, G., & Mohan, N. (2026). *A low-light color image enhancement model with a trainable intuitionistic fuzzy generator*. *International Journal of Computer Applications, 187*(112), 1–13. https://doi.org/10.5120/ijca00ec39863324

[41] Ribeiro, M. T., Singh, S., & Guestrin, C. (2016). "Why should I trust you?": Explaining the predictions of any classifier. In *Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining* (pp. 1135–1144). https://doi.org/10.1145/2939672.2939778

[42] Rivest, R. L., Adleman, L., & Dertouzos, M. L. (1978). *On data banks and privacy homomorphisms*. In *Foundations of Secure Computation* (pp. 169–180). Academic Press.

[43] Russell, S., & Norvig, P. (2021). *Artificial intelligence: A modern approach* (4th ed.). Pearson.

[44] Samek, W., Montavon, G., Lapuschkin, S., Anders, C. J., & Müller, K.-R. (2021). *Explaining deep neural networks and beyond: A review of methods and applications*. *Proceedings of the IEEE, 109*(3), 247–278. https://doi.org/10.1109/JPROC.2021.3060483

[45] Sattar, S., Khan, S., Khan, M. I., Akhmediyarova, A., Mamyrbayev, O., Kassymova, D., Oralbekova, D., & Alimkulova, J. (2025). *Anomaly detection in encrypted network traffic using self-supervised learning*. *Scientific Reports, 15*, Article 26585. https://doi.org/10.1038/s41598-025-08568-0

[46] Scarfone, K., & Mell, P. (2007). *Guide to intrusion detection and prevention systems (IDPS)* (NIST Special Publication 800-94). National Institute of Standards and Technology.

[47] Shi, W., Cao, J., Zhang, Q., Li, Y., & Xu, L. (2016). Edge computing: Vision and challenges. *IEEE Internet of Things Journal, 3*(5), 637–646. https://doi.org/10.1109/JIOT.2016.2579198

[48] Singh, A., Chouhan, P. K., & Aujla, G. S. (2024). *SecureFlow: Knowledge and data-driven ensemble for intrusion detection and dynamic rule configuration in software-defined IoT environment*. *Ad Hoc Networks, 156*, 103404. https://doi.org/10.1016/j.adhoc.2024.103404

[49] Sommer, R., & Paxson, V. (2010). Outside the closed world: On using machine learning for network intrusion detection. In *2010 IEEE Symposium on Security and Privacy* (pp. 305–316). IEEE. https://doi.org/10.1109/SP.2010.25

[50] Stallings, W. (2020). *Data and computer communications* (11th ed.). Pearson.

[51] Tanenbaum, A. S., & Wetherall, D. J. (2021). *Computer networks* (6th ed.). Pearson.

[52] Tsigos, K., Apostolidis, E., Baxevanakis, S., Papadopoulos, S., & Mezaris, V. (2024). *Towards quantitative evaluation of explainable AI methods for deepfake detection*. In *Proceedings of the 3rd ACM International Workshop on Multimedia AI against Disinformation (MAD '24)* (pp. 37–45). Association for Computing Machinery. https://doi.org/10.1145/3643491.3660292

[53] Vaswani, A., Shazeer, N., Parmar, N., Uszkoreit, J., Jones, L., Gomez, A. N., Kaiser, Ł., & Polosukhin, I. (2017). Attention is all you need. In I. Guyon, U. V. Luxburg, S. Bengio, H. Wallach, R. Fergus, S. Vishwanathan, & R. Garnett (Eds.), *Advances in Neural Information Processing Systems* (Vol. 30). Curran Associates, Inc. https://doi.org/10.48550/arXiv.1706.03762

[54] Wang, J., Huang, N., Zhang, H., Liu, L., Fu, Q., Cao, K., Guo, X., & Jung, H. (2025). Self-learning model fusion for network anomaly detection: A hybrid CNN–LSTM–Transformer framework. *PLOS ONE, 20*(10), e0332502. https://doi.org/10.1371/journal.pone.0332502

[55] Wang, J., Si, C., Wang, Z., & Fu, Q. (2024). *A new industrial intrusion detection method based on CNN-BiLSTM*. *Computers, Materials & Continua, 79*(3), 4297–4318. https://doi.org/10.32604/cmc.2024.050223

[56] Yang, K., Wang, J., & Li, M. (2024). *An improved intrusion detection method for IIoT using attention mechanisms, BiGRU, and Inception-CNN*. *Scientific Reports, 14*, 19339. https://doi.org/10.1038/s41598-024-70094-2

[57] Zhang, C., Bengio, S., Hardt, M., Recht, B., & Vinyals, O. (2023). Understanding deep learning (still) requires rethinking generalization. *Communications of the ACM, 66*(3), 107–115. https://doi.org/10.1145/3583857

[58] Zhou, Y., Chen, X., Li, H., & Wang, Z. (2023). Artificial intelligence for cloud-edge-IoT security: A survey. *IEEE Access, 11*, 114256–114281. https://doi.org/10.1109/ACCESS.2023.3326437

[59] Zhou, Z.-H. (2021). *Ensemble methods: Foundations and algorithms* (2nd ed.). CRC Press.

[60] Alshahrani, A., Alghamdi, W., Alsubai, S., Aljameel, S. S., Alharbi, A., & Alshamrani, A. (2024). *Explainable artificial intelligence: A survey of needs, techniques, applications, and future direction*. *Neurocomputing, 599*, 128111. https://doi.org/10.1016/j.neucom.2024.128111