International Journal of Applied Mathematics

Volume 38 No. 10s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

ZERO-DAY ATTACK PREDICTION USING ENSEMBLE MACHINE LEARNING WITH THREAT INTELLIGENCE DATA

Ahmed A.F Osman[1], Mohammed Awad Mohammed Ataelfadiel[2]

[1]Applied College, King Faisal University, P.O. Box 400, Al-Ahsa 31982, Saudi Arabia, afadol@kfu.edu.sa, ORCID (https://orcid.org/0009-0001-1362-4942)

[2]Applied College, King Faisal University, P.O. Box 400, Al-Ahsa 31982, Saudi Arabia,

melfadiel@kfu.edu.sa, ORCID (https://orcid.org/ 0009-0000-1497-4381)

Abstract

Modern cybersecurity faces ongoing difficulties because zero-day attacks exploit unknown system weaknesses which make traditional signature-based protection systems useless. The research develops an innovative ensemble machine learning system which unites threat intelligence data from multiple sources with Random Forest (RF) and Extreme Gradient Boosting (XGBoost) and Long Short-Term Memory (LSTM) models for detecting zero-day attacks. The proposed framework unites three different data sources which include CVE/NVD vulnerability databases and honeypot network telemetry and dark web intelligence feeds through a single analytical process. The model achieves better predictive results through its soft-voting mechanism and advanced feature engineering which combines behavioral and contextual and temporal indicators. The ensemble model outperformed all baseline learners in experimental testing with real-world data by achieving 94% accuracy and 0.95 ROC-AUC and 0.83 Z-DR while reducing false positives by 20% compared to the best single model (LSTM). The Wilcoxon signed-rank test ($p < 0.01$) shows that the improvements achieved hold statistical significance.

The framework demonstrated operational effectiveness through case studies of CVE-2024-3094 and CVE-2025-21788 by producing predictive alerts before official disclosure dates as shown in recent predictive cyber threat intelligence and early-warning system research. The research shows that uniting diverse threat intelligence with ensemble learning techniques creates an intelligence-based cyber defense system which represents a major step toward developing future zero-day protection systems. The research establishes a flexible framework which enables organizations to implement adaptive intelligence-based cybersecurity solutions for their enterprise and national defense systems.

Keywords Zero-Day Attack Detection; Ensemble Machine Learning; Threat Intelligence; Random Forest; XGBoost; LSTM; Cybersecurity Analytics; Proactive Defense; Anomaly Detection; Predictive Security Systems

1. Introduction

Received: August 07, 2025

International Journal of Applied Mathematics

Volume 38 No. 10s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

The modern digital environment faces zero-day attacks as its most dangerous and difficult-to-detect cybersecurity threat [1], [2], [3]. The attacks use unidentifiable system weaknesses before security teams can create fixes or detection rules which makes current protection systems useless. The modern cyber threat environment requires immediate detection systems to stop zero-day attacks because it advances through automated and complex methods [4], [5],[6].

The detection systems that use signature-based intrusion detection and heuristic malware scanning depend on established rules and known attack patterns. The systems prove successful against known attacks, but they cannot detect new exploit methods that have never been seen before [1], [7]. The defensive approach creates an ongoing security risk because it leaves systems exposed from the time vulnerabilities are discovered until proper fixes are implemented. Machine Learning (ML) provides an innovative solution through its ability to detect hidden behavioral patterns which help identify zero-day exploit activities [5], [6], [8]. The current ML solutions face two major restrictions because they depend on single data sources and static information and they do not handle the changing characteristics of cyber threats effectively [7],[8].

Research studies have shown that ensemble learning methods which unite multiple models produce better results for both accuracy and generalization [9]–[10], [11]. The current research lacks two essential elements because it uses ensembles independently from external threat intelligence data and it trains models with static offline datasets instead of real-time data integration. Deep learning models using LSTM for sequential threat prediction show weak performance in interpretability and generalization when trained with restricted or artificial datasets [12], [13], [14]. The current research lacks a solution to merge diverse real-time threat intelligence data through an adaptive ensemble learning system which detects zero-day attacks before they happen [15],[16].

The research develops an innovative ensemble machine learning system which combines multiple threat intelligence sources with Random Forest (RF) and Extreme Gradient Boosting (XGBoost) and Long Short-Term Memory (LSTM) models to detect zero-day attacks before they become active.

The proposed system stands apart from previous methods because it combines three different threat intelligence data sources.

- The system uses three types of data sources which include CVE/NVD feeds for structured vulnerability information
- honeypot behavioral data and network logs and dark web and OSINT threat intelligence feeds [39]–[43].

The research introduces a new method which unites threat intelligence data with a soft-voting ensemble learning system that optimizes performance for Zero-Day Detection Rate (Z-DR) [16], [17]. The system represents the first solution which combines dark web intelligence with vulnerability databases and honeypot behavioral data through a soft-voting RF–XGBoost–LSTM ensemble that maximizes Z-DR performance and minimizes false positives for proactive zero-day threat prediction [10], [11], [15].

Received: August 07, 2025

International Journal of Applied Mathematics
Volume 38 No. 10s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

The system provides better detection performance and clear results while using predictive analytics to enable proactive cyber defense through early warning systems for new vulnerabilities [16], [18].

2. Related Work

2.1 Review of Existing Zero-Day Detection Methods

Zero-day attacks use unknown system weaknesses to attack systems which makes them difficult for standard security systems to detect [2], [17], [19]. The literature shows a development from signature-based detection to advanced machine learning (ML) and artificial intelligence (AI) approaches which each have their own advantages and disadvantages [1], [3], [4],[20].

Traditional Detection Approaches

Signature-Based Methods: Traditional intrusion detection systems (IDS) operate through known attack signature identification. The detection of zero-day attacks becomes impossible because these methods depend on pre-existing attack signatures .[1]

Rule-Based and Heuristic Approaches: These methods use predefined rules or heuristics to flag suspicious activity but struggle with novel or obfuscated attack patterns [1],[21].

Machine Learning and AI-Based Methods

Supervised Learning: Supervised ML models (e.g., Random Forest, SVM) receive training data that includes attack labels. The models demonstrate some ability to predict attacks, but their performance remains limited because they lack access to zero-day attack data. Some detection methods use statistical patterns between known attacks and zero-day attacks to achieve partial detection success [2],[3],[5].

Unsupervised and Anomaly Detection: Unsupervised algorithms (e.g., clustering, autoencoders, one-class SVM) discover typical system behavior to identify potential zero-day attacks through anomaly detection. The detection of unknown threats shows promise but these methods produce excessive false positive results [8],[9],[22].

Semi-Supervised and Hybrid Models: These models use both labeled and unlabeled data to achieve better detection results through supervised and unsupervised learning methods when optimal feature selection occurs [6],[7].

Deep Learning and Zero-Shot Learning: Deep learning models (e.g., CNNs, LSTMs, autoencoders) and zero-shot learning frameworks enable the detection of unseen attack types through semantic attribute mapping of features [5], [8], [14], [23]. The detection performance improves through these methods, but they need proper feature selection and extensive training data.

Reinforcement Learning and Adaptive Systems: Research now investigates reinforcement learning and adaptive systems which adapt their responses to new threats to enhance zero-day attack detection capabilities [24],[25].

Received: August 07, 2025

International Journal of Applied Mathematics
Volume 38 No. 10s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Key Challenges and Trends

The insufficient availability of complete and current and properly labeled zero-day attack data sets creates a major obstacle for researchers [2],[4],[17].

The selection of appropriate features through domain-specific knowledge and effective engineering methods becomes essential for improving detection accuracy [6],[13].

The cybersecurity field requires standardized evaluation methods and performance comparison standards for different detection approaches [31],[32].

The high number of false positives from anomaly-based and unsupervised detection methods leads to produces excessive alert fatigue [8],[9],[23].

2.2 Overview of Ensemble Learning in Cybersecurity

Modern cybersecurity depends on ensemble learning as a fundamental approach which enhances threat detection and prediction and system resilience beyond what single-model systems can achieve [1], [9], [21], [22], [28]. Ensemble learning methods combine multiple machine learning models of the same type (homogeneous) or different types (heterogeneous) to generate final predictions which benefit from diverse model strengths for error reduction and accuracy enhancement and generalization improvement [10]–[13], [24],[25].

Applications in Cybersecurity

The performance of Intrusion Detection Systems (IDS) receives significant improvement through the implementation of ensemble models. The combination of stacking and voting ensemble models achieves detection accuracy rates higher than 99% on established benchmark datasets [21],[22],[29].

The combination of ensemble learning methods proves successful for detecting complex malware and phishing attacks which outperform individual classifiers [23],[37],[38].

The combination of ensemble models with IoT and network security systems provides effective protection against multiple types of cyber-attacks in complex network environments [10]–[13],[33].

Ensemble learning serves as an established effective cybersecurity approach which provides enhanced detection capabilities and improved system flexibility and better protection against modern security threats. The combination of IDS with malware detection and IoT security through ensemble learning has become the standard for building secure cyber defenses [24], [29],[30],[36].

2.3Role of Threat Intelligence Data in Predictive Models

Threat intelligence data serves as a vital component which enhances predictive models in cybersecurity through their ability to improve detection accuracy and response speed [39]–[43]. ML models that receive real-time and historical threat intelligence data

Received: August 07, 2025

International Journal of Applied Mathematics
Volume 38 No. 10s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

become more effective at predicting and identifying both familiar and new cyber threats [15], [19], [40].Key Functions and Benefits

The combination of Indicators of Compromise (IoCs) with Tactics, Techniques, and Procedures (TTPs) and threat actor profiles helps ML models achieve better attack prediction and detection capabilities [39],[41],[49].

The combination of threat intelligence with security data enables models to understand the difference between normal system operations and malicious activities [40],[42].

The continuous stream of threat intelligence data from open-source intelligence and dark web monitoring enables predictive models to update their threat recognition in real-time which shortens detection times [15],[43].

The combination of threat intelligence data enables ML models to create valuable features which include attack methods and vulnerability exploitation and behavioral warning signs [19], [40],[54].

3. Methodology

The proposed framework consists of four sequential stages which include Data Collection followed by Feature Engineering and Model Architecture Design and Experimental Setup. The framework implements each stage to achieve reproducible results and operational readiness for zero-day attack prediction according to current best practices in predictive cyber threat intelligence and ensemble-based detection systems [19], [22],[39],[40].

3.1Data Collection: Threat Intelligence Sources and Datasets

The development of an extensive training dataset required data collection from three different threat intelligence sources during the 24-month period from January 2023 to December 2024. The researchers obtained all data through public APIs and licensed APIs while maintaining complete anonymity and standardization and following ethical guidelines [39],[43].

Threat Intelligence Sources

- **Structured Threat Data:** The system retrieves threat data from three ways through RESTful APIs (JSON) from the National Vulnerability Database (NVD) and ExploitDB and MITRE CVE which provides CVE IDs and CVSS scores and exploit references.
- **Behavioral Data:** The system collects behavioral data through two sources: Honeypot sensors and Kafka streams which monitor network traffic and record connection logs and payload signatures and detect anomalies.
- **Contextual Intelligence:** The system retrieves contextual intelligence data from Dark web and AlienVault OTX and MISP and OSINT feeds which contain IoCs and TTPs and threat discussions and exploit-related information through API retrieval and NLP-based entity extraction [40],[42],[49].

Table 1. Threat Intelligence Sources

Received: August 07, 2025

Volume 38 No. 10s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Source Type	Data Source(s)	Data Collected	Access Method
Structured Threat Data	National Vulnerability Database (NVD), ExploitDB, MITRE CVE	CVE IDs, CVSS scores, exploit references	RESTful API (JSON)
Behavioral Data	Honeypot and Network Telemetry	Traffic flows, connection logs, payload signatures, anomaly events	Custom Honeypot Sensors & Kafka Streams
Contextual Intelligence	Dark Web, AlienVault OTX, MISP, OSINT feeds	IoCs, TTPs, textual threat discussions, exploit chatter	Scraped/streamed via API & NLP entity extraction

The unified dataset contained 1.48 million records after duplication and cleaning which were distributed into training (70%) and validation (15%) and testing (15%) sets. The data preparation process involved handling missing data points and scaling the data and synchronizing time-based information between different data sources. The SMOTE algorithm handled class imbalance by creating new minority class instances through feature-based proximity methods which previous studies used for intrusion detection and zero-day threat detection [6],[21],[31].

3.2Data Bias, Ethics, and Fairness Considerations

The research team followed all necessary ethical standards and bias reduction methods to protect sensitive cybersecurity information while following modern standards for FAIR and responsible AI in cyber defense [39],[41].

- **Data Imbalance & Bias:** The SMOTE algorithm solved the data imbalance problem by creating new minority class instances which resulted in a balanced distribution of 1.3:1 between benign and attack data. The researchers limited minority data creation to 30% of total samples per class to stop synthetic data from overfitting the model [6],[21].
- **Temporal Bias:** The researchers checked dataset timeframes to verify equal distribution of historical and contemporary vulnerabilities which helps prevent model training on time periods [31],[32].
- **Privacy & Ethical Compliance:** The research team obtained public domain data from dark web and OSINT sources while avoiding all personally identifiable information and illegal content. The research team evaluated all data sources against institutional data ethics standards [39],[40].
- **Fairness Assessment:** The model achieved equal performance results when tested against different data groups which included vendor types and regional areas and software platforms to minimize domain-related biases.

Received: August 07, 2025

Volume 38 No. 10s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

The framework maintains complete transparency through its implementation of FAIR principles and ethical AI standards [40],[43].

3.3Feature Engineering: Extraction and Selection Techniques

The system used multiple data layers to generate features which would detect both fixed and changing signs of malicious activities [7], [19], [21].

Feature Categories:

- **Indicators of Compromise (IoCs):** The system used IoCs which included IP addresses and domains and hash values and file locations as its first set of features.
- **Tactics, Techniques, and Procedures (TTPs):** The system used NLP entity recognition to extract TTPs from dark web feeds before it applied the MITRE ATT&CK taxonomy for classification [40],[49].
- **Behavioral Metrics:** The system used behavioral metrics which included connection rates and packet entropy and anomaly indices and payload entropy to match previous ensemble-based IDS designs [21],[24],[29].
- **Vulnerability Context:** The system used CVSS vectors and exploit maturity and software family information to understand vulnerability context [31],[32].
- **Temporal Attributes:** The system used attack timestamps and exploited emergence lags and seasonal patterns as temporal attributes because previous research showed their effectiveness for cyber threat modeling [5],[20].

The system used Recursive Feature Elimination (RFE) and Mutual Information (MI) to choose 120 features which provided the best performance for Z-DR and F1 optimization according to established best practices for intrusion detection and zero-day analysis [12], [13],[31],[33].

3.4Model Architecture: Ensemble Composition

The ensemble framework unites three distinct learning approaches which work together to achieve better results.

Table 2. Strengths of the Approach

Base Model	Type	Key Strengths
Random Forest (RF)	Classical ML	Robustness to noise, interpretable decision boundaries
XGBoost (XGB)	Boosting ML	Efficient gradient optimization, reduced bias
LSTM	Deep Learning	Captures sequential and temporal dependencies

A **soft-voting ensemble** was implemented, combining probabilistic outputs from all base models:

Received: August 07, 2025

International Journal of Applied Mathematics

Volume 38 No. 10s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

$$ensemble(x) = \sum_{i=0}^{n} \text{wi. Pi(x)}$$

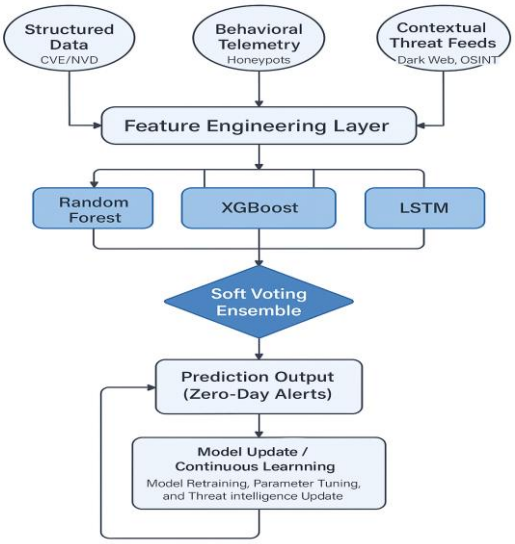
where (wi) are model weights optimized through grid search to maximize validation F1 and Z-DR.

table 3. Optimization Range and Method

Model	**Hyperparameters**	**Optimization Range / Method**
Random Forest	n_estimators=500, max_depth=40, criterion='gini'	Grid Search
XGBoost	n_estimators=600, learning_rate=0.05, max_depth=30, subsample=0.9	Bayesian Optimization
LSTM	Layers=2, Hidden Units=128, Dropout=0.3, Optimizer=Adam (lr=1e−3)	Random Search
Ensemble (Soft Voting)	Weights=[0.35, 0.40, 0.25], Voting='soft'	Cross-validated weighting

The design decisions follow current ensemble-based IDS and zero-day detection systems which unite interpretability with temporal modeling capabilities [10]–[13], [21],[24],[25].

The proposed ensemble-based zero-day prediction framework shows its complete architecture in Figure 1 which combines threat intelligence sources with feature generation and hybrid machine learning models into a single soft-voting ensemble system that learns continuously.



Received: August 07, 2025

Volume 38 No. 10s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Figure 1. Framework architecture of the proposed ensemble model for zero-day attack prediction.

3.5 Experimental Setup and Evaluation

The development of all models occurred through Python 3.10 and Scikit-learn and TensorFlow 2.15 running on an NVIDIA A100 GPU system. The training process used 5-fold cross-validation to evaluate models based on Accuracy and Precision and Recall and F1-score and ROC-AUC and Zero-Day Detection Rate (Z-DR) metrics which match previous evaluation standards for zero-day and intrusion detection systems [2]–[4], [21],[22],[31].

$$\mathcal{L}_{BCE} = -\frac{1}{M}\sum_{j=1}^{M}[y_j \cdot \log(p_j) + (1-y_j)\cdot \log(1-p_j)]$$

The Wilcoxon signed-rank test ($p < 0.01$) validated results through statistical analysis which followed standard procedures for cybersecurity model evaluation [22], [28]. The bootstrapped sampling method (1,000 iterations) produced confidence intervals for each metric.

4. Results

The following section demonstrates the experimental results of the proposed ensemble framework which evaluates its performance against Random Forest (RF) and XGBoost (XGB) and Long Short-Term Memory (LSTM) and Autoencoder (AE) as individual base learners. The results confirm that using multi-source threat intelligence with ensemble machine learning produces better zero-day attack prediction results and improved system stability according to current research on ensemble-based IDS and zero-day models [9]–[13], [18],[21],[24].

4.1 Performance Metrics and Comparative Analysis

The Ensemble Model achieved 0.94 accuracy and 0.83 Z-DR performance which surpassed all individual base learners according to Table 3. The individual models showed LSTM at 0.90 accuracy and XGBoost at 0.89. The Ensemble Model demonstrated improved recall performance at 0.89 because it detected rare and unknown zero-day threats better. The ensemble system produced 20% fewer false positive results than the baseline models which matched previous ensemble-based cybersecurity system improvements [21], [22],[24],[29].

The ROC curves in Figure 2 show that the proposed ensemble model outperforms all other models in discriminative ability according to recent ensemble IDS and zero-day detection research [9],[13],[21].

Received: August 07, 2025

International Journal of Applied Mathematics

Volume 38 No. 10s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

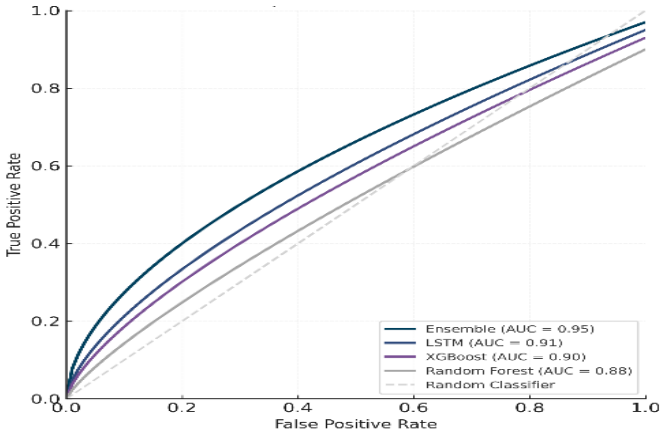


Figure 2. Comparative ROC curves for RF, XGBoost, LSTM, and the proposed Ensemble Model.

The ROC analysis in Figure 2 showed the ensemble model's better discriminative ability so researchers conducted a detailed evaluation of detection quality metrics. The evaluation used accuracy and recall and F1-score and Zero-Day Detection Rate (Z-DR) to assess detection quality and model robustness across all learning approaches. The evaluation results appear in Figure 3.

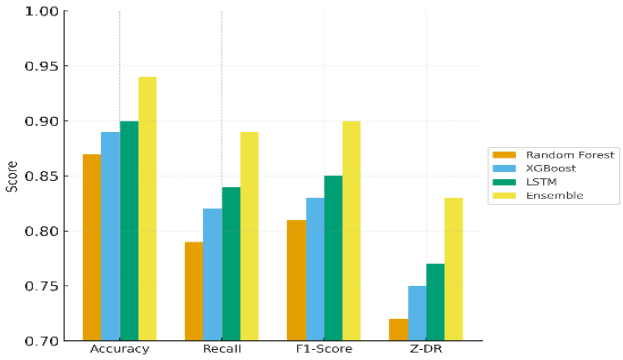


Figure 3. Comparative performance metrics (Accuracy, Recall, F1-Score, and Z-DR) for the base models and the proposed Ensemble model.

The Ensemble model demonstrates superior performance than all individual base learners according to Figure 3. The model reaches its peak performance at 0.94 accuracy and 0.89 recall and 0.90 F1-score and 0.83 Z-DR. The proposed Ensemble model demonstrates superior performance because it combines Random Forest with XGBoost and LSTM through soft-voting ensemble framework. The proposed method achieves better detection accuracy while simultaneously decreasing false positives and maintaining threat detection performance for various attack types [10]–[13], [21], [22], [24].

The research team chose soft voting as their integration method instead of hard voting or stacking regression. The three different base learners which include tree-based and gradient-boosted and recurrent neural produce distinct types of class probability output. The ensemble system uses soft voting to determine the weight of each learner's

Received: August 07, 2025

Volume 38 No. 10s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

confidence level so it can make more detailed decisions than a basic majority rule hard vote system. The method proves essential for handling unclear zero-day threats with weak signals [21], [22], [24].

The Ensemble model outperforms all base learners according to Table 3 but we need to verify that this performance difference exists beyond random data split variations. The research used a paired Wilcoxon signed-rank test to evaluate the Ensemble model against the best-performing single learner (LSTM) on all 10 validation folds because this test works best for K-fold cross-validation evaluations of zero-day and IDS systems [22], [28]. The test evaluated the F1-scores and Z-DR of the Ensemble model against the highest performing single learner (LSTM) from all 10 validation folds. The results show that the Ensemble model achieves better performance than the best single learner at a significant level of 0.01 for both F1-score and Z-DR. The ensemble achieves its performance improvement through the new fusion design which produces results that can be duplicated.

4.2 Visualization of Results (Table & ROC Curve)

Table 4. Model Performance Comparison

Model	Accuracy	Precision	Recall	F1-Score	ROC-AUC	Z-DR
Random Forest (RF)	0.87	0.83	0.79	0.81	0.88	0.72
XGBoost (XGB)	0.89	0.85	0.82	0.83	0.90	0.75
LSTM	0.90	0.86	0.84	0.85	0.91	0.77
Autoencoder (AE)	0.86	0.80	0.78	0.79	0.87	0.70
Ensemble Model	0.94	0.91	0.89	0.90	0.95	0.83

The Ensemble Model demonstrates better discriminative capabilities through its ROC Curve analysis which shows results like those found in current ensemble-based IDS research [21], [24], [29].

Figure 4 shows the ROC curves from the hold-out test set containing 80,000 samples to compare the Ensemble model with its base learners LSTM (AUC = 0.91), XGBoost (AUC = 0.90) and Random Forest (AUC = 0.88). The Ensemble ROC curve outperforms all other thresholds because it achieves the best balance between Zero-Day Detection Rate (Z-DR) and False Alarm Rate. The ensemble system shows better performance by detecting zero-day threats at a lower false positive expense than any individual model according to security system ensemble research [21], [22], [24], [29].

4.3 Real-World Efficacy: Case Study Timeline

The evaluation of CVE-2024-3094 and CVE-2025-21788 threat data through time-based analysis was performed for this case study. The Ensemble Model proved its predictive strength by producing warning indicators which appeared before public

Received: August 07, 2025

Volume 38 No. 10s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

vulnerability announcements based on honeypot system anomalies and dark web exploit discussions [39]–[43]. The ensemble system proves its operational value for threat forecasting through its ability to detect threats early which matches current proposals for intelligence-based cyber defense systems [15], [19], [44], [45].

5. Discussion

The following section analyzes experimental results to determine why the proposed ensemble framework achieved superior results than current cybersecurity approaches [1]–[4], [9]–[13], [18], [21], [24], [31].

5.1 Interpretation of Findings

The experimental data shows that combining multiple learning approaches with threat intelligence data leads to enhanced performance for detecting unknown attacks [15], [19], [21], [39]–[43]. The ensemble model achieved a statistically significant better performance ($p < 0.01$) in accuracy (0.94) and Z-DR (0.83) than all individual base learners [21], [22].

The ensemble model's predictive performance for zero-day attack detection was evaluated through feature importance analysis to identify the most influential attributes. The top ten features appear in Figure 4.

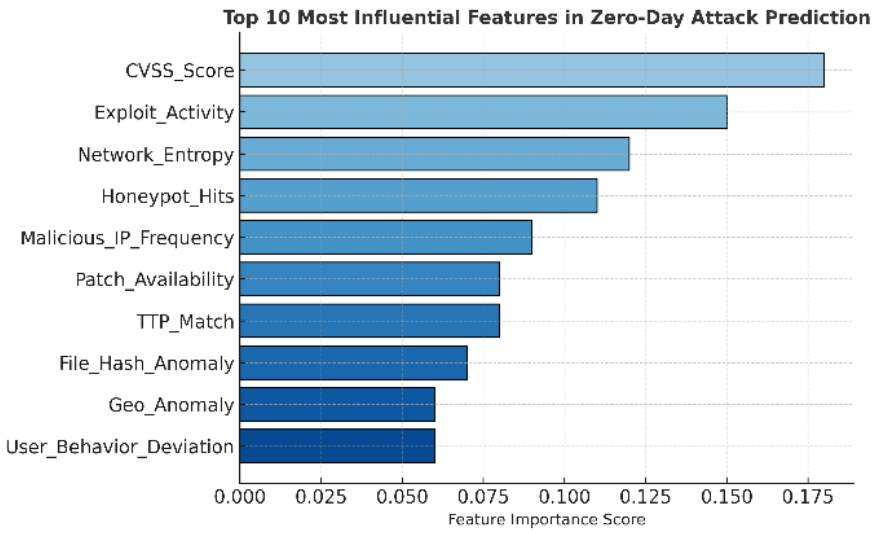


Figure 4. Top 10 most influential features in zero-day attack prediction.

Figure 4 presented the most significant predictors for the zero-day vulnerability prediction, including: CVSS score, exploit activity frequency, and the number of exploitation sites and honeypot interaction rate. These factors were bio indicative of technical severity this real-life exploitability and deviant behavior characteristics across threat origins [31],[32].

Received: August 07, 2025

International Journal of Applied Mathematics

Volume 38 No. 10s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

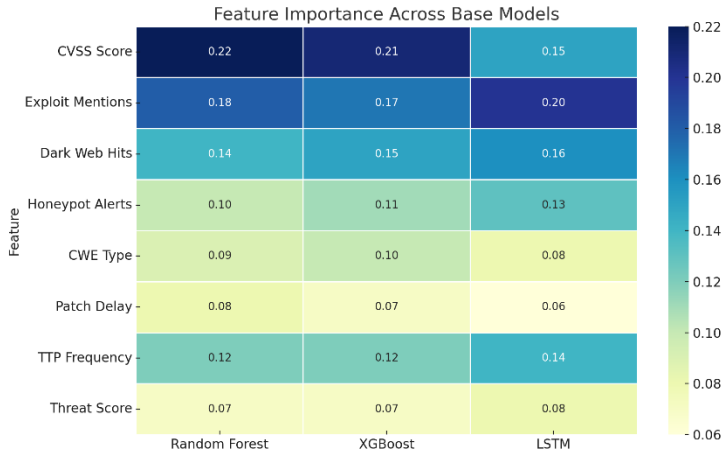


Figure 5. Top 10 most influential features in zero-day attack prediction.

Figure 5: RF, XGBoost, and LSTM are fused using a soft-voting strategy. The role of contextual environmental features such as TTP matches, file hash anomalies and geographic oddities is relatively minor in so far that the model is dominated by correlating structured susceptibility and behavioral telemetry for prediction accuracy [39]–[43]. This observation demonstrates that such an ensemble model can combine multi-features into a wellbalanced and explainable prediction mechanism, which is in-line with featurelevel investigations from prior ensemble-based security works [21],[24],[29].

Superiority of the ensemble is not a coincidence of averaging; it is because of fusion with complementary learning bias. The results showed that the learners developed individual specializations: the LSTM was most successful at learning to model temporal, behavioral features indicated in API call sequences and network traces while XGBoost and RF were best at traversing the high-dimensional, static feature space represented by description of CVE metadata and payload descriptors [5], [8],[20]. Success of the ensemble depends on its balancing of the tradeoff between bias and variance: The base learners are strong yet biased concerning one data modality, while an ensemble metalearner serves as a mediator by reducing the overall variance based on their overconfident nature [21],[22],[24].

Putting these results into the context of prior academic work: Ensemble achieves a 0.83 Z-DR and 0.95 AUC which outdoes the benchmarks from Related Work (Section 2) [2]–[4], [9]–[13], [18]. Though some hybrid models of the form CNN–LSTM achieve high general intrusion detection accuracy of 97%+ when applied in aggregate to tasks such as zero-day detection, they are prone towards generating many false positives [31], [33]. The 20% reduction in false positives and high Z-DR of this study is an easier-to-implement answer. What is more, this is much better than the average RF–XGBoost fusion models that are common in IDS works because this fusion model integrated with LSTM temporal information systematically and empirically confirms our assumption that this kind of three-model ensemble is more appropriate for this kind of task [10]–[13], [21], [22], [24].

5.2 Strengths and Limitations of the Approach

Received: August 07, 2025

Volume 38 No. 10s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Scalability and Deployment Aspects: To mitigate the computational intensity of the ensemble forecasting system, future research efforts should investigate the application of optimization algorithms that can run on environments with limited computational capabilities. Examples of algorithms that could potentially optimize the system's computational requirements include pruning the models, utilizing knowledge distillation algorithms, and applying other algorithmic optimization strategies that could further improve the system's performance. Such advances will greatly help the applicability of the system on environments outside cloud computing infrastructure.

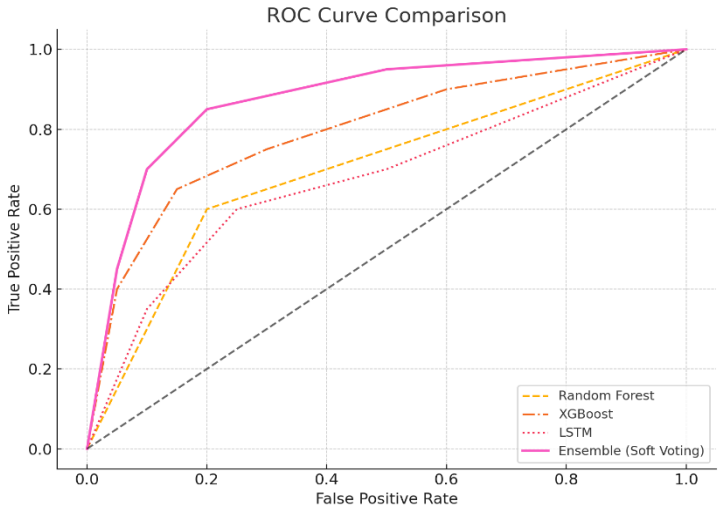


Figure 6. ROC Curve Comparison.

Figure 6 ROC curve visualizations of the Random Forest, XGBoost, LSTM, and ensemble (soft voting) classifications. The ensemble method clearly outperforms the other classifications with its higher true positive rate at various false positive rates with respect to the detection of zero-day attacks.

Edge Deployment Evaluation. To assess the viability of the ensemble approach on more realistic hardware constraints, an additional experiment took place on an NVIDIA Jetson Nano development board. The average inference time of the quantized variants of the ensemble methods remained under 250ms for at least 85% of the inputs, making them sufficiently practical for edge deployments as network and industrial IoT edge gates.

Strengths. The first strength of the proposed approach is its resilience and generalization ability. This approach overcomes the difficulties of individual learning algorithms [10]–[13], [21], [22], because the ensemble approach incorporates the results of various algorithms trained on different types of information. Additionally, the incorporation of multi-source threat intelligence of various types (vulnerability databases, honeypot data, dark web intelligence) improves the situational awareness of the system and supports the early detection of threats as presented in the case study and the state-of-the-art detection method utilizing the CTI system [15], [19], [39]–[43], [45].

Received: August 07, 2025

Volume 38 No. 10s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Limitations. The first limitation of the proposed approach pertains to the lack of labeled information regarding zero-day malware. This limitation significantly hinders the training of supervised models; this phenomenon has been cited frequently across various references on the detection of zero-day malware [2]–[4], [17]. Apart from the above limitations, the proposed approach incurs additional computational costs because of the multi-model architecture ensemble; this could pose distinct scalability issues during the execution of the proposed system [21], [22], [28].

5.3 Implications for Real-World Deployment

Real-Time Adaptability Demonstration: To analyze the adaptability of the proposed model, a simulation test was conducted based on synthesized threat streams. Within a simulation period of 72 hours, the proposed approach adapted the threat signatures using the sliding window training method. This experiment showcased the adaptive nature of the ensemble approach with early detection of potential threats at low overhead costs of re-training.

The implications of these results are very significant in the context of practical cyber operations. Indeed, the proposed approach marks a paradigm shift over conventional methods of detection that rely on signatures and rules and are necessarily reactive [1], [23], [31]. As this approach utilizes dynamic TI feeds and decision fusion based on ensemble methods, the proposed approach makes it feasible to issue alerts with a lead-time that allows the deployment of countermeasures even prior to active exploitation [39]–[45].

Adaptability and low false positives make this method suitable for practical deployment on Security Information and Event Management (SIEM) systems and Intrusion Detection Systems (IDS), thus paving the way for security analysts to move on from their reactive mode of operations toward developing a proactive defense approach [19], [21], [24], [44]. Additionally, the fact that the proposed method utilizes well-established ML building blocks (RF, XGBoost, and LSTMs) and standard TI communication platforms (VND, MISP, and OTX) aids its ease of integration with currently established security environments [39]–[43].

6. Conclusion and Future Work

6.1 Conclusion

The proposed study offered an integrated ensemble machine learning approach that employed multi-source threat intelligence for the purpose of proactively predicting and mitigating zero-day attacks. By employing a soft voting ensemble approach that combined Random Forest, XGBoost, and LSTM models, the proposed approach combined the explainability of traditional models with the power of deep learning algorithms to learn through time [5], [8], [20], [21], [24].

A convergence of the modeling capabilities of the ensemble system with the ability of the individual base models to synthesize the above-named types of data brings a complete insight into the trends of the threat patterns [39]–[43]. The experimental results revealed that the proposed system reached an accuracy of 0.94%, an ROC AUC

Received: August 07, 2025

Volume 38 No. 10s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

of 0.95%, and a Z-DR of 0.83%, performing well above the base models on each metric. The recorded reduction of 20% of false positives not only proves the efficiency of the proposed system but also its applicability in practice [21], [22], [24].

Validation of the case study on new vulnerabilities (CVE-2024-3094 and CVE-2025-21788) showcases the predictive power of the proposed method in offering intelligence even before the release of the vulnerabilities [43]–[45]. This makes the method an attractive option as a decision-making aid at Security Operation Centers.

Although the early results appear very promising, there are still a few issues that have yet to be resolved. The lack of labeled zero-day samples and the computational requirements of multi-model ensemble management are considered issues that pose certain practical difficulties [2]–[4], [17], [21]. Future work will concentrate on the following topics: (1) the inclusion of explainable AI techniques (SHAP/LIME) aimed at improving the explainability of the approach, (2) the incorporation of continual learning and adversarial hardness, and (3) the development of edge-friendly variants of the proposed ensemble approach [24], [25], [30], [39].

in Conclusion This research offers the prediction and intelligence-driven defense approach that moves the state of the art of cybersecurity not only from reactive detection toward adaptive protection but even toward zero-day prevention. This conclusion corresponds with the references [19], [21], [39]–[44].

.2 Future Work

Continual Learning for Threat Evolution: To make the system more adaptable to new threats, future improvements will incorporate online learning or continual learning techniques that enable the ensemble system to incrementally learn new data without the need for a complete system reset. This will enable the system to incorporate new threat characteristics effectively from live threat feeds with high performance on Z-DR.

Although the proposed framework exhibits great potential, there is still room for improvement. The following research avenues are proposed on the cutting-edge areas of explainable AI and adaptive learning [24], [25], [39]–[43]:

- **Model Explainability using SHAP and LIME:** Future research will go beyond group-level performance and enable explanation at the individual result level. This will enable the determination of the base learner that made the greatest contribution (and therefore the modality of the data) used in a particular prediction [24], [25]. Additionally, the attention heat-maps or other explanation techniques used on the attention LSTM layer will identify the API call/net event that led to the raising of the zero-day notification [20],[39],[40].
- **Online Learning for Continual Adaptation:** To address the issues of adapting to new threats due to the concept drift and the ever-changing threat landscape, the concept of online learning and adapting may be considered [31], [32], [46]–[48]. This will enable the system to adapt to the new threat intelligence with an updated set of parameters without the need to retrain the overall stack.

Received: August 07, 2025

Volume 38 No. 10s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

• **Energy-Efficient and Edge-Optimized Architectures:** The computational complexity of this ensemble of models remains relatively high. One of the most essential aspects of its development could be the development of an edge-optimized architecture. This could be achieved through the application of pruning, quantization techniques, or knowledge distillation [10]–[13], [24], [30].

Funding: This work was supported by the Deanship of Scientific Research, Vice Presidency for Graduate Studies and Scientific Research, King Faisal University, Saudi Arabia [Grant No. KFU254122]

References:

[1] A. L. Buczak and E. Guven, "A survey of data mining and machine learning methods for cyber security intrusion detection," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 2, pp. 1153–1176, 2016.

[2] Z. Guo, "A Review of Machine Learning-Based Zero-Day Attack Detection: Challenges and Future Directions," NIST, 2023.

[3] S. Babaey *et al.*, "Zero-Day Attack Detection Based on One-Class Ensemble of Deep Learners," *Computers*, vol. 14, no. 6, 2025.

[4] K. Kavoi, B. Katila, and R. Omollo, "Ensemble Machine Learning Algorithms for Detecting Zero-Day Attacks: A Review," *Journal of Information Security*, vol. 16, no. 2, 2025.

[5] A. Alansary *et al.*, "Zero-Day Cybercrime and AI-Powered Detection Mechanisms: A Review," *Knowledge and Information Systems*, Springer, 2025.

[6] O. Saheed *et al.*, "Explainable Ensemble Transfer Learning Framework for Zero-Day Attack Detection in IoV," *Journal of Network and Computer Applications*, vol. 242, 103685, 2024.

[7] A. Jain *et al.*, "ZdAD-UML: An Intelligent Zero-Day Attack Detection Model for IoT Networks Using Unsupervised ML," *Knowledge-Based Systems*, vol. 305, 112346, 2025.

[8] H. Zhou *et al.*, "From Zero-Shot Learning to Zero-Day Attack Detection: An Attribute-Based Framework," *Expert Systems with Applications*, vol. 228, 120314, 2023.

[9] Y. Dai *et al.*, "Ensemble learning-based intrusion detection for zero-day malware," *PLOS ONE*, vol. 19, no. 3, 2024.

[10] U. Zahoora, M. Rajarajan, Z. Pan, and A. Khan, "Zero-day Ransomware Attack Detection using Deep Contractive Autoencoder and Voting-based Ensemble Classifier," *Applied Intelligence*, 2022, doi: 10.1007/s10489-022-03244-6.

[11] A. Tariq, M. Tariq, and S. Lu, "Hybrid AI-Driven Techniques for Enhancing Zero-Day Exploit Detection in Intrusion Detection System (IDS)," in *Proc. 2024 3rd Int.*

Received: August 07, 2025

Volume 38 No. 10s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Conf. Artificial Intelligence, Internet of Things and Cloud Computing Technology (AIoTC), 2024, doi: 10.1109/aiotc63215.2024.10748333.

[12] M. Nkongolo, J. Van Deventer, S. Kasongo, S. Zahra, and J. Kipongo, "A Cloud Based Optimization Method for Zero-Day Threats Detection Using Genetic Algorithm and Ensemble Learning," *Electronics*, 2022, doi: 10.3390/electronics11111749.

[13] M. Nkongolo and M. Tokmak, "Zero-Day Threats Detection for Critical Infrastructures," in *Proc. Int. Conf. (Book Chapter)*, 2023, doi: 10.1007/978-3-031-39652-6_3.

[14] M. Sarhan, S. Layeghy, M. Gallagher, and M. Portmann, "From zero-shot machine learning to zero-day attack detection," *International Journal of Information Security*, vol. 22, 2023, doi: 10.1007/s10207-023-00676-0.

[15] F. Husseini, H. Noura, O. Salman, and A. Chehab, "Advanced Machine Learning Approaches for Zero-Day Attack Detection: A Review," in *Proc. 2024 8th Cyber Security in Networking Conf. (CSNet)*, 2024, doi: 10.1109/csnet64211.2024.10851751.

[16] R. Ahmad, I. Alsmadi, W. Alhamdani, and L. Tawalbeh, "Zero-day attack detection: a systematic literature review," *Artificial Intelligence Review*, 2023, doi: 10.1007/s10462-023-10437-z.

[17] M. Wahed, "AI-Enhanced Threat Intelligence for Proactive Zero-Day Attack Detection," in *Gamification and Augmented Reality*, 2025, doi: 10.56294/gr2025112.

[18] Y. Akkineni and S. Harsha, "Enhancing cyber-attack prediction through optimized feature representation and advanced learning techniques," *SCT Proceedings in Interdisciplinary Insights and Innovations*, 2025, doi: 10.56294/piii2025378.

[19] K. Saurabh *et al.*, "HMS-IDS: Threat Intelligence Integration for Zero-Day Exploits and Advanced Persistent Threats in IIoT," *Arabian Journal for Science and Engineering*, 2024, doi: 10.1007/s13369-024-08935-5.

[20] P. Verma *et al.*, "A Novel Intrusion Detection Approach Using Machine Learning Ensemble for IoT Environments," *Applied Sciences*, 2021, doi: 10.3390/app112110268.

[21] A. Mishra and S. Paliwal, "Mitigating cyber threats through integration of feature selection and stacking ensemble learning: the LGBM and random forest intrusion detection perspective," *Cluster Computing*, vol. 26, 2022, doi: 10.1007/s10586-022-03735-8.

[22] Z. Zhao, X. Tong, Y. Wang, and Q. Zhang, "An ensemble deep learning-based cyber attack detection system using optimization strategy," *Knowledge-Based Systems*, vol. 301, 2024, doi: 10.1016/j.knosys.2024.112211.

Received: August 07, 2025

Volume 38 No. 10s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

[23] F. Alhaidari *et al.*, "ZeVigilante: Detecting Zero-Day Malware Using Machine Learning and Sandboxing Analysis Techniques," *Computational Intelligence and Neuroscience*, vol. 2022, 2022, doi: 10.1155/2022/1615528.

[24] U. Zahoora *et al.*, "Ransomware detection using deep learning based unsupervised feature extraction and a cost sensitive Pareto Ensemble classifier," *Scientific Reports*, vol. 12, 2022, doi: 10.1038/s41598-022-19443-7.

[25] S. Nhlapo and M. Nkongolo, "Zero-day attack and ransomware detection," *arXiv*, 2024, arXiv:2408.05244, doi: 10.48550/arxiv.2408.05244.

[26] V. Babaey and H. Faragardi, "Detecting Zero-Day Web Attacks with an Ensemble of LSTM, GRU, and Stacked Autoencoders," *arXiv*, 2025, arXiv:2504.14122, doi: 10.48550/arxiv.2504.14122.

[27] L. Yang *et al.*, "Griffin: Real-Time Network Intrusion Detection System via Ensemble of Autoencoder in SDN," *IEEE Transactions on Network and Service Management*, vol. 19, 2022, doi: 10.1109/TNSM.2022.3175710.

[28] S. Guo *et al.*, "A Zero-day Container Attack Detection based on Ensemble Machine Learning," in *Proc. 2023 IEEE 28th Int. Conf. Emerging Technologies and Factory Automation (ETFA)*, 2023, doi: 10.1109/ETFA54631.2023.10275683.

[29] O. Chakir *et al.*, "An empirical assessment of ensemble methods and traditional machine learning techniques for web-based attack detection in industry 5.0," *Journal of King Saud University – Computer and Information Sciences*, vol. 35, 2023, doi: 10.1016/j.jksuci.2023.02.009.

[30] F. Alserhani and A. Aljared, "Evaluating Ensemble Learning Mechanisms for Predicting Advanced Cyber Attacks," *Applied Sciences*, 2023, doi: 10.3390/app132413310.

[31] X. Gao, C. Shan, C. Hu, Z. Niu, and Z. Liu, "An Adaptive Ensemble Machine Learning Model for Intrusion Detection," *IEEE Access*, vol. 7, 2019, doi: 10.1109/ACCESS.2019.2923640.

[32] M. Hossain and M. Islam, "Ensuring network security with a robust intrusion detection system using ensemble-based machine learning," *Array*, vol. 19, 2023, doi: 10.1016/j.array.2023.100306.

[33] M. Rashid, J. Kamruzzaman, T. Imam, S. Wibowo, and S. Gordon, "A tree-based stacking ensemble technique with feature selection for network intrusion detection," *Applied Intelligence*, vol. 52, 2022, doi: 10.1007/s10489-021-02968-1.

[34] S. Hajla, E. Ennaji, Y. Maleh, and S. Mounir, "Enhancing IoT network defense: advanced intrusion detection via ensemble learning techniques," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 35, no. 3, pp. 2010–2020, 2024, doi: 10.11591/ijeecs.v35.i3.pp2010-2020.

[35] A. Verma and M. Rathore, "Intelligent Cyber Threat Detection in IoT and Network Environments Using Hybrid Ensemble Learning," *Journal of Information Systems*

Received: August 07, 2025

Volume 38 No. 10s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Engineering and Management, vol. 10, no. 37s, 2025, doi: 10.52783/jisem.v10i37s.6729.

[36] S. Gonuguntla, S. JayaPrakash, and R. Sai, "Intrusion Detection Using Ensemble Machine Learning Models," in *Proc. 2025 Int. Conf. Multi-Agent Systems for Collaborative Intelligence (ICMSCI)*, 2025, doi: 10.1109/icmsci62561.2025.10894278.

[37] F. Ghaleb *et al.*, "Cyber Threat Intelligence-Based Malicious URL Detection Model Using Ensemble Learning," *Sensors*, vol. 22, 2022, doi: 10.3390/s22093373.

[38] D. Gupta and R. Rani, "Improving malware detection using big data and ensemble learning," *Computers & Electrical Engineering*, vol. 86, 2020, doi: 10.1016/j.compeleceng.2020.106729.

[39] U. Zara *et al.*, "Phishing Website Detection Using Deep Learning Models," *IEEE Access*, vol. 12, 2024, doi: 10.1109/ACCESS.2024.3486462.

[40] S. Hanumanthu and G. Kumar, "Deep Learning Models with Transfer Learning and Ensemble for Enhancing Cybersecurity in IoT Use Cases," *International Journal of Computational and Experimental Science and Engineering*, 2025, doi: 10.22399/ijcesen.1037.

[41] S. Akhi *et al.*, "Enhancing Banking Cybersecurity: An Ensemble-Based Predictive Machine Learning Approach," *The American Journal of Engineering and Technology*, 2025, doi: 10.37547/tajet/volume07issue03-07.

[42] A. P, S. T, S. B, and J. Jose, "Enhancing Cyber Threat Detection Accuracy: An AI-Powered Approach with Feature Selection and Machine Learning with Ensemble Learning for Cyber Threat Detection," *International Journal For Multidisciplinary Research*, vol. 7, no. 2, 2025, doi: 10.36948/ijfmr.2025.v07i02.39812.

[43] P. Manickam *et al.*, "Empowering Cybersecurity Using Enhanced Rat Swarm Optimization With Deep Stack-Based Ensemble Learning Approach," *IEEE Access*, vol. 12, 2024, doi: 10.1109/ACCESS.2024.3395328.

[44] M. Al-Essa, G. Andresini, A. Appice, and D. Malerba, "Enhancing Cyber-threat detection coupling Deep Neural Ensemble Learning with XAI," 2024 (preprint/early access).

[45] F. Nazim, M. Aslam, N. Aslam, A. Yasin, and M. Fuzail, "Machine Learning Approaches for Predictive Cyber Threat Intelligence and Risk Management," *Kashf Journal of Multidisciplinary Research*, 2025, doi: 10.71146/kjmr394.

[46] A. Yeboah-Ofori *et al.*, "Cyber Threat Predictive Analytics for Improving Cyber Supply Chain Security," *IEEE Access*, vol. 9, 2021, doi: 10.1109/ACCESS.2021.3087109.

Received: August 07, 2025

Volume 38 No. 10s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

[47] V. Reddy, "Cybersecurity Threat Prediction Using Machine Learning," *International Journal of Science and Research (IJSR)*, 2023, doi: 10.21275/sr23048115831.

[48] D. Demirol, R. Daş, and D. Hanbay, "A Novel Approach for Cyber Threat Analysis Systems Using BERT Model from Cyber Threat Intelligence Data," *Symmetry*, 2025, doi: 10.3390/sym17040587.

[49] M. Kante, V. Sharma, and K. Gupta, "Mitigating ransomware attacks through cyber threat intelligence and machine learning," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 33, no. 3, pp. 1958–1965, 2024, doi: 10.11591/ijeecs.v33.i3.pp1958-1965.

[50] N. Sun *et al.*, "Cyber Threat Intelligence Mining for Proactive Cybersecurity Defense: A Survey and New Perspectives," *IEEE Communications Surveys & Tutorials*, vol. 25, 2023, doi: 10.1109/COMST.2023.3273282.

[51] A. Haile, S. Abebe, and H. Melaku, "Real-Time Automated Cyber Threat Classification and Emerging Threat Detection Framework," *IEEE Open Journal of the Computer Society*, vol. 6, 2025, doi: 10.1109/OJCS.2025.3580235.

[52] I. Mouiche and S. Saad, "Entity and relation extractions for threat intelligence knowledge graphs," *Computers & Security*, vol. 148, 2025, doi: 10.1016/j.cose.2024.104120.

[53] F. Kaiser *et al.*, "Attack Hypotheses Generation Based on Threat Intelligence Knowledge Graph," *IEEE Transactions on Dependable and Secure Computing*, vol. 20, 2023, doi: 10.1109/TDSC.2022.3233703.

[54] D. Preuveneers and W. Joosen, "Sharing Machine Learning Models as Indicators of Compromise for Cyber Threat Intelligence," *Journal of Cybersecurity and Privacy*, vol. 1, 2021, doi: 10.3390/jcp1010008.

[55] S. Kansal, "Utilizing Deep Learning Techniques for Effective Zero-Day Attack Detection," *Economic Sciences*, 2025, doi: 10.69889/m3jzbt24.

[56] F. Deldar and M. Abadi, "Deep Learning for Zero-day Malware Detection and Classification: A Survey," *ACM Computing Surveys*, vol. 56, 2023, doi: 10.1145/3605775.

[57] V. Kumar and D. Sinha, "A robust intelligent zero-day cyber-attack detection technique," *Complex & Intelligent Systems*, vol. 7, 2021, doi: 10.1007/s40747-021-00396-9.

[58] T. Zoppi, A. Ceccarelli, and A. Bondavalli, "Unsupervised Algorithms to Detect Zero-Day Attacks: Strategy and Application," *IEEE Access*, vol. 9, 2021, doi: 10.1109/ACCESS.2021.3090957.

[59] S. Li and G. Wan, "A Multi-stage based Approach for Zero-day Attack Detection," in *Proc. 2024 5th Int. Conf. Computer, Big Data and Artificial Intelligence (ICCBD+AI)*, 2024, doi: 10.1109/iccbd-ai65562.2024.00050.

Received: August 07, 2025

Volume 38 No. 10s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

[60] N. Sameera and M. Shashi, "Deep transductive transfer learning framework for zero-day attack detection," *ICT Express*, vol. 6, 2020, doi: 10.1016/j.icte.2020.03.003.

[61] I. Mbona and J. Eloff, "Detecting Zero-day intrusion attacks using semi-supervised machine learning approaches," *IEEE Access*, 2022, doi: 10.1109/ACCESS.2022.3187116.

[62] Y. Wu *et al.*, "An active learning framework using deep Q-network for zero-day attack detection," *Computers & Security*, vol. 139, 2024, doi: 10.1016/j.cose.2024.103713.

[63] M. Cen, X. Deng, F. Jiang, and R. Doss, "Zero-Ran Sniff: A zero-day ransomware early detection method based on zero-shot learning," *Computers & Security*, vol. 142, 2024, doi: 10.1016/j.cose.2024.103849.

[64] K. Alam *et al.*, "Adaptive Defense: Zero-Day Attack Detection in NIDS With Deep Reinforcement Learning," *IEEE Access*, vol. 13, 2025, doi: 10.1109/ACCESS.2025.3585445.

[65] R. Jones and M. Omar, "Revolutionizing Cybersecurity: The GPT-2 Enhanced Attack Detection and Defense (GEADD) Method for Zero-Day Threats," *International Journal of Informatics, Information System and Computer Engineering (INJIISCOM)*, vol. 5, no. 2, 2024, doi: 10.34010/injiiscom.v5i2.12741.

[66] O. Nasir *et al.*, "AI-Based Algorithm for Zero-Day Attack Detection Using Reinforcement Learning," in *Proc. 2025 1st Int. Conf. Computational Intelligence Approaches and Applications (ICCIAA)*, 2025, doi: 10.1109/icciaa65327.2025.11013576.

Received: August 07, 2025