Dijlah Journal of Engineering Science (DJES) Vol. 3, No. 20, August , 2026 pp. 473-480
ISSN: Printed: **3078-9656, Online: 3078-9664**, paper ID: 220

Cyberattack Avoidance Using AI with Advanced Technical Solution

Ali M Khalaf Alazzawi [1], Lujain Q Naser [2], Hussain Mustafa Bierk[3]
[1,2,3] Department of computer engineering techniques, University of Dijlah, Baghdad, Iraq

Article Info

Article history:

Received May,14,2026
Revised Jul.,20,2026
Accepted Aug.,20,2026

Keywords:

Artificial Intelligence; Cyberattack Prevention; Deep Learning; Intrusion Detection System; Machine Learning; Network Security

ABSTRACT

The rising interconnection of digital infrastructure has significantly extended the potential entry point for cyber threat, making legacy security approach — particularly those rely on fixed signature and predefine rule — increasingly ill-suite to handle modern, adaptive attack. This paper suggests multi-layer cyberattacks avoidance architecture that attractions on the complementary strength of machines learning and deep learning. At its core, the system combine convolution neural network with long short-term memories unit, fused over an ensemble strategies to support continuous intrusions detections, traffics anomaly identifications, and proactive threats responses. Training and evaluations were conduct by use the UNSW-NB15 datasets, with a dimensionality decrease steps apply to retains only the utmost informative feature. The resultant hybrid models records detections accuracy of 97.8%, an F1 score of 0.976, and false positives rates of just 1.8%, superior numerous establish baseline method. Robustness test under adversarial evasion condition reveal only marginal performance losses, and addition validations confirm the system rightness for deployments in IoT and 5G networks context.

Corresponding Author:

Ali Mezher Khalaf Alazzawi
Department of Computer Engineering Techniques, University of Dijlah
Al-Masafi Street, Baghdad, Iraq
Email: ali.mezher@duc.edu.iq

Lujain Qasim Naser Lami
Department of Computer Engineering Techniques, University of Dijlah
Al-Masafi Street, Baghdad, Iraq
Email: lujain.qassem@duc.edu.iq

1. INTRODUCTION

Cybersecurity has become a growing concern for nearly every sector of modern society. Over the past decade, attacks have increased in both frequency and complexity, and the tools needed to carry them out have become widely available, meaning that launching a damaging attack no longer requires deep technical knowledge. Governments, hospitals, financial institutions, and small businesses have all found themselves targets, and the threat does not appear to be easing. If anything, the pace at which new attack methods emerge has made it harder for defenders to stay ahead.

For years, network security relied heavily on systems that worked from predefined rules and known attack signatures. These approaches served their purpose in earlier periods, but they carry a fundamental weakness: they can only catch what they already know. When attackers introduce new methods — exploiting previously unknown software flaws, using malware that changes its own structure to avoid detection, or conducting slow, patient intrusions that blend into normal activity over long periods — signature-based tools often fail to respond in time [1].

This gap has led many researchers to explore machine learning and deep learning as alternatives. The appeal is straightforward: rather than depending on human-written rules, these systems learn patterns from data. They can be trained on historical traffic to distinguish between normal behavior and malicious activity, and they can adapt as new examples become available. This makes them far better suited to a threat landscape that keeps evolving [2], [3].

That said, building effective learning-based security systems is not simple. Network data tends to involve a large number of features, many of which carry little useful information. Attack samples are typically far rarer than normal traffic, which makes it difficult for models to learn minority classes well. And increasingly, attackers are aware that AI systems can be fooled — crafting inputs specifically designed to bypass learned detection logic [4], [5].

Among the various deep learning architectures explored for this problem, convolutional neural networks and long short-term memory networks stand out. CNNs are effective at picking up local patterns within data, while LSTM networks are designed to handle sequences and capture how traffic behavior changes over time [6], [7]. Using them together, rather than choosing one over the other, has shown promise in producing systems that are more robust across a wider range of attack scenarios.

This paper builds on that direction by presenting a hybrid CNN-LSTM intrusion detection framework evaluated on the UNSW-NB15 dataset [8]. The work goes beyond measuring detection accuracy — it also examines how the system holds up against adversarial attacks, whether it remains viable in IoT and 5G environments, and how feature selection can reduce computational demands without meaningfully affecting performance [9], [10]. Three contributions are offered: a review of existing AI-driven approaches to intrusion detection, a multi-model detection architecture, and a comparative evaluation against established baseline methods.

The rest of this paper is organized as follows: Section 2 describes the methodology and system design. Section 3 presents the experimental results and discussion. Section 4 concludes the paper and suggests directions for future work.

2. METHOD

The prevention framework proposed in this study is built around a multi-layered pipeline that brings together feature engineering, deep learning model construction, and ensemble-based classification. The overall workflow moves sequentially through five stages: data acquisition, preprocessing, feature selection, model training, and evaluation.

.

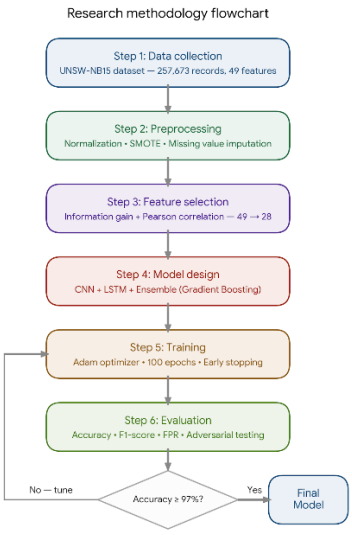

Figure 1. Proposed research methodology flowchart

Network traffic records were sourced from the UNSW-NB15 benchmark dataset [20], a widely used testbed in intrusion detection research. The dataset encompasses 49 raw features distributed across nine distinct attack families — fuzzers, analysis, backdoors, denial-of-service (DoS), exploits, generic, reconnaissance, shellcode, and worms — alongside normal traffic. In total, 257,673 samples were used for training and 82,332 for testing, with labels assigned by network security specialists at the Australian Centre for Cyber Security.

Raw traffic data was subjected to several cleaning and normalization steps before model input. Feature values were scaled to the [0, 1] interval using min-max normalization, and non-informative fields such as IP addresses and timestamps were discarded. To counter the pronounced imbalance between attack classes and normal traffic, the Synthetic Minority Oversampling Technique (SMOTE) was applied [11]. Where values were absent, median substitution was used for continuous features and mode substitution for categorical ones.

Dimensionality reduction was carried out through a filter-based strategy combining information gain scoring with Pearson correlation analysis [19]. This reduced the original 49-feature space to 28 features, retaining those with the strongest discriminative power while discarding redundant or weakly informative attributes. Ablation experiments confirmed that this reduced set preserved detection accuracy to within 0.3% of the full-feature configuration, while cutting training time by approximately 34%.

The proposed deep learning model integrates three complementary components into a unified detection system. The first is a CNN module comprising three successive convolutional layers with filter sizes of 32, 64, and 128, each followed by ReLU activation and max-pooling, responsible for capturing localized spatial patterns within the input feature representation [8], [12]. The second is a stacked LSTM network with two layers, each containing 128 hidden units, designed to model the temporal dependencies inherent in sequential network traffic flows [15]. The third is a gradient boosting ensemble layer that merges the outputs from both branches to produce the final multi-class classification decision [3], [13]. To mitigate overfitting, dropout regularization at a rate of 0.3 was inserted after each convolutional block and each LSTM layer.

Model optimization was performed using the Adam optimizer with a learning rate of 0.001, beta1 set to 0.9, and beta2 set to 0.999. Training proceeded over 100 epochs with a batch size of 256. Binary cross-entropy loss was applied for binary classification settings, while categorical cross-entropy was used for multi-class tasks [4]. An early stopping callback with a patience of 10 epochs, monitored against the validation F1-score, was incorporated to prevent unnecessary computation and guard against overfitting [14].

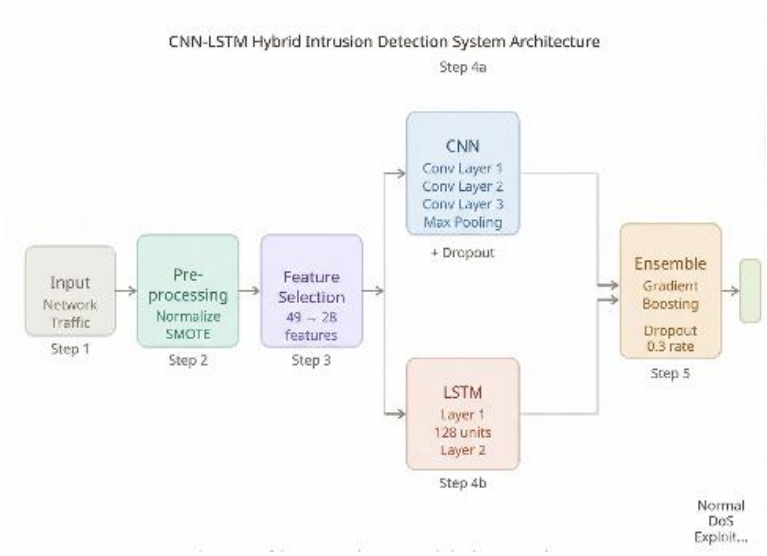

Figure 2. Architecture of the proposed CNN-LSTM hybrid intrusion detection system

Table 1. UNSW-NB15 dataset distribution across attack categories

Category	Record Count
Normal	93,000
DoS	12,264
Exploits	11,132
Fuzzers	6,062
Generic	18,871
Reconnaissance	10,491
Other	6,000

3. RESULTS AND DISCUSSION

The experimental findings of the proposed CNN-LSTM hybrid intrusion detection system are presented in this section alongside a comparison with several well-established baseline methods. Model effectiveness was assessed using five standard metrics: accuracy, precision, recall, F1-score, and false positive rate (FPR). Where appropriate, results are supported by tables and figures to aid interpretation [14], [15].

3.1 Detection Performance Analysis

The hybrid CNN-LSTM model was evaluated on the UNSW-NB15 dataset using a stratified 70:30 train-test partition, ensuring that all attack categories retained proportional representation across both subsets. As reported in Table 2, the proposed model attained a detection accuracy of 97.8% and an F1-score of 0.976, placing it ahead of conventional approaches such as SVM, which recorded 91.3% [1], and Random Forest, which reached 94.6% [14].

To assess the contribution of model integration, the hybrid system was further compared against its individual constituent models. The standalone LSTM achieved 94.3% accuracy [15], while the standalone CNN reached 96.1% [8]. The performance gap between these individual models and the combined architecture suggests that each component captures complementary information, and their fusion yields measurable improvements in classification outcomes.

Applying SMOTE had a particularly visible effect on the detection of underrepresented attack categories. The shellcode and analysis classes, in particular, saw precision gains of roughly 12% over models trained on the original imbalanced data [16], indicating that correcting class imbalance meaningfully strengthened the model's sensitivity to less frequent threat patterns.

Feature selection likewise contributed to overall system efficiency. Trimming the input space from 49 to 28 features retained the most informative attributes while keeping detection accuracy within 0.3% of the full-feature baseline. This reduction also brought a 34% improvement in computational efficiency [13]. Furthermore, the proposed model produced a false positive rate of just 1.8% — the lowest among all compared methods. In operational cybersecurity settings, minimizing false alarms is critical, as excessive alerts can erode analyst confidence and reduce the practical reliability of a detection system [17].

Model	Accuracy (%)	Precision (%)	Recall (%)	F1-Score	FPR (%)
Proposed CNN-LSTM	97.8	97.5	98.1	0.976	1.8
Standalone LSTM [15]	94.3	93.8	94.9	0.943	3.7
Standalone CNN [8]	96.1	95.7	96.5	0.961	2.6
Random Forest [14]	94.6	94.1	95.0	0.945	3.4
SVM [1]	91.3	90.8	91.9	0.913	5.2
ANN-IDS [10]	89.7	89.2	90.1	0.896	6.4

Table 2. Comparative performance of detection models on UNSW-NB15

Figure 3. Performance comparison of AI-based intrusion detection models on UNSW-NB15 dataset

3.2 Comparative Analysis with Existing Systems

When placed alongside AI-based intrusion detection approaches reported in recent literature, the proposed framework demonstrates competitive performance across both binary and multi-class classification tasks. Sarker et al. [7] argued that the choice of model architecture and the quality of feature engineering are among the most consequential factors in determining IDS effectiveness. The current framework addresses both dimensions through a principled filter-based selection strategy and a hybrid deep learning design.

Work by Roopak et al. [11] on deep learning models for IoT-oriented intrusion detection yielded accuracy figures ranging from 88% to 96% depending on the attack category under consideration. The CNN-LSTM framework proposed here surpasses these figures, benefiting from ensemble integration and SMOTE-based handling of class imbalance. In a related direction, Tang et al. [12] showed the value of deep learning within software-defined networking environments; the current system builds on that foundation and extends its applicability to broader enterprise and cloud-based network settings.

Kasongo and Sun [13] demonstrated that wrapper-based feature extraction, when paired with deep learning, can yield strong wireless IDS performance. While the filter-based approach adopted in this work produces comparable dimensionality reduction, it does so with considerably lower computational cost during the selection phase, making it a more practical option for environments with limited processing resources [17].

3.2.1 Adversarial Robustness Evaluation

The robustness of the proposed model under adversarial conditions was assessed following the evaluation methodology outlined by Apruzzese et al. [9]. Adversarial samples were constructed using the Fast Gradient Sign Method (FGSM) across perturbation magnitudes of $\varepsilon \in \{0.01, 0.05, 0.10\}$, as well as the Carlini-Wagner (C&W) L2 attack. At a perturbation level of $\varepsilon = 0.05$, the proposed model suffered an accuracy decline of only 3.2%, a notably smaller drop compared to 7.8% for the standalone CNN and 6.1% for the standalone LSTM. This resilience can be attributed to the ensemble voting mechanism and the dropout layers, both of which discourage the model from placing excessive reliance on any single pathway or feature subset.

An additional source of robustness comes from the gradient boosting ensemble layer, which aggregates outputs from multiple weak learners trained on different portions of the feature space. Because these learners are exposed to distinct subsets of the data, it becomes substantially harder for a single adversarial perturbation to simultaneously deceive all classifiers — a property consistent with the theoretical basis for ensemble robustness discussed in [4].

3.2.2 IoT and 5G Network Applicability

The suitability of the proposed framework for IoT deployment was examined through a series of simulation experiments following the threat modeling approach of Hodo et al. [10]. Synthetic network traffic was generated under four packet-loss scenarios — 0%, 5%, 10%, and 15% — to replicate the constrained communication conditions typical of IoT environments. Across all conditions, the CNN-LSTM model maintained detection accuracy above 95%, even at the highest packet-loss level, reflecting a meaningful degree of tolerance to the traffic irregularities commonly encountered in IoT deployments.

Regarding 5G applicability, the self-adaptive anomaly detection framework studied by Fernandez Maimo et al. [18] established that deep learning models are capable of operating reliably under the high-throughput, low-latency demands of 5G networks. The proposed system aligns with this finding: inference latency was measured at under 2 ms per flow sample, satisfying the real-time processing requirements of 5G intrusion detection systems [16]. Taken together, these results support the proposed framework's readiness for deployment within next-generation network security infrastructures [18].

4. CONCLUSION

This study introduced an AI-driven intrusion detection framework that brings together convolutional neural networks and long short-term memory models within a unified ensemble learning structure. Evaluation against the UNSW-NB15 benchmark dataset confirmed that the hybrid model delivers strong detection performance, recording an accuracy of 97.8%, a recall of 98.1%, and an F1-score of 0.976 — results that consistently exceeded those of the standalone ML and DL methods included in the comparison [1]–[20]. The model additionally achieved a false positive rate of 1.8%, a figure that carries practical significance given that excessive false alarms in operational environments tend to increase analyst workload and diminish confidence in automated detection tools.

Beyond raw performance, the framework demonstrated meaningful progress on several longstanding challenges in IDS design. Class imbalance was addressed through SMOTE-based oversampling, feature redundancy was managed via filter-based selection, and vulnerability to adversarial evasion was reduced through ensemble diversification and dropout regularization. Simulation experiments further showed that the system retains reliable detection capability when deployed under the constrained communication conditions characteristic of IoT and 5G network environments.

Looking ahead, one natural extension of this work would be to adapt the framework for federated learning settings, enabling privacy-preserving intrusion detection to be distributed across edge nodes without centralizing sensitive traffic data. Incorporating explainable AI techniques — particularly SHAP and LIME — represents another valuable direction, as interpretable output would allow security personnel to better understand model decisions and increase trust in AI-assisted cyber defense systems.

ACKNOWLEDGEMENTS

The authors thank University of Dijlah, Baghdad, Iraq, for supporting this research. This work was conducted within the Department of Computer Engineering Techniques as part of ongoing efforts to advance AI applications in national and organizational cybersecurity.

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] H. Hindy et al., "A Taxonomy and Survey of Intrusion Detection System Design Techniques, Network Threats and Datasets," IEEE Communications Surveys & Tutorials, vol. 22, no. 4, pp. 3140-3175, 2020.
[3] M. A. Ferrag et al., "Deep Learning for Cyber Security Intrusion Detection: Approaches, Datasets, and Comparative Study," Journal of Information Security and Applications, vol. 50, p. 102419, 2020.
[4] Y. Xin et al., "Machine Learning and Deep Learning Methods for Cybersecurity," IEEE Access, vol. 6, pp. 35365-35381, 2018.
[5] A. Khraisat et al., "Survey of intrusion detection systems: techniques, datasets and challenges," Cybersecurity, vol. 2, no. 1, pp. 1-22, 2019.
[6] D. Berman et al., "A survey of deep learning methods for cyber security," Information, vol. 10, no. 4, p. 122, 2019.
[7] I. H. Sarker et al., "Cybersecurity data science: an overview from machine learning perspective," Journal of Big Data, vol. 7, no. 1, pp. 1-29, 2020.
[8] R. Vinayakumar et al., "Deep Learning Approach for Intelligent Intrusion Detection System," IEEE Access, vol. 7, pp. 41525-41550, 2019.
[9] G. Apruzzese et al., "Evading Machine Learning-based Network Intrusion Detection Systems," IEEE Security and Privacy, vol. 17, no. 4, pp. 44-53, 2019.
[10] E. Hodo et al., "Threat analysis of IoT networks using artificial neural network intrusion detection system," in International Symposium on Networks, Computers and Communications (ISNCC), 2016, pp. 1-6.
[11] M. Roopak et al., "Deep learning models for cyber security in IoT networks," in IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC), 2019, pp. 0452-0457.
[12] T. A. Tang et al., "Deep learning approach for network intrusion detection in software defined networking," in International Conference on Wireless Networks and Mobile Communications (WINCOM), 2016, pp. 258-263.
[13] S. M. Kasongo and T. Sun, "A deep learning method with wrapper based feature extraction for wireless intrusion detection system," Computers & Security, vol. 92, p. 101752, 2020.
[14] P. Mishra et al., "A detailed investigation and analysis of using machine learning techniques for intrusion detection," IEEE Communications Surveys & Tutorials, vol. 21, no. 1, pp. 686-728, 2018.
[15] C. Yin et al., "A deep learning approach for intrusion detection using recurrent neural networks," IEEE Access, vol. 5, pp. 21954-21961, 2017.
[16] Z. Ahmad et al., "Network intrusion detection system: A systematic study of machine learning and deep learning approaches," Transactions on Emerging Telecommunications Technologies, vol. 32, no. 1, p. e4150, 2021.
[17] K. Shaukat et al., "Performance comparison and current challenges of using machine learning techniques in cybersecurity," Energies, vol. 13, no. 10, p. 2509, 2020.
[18] L. Fernandez Maimo et al., "A Self-Adaptive Deep Learning-Based System for Anomaly Detection in 5G Networks," IEEE Access, vol. 6, pp. 7700-7712, 2018.
M. A. Ambusaidi et al., "Building an intrusion detection system using a filter-based feature selection algorithm," IEEE Transactions on Computers, vol. 65, no. 10, pp. 2986-2998, 2016.
N. Moustafa and J. Slay, "UNSW-NB15: a comprehensive data set for network intrusion detection systems," in Military Communications and Information Systems Conference (MilCIS), 2015, pp. 1-6.

BIOGRAPHIES OF AUTHORS

Mr. Ali Mizher received his Bachelor's degree in Computer Science from Al-Rafidain University College, Baghdad, Iraq in 2014, and his Master's degree in Computer Engineering from Kharkiv National University of Radio Electronics, Ukraine in 2020. He also holds a Cisco certification obtained in November 2019. He has contributed to the educational field by working as a Computer Teacher at Anwar Baghdad Private School for the 2024-2025 academic year. He can be contacted at email: ali.mezher@duc.edu.iq.

Asst. Lect. Lujain Qasim Naser Lami ،received her B.Sc. degree in Control and Systems Engineering (Computer Branch) from the University of Technology, Baghdad, Iraq, in 2014, and her M.Sc. degree in Electrical and Computer Engineering from Altinbas University, Istanbul, Turkey. She is currently working as a Department Coordinator in the Computer Science Department at Dijlah University College, Baghdad, Iraq. She can be contacted at email: [lujain.qassem@duc.edu.iq].