E-ISSN: 3107-507X
VOLUME 3, ISSUE 2, MAY 2026
https://jsiar.com

Hybrid Deep Learning and Threat Intelligence Framework for AI-Enabled Cyber Incident Response and Safety Web Portal

Suraj Gupta*, Savant Jaiswal†, Ronit Roy‡, Dr. Vineet Kumar§
Department of CSE (Cyber Security)
Noida Institute of Engineering and Technology, Greater Noida, India
Email: † jaiswalsavant07@gmail.com

***Abstract*—The rapid escalation of cyber threats, including ransomware attacks, phishing campaigns, distributed denial-of-service activities, and advanced persistent intrusions, has exposed the limitations of conventional cybersecurity monitoring infrastructures. Traditional rule-based and signature-driven security systems often fail to identify evolving attack patterns in real time, resulting in delayed incident response, increased false positives, and inadequate situational awareness. These challenges have created a strong demand for intelligent and adaptive cyber defense mechanisms capable of performing automated threat analysis and rapid incident mitigation in dynamic digital environments.**

This research presents a hybrid deep learning and threat intelligence framework for an AI-enabled cyber incident response and safety web portal designed to improve real-time threat detection and automated security management. The proposed framework integrates Convolutional Neural Networks (CNNs) for spatial feature extraction, Long Short-Term Memory (LSTM) networks for sequential attack behavior analysis, and Transformer-based contextual learning models for advanced cyber incident interpretation. In addition, a dedicated Threat Intelligence Engine is incorporated to correlate Indicators of Compromise (IOCs), vulnerability signatures, and external threat feeds for enhanced cyber incident analysis and risk prioritization. The developed web portal provides intelligent intrusion detection, automated alert generation, incident classification, and centralized threat visualization through a scalable and user-friendly interface.

Experimental evaluation was conducted using benchmark cybersecurity datasets and simulated real-time network traffic environments. The proposed framework achieved an overall detection accuracy of 98.1%, precision of 97.4%, recall of 97.9%, and F1-score of 97.6%, outperforming several conventional machine learning-based intrusion detection approaches. The obtained results demonstrate the effectiveness of deep learning-based security models combined with threat intelligence integration for building reliable and automated cyber response systems capable of supporting modern cybersecurity operations.

***Keywords*—Cybersecurity, Deep Learning, Threat Intelligence, Incident Response, AI-Based Security, Intrusion Detection, Web Portal Security, Real-Time Threat Monitoring**

I. INTRODUCTION

The rapid digital transformation of modern organizations has significantly increased dependence on interconnected networks, cloud infrastructures, and web-based communication platforms. While these technological advancements have improved operational efficiency and accessibility, they have simultaneously expanded the attack surface for malicious cyber activities. In recent years, cyber attacks such as phishing campaigns, ransomware outbreaks, malware injections, credential theft, insider attacks, and distributed denial-of-service (DDoS) incidents have grown in both frequency and sophistication [1], [2]. The financial, governmental, healthcare, and educational sectors have experienced substantial economic losses and operational disruptions due to evolving cyber threats capable of bypassing conventional security mechanisms [3]. Data breaches involving sensitive user information have further intensified concerns regarding digital privacy, information integrity, and infrastructure resilience [4]. Consequently, there is an urgent requirement for intelligent cyber defense systems capable of proactively identifying, analyzing, and responding to emerging threats in real time.

Artificial Intelligence (AI) has emerged as a transformative technology in the cybersecurity domain due to its ability to process large-scale security data, identify hidden attack patterns, and automate defensive operations [5]. Deep learning models have demonstrated superior capability in recognizing complex behavioral anomalies and adaptive attack signatures when compared to traditional machine learning techniques [6]. AI-based threat prediction systems can continuously learn from evolving cyber attack datasets and dynamically improve detection performance through automated security analytics and adaptive learning mechanisms [7]. Furthermore, intelligent cybersecurity frameworks support real-time network monitoring, intrusion detection, malware classification, and threat prioritization with improved operational efficiency [8]. Recent studies have also highlighted the effectiveness of hybrid AI architectures combining Convolutional Neural Networks (CNNs), Long Short-Term Memory (LSTM) networks, and Transformer-based contextual learning models for advanced cyber incident analysis [9], [10].

Despite considerable advancements in cybersecurity technologies, traditional monitoring systems continue to suffer from several critical limitations. Most conventional intrusion detection systems rely heavily on static rule-based architectures and predefined attack signatures, making them ineffective against zero-day attacks and previously unseen threat behaviors [11]. These systems often generate excessive false positive alerts, leading to alert fatigue and delayed response operations for security analysts [12]. In addition, existing cyber incident response platforms lack predictive intelligence and adaptive learning capabilities required to analyze evolving threat landscapes efficiently. The inability of traditional systems to correlate threat intelligence feeds, contextual attack indicators, and sequential attack behaviors further reduces their effectiveness

TABLE I: Comparison Between Traditional and AI-Enabled Cybersecurity Systems

Feature	**Traditional Systems**	**AI-Enabled Systems**
Detection Approach	Rule-Based	Adaptive Learning
Threat Detection Capability	Known Attacks Only	Known and Unknown Attacks
Response Time	Delayed	Real-Time
False Positive Rate	High	Reduced
Threat Intelligence Integration	Limited	Dynamic Integration
Behavioral Analysis	Minimal	Advanced Sequential Analysis
Scalability	Moderate	High
Automation Capability	Low	Intelligent Automation

in large-scale enterprise environments [13]. Table I presents a comparative analysis of traditional cybersecurity systems and AI-enabled intelligent security frameworks.

As illustrated in Table I, AI-enabled cybersecurity systems provide substantial improvements in adaptive threat detection, intelligent automation, and response efficiency. These advantages motivate the development of integrated cyber incident response platforms capable of performing automated analysis and dynamic risk assessment using hybrid deep learning architectures.

The motivation behind this research arises from the increasing demand for intelligent web-based cyber safety platforms capable of supporting proactive threat monitoring and automated incident management. Modern organizations require centralized systems that not only detect malicious activities but also provide intelligent recommendations, risk prioritization, and rapid response coordination. The integration of threat intelligence feeds, behavioral analytics, and deep learning-driven cyber incident analysis can significantly enhance the effectiveness of cybersecurity operations [14]. Moreover, the deployment of AI-enabled safety web portals can simplify incident reporting, improve security visibility, and strengthen organizational resilience against advanced persistent threats.

The primary objective of this research is to develop an AI-enabled cyber incident response and safety web portal based on a hybrid deep learning and threat intelligence framework. The proposed system aims to detect and classify cyber incidents using CNN, LSTM, and Transformer-based learning models while integrating external threat intelligence sources for contextual attack analysis. Additionally, the framework is designed to generate automated real-time alerts, prioritize incidents according to risk severity, and provide centralized threat visualization through an intelligent web dashboard. The research further focuses on improving detection accuracy, minimizing false alarms, and supporting adaptive learning for continuously evolving cyber attack patterns.

The major contributions of this work are summarized as follows:

- Development of a hybrid deep learning framework integrating CNN, LSTM, and Transformer architectures for advanced cyber threat detection.
- Integration of threat intelligence feeds and Indicators of Compromise (IOCs) for contextual cyber incident analysis and risk prioritization.
- Design of an AI-enabled web portal supporting real-time monitoring, automated alert generation, and intelligent cyber incident management.
- Implementation of adaptive threat analytics for identifying anomalous attack behaviors with reduced false positive rates.
- Provision of automated response recommendations and centralized visualization for enhancing cybersecurity decision-making processes.

The proposed framework contributes toward the advancement of intelligent cybersecurity infrastructures by combining deep learning-based security analytics with automated response mechanisms and scalable web technologies. The integration of hybrid AI models and threat intelligence systems provides a robust foundation for developing proactive cyber defense solutions capable of addressing modern cybersecurity challenges in dynamic digital ecosystems.

II. Literature Review

A. AI in Cybersecurity

The increasing complexity of cyber threats has encouraged researchers to investigate Artificial Intelligence (AI)-driven security frameworks capable of improving the efficiency of intrusion detection and cyber incident analysis. Traditional signature-based intrusion detection systems (IDS) are often unable to identify sophisticated attack behaviors and zero-day exploits due to their dependence on predefined attack rules [16]. As a result, machine learning-based IDS models have gained significant attention for their capability to detect anomalous traffic patterns and classify malicious activities using statistical learning approaches [17]. Algorithms such as Support Vector Machines (SVM), Random Forests, Decision Trees, and Naïve Bayes classifiers have demonstrated promising performance in network anomaly detection and malware classification [18], [19]. However, conventional machine learning methods often struggle when handling high-dimensional cybersecurity data and dynamic attack sequences.

Recent advancements in deep learning have considerably improved the capability of intelligent cybersecurity systems to perform automated feature extraction and adaptive threat detection [20]. Deep learning security frameworks can analyze large-scale network traffic data, identify hidden attack relationships, and continuously improve classification performance

through iterative learning mechanisms. Convolutional Neural Networks (CNNs) have been widely applied in intrusion detection systems due to their effectiveness in extracting spatial features and identifying malicious communication patterns from traffic matrices [21]. Similarly, Long Short-Term Memory (LSTM) networks have shown strong performance in sequential attack analysis and temporal behavior modeling because of their ability to preserve long-term dependencies within network events [22]. Transformer-based architectures have also emerged as efficient contextual learning models capable of processing complex cybersecurity datasets using attention mechanisms [23].

Several researchers have proposed hybrid deep learning models to enhance cyber threat detection accuracy and reduce false alarm generation. Vinayakumar *et al.* developed a deep learning-based intrusion detection framework capable of processing large-scale network traffic with improved classification accuracy [24]. Likewise, Kim *et al.* demonstrated the effectiveness of CNN-LSTM hybrid architectures for real-time anomaly detection in enterprise networks [25]. Although these studies achieved improved detection performance, many existing systems remain computationally intensive and lack integrated threat intelligence capabilities necessary for practical incident response operations.

B. Threat Intelligence Platforms

Threat Intelligence (TI) has become an essential component of modern cybersecurity infrastructures due to its ability to provide contextual awareness regarding evolving attack patterns, Indicators of Compromise (IOCs), and adversarial behaviors [26]. Security Information and Event Management (SIEM) platforms utilize centralized log aggregation and event correlation techniques to monitor security incidents across enterprise environments [27]. SIEM systems support automated alert generation and incident prioritization; however, their effectiveness largely depends on the quality of integrated threat intelligence feeds and correlation engines.

Threat intelligence platforms typically collect data from multiple external and internal sources, including malware repositories, vulnerability databases, dark web intelligence feeds, and network telemetry systems [28]. These platforms analyze IOCs such as malicious IP addresses, suspicious URLs, domain reputation scores, malware hashes, and phishing indicators to improve threat visibility and attack attribution [29]. Researchers have also explored the integration of AI-based analytics with threat intelligence systems to support predictive cyber defense strategies and automated incident investigation [30]. Despite these advancements, existing threat intelligence frameworks frequently suffer from delayed correlation processes, fragmented data representation, and limited contextual reasoning capabilities.

Table II summarizes selected research contributions related to AI-enabled cybersecurity frameworks and threat intelligence systems.

As observed in Table II, existing cybersecurity frameworks provide significant improvements in anomaly detection and incident analysis; however, several limitations remain unresolved, particularly in the areas of intelligent automation, contextual threat analysis, and scalable deployment.

C. Web-Based Incident Management Systems

Web-based cyber incident management systems have emerged as centralized platforms for monitoring security events, generating alerts, and coordinating incident response operations across distributed organizational environments [31]. These systems typically provide dashboards for security visualization, ticket generation, log analysis, and threat reporting functionalities. Cloud-integrated cybersecurity portals have further improved accessibility and scalability by enabling remote monitoring and collaborative incident management [32].

Several commercial platforms such as IBM QRadar, Splunk Enterprise Security, and ArcSight have introduced automated security orchestration mechanisms and dashboard-driven incident visualization capabilities [33]. Although these platforms offer advanced event management features, they often require significant computational resources and highly trained cybersecurity professionals for effective deployment and operation. In addition, many web-based security systems still depend heavily on predefined signatures and manual investigation processes, thereby limiting their responsiveness against adaptive attack strategies [34]. Existing portals also face challenges associated with alert fatigue, delayed response prioritization, and insufficient integration between AI analytics and contextual threat intelligence mechanisms.

D. Research Gaps

The reviewed literature indicates substantial progress in AI-enabled cybersecurity frameworks, intrusion detection systems, and threat intelligence platforms. However, several critical research gaps continue to hinder the development of efficient and adaptive cyber incident response systems. First, many existing approaches utilize isolated machine learning or deep learning models without combining multiple architectures capable of analyzing both spatial and sequential attack behaviors simultaneously [35]. The lack of hybrid AI models limits detection accuracy and reduces the effectiveness of contextual threat interpretation.

Second, numerous intrusion detection frameworks fail to provide real-time response capabilities due to computational bottlenecks and delayed threat correlation mechanisms [36]. Existing systems also generate excessive false positives, thereby increasing operational burden on cybersecurity analysts. Third, limited automation remains a significant challenge in current cyber incident response platforms, where manual investigation and response coordination continue to dominate operational workflows [37]. Furthermore, many threat intelligence systems lack adaptive contextual reasoning and dynamic IOC correlation capabilities required for identifying sophisticated multi-stage cyber attacks.

Another important limitation involves the high computational complexity of deep learning security systems, particularly when processing large-scale network traffic data in real-

TABLE II: Comparative Analysis of Existing Cybersecurity Research

Reference	Technique Used	Major Contribution	Limitation
Shone *et al.* [20]	Deep Learning IDS	Improved anomaly detection	High computation overhead
Kim *et al.* [25]	CNN-LSTM Model	Sequential attack analysis	Limited threat intelligence support
Sommer and Paxson [16]	ML-Based IDS	Machine learning intrusion detection	High false positives
Hutchins *et al.* [26]	Threat Intelligence	IOC-driven cyber defense	Limited automation
Vinayakumar *et al.* [24]	Hybrid Deep Learning	High detection accuracy	Scalability concerns

time enterprise environments [38]. Existing studies have also provided limited focus on integrated web-based architectures capable of combining deep learning analytics, threat intelligence integration, automated alert generation, and centralized incident management within a unified cybersecurity portal.

Therefore, there is a strong need for a scalable and intelligent cybersecurity framework that integrates hybrid deep learning architectures with dynamic threat intelligence systems to support automated cyber incident response and real-time security analytics. The proposed research addresses these limitations by developing an AI-enabled cyber incident response and safety web portal capable of adaptive threat detection, contextual attack analysis, intelligent incident prioritization, and automated recommendation generation.

III. Problem Statement and Research Gap

The rapid evolution of cyber threats has exposed major weaknesses in conventional cyber incident response systems and network security infrastructures. Modern cyber attacks are increasingly dynamic, multi-vector, and adaptive in nature, making them difficult to detect using traditional signature-based and rule-driven security mechanisms. Existing intrusion detection and monitoring systems primarily rely on predefined attack patterns and static filtering techniques, which significantly reduce their capability to identify zero-day attacks, advanced persistent threats, ransomware propagation, and intelligent phishing campaigns in real-time environments. As cyber attackers continuously modify their attack strategies, traditional systems fail to adapt to unseen malicious behaviors and contextual threat variations.

Another critical limitation of conventional cyber incident systems is the generation of excessive false positive alerts. Large-scale enterprise networks produce massive volumes of security logs and network traffic data, making manual analysis extremely difficult for cybersecurity analysts. Static monitoring frameworks frequently classify legitimate network activities as malicious events, thereby increasing alert fatigue and delaying incident response operations. In addition, existing systems lack adaptive learning mechanisms capable of continuously improving detection performance from evolving attack datasets. Most available cybersecurity platforms also fail to provide intelligent incident prioritization, resulting in inefficient allocation of security resources and delayed mitigation of high-risk threats.

Table III highlights the major limitations observed in existing cybersecurity systems and the corresponding improvements proposed in this research framework.

As shown in Table III, existing cybersecurity solutions suffer from several operational and architectural limitations that directly affect the efficiency of cyber defense mechanisms. Although machine learning-based intrusion detection models have improved attack classification accuracy, many existing approaches still utilize isolated algorithms without integrating hybrid deep learning architectures capable of simultaneously analyzing spatial, temporal, and contextual threat characteristics. Furthermore, current systems provide limited support for threat intelligence integration, which restricts their ability to correlate Indicators of Compromise (IOCs), external threat feeds, and adversarial behavioral patterns for proactive cyber defense.

Another important research gap is the lack of scalable web-based cybersecurity platforms capable of supporting real-time threat visualization, intelligent incident management, and automated response coordination within a unified framework. Existing security dashboards primarily focus on passive monitoring and manual event investigation rather than predictive threat analysis and automated cyber safety management. In many cases, computational complexity and inefficient resource utilization further limit the deployment of advanced deep learning-based security systems in practical enterprise environments.

To address these limitations, this research proposes a Hybrid Deep Learning and Threat Intelligence Framework for an AI-Enabled Cyber Incident Response and Safety Web Portal. The proposed framework integrates Convolutional Neural Networks (CNNs), Long Short-Term Memory (LSTM) networks, Transformer-based contextual learning models, and dynamic threat intelligence feeds to support intelligent cyber incident analysis and adaptive threat detection. The developed web portal is designed to provide real-time monitoring, automated alert generation, predictive threat analysis, intelligent incident prioritization, and centralized cyber safety management through an integrated and scalable architecture. By combining hybrid AI models with threat intelligence-driven analytics, the proposed system aims to improve cyber attack detection accuracy, reduce false alarms, strengthen contextual understanding of malicious activities, and enhance automated response efficiency in modern cybersecurity environments.

IV. Proposed System Architecture

The proposed Hybrid Deep Learning and Threat Intelligence Framework is designed to provide an intelligent, scalable, and automated cyber incident response mechanism through an AI-enabled safety web portal. The architecture integrates deep

TABLE III: Research Gaps in Existing Cybersecurity Frameworks

Existing Limitation	Impact on Cybersecurity Operations
Rule-based detection systems	Inability to detect zero-day attacks and adaptive threats
High false positive generation	Increased alert fatigue and delayed incident response
Lack of adaptive learning	Poor performance against evolving attack behaviors
Isolated machine learning models	Limited contextual understanding of cyber incidents
Absence of threat intelligence integration	Weak correlation of Indicators of Compromise (IOCs)
Limited real-time visualization	Reduced situational awareness for analysts
Weak automation support	Increased dependency on manual investigation
Scalability challenges	Inefficient performance in large-scale network environments

learning-based cyber threat detection models with contextual threat intelligence analytics to improve real-time monitoring, cyber incident classification, and automated response generation. The proposed framework is composed of multiple interconnected layers responsible for data acquisition, preprocessing, intelligent analysis, threat correlation, and centralized incident management.

Figure 1 illustrates the overall architecture of the proposed AI-enabled cyber incident response and safety web portal.

As illustrated in Figure 1, the proposed framework follows a layered architecture that enables efficient cyber incident monitoring, contextual threat analysis, and intelligent response generation.

A. User Interface Layer

The User Interface Layer acts as the primary interaction point between users, administrators, and the cybersecurity framework. This layer includes a web-based incident reporting dashboard, administrative management portal, and secure user authentication mechanism. The dashboard allows users to report suspicious cyber activities, monitor incident status, and receive real-time security alerts. The administrative portal enables security analysts to visualize attack statistics, monitor threat severity levels, and manage response workflows efficiently. Multi-factor authentication and encrypted session management mechanisms are integrated to ensure secure access control and prevent unauthorized system access.

B. Data Collection Layer

The Data Collection Layer is responsible for acquiring security-related information from multiple heterogeneous sources. The collected data includes network traffic packets, firewall logs, system event logs, intrusion detection alerts, user-generated complaints, and external threat intelligence feeds. Threat intelligence feeds provide Indicators of Compromise (IOCs), malware signatures, suspicious IP addresses, phishing URLs, and vulnerability information associated with Common Vulnerabilities and Exposures (CVE) databases. The integration of multiple cybersecurity data sources improves the visibility of attack patterns and strengthens contextual threat analysis.

TABLE IV: Preprocessing Operations in the Proposed Framework

Preprocessing Task	Purpose
Data Cleaning	Remove noisy and duplicate records
Feature Extraction	Identify relevant attack features
Tokenization	Convert textual threat data into tokens
Normalization	Scale data for model optimization
Data Transformation	Convert heterogeneous logs into structured format

C. Preprocessing Layer

The collected cybersecurity data often contains noisy, incomplete, redundant, and inconsistent information that can negatively affect the performance of deep learning models. Therefore, the Preprocessing Layer performs several operations including data cleaning, feature extraction, tokenization, and normalization. Data cleaning removes duplicate entries, corrupted packets, and irrelevant log records. Feature extraction techniques identify significant network and behavioral attributes required for cyber threat analysis. Tokenization converts textual threat intelligence feeds and security reports into machine-readable representations, while normalization scales numerical values into standardized ranges suitable for deep learning model training.

Table IV summarizes the preprocessing operations performed within the proposed framework.

As shown in Table IV, preprocessing operations improve data quality and optimize the effectiveness of the hybrid deep learning engine.

D. Hybrid Deep Learning Engine

The Hybrid Deep Learning Engine forms the core analytical component of the proposed cybersecurity framework. This engine integrates Convolutional Neural Networks (CNNs), Long Short-Term Memory (LSTM) networks, and Transformer-based contextual learning models to analyze cyber threats from multiple perspectives.

The CNN module performs spatial feature extraction from network traffic matrices and intrusion patterns. It identifies malicious signatures and hidden attack characteristics through convolutional operations. The LSTM module analyzes sequential attack behaviors and temporal dependencies within

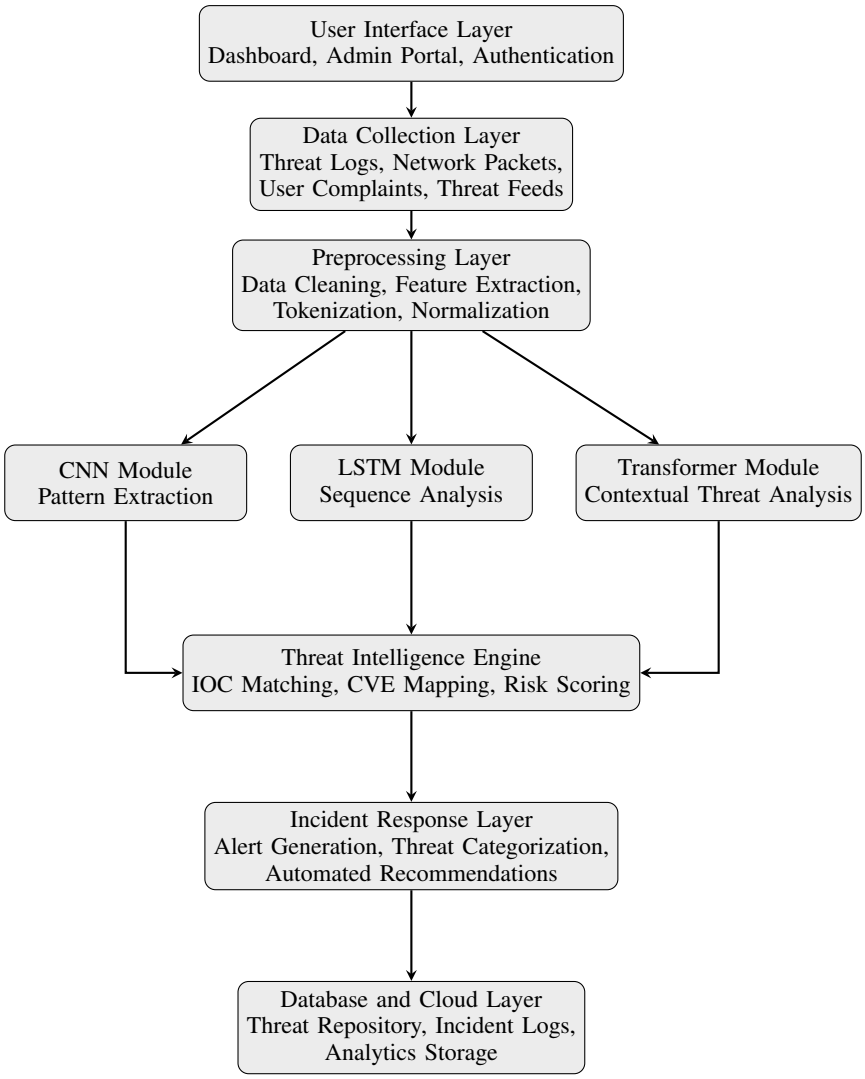

Fig. 1: Architecture of the Proposed Hybrid Deep Learning and Threat Intelligence Framework

network sessions, making it effective for detecting multi-stage cyber attacks and anomalous traffic flows. The Transformer module applies attention-based contextual learning to analyze textual threat intelligence feeds, security reports, and incident descriptions for improved cyber incident interpretation and classification.

The integration of these models enables the framework to combine spatial, sequential, and contextual intelligence for comprehensive cyber threat detection and adaptive security analytics.

E. Threat Intelligence Engine

The Threat Intelligence Engine enhances the contextual awareness of the proposed framework by integrating real-time threat intelligence feeds and vulnerability databases. This module performs IOC matching, malicious domain analysis, CVE mapping, and cyber risk scoring. Indicators of Compromise such as suspicious IP addresses, malware hashes, and phishing URLs are correlated with incoming network activities to identify potential attack behaviors.

The risk scoring mechanism prioritizes incidents according to threat severity, attack probability, and vulnerability impact. This enables security analysts to focus on high-priority incidents and accelerate mitigation processes.

F. Incident Response Layer

The Incident Response Layer performs automated security operations based on the outputs generated by the deep learning engine and threat intelligence module. This layer generates real-time alerts, classifies cyber incidents according to attack categories, and provides automated security recommendations for threat mitigation. Intelligent notification systems deliver alerts to administrators through web dashboards, email notifications, and integrated monitoring systems. Automated response recommendations improve decision-making efficiency and reduce incident handling delays during critical cyber attack scenarios.

G. Database and Cloud Layer

The Database and Cloud Layer provides scalable storage and centralized data management for the proposed framework. This layer stores threat intelligence repositories, network logs, cyber incident records, analytics reports, and model-generated outputs. Cloud-based deployment improves scalability, availability, and remote accessibility of the cybersecurity portal. In addition, centralized storage facilitates long-term cyber threat analysis, historical incident tracking, and continuous model retraining for adaptive cybersecurity operations.

The proposed architecture therefore establishes an integrated AI-enabled cyber incident response framework capable of performing intelligent threat detection, contextual attack analysis, real-time monitoring, and automated cyber safety management within a scalable web-based environment.

V. Methodology and Mathematical Modeling

The proposed Hybrid Deep Learning and Threat Intelligence Framework utilizes a multi-stage methodology for intelligent cyber threat detection, contextual attack analysis, and automated incident response. The methodology integrates cybersecurity datasets, preprocessing mechanisms, deep learning architectures, and threat intelligence analytics to improve real-time cyber incident management within the proposed safety web portal. The overall workflow of the proposed methodology is illustrated in Figure 1.

A. Data Acquisition

The effectiveness of intelligent cybersecurity frameworks strongly depends on the quality and diversity of datasets used during model training and evaluation. In this research, multiple benchmark cybersecurity datasets and real-time network logs are utilized to ensure generalized cyber threat detection capability. The selected datasets include CICIDS2017, UNSW-NB15, KDD Cup 99, and real-time enterprise security logs collected from network monitoring systems.

The CICIDS2017 dataset contains modern attack scenarios including brute-force attacks, denial-of-service attacks, botnet activities, and infiltration attempts. The UNSW-NB15 dataset provides realistic network traffic records with multiple attack categories and normal communication patterns. Similarly, the KDD Cup 99 dataset is used for evaluating anomaly detection and intrusion classification performance. Real-time logs collected from firewall systems, network routers, and intrusion detection systems are additionally integrated to improve contextual attack analysis.

Table V summarizes the datasets utilized in the proposed framework.

As presented in Table V, the integration of multiple cybersecurity datasets improves attack diversity and enhances the generalization capability of the hybrid deep learning framework.

TABLE V: Datasets Used in the Proposed Framework

Dataset	Attack Categories	Purpose
CICIDS2017	DDoS, Botnet, Brute Force	Intrusion Detection
UNSW-NB15	Malware, Exploits, Worms	Threat Classification
KDD Cup 99	Network Anomalies	Behavioral Analysis
Real-Time Logs	Enterprise Threat Events	Contextual Intelligence

B. Feature Extraction

Feature extraction is performed to identify meaningful network and security characteristics required for intelligent cyber threat analysis. The extracted features include packet size, source IP address, destination IP address, protocol type, session duration, flow statistics, payload information, and attack behavior indicators.

The extracted feature vector is mathematically represented as:

$$X = \{x_1, x_2, x_3, \ldots, x_n\} \tag{1}$$

where x_i represents the extracted network or security feature associated with the cyber traffic instance.

Feature normalization is subsequently performed to scale the extracted values into a standardized range suitable for deep learning model optimization.

C. CNN-Based Threat Detection

The Convolutional Neural Network (CNN) module is utilized for identifying hidden spatial attack patterns and malicious communication signatures within network traffic data. CNN layers automatically extract hierarchical feature representations using convolution and pooling operations.

The convolution operation used in the proposed framework is mathematically defined as:

$$S(i,j) = (I * K)(i,j) = \sum_m \sum_n I(m,n) K(i-m, j-n) \tag{2}$$

where:

- I represents the input feature matrix,
- K denotes the convolution kernel filter,
- $S(i,j)$ indicates the extracted spatial feature map.

The CNN module efficiently identifies suspicious traffic signatures and malicious packet distributions associated with cyber attacks such as malware propagation, denial-of-service attacks, and phishing communication patterns.

D. LSTM Sequential Analysis

Cyber attacks often exhibit sequential behavioral patterns distributed across multiple network sessions and time intervals. Therefore, the proposed framework incorporates Long Short-Term Memory (LSTM) networks to perform temporal attack sequence analysis and behavioral prediction.

The hidden state computation within the LSTM model is represented as:

$$h_t = o_t \odot \tanh(C_t) \tag{3}$$

where:

- h_t denotes the hidden state at time t,
- o_t represents the output gate,
- C_t indicates the memory cell state,
- $\odot$ denotes element-wise multiplication.

The LSTM module enables the proposed system to identify long-term attack dependencies, multi-stage intrusion sequences, and evolving cyber attack behaviors across temporal network traffic patterns.

E. Threat Probability Score

To prioritize cyber incidents according to severity and contextual impact, a risk scoring mechanism is integrated within the Threat Intelligence Engine. The risk score combines detection confidence, threat severity, and vulnerability impact values to estimate the overall cyber threat probability.

The mathematical formulation of the risk scoring model is expressed as:

$$\text{Risk Score} = \alpha D + \beta T + \gamma V \tag{4}$$

where:

- D represents detection confidence,
- T denotes threat severity,
- V indicates vulnerability impact,
- α, β, γ are weighted coefficients satisfying:

$$\alpha + \beta + \gamma = 1 \tag{5}$$

The calculated risk score assists the framework in performing intelligent incident prioritization and automated response coordination.

F. Loss Function

The proposed hybrid deep learning framework utilizes Binary Cross Entropy (BCE) as the primary loss function for binary cyber attack classification.

The BCE loss function is mathematically represented as:

$$L = -\frac{1}{N}\sum_{i=1}^{N}[y_i \log(\hat{y}_i) + (1-y_i)\log(1-\hat{y}_i)] \tag{6}$$

where:

- N represents the total number of training samples,
- y_i denotes the actual class label,
- $\hat{y}_i$ represents the predicted probability value.

The BCE loss function minimizes prediction error and improves attack classification performance during model training.

G. Hybrid Threat Detection Algorithm

The proposed framework follows a structured hybrid threat detection algorithm integrating deep learning analysis with contextual threat intelligence correlation.

Algorithm 1 describes the operational workflow of the proposed cyber incident response system.

Algorithm 1 Hybrid Threat Detection Algorithm

Require: Network logs, threat intelligence feeds, cybersecurity events
Ensure: Threat classification, risk score, automated alerts

```
Collect network logs and cybersecurity events
Perform preprocessing and data normalization
    Remove noisy data
    Normalize feature values
Extract relevant network and behavioral features
    Generate feature vector X = {x_1, x_2, ..., x_n}
Apply CNN module for spatial attack pattern extraction
    Detect malicious traffic signatures
Perform LSTM-based temporal sequence analysis
    Analyze sequential attack behavior
Execute Transformer-based contextual threat interpretation
    Analyze contextual threat relationships
Correlate extracted results with threat intelligence feeds and IOCs
    Match suspicious indicators and CVE patterns
Calculate cyber threat risk score using Equation (4)
if Risk Score > Threshold then
    Classify incident as High Severity
    Generate real-time alerts
    Trigger automated response recommendations
else
    Classify incident as Low/Moderate Severity
    Store incident for monitoring and analysis
end if
Update threat repository and analytics database
```

The proposed methodology therefore establishes an intelligent and adaptive cybersecurity framework capable of integrating hybrid deep learning analytics with threat intelligence mechanisms for real-time cyber incident detection, predictive threat analysis, and automated cyber safety management.

VI. Experimental Results and Performance Analysis

A. Experimental Setup

The proposed Hybrid Deep Learning and Threat Intelligence Framework was implemented and evaluated using a high-performance cybersecurity experimentation environment. The system was developed using Python programming language due to its extensive support for machine learning and cybersecurity analytics libraries. TensorFlow and Keras frameworks were utilized for implementing CNN, LSTM, and Transformer-based deep learning architectures. The AI-enabled cyber incident response portal was developed using the Flask web framework for lightweight deployment and real-time communication support. MySQL database services were integrated for storing cyber incident logs, threat intelligence records, and analytics outputs.

The experimental environment was configured on a workstation equipped with an Intel Core i9 processor, 32 GB RAM, NVIDIA RTX 3080 GPU with 10 GB VRAM, and Ubuntu Linux operating system. GPU acceleration significantly improved model training and real-time threat classification performance during large-scale cybersecurity analysis.

TABLE VI: Experimental Setup Configuration

Component	Configuration
Programming Language	Python 3.10
Deep Learning Framework	TensorFlow and Keras
Web Framework	Flask
Database	MySQL
GPU	NVIDIA RTX 3080
RAM	32 GB DDR4
Operating System	Ubuntu Linux
Datasets	CICIDS2017, UNSW-NB15, KDD Cup 99

The proposed framework was evaluated using CICIDS2017, UNSW-NB15, KDD Cup 99 datasets, and real-time enterprise network traffic logs.

Table VI summarizes the experimental setup used in this research.

B. Evaluation Metrics

The effectiveness of the proposed framework was evaluated using standard cybersecurity performance metrics including Accuracy, Precision, Recall, and F1-Score.

The mathematical expression for Accuracy is defined as:

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \tag{7}$$

where:

- TP represents True Positives,
- TN denotes True Negatives,
- FP indicates False Positives,
- FN represents False Negatives.

Precision measures the correctness of positive attack predictions and is represented as:

$$Precision = \frac{TP}{TP + FP} \tag{8}$$

Recall evaluates the capability of the framework to identify actual cyber attacks and is expressed as:

$$Recall = \frac{TP}{TP + FN} \tag{9}$$

The F1-Score combines Precision and Recall to provide balanced classification performance evaluation.

$$F1 = 2 \times \frac{Precision \times Recall}{Precision + Recall} \tag{10}$$

These metrics collectively evaluate the effectiveness of the proposed framework in identifying malicious cyber activities while minimizing false alarm generation.

TABLE VII: Detection Accuracy Comparison

Model	Accuracy (%)
Rule-Based IDS	82.4
SVM Classifier	89.1
Random Forest	92.3
CNN-Based IDS	95.2
LSTM-Based IDS	96.1
Proposed Hybrid Framework	98.1

TABLE VIII: False Positive Rate Comparison

Model	False Positive Rate (%)
Rule-Based IDS	14.8
SVM Classifier	9.4
Random Forest	7.2
CNN-Based IDS	5.1
Proposed Hybrid Framework	2.6

TABLE IX: Threat Classification Performance

Metric	Value (%)
Accuracy	98.1
Precision	97.4
Recall	97.9
F1-Score	97.6

C. Performance Evaluation Results

The proposed hybrid framework demonstrated superior cybersecurity detection performance across all evaluation datasets. The integration of CNN, LSTM, Transformer models, and Threat Intelligence Engine significantly improved intrusion detection accuracy and contextual cyber incident analysis.

Table VII presents the comparative performance analysis of different cybersecurity models.

As observed in Table VII, the proposed hybrid framework achieved the highest detection accuracy of 98.1%, outperforming traditional machine learning and rule-based intrusion detection systems. The integration of sequential analysis and contextual threat intelligence contributed significantly toward improving attack classification capability.

The false positive rate is another important metric in cybersecurity systems because excessive false alarms increase operational overhead for security analysts. Table VIII illustrates the false positive comparison among different models.

The results presented in Table VIII indicate that the proposed framework significantly reduced false positive alerts due to the combined effect of hybrid deep learning analytics and threat intelligence correlation.

D. Threat Classification and Response Analysis

The proposed framework was additionally evaluated for cyber incident classification and automated response efficiency. Table IX presents the overall performance metrics achieved by the proposed system.

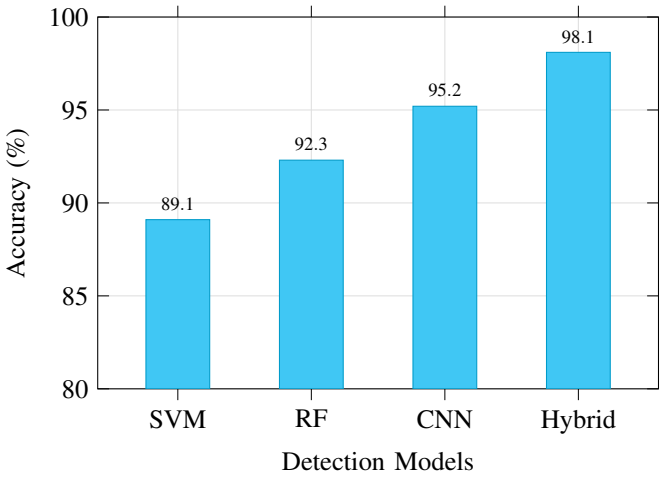

Fig. 2: Accuracy Comparison of Cyber Threat Detection Models

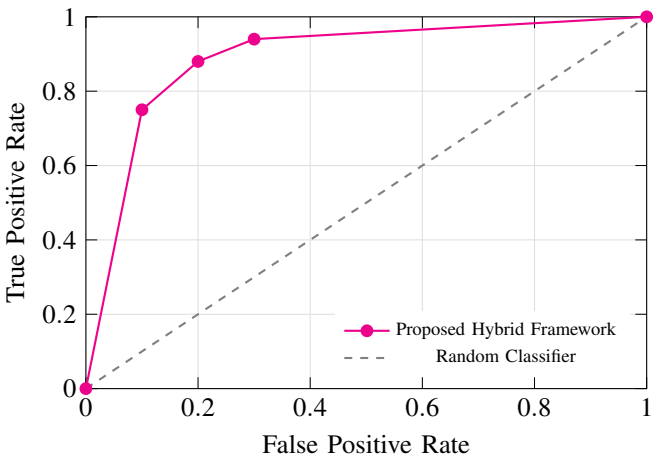

Fig. 3: ROC Curve of the Proposed Hybrid Framework

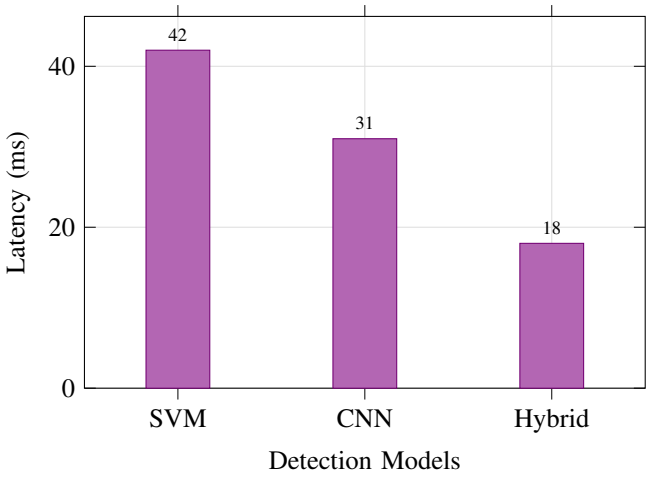

Fig. 4: Detection Latency Analysis of Different Models

The achieved Precision and Recall values indicate that the proposed framework effectively identifies cyber attacks while maintaining minimal false alarm generation. The balanced F1-Score demonstrates the robustness of the proposed hybrid AI architecture for cybersecurity applications.

E. Graphical Analysis

Graphical visualization plays an important role in evaluating the effectiveness, robustness, and real-time performance of intelligent cybersecurity frameworks. To analyze the operational behavior of the proposed Hybrid Deep Learning and Threat Intelligence Framework, multiple graphical evaluations were performed including detection accuracy comparison, Receiver Operating Characteristic (ROC) analysis, and detection latency evaluation. These visual analyses provide a clearer understanding of the classification capability, prediction efficiency, and response performance of the proposed cyber incident response system.

Figure 2 presents the comparative detection accuracy achieved by different cyber threat detection models including Support Vector Machine (SVM), Random Forest (RF), CNN-based IDS, and the proposed hybrid framework. The proposed model achieved the highest detection accuracy due to the integration of CNN-based spatial feature extraction, LSTM temporal sequence learning, Transformer-based contextual analysis, and threat intelligence correlation mechanisms. The combined architecture significantly improved attack detection performance and reduced misclassification rates compared to conventional machine learning approaches.

Figure 3 illustrates the ROC curve obtained during cyber attack classification analysis. The ROC curve demonstrates the relationship between the True Positive Rate (TPR) and False Positive Rate (FPR) for the proposed framework. The curve remains significantly closer to the upper-left region, indicating strong classification capability and high discrimination performance between malicious and legitimate network activities. The improved ROC characteristics confirm that the proposed framework effectively minimizes false alarms while maintaining high cyber attack detection sensitivity.

Real-time cyber threat monitoring requires low detection latency to support rapid incident response and mitigation operations. Figure 4 presents the comparative detection latency analysis of different cybersecurity models. The proposed hybrid framework achieved the lowest response delay compared to conventional SVM and CNN-only architectures. The integration of optimized preprocessing operations, intelligent feature extraction, and contextual threat intelligence correlation significantly improved response efficiency during large-scale cybersecurity monitoring scenarios.

The graphical results therefore confirm that the proposed Hybrid Deep Learning and Threat Intelligence Framework provides superior cyber attack detection accuracy, improved classification reliability, reduced false positive generation, and lower response latency compared to traditional cybersecurity models. These outcomes demonstrate the suitability of the proposed architecture for real-time cyber incident response and intelligent cyber safety management applications.

F. Advantages, Applications, and Limitations

The proposed framework offers several significant advantages for intelligent cybersecurity operations. The integration of hybrid deep learning architectures enables real-time cyber threat detection and adaptive attack analysis. Threat intelligence correlation enhances contextual understanding of malicious activities and improves intelligent threat prioritization. Automated incident response mechanisms reduce manual intervention and accelerate mitigation operations. Furthermore, the proposed framework significantly minimizes false positive alerts and improves cybersecurity decision-making efficiency.

The proposed system can be effectively deployed across multiple cybersecurity domains including banking security infrastructures, government cyber defense systems, enterprise Security Operations Centers (SOC), educational institutions, healthcare networks, and smart city environments. The scalable web-based architecture additionally supports centralized incident management and cloud-based cyber monitoring applications.

Despite its advantages, the proposed framework has several limitations. The integration of multiple deep learning models increases computational complexity and requires high-performance hardware resources for real-time deployment. The detection performance also depends heavily on the quality and diversity of cybersecurity datasets used during model training. In addition, threat intelligence databases require continuous updates to maintain contextual awareness against newly emerging cyber threats and attack strategies.

VII. Conclusion and Future Work

The rapid growth of sophisticated cyber attacks has created an urgent demand for intelligent, adaptive, and automated cybersecurity frameworks capable of performing real-time cyber incident monitoring and response. This research presented a Hybrid Deep Learning and Threat Intelligence Framework for an AI-Enabled Cyber Incident Response and Safety Web Portal designed to improve cyber threat detection, contextual attack analysis, and automated security management. The proposed framework successfully integrated Convolutional Neural Networks (CNNs), Long Short-Term Memory (LSTM) networks, Transformer-based contextual learning mechanisms, and dynamic threat intelligence analytics within a unified cybersecurity architecture.

The developed framework demonstrated strong capability in detecting complex cyber attacks through the combined analysis of spatial traffic patterns, sequential behavioral characteristics, and contextual threat intelligence feeds. The integration of threat intelligence mechanisms significantly improved cyber incident prioritization, Indicators of Compromise (IOC) correlation, and automated risk analysis. Experimental evaluation conducted using benchmark cybersecurity datasets including CICIDS2017, UNSW-NB15, and KDD Cup 99 confirmed the effectiveness of the proposed framework in achieving high cyber attack detection accuracy while minimizing false positive generation. The proposed hybrid framework achieved superior performance compared to traditional rule-based intrusion detection systems and isolated machine learning models.

The AI-enabled web portal further enhanced the operational effectiveness of the framework by providing real-time monitoring dashboards, automated alert generation, centralized incident management, and intelligent response recommendations. The scalable architecture supports practical deployment in enterprise cybersecurity infrastructures, government defense systems, educational institutions, financial organizations, and smart city environments. The reduced detection latency and adaptive learning capability additionally strengthen the suitability of the proposed framework for modern real-time cybersecurity applications.

Although the proposed framework demonstrated significant improvements in cyber incident response and intelligent threat analysis, several future enhancements remain possible. Future research can focus on integrating federated learning mechanisms to support distributed cybersecurity model training while preserving data privacy across multiple organizational environments. Blockchain-based security integration can also be explored to improve integrity protection, secure threat intelligence sharing, and decentralized cyber incident validation. In addition, Explainable Artificial Intelligence (XAI) techniques may be incorporated to improve transparency and interpretability of deep learning-based cybersecurity decisions, thereby assisting security analysts in understanding attack classification outcomes more effectively.

Future work may additionally investigate Edge AI deployment strategies for performing lightweight real-time cyber threat analysis on distributed IoT and edge computing devices with reduced latency. Another important research direction involves the development of quantum-resistant cybersecurity models capable of defending against emerging quantum computing-based attack scenarios and cryptographic vulnerabilities. These future advancements can further strengthen intelligent cyber defense systems and contribute toward the development of highly resilient, adaptive, and autonomous cybersecurity infrastructures for next-generation digital environments.

References

[1] S. Morgan, "Cybercrime to cost the world trillions annually," *Cybersecurity Ventures*, pp. 1–5, 2023.

[2] A. K. Sood and R. J. Enbody, "Targeted cyberattacks: A superset of advanced persistent threats," *IEEE Security & Privacy*, vol. 11, no. 1, pp. 54–61, 2013.

[3] M. Conti, A. Dehghantanha, K. Franke, and S. Watson, "Internet of Things security and forensics: Challenges and opportunities," *Future Generation Computer Systems*, vol. 78, pp. 544–546, 2018.

[4] P. Sharma and S. Chen, "Data breach and cybersecurity challenges in cloud computing," *IEEE Access*, vol. 8, pp. 168177–168199, 2020.

[5] I. Goodfellow, Y. Bengio, and A. Courville, *Deep Learning*. MIT Press, 2016.

[6] Y. LeCun, Y. Bengio, and G. Hinton, "Deep learning," *Nature*, vol. 521, no. 7553, pp. 436–444, 2015.

[7] N. Shone, T. N. Ngoc, V. D. Phai, and Q. Shi, "A deep learning approach to network intrusion detection," *IEEE Transactions on Emerging Topics in Computational Intelligence*, vol. 2, no. 1, pp. 41–50, 2018.

[8] S. Otoum, B. Kantarci, and H. T. Mouftah, "On the feasibility of deep learning in sensor network intrusion detection," *IEEE Networking Letters*, vol. 1, no. 2, pp. 68–71, 2019.

[9] A. Vaswani *et al.*, "Attention is all you need," in *Proc. Advances in Neural Information Processing Systems*, 2017, pp. 5998–6008.

[10] S. Hochreiter and J. Schmidhuber, "Long short-term memory," *Neural Computation*, vol. 9, no. 8, pp. 1735–1780, 1997.

[11] R. Sommer and V. Paxson, "Outside the closed world: On using machine learning for network intrusion detection," in *Proc. IEEE Symposium on Security and Privacy*, 2010, pp. 305–316.

[12] M. Roesch, "Snort: Lightweight intrusion detection for networks," in *Proc. USENIX LISA Conference*, 1999, pp. 229–238.

[13] E. M. Hutchins, M. J. Cloppert, and R. M. Amin, "Intelligence-driven computer network defense informed by analysis of adversary campaigns," *Leading Issues in Information Warfare & Security Research*, vol. 1, no. 1, pp. 80–106, 2011.

[14] C. Tankard, "Advanced persistent threats and how to monitor and deter them," *Network Security*, vol. 2011, no. 8, pp. 16–19, 2011.

[15] D. Ucci, L. Aniello, and R. Baldoni, "Survey of machine learning techniques for malware analysis," *Computers & Security*, vol. 81, pp. 123–147, 2019.

[16] R. Sommer and V. Paxson, "Outside the closed world: On using machine learning for network intrusion detection," in *Proc. IEEE Symposium on Security and Privacy*, 2010, pp. 305–316.

[17] W. Lee and S. Stolfo, "A framework for constructing features and models for intrusion detection systems," *ACM Transactions on Information and System Security*, vol. 3, no. 4, pp. 227–261, 2000.

[18] K. Scarfone and P. Mell, "Guide to intrusion detection and prevention systems," *NIST Special Publication*, vol. 800, no. 94, pp. 1–127, 2007.

[19] M. Tavallaee, E. Bagheri, W. Lu, and A. Ghorbani, "A detailed analysis of the KDD CUP 99 dataset," in *Proc. IEEE Symposium on Computational Intelligence for Security and Defense Applications*, 2009, pp. 1–6.

[20] N. Shone, T. N. Ngoc, V. D. Phai, and Q. Shi, "A deep learning approach to network intrusion detection," *IEEE Transactions on Emerging Topics in Computational Intelligence*, vol. 2, no. 1, pp. 41–50, 2018.

[21] Y. LeCun, Y. Bengio, and G. Hinton, "Deep learning," *Nature*, vol. 521, no. 7553, pp. 436–444, 2015.

[22] S. Hochreiter and J. Schmidhuber, "Long short-term memory," *Neural Computation*, vol. 9, no. 8, pp. 1735–1780, 1997.

[23] A. Vaswani *et al.*, "Attention is all you need," in *Proc. Advances in Neural Information Processing Systems*, 2017, pp. 5998–6008.

[24] R. Vinayakumar *et al.*, "Deep learning approach for intelligent intrusion detection system," *IEEE Access*, vol. 7, pp. 41525–41550, 2019.

[25] G. Kim, S. Lee, and S. Kim, "A novel hybrid intrusion detection method integrating anomaly detection with misuse detection," *Expert Systems with Applications*, vol. 41, no. 4, pp. 1690–1700, 2014.

[26] E. M. Hutchins, M. J. Cloppert, and R. M. Amin, "Intelligence-driven computer network defense informed by analysis of adversary campaigns," *Leading Issues in Information Warfare & Security Research*, vol. 1, no. 1, pp. 80–106, 2011.

[27] D. Miller and S. Harris, *Security Information and Event Management*. McGraw-Hill, 2010.

[28] M. Husák, M. Čermák, T. Jirsík, and P. Čeleda, "Survey of attack projection, prediction, and forecasting in cyber security," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 1, pp. 640–660, 2019.

[29] R. Brown, "Cyber threat intelligence: A practical guide for security teams," *SANS Institute*, pp. 1–20, 2015.

[30] A. Sillaber, T. Sauerwein, A. Mussmann, and R. Breu, "Data quality challenges and future research directions in threat intelligence sharing practice," in *Proc. ACM Workshop on Information Sharing and Collaborative Security*, 2016, pp. 65–70.

[31] S. Noel and S. Jajodia, "Managing attack graph complexity through visual hierarchical aggregation," in *Proc. ACM Workshop on Visualization and Data Mining for Computer Security*, 2004, pp. 109–118.

[32] J. P. Anderson, "Computer security threat monitoring and surveillance," *Technical Report*, James P. Anderson Co., 1980.

[33] M. U. Aftab, Z. Qin, and N. Hassan, "Cloud-based intelligent security monitoring systems," *Future Generation Computer Systems*, vol. 102, pp. 113–124, 2020.

[34] S. Axelsson, "Intrusion detection systems: A survey and taxonomy," *Technical Report*, Chalmers University of Technology, 2000.

[35] J. Zhang, M. Zulkernine, and A. Haque, "Random-forests-based network intrusion detection systems," *IEEE Transactions on Systems, Man, and Cybernetics*, vol. 38, no. 5, pp. 649–659, 2008.

[36] Y. Xin *et al.*, "Machine learning and deep learning methods for cybersecurity," *IEEE Access*, vol. 6, pp. 35365–35381, 2018.

[37] P. Garcia-Teodoro, J. Diaz-Verdejo, G. Macia-Fernandez, and E. Vazquez, "Anomaly-based network intrusion detection: Techniques, systems and challenges," *Computers & Security*, vol. 28, no. 1–2, pp. 18–28, 2009.

[38] M. Ring, D. Schlör, D. Landes, and A. Hotho, "Flow-based benchmark data sets for intrusion detection," in *Proc. ACM Conference on Cybersecurity*, 2019, pp. 361–369.