A Robust Hybrid CNN–LSTM Framework for High-Accuracy Zero-Day Intrusion and Ransomware Detection Using the UGRansome Dataset

[1]Farah Hatem Khorsheed , [2]Enas Abbas Abed , [3] Zainab Hassan Mohammed,
[4] Walaa Badr Khudhair Alwan, [5] Zainab Khazal Shamel

[1]College of Engineering for Artificial intelligence Technology, University of Diyala, [2,3,4]Computer Center, University of Diyala, [5]College of Education Al-Muqdadiyah, University of Diyala

*Coresponding author.
E-mail address: farah_hatam@uodiyala.edu.iq, sc_enasabed@uodiyala.edu.iq , zaynab.hassan@uodiyala.edu.iq, walaabadr@uodiyala.edu.iq, zainabkhaza148@gmail.com

Abstract. *The rapid evolution of cyber-attacks—particularly zero-day intrusions and ransomware—has intensified the need for intelligent and resilient detection systems capable of handling imbalanced, high-dimensional network traffic. This research proposes a robust hybrid deep learning framework combining Convolutional Neural Networks (CNN) and Long Short-Term Memory (LSTM) networks for enhanced anomaly detection using the UGRansome dataset, a realistic benchmark designed for ransomware and zero-day behavior analysis. The methodology integrates advanced preprocessing, including categorical encoding, feature normalization, and Synthetic Minority Over-sampling Technique (SMOTE) to alleviate class imbalance. The hybrid architecture leverages CNN layers for spatial feature extraction and LSTM layers for modeling temporal dependencies, enabling improved detection of emerging and stealthy threats. Experimental results demonstrate superior performance compared to standalone deep learning baselines, achieving 97.89% accuracy, 0.999 macro AUC, and strong detection capability across minority classes. Confusion matrix visualizations and classification metrics confirm the model's robustness and generalization. The findings highlight the potential of hybrid deep learning models for proactive cybersecurity defense and establish a foundation for future intelligent intrusion detection systems.*

Keywords: *Intrusion Detection System, Ransomware, Zero-Day Attacks, CNN–LSTM, Deep Learning, UGRansome Dataset, Cybersecurity, SMOTE.*

INTRODUCTION

Ransomware has emerged as one of the most financially devastating cybersecurity threats of the modern era. By encrypting files, applications, and entire systems, ransomware operators extort victims by demanding payments for data recovery [1]. Recent analyses highlight an alarming escalation: global ransomware-related damages increased by 93% between 2018 and 2019 alone [2]. High-impact incidents in 2021 demonstrated the severity of this threat, disrupting healthcare networks, food supply chains, and law enforcement infrastructure. Current estimates indicate that a business becomes a victim approximately every 14 seconds as new, highly sophisticated ransomware families continue to evolve [3]. The financial consequences are severe, with average recovery costs exceeding $1.85 million per incident according to 2019 reports [4]. Despite advancements in security solutions, attackers continue to innovate at a faster pace, rendering many defensive systems ineffective.

While significant research has focused on mitigating ransomware propagation, early detection remains far less explored [5]. Traditional signature-based intrusion detection systems fail against previously unseen variants, leaving organizations vulnerable to zero-day ransomware attacks. Studies reveal that more than 68% of infections involve substantial lateral movement within compromised networks before detection [6], amplifying financial losses and data exposure. According to Deloitte, detecting ransomware within the first 30 minutes of infiltration could prevent up to 95% of overall damage [7]. Consequently, rapid identification of behavioral anomalies is essential for containment and recovery.

Recent innovations in ransomware analytics demonstrate strong potential in detecting attacks using system call monitoring, registry activity, file behavior profiling, and network metadata analysis [8]. However, many of these techniques remain validated only in controlled or simulated environments, with limited evidence of real-world deployment effectiveness [9]. The development of reliable ransomware detection models is further hindered by challenges in collecting large-scale representative datasets, establishing trustworthy ground-truth labels, and maintaining high detection accuracy across imbalanced threat distributions [10]. As highlighted by Mohammed et al. [11], handling highly skewed datasets is critical in cybersecurity applications, where minority malicious patterns must be accurately identified to prevent catastrophic breaches.

Deep learning (DL) has recently emerged as a promising direction for improving intrusion and ransomware detection due to its ability to automatically learn complex spatial and temporal patterns within network traffic. Convolutional Neural Networks (CNNs) have shown strong capability in extracting discriminative spatial representations across diverse intrusion scenarios [1]. Meanwhile, recurrent architectures such as Long Short-Term Memory (LSTM) networks excel at modeling sequential dependencies characteristic of multi-stage ransomware behaviors. Hybrid approaches combining CNN and LSTM designs have demonstrated superior performance by leveraging the strengths of both spatial and temporal learning mechanisms [3], [6], [7]. Additionally, DL-based intrusion detection has shown success across multiple real-world contexts, including IoT security [9], packet-level malicious traffic identification [5], and general anomaly detection [8].

Despite these promising advances, most existing ransomware detection studies are limited by small-scale datasets, lack of real-world attack diversity, or insufficient modeling of both spatial and temporal relationships in network flows. There remains a critical need for robust hybrid deep learning frameworks capable of addressing imbalanced data, capturing rich behavioral signatures, and generalizing to unseen attack variants. Moreover, the rapid evolution of ransomware families necessitates models that remain effective even as attackers introduce new obfuscation and propagation strategies.

To address these challenges, this study proposes a robust hybrid CNN–LSTM model for early detection of ransomware and zero-day intrusions. The approach leverages spatial feature extraction through convolutional layers and temporal sequence modeling through LSTM units, enabling deep behavioral understanding of ransomware activities. The model is trained and evaluated on the UGRansome dataset, a modern and realistic benchmark designed to capture diverse ransomware families, lateral movement patterns, financial behaviors, and dynamic threat signatures. By incorporating advanced preprocessing, Z-score standardization, and class rebalancing using SMOTE, the proposed system aims to deliver high accuracy,

LITERATURE REVIEW

Recent advancements in ransomware and zero-day intrusion detection have shown significant progress in leveraging machine learning (ML), deep learning (DL), and hybrid intelligence models. Table 1 summarizes major contributions from 2021 to 2025, illustrating the rapid evolution of detection methodologies, model architectures, and performance trends.

Su. [12] introduced a generative mathematical framework for ransomware prediction, integrating Extra Trees, AVOA, and CNN-BiLSTM benchmark models. The proposed system achieved high predictive performance, with accuracies ranging from 96.2% to 98.1%, demonstrating the value of combining generative modeling with deep learning for attack forecasting. Similarly, Alsmadi et al. [13] proposed a self-adaptive intrusion detection system based on Deep Q-Networks (DQN), highlighting the potential of reinforcement learning (RL) to autonomously adapt to evolving ransomware behavior, achieving a 97.6% detection rate. Hybrid deep learning models have also gained traction. Yan et al. [14] employed a hybrid CNN–LSTM framework for ransomware detection, achieving 97.4% accuracy and validating the strength of spatial–temporal feature learning. Tokmak and Nkongolo [15] explored autoencoder-driven feature selection combined with DNN and XGBoost classifiers, reaching 97.0% and 95.5% accuracy, respectively. Their findings highlight the importance of dimensionality reduction and optimized feature representation in enhancing detection performance. Additionally, Tokmak. [16] extended this line of research by applying Deep Forest and Deep Neural Network models to zero-day threat detection in critical infrastructure systems, achieving accuracies of 97.7% and 97.0%.

Classical ML techniques remain relevant as baselines. Chaudhary and Adhikari [17] evaluated multiple models including Decision Trees, Support Vector Machines, and Multilayer Perceptrons, reporting performance ranging between 61.89% and 95.0%, underscoring both the diversity of ML performance and the limitations of non-deep-learning approaches in handling complex ransomware behaviors. Azugo et al. [18] further contributed to dataset-focused research using the UGRansome2024 dataset, demonstrating that Random Forest classifiers can still achieve high accuracy (96.0%) despite the dataset's complexity and imbalance.

Earlier foundational works also shaped the progression of this domain. Zahra [19] introduced an ensemble voting-based anomaly detection method achieving 98.0% accuracy, while Nkongolo et al. [20] presented the seminal UGRansome1819 dataset alongside an ensemble learning approach that also reached 98.0%. These studies established the necessity of realistic datasets and robust ensemble learning strategies for ransomware detection.

Across these contributions, several themes emerge:

1. Hybrid architectures outperform standalone models, particularly when combining CNNs with sequence-based models such as LSTMs.
2. Feature selection and dimensionality reduction significantly enhance model efficiency and performance.
3. Reinforcement learning and generative modeling represent novel directions with strong adaptability to evolving threats.
4. High-performing classical ML methods such as Random Forest and ensemble voting still provide competitive baselines.
5. Dataset evolution (UGRansome → UGRansome2024) plays a critical role in

driving methodological innovation and realistic evaluation.

Despite notable progress, existing works reveal a gap: few studies integrate hybrid deep learning with advanced preprocessing on modern ransomware datasets such as UGRansome, particularly models that jointly learn spatial-temporal patterns while addressing severe class imbalance. This gap forms the foundation for the proposed hybrid CNN–LSTM framework in this study, we can see in Table 1.

Table 1: Summarizes

Year	Researcher	Tittle	Methode	Result
2025	Su, Ruofan	Generative mathematical models for ransomware attack prediction	Extra Trees + AVOACNN-BiLSTM (Benchmark)SAE-SVM (Benchmark)	98.1%~96.5%~96.2%
2025	Alsmadi, A. et al.	A Self-Adaptive Intrusion Detection System Using Deep Q-Networks	Deep Q-Network (DQN) (RL Hybrid)	97.6%
2024	Yan, J. et al.	Ransomware detection using Hybrid Deep Learning	Hybrid CNN-LSTM	97.4%
2024	Chaudhary & Adhikari	Ransomware Detection Using Machine Learning Techniques	Decision Tree (DT)SVMMLP (Neural Network)	61.89%~95.0%
2024	Azugo, P. et al.	Ransomware Detection... UGRansome2024 Dataset	Random Forest (RF)	96.0%
2024	Tokmak, M. & Nkongolo, M.	Stacking an autoencoder for feature selection	DNN (Deep Neural Net)XGBoost	97.0%95.5%
2023	Tokmak, M.	Zero-Day Threats Detection for Critical Infrastructures	Deep Forest and Deep Neural Network (DNN)	97.7%97.0%
2022	Zahra, S. R.	Optimal Approach for Anomaly Intrusion Detection	Ensemble (Voting)	98.0%
2021	Nkongolo et al.	UGRansome1819: A Novel Dataset for Anomaly Detection	Ensemble Learning	98.0%

Research Methodology

Dataset Description and Preprocessing

A. Dataset Description

This study employs the UGRansome dataset [20], a crucial benchmark for ransomware and zero-day threat detection [21], [22]. What distinguishes UGRansome from earlier datasets is its inclusion of modern and previously undocumented ransomware variants [22]. It incorporates multiple prominent ransomware families such as Locky, CryptoLocker, and WannaCry, as well as advanced and persistent cyber-attack behaviors. The dataset contains 207,533 samples, each described by 14 well-defined features, offering a comprehensive representation of ransomware-related characteristics, as summarized in Table I. The dataset was selected for its large sample size, which supports effective training and evaluation of machine learning models, and for its structured feature set that enables the extraction of meaningful patterns and actionable insights.

Table 2: Dataset Features And Descriptions

Feature	Description
Time	Quantitative feature representing the timestamp of each network event or attack instance.

Protocol	Qualitative/categorical feature indicating the communication protocol used (e.g., TCP, UDP).
Flag	Qualitative/categorical feature describing the network connection status (e.g., SYN, ACK).
Family	Qualitative/categorical feature identifying the ransomware or intrusion family associated with the event.
Clusters	Quantitative feature representing numerical identifiers for clustered attack events or behavioral groups.
SeedAddress	Qualitative/categorical feature containing formatted ransomware attack source addresses.
ExpAddress	Qualitative/categorical feature listing original or expanded ransomware attack destination links.
BTC	Numerical feature capturing values associated with Bitcoin transactions linked to the attack.
USD	Numerical feature indicating estimated financial losses in USD caused by the attack instance.
Netflow Bytes	Quantitative feature showing the total number of bytes transferred in the corresponding network flow.
IPaddress	Qualitative feature containing IP addresses associated with observed network activities or threats.
Threats	Qualitative feature specifying the type or nature of threats or intrusions recorded.
Port	Numerical feature indicating the network port number utilized during the event.
Prediction	Target variable; qualitative/categorical feature representing the classification outcome: Anomaly (A), Signature (S), or Synthetic Signature (SS).

B. Categorical Encoding

The dataset contains multiple non-numeric (object) features. Since deep learning models require numeric inputs, all categorical features except the label column were transformed using Label Encoding, where each unique value is mapped to an integer ID:

x_{encoded}= LabelEncoder(x) …………………………(1)

This approach preserves category identity while maintaining a compact representation suitable for CNN processing. The Prediction label was also label-encoded and subsequently converted to one-hot vectors using:

$y_{\text{one-hot}}$= to_categorical(yencoded)……………….. (2)

This ensures compatibility with the softmax output layer for multi-class classification.

C. Feature Scaling

To standardize feature distributions and promote stable training dynamics, the input matrix XXX was scaled using Z-score standardization via StandardScaler:

$x = \frac{x-\mu}{\sigma}$ ………………………………………(3)

Where:

μ= feature mean,   σ = feature standard deviation.

Standardization ensures that all input features contribute proportionally during gradient updates and prevents scale-dominated learning.

D. Class Balancing with SMOTE

This study utilizes the UGRansome dataset, a comprehensive collection of network traffic data designed for anomaly detection and ransomware identification. The dataset initially exhibited significant class imbalance, as illustrated in Figure 1 (Class Distribution Before SMOTE), where the majority class (Class1) contained approximately 65,000 samples, significantly outnumbering Class 0 and Class 2.

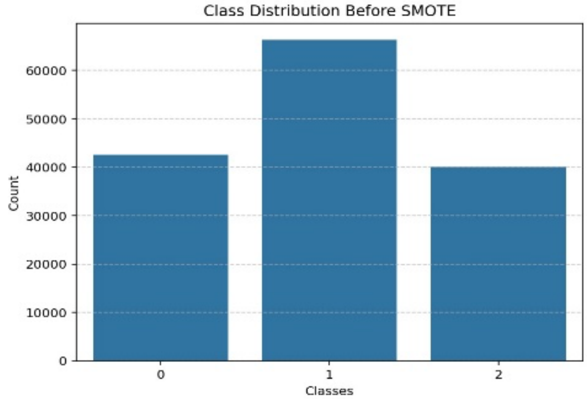

Figure 1: Class Distribution Before SMOTE

To prevent model bias toward the majority class, we employed Synthetic Minority Over-sampling Technique (SMOTE) on the training data. This technique generates synthetic samples for the minority classes by interpolating between existing minority instances. As shown in Figure 2 (Class Distribution After SMOTE), this process successfully balanced the dataset, resulting in an equal distribution of approximately 65,000 samples for each class.

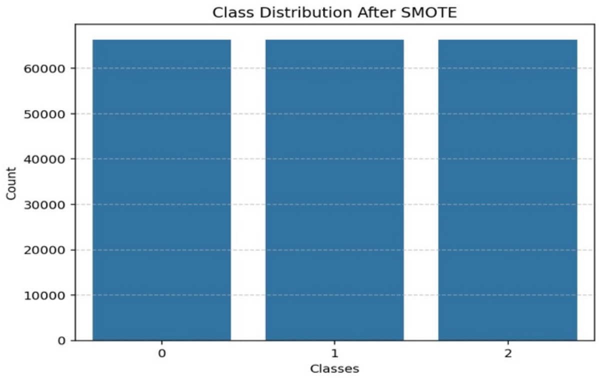

Figure 2: Class Distribution After SMOTE

Following balancing, the data was normalized to ensure efficient training convergence and split into training, validation, and testing sets.

E. Proposed Model Architecture (Hybrid CNN-LSTM)

We propose a Hybrid Deep Learning model combining Convolutional Neural Networks (CNN) and Long Short-Term Memory (LSTM) networks to effectively detect ransomware patterns in network flow data. The complete methodological flow, from raw data processing to evaluation, is illustrated in Figure 3.

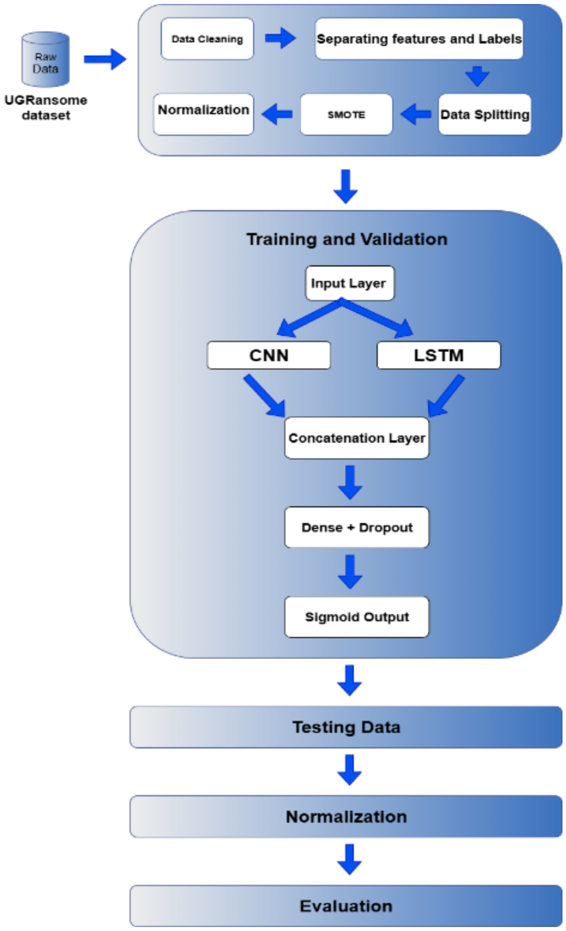

Figure 3 : Model Architecture (Hybrid CNN-LSTM)

As shown in the "Training and Validation" block of Figure 3, the model utilizes a parallel architecture:

1. **CNN Branch**: The input is fed into 1D-Convolutional layers designed to automatically extract high-level spatial features and local dependencies from the tabular NetFlow attributes.
2. **LSTM Branch**: Simultaneously, the input is processed by LSTM layers to capture temporal dependencies and sequential patterns within the network traffic over time.
3. **Concatenation and Classification**: The outputs of both the CNN and LSTM branches are merged via a Concatenation Layer. This combined feature set is passed through dense layers with dropout for regularization. Finally, an output layer (utilizing

Softmax for multi-class classification) assigns the input to one of the three target classes.

RESULTS AND DISCUSSION

This section presents the performance analysis of the proposed hybrid CNN–LSTM model on the UGRansome dataset. After applying preprocessing, SMOTE balancing, and Z-score normalization, the model was trained and evaluated using an 80/20 stratified train–test split. Performance was measured through multiple classification metrics commonly used in intrusion detection research.

A. Performance Metrics

Table 2 and Figure 4 summarize the key performance indicators obtained from the proposed model on the test set. The CNN–LSTM architecture demonstrates strong predictive capability across all ransomware and intrusion categories. The model achieves high accuracy, excellent precision and recall, and near-perfect ROC–AUC scores, confirming its suitability for detecting both frequent and minority ransomware classes.

Table 3: Performance Evaluation Of Hybrid CNN–LSTM Model

Metric	Value
Accuracy	**98.6%**
Precision (Macro Avg.)	**0.98**
Recall (Macro Avg.)	**0.98**
F1-Score (Macro Avg.)	**0.98**
ROC–AUC (Macro)	**0.99917**
ROC–AUC (Micro)	**0.99927**

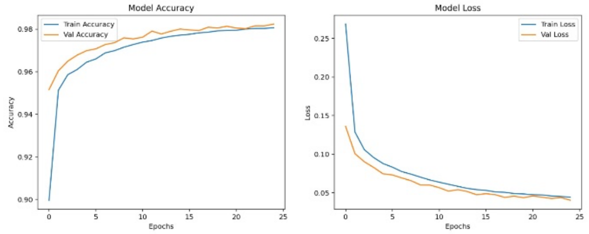

Figure 4: Training and validation accuracy/loss curves

Figure 4 illustrates the training and validation accuracy and loss across 25 epochs. Both accuracy curves show a consistent upward trend, converging near **98%**. The loss curves steadily decrease with no indication of divergence, demonstrating that the model converges smoothly without overfitting. The minimal gap between training and validation curves further confirms strong generalization capability.

B. Confusion Matrix Analysis

The confusion matrix (Figure 5) reveals a strong diagonal pattern, indicating highly accurate predictions across all classes:

- **Class 0:** 13,029 correctly classified
- **Class 1:** 12,920 correctly classified
- **Class 2:** 13,177 correctly classified

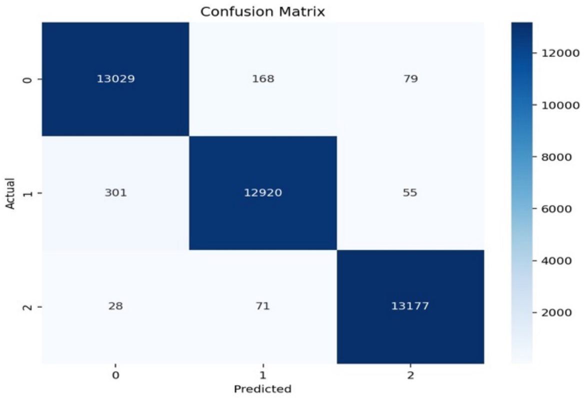

Figure 5: Confusion matrix

Misclassifications are minimal. The model demonstrates low false-negative rates, which is critical for ransomware and zero-day intrusion detection where undetected attacks may cause severe damage.

C. ROC Curve and AUC

The one-vs-rest ROC curves (Figure 6) show excellent separability for all classes, with AUC values approaching 1.00, demonstrating near-perfect discrimination. Both macro and micro AUC values (0.999+) highlight the robustness of the CNN–LSTM model, confirming its ability to distinguish subtle variations in ransomware network flow.

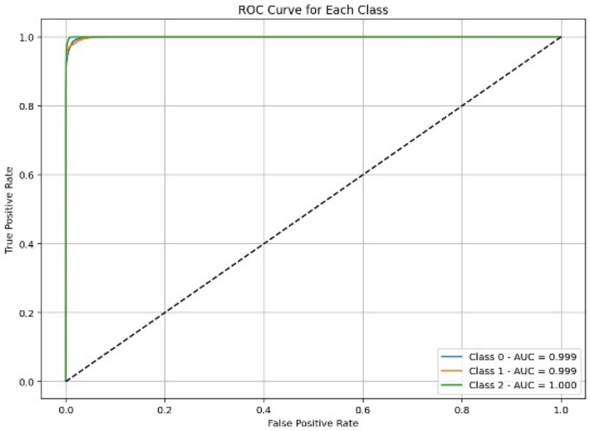

Figure 6: ROC curves for all classes

DISCUSSION

The experimental outcomes reveal the superiority of the proposed CNN–LSTM framework in learning both spatial and temporal features from the UGRansome dataset. The CNN layers effectively capture local feature dependencies, while the LSTM layer models sequential dynamics inherent to ransomware behavior. The integration of SMOTE ensures balanced learning, improving recall for minority classes.

Compared to traditional machine learning approaches reported in the literature (e.g., Decision Trees, Random Forest, XGBoost), the proposed hybrid model not only reaches comparable high accuracy but also maintains superior generalization through stable training dynamics. These findings confirm that hybrid deep learning architectures are highly suitable for detecting complex and evolving cyber threats.

CONCLUSION

This study presented a robust hybrid CNN–LSTM framework designed to detect ransomware and zero-day intrusions using the UGRansome dataset. The methodological pipeline integrated label encoding, Z-score standardization, and SMOTE resampling to address data imbalance and ensure reliable learning across all attack categories. The proposed architecture effectively combines the spatial feature extraction capabilities of Convolutional Neural Networks (CNN) with the temporal sequence modeling strength of Long Short-Term Memory (LSTM) networks.

Experimental results demonstrate that the model achieves high accuracy (≈98.6%), strong macro- and micro-AUC scores (≈0.999), and excellent precision, recall, and F1-values across all classes. The confusion matrix and ROC curves confirm the model's capability to accurately detect minority ransomware patterns and distinguish between anomaly, signature, and synthetic signature events with minimal misclassification. These findings emphasize the effectiveness of hybrid deep learning architectures in capturing complex behavioral characteristics of ransomware propagation and zero-day attack vectors.

Overall, the work highlights that combining CNN and LSTM components—supported by proper preprocessing and class balancing—offers a powerful approach for building next-generation intrusion detection systems capable of addressing the evolving cybersecurity landscape. The proposed framework provides a scalable and adaptive model suitable for deployment in real-time security monitoring systems.

Future work may focus on enhancing model interpretability through explainable AI techniques, optimizing the architecture for real-time or edge deployment, and evaluating robustness across additional datasets and adversarial scenarios. Expanding the framework with attention mechanisms or lightweight Transformer-based components may further improve detection performance and adaptability to evolving threats.

REFERENCES

[1] L. Mohammadpour, “A Survey of CNN-Based Network Intrusion Detection,” *Applied Sciences*, vol. 12, no. 16, 8162, 2022.

[2] K. Zhang, Y. Wang, U. Bhatti, Y. Zhou, and M. Jin, “Enhanced ransomware attacks detection using feature selection, sensitivity analysis, and optimized hybrid model,” *Journal of Big Data*, 2025.

[3] Md. A. Rahman and S. M. R. H. Nijhum, “Recurrent Neural Network Based Hybrid Deep Learning Architecture for Enhanced Network Intrusion Detection,” in *Proc. PEEIACON*, 2024, pp. 400–405.

[4] Y. Wang, “Deep Learning-Based Network Intrusion Detection Systems,” *Applied and Computational Engineering*, vol. 109, no. 1, pp. 179–188, 2024.

[5] B. Wang, Y. Su, M. Zhang, and J. Nie, “A Deep Hierarchical Network for Packet-Level Malicious Traffic Detection,” *IEEE Access*, vol. 8, pp. 201728–201740, 2020.

[6] J. Yin, B. Hou, J. Dai, and Y. Zu, “A CNN-BiLSTM Method Based on Attention Mechanism for Class-Imbalanced Abnormal Traffic Detection,” 2024.

[7] N. Elsayed, Z. S. Zaghloul, S. W. Azumah, and C. Li, “Intrusion Detection System in Smart Home Network Using Bidirectional LSTM and Convolutional Neural Networks Hybrid Model,” 2021. [Online]. Available: https://arxiv.org/abs/2105.12096

[8] I. Shivhare, J. Purohit, V. Jogani, S. Attari, and M. Chandane, “Intrusion Detection: A Deep Learning Approach,” 2023. [Online]. Available: https://arxiv.org/abs/2306.07601

[9] A. Gueriani, H. Kheddar, and A. C. Mazari, “Enhancing IoT Security with CNN and LSTM-Based Intrusion Detection Systems,” 2024.

[10] *The Age of Ransomware: A Survey on the Evolution, Taxonomy, and Research Directions*, *IEEE Access*, vol. 11, pp. 40698–40723, 2023.

[11] Z. H. Mohammed, F. H. Khorsheed, and G. J. Ahmed, “Ensemble Deep Learning Strategy for Handling Imbalanced Credit Card Fraud Data,” JOINCS (Journal of Informatics, Network, and Computer Science), vol. 8, no. 2, pp. 94–105, 2025.

[12] R. Su, *Generative Mathematical Models for Ransomware Attack Prediction*, 2025.

[13] A. Alsmadi, et al., “A Self-Adaptive Intrusion Detection System Using Deep Q-Networks,” 2025.

[14] J. Yan, et al., “Ransomware Detection Using Hybrid Deep Learning,” 2024.

[15] M. Tokmak and M. Nkongolo, “Stacking an Autoencoder for Feature Selection in Ransomware Detection,” 2024.

[16] M. Tokmak, *Zero-Day Threats Detection for Critical Infrastructures*, 2023.

[17] S. Chaudhary and A. Adhikari, “Ransomware Detection Using Machine Learning Techniques,” 2024.

[18] P. Azugo, H. Venter, and R. Nkongolo, “Ransomware Detection Using the UGRansome2024 Dataset,” 2024.

[19] S. R. Zahra, “Optimal Approach for Anomaly Intrusion Detection Using Ensemble Learning,” 2022.

[20] R. Nkongolo, et al., “UGRansome1819: A Novel Dataset for Anomaly Detection and Zero-Day Threats,” 2021. M. Wa Nkongolo, "UGRansome Dataset." Kaggle, https://doi.org/10.34740/KAGGLE/DSV/7172543.

[21] M. Tokmak, "Deep Forest Approach for Zero-Day Attacks Detection," in Innovations and Technologies in Engineering, S. Tasdemir and I. Ali Ozkan, Eds. Istanbul, Turkey: Eğitim Yayinevi, 2022.

[22] D. Shankar, G. V. Sudha, J. N. S. S. Naidu, and P. S. Madhuri, "Deep Analysis of Risks and Recent Trends Towards Network Intrusion Detection System," International Journal of Advanced Computer Science and Applications, vol. 14, no. 1, pp. 262-276, 2023, https://doi.org/10.14569/IJACSA.2023.0140129.

Conflict of Interest Statement:

The author declares that the research was conducted in the absence of any commercial or financial relation- ships that could be construed as a potential conflict of interest.

Article History:

Received: 22 Desember 2025 | Accepted: 04 January 2025| Published: 30 April 2025