International Journal of Advanced Research in Basic Engineering Sciences and Technology (IJARBEST)

DEEP LEARNING-BASED CYBER INTRUSION DETECTION USING LSTM WITH ATTACK TREE APPROXIMATION AND MITRE ATT&CK MAPPING

Carolin G Arnold
Computer Science and Engineering
St. Joseph College of Engineering, Chennai
carolinpinto58@gmail.com

Dr. M. Navaneetha Krishnan M.E., Ph.D.
Computer Science and Engineering
St. Joseph College of Engineering, Chennai

ABSTRACT

The increasing complexity and frequency of cyberattacks necessitate intelligent and adaptive intrusion detection systems capable of identifying both known and emerging threats. Traditional signature-based and rule-based systems are insufficient in detecting sophisticated multi-stage and zero-day attacks due to their limited generalization capability. This paper presents a deep learning-based cyber intrusion detection framework that leverages Long Short-Term Memory (LSTM) networks, combined with a rule-based risk- scoring mechanism, Attack Tree approximation, and MITRE ATT&CK mapping for enhanced interpretability.

The proposed system uses an LSTM as the primary classification model to identify malicious network activity from high-dimensional traffic data. Although the dataset lacks inherent temporal sequencing, feature vectors are transformed into a pseudo-sequential format to exploit LSTM's pattern recognition capabilities. The system incorporates a probabilistic risk scoring mechanism to categorize threats into multiple severity levels, thereby improving decision-making for security analysts.

To enhance contextual understanding, the detected intrusions are mapped to simplified attack tree structures based on domain-specific heuristics, particularly network port behavior. Furthermore, the MITRE ATT&CK framework is integrated through rule-based mappings to associate detected activities with standardized adversarial tactics and techniques.

The system is evaluated using benchmark datasets, demonstrating high detection accuracy and reduced false positive rates. While maintaining computational efficiency, the framework provides improved interpretability compared to conventional black-box models. This research contributes to the development of practical and explainable intrusion detection systems suitable for deployment in enterprise and IoT environments.

KEYWORDS

Intrusion Detection System, LSTM, Cybersecurity, MITRE ATT&CK, Attack Tree Analysis, Deep Learning, Network Security

1. INTRODUCTION

The rapid evolution of digital technologies, including cloud computing, Internet of Things (IoT), and distributed network infrastructures, has significantly expanded the attack surface of modern systems. As a result, cybersecurity threats have become increasingly sophisticated, involving multi-stage attacks, stealth techniques, and adaptive adversarial behaviors. Intrusion Detection Systems (IDS) play a critical role in safeguarding network environments; however, conventional IDS approaches—primarily based on signature matching and static rule sets—are inadequate in detecting unknown or evolving threats.

In recent years, deep learning techniques have gained prominence in cybersecurity due to their ability to automatically learn complex patterns from large-scale data. Among these, Long Short-Term Memory (LSTM) networks have demonstrated effectiveness in modeling sequential dependencies and capturing hidden relationships within data. Although LSTM models are typically designed for time-series data, they can also be adapted to non-sequential datasets through structural transformations.

Despite their advantages, deep learning-based IDS models often suffer from a lack of interpretability, making it difficult for security analysts to understand and respond to detected threats. This limitation reduces their practical applicability in real-world security operations.

To address this challenge, this research proposes an intrusion detection framework that combines LSTM-based classification with rule-based contextual analysis. The system introduces a risk scoring mechanism to quantify threat severity and incorporates simplified Attack Tree approximation to represent potential attack pathways. Additionally, the MITRE ATT&CK framework is used to map detected intrusions to standardized adversarial techniques, thereby enhancing situational awareness.

The primary objectives of this study are: (i) to develop an efficient LSTM-based intrusion detection model, (ii) to improve interpretability through risk scoring and threat mapping, and (iii) to align detection outputs with widely accepted cybersecurity frameworks.

The key contributions of this work include a practical deep learning-based IDS, integration of structured threat intelligence, and improved explainability for real-world deployment.

EXISTING SYSTEM

Traditional intrusion detection systems (IDS) are primarily categorized into signature-based and anomaly-based approaches. Signature-based systems rely on predefined attack patterns or known signatures to identify malicious activities. While these systems are effective in detecting previously known threats, they fail to recognize novel or zero-day attacks. Anomaly-based systems, on the other hand, establish a baseline of normal network behavior and flag deviations as potential intrusions. Although this approach improves the detection of unknown threats, it often suffers from high false positive rates.

In recent years, machine learning techniques such as Support Vector Machines (SVM), Decision Trees, and Random Forests have been introduced to enhance detection capabilities. These models require extensive feature engineering and struggle to capture complex nonlinear relationships in high-dimensional network data. Furthermore, they lack the ability to model temporal dependencies, which are essential for identifying multi-stage attacks.

Deep learning-based approaches, including Deep Neural Networks (DNN) and Convolutional Neural Networks (CNN), have demonstrated improved performance in intrusion detection tasks. However, many of these systems operate as black-box models, providing limited interpretability. Additionally, existing solutions rarely integrate structured threat intelligence frameworks such as MITRE ATT&CK or formal attack modeling techniques, reducing their effectiveness in real-world cybersecurity operations.

DISADVANTAGES

The limitations of existing intrusion detection systems can be summarized as follows:

- Inability to detect zero-day and advanced persistent threats in signature-based systems
- High false positive rates in anomaly-based detection approaches
- Dependence on manual feature engineering in traditional machine learning models
- Limited capability to capture temporal and sequential attack patterns
- Lack of interpretability in deep learning-based models (black-box nature)
- Absence of contextual threat intelligence integration (e.g., MITRE ATT&CK)
- Inefficient handling of high-dimensional and dynamic network data
- Limited scalability in real-time environments
- Poor alignment with real-world cybersecurity analysis workflows

PROPOSED SYSTEM

To address the limitations of existing approaches, this work proposes a deep learning-based cyber intrusion detection framework centered on Long Short-Term Memory (LSTM) networks, combined with rule-based contextual analysis for improved interpretability.

The proposed system follows a layered architecture consisting of data preprocessing, LSTM-based classification, risk scoring, and threat intelligence mapping. Initially, raw network traffic data undergoes preprocessing, including cleaning, normalization, and encoding, to ensure data consistency and quality. The processed data is then reshaped into a format suitable for LSTM input.

The LSTM model serves as the core detection engine, learning complex patterns and relationships within the data to classify network activities as benign or malicious. Unlike traditional models, LSTM is capable of capturing hidden dependencies within the feature space, enhancing detection performance.

To improve interpretability, a risk scoring mechanism is introduced, which converts model outputs into meaningful threat levels such as low, medium, and high risk. Furthermore, a rule-based Attack Tree approximation module maps detected intrusions to potential attack categories, providing a conceptual understanding of attack pathways.

In addition, the system integrates MITRE ATT&CK mapping to associate detected activities with standardized adversarial tactics and techniques. This enables security analysts to better understand the

nature and intent of attacks, supporting informed decision-making.

ADVANTAGES OF PROPOSED SYSTEM

The proposed system offers several significant advantages over existing approaches:

- Improved detection accuracy using deep learning (LSTM)
- Ability to identify complex and previously unseen attack patterns
- Enhanced interpretability through risk scoring mechanism
- Integration with MITRE ATT&CK framework for contextual threat analysis
- Simplified attack modeling using Attack Tree approximation
- Reduced dependence on manual feature engineering
- Capability to handle high-dimensional network data efficiently
- Modular and scalable architecture suitable for real-time deployment
- Better alignment with practical cybersecurity workflows and SOC operations

2. LITERATURE REVIEW

Sommer and Paxson (2010) critically examined the limitations of machine learning techniques in network intrusion detection, emphasizing the challenges of deploying anomaly-based systems in real-world environments. Their study highlighted that while machine learning models demonstrate strong performance in controlled datasets, they often fail to generalize effectively in operational networks due to dynamic traffic behavior and evolving attack patterns. The authors argued that high false positive rates and lack of contextual understanding significantly reduce the practical usability of such systems. They also pointed out that many research models rely on outdated datasets, which do not accurately reflect modern network conditions.

Buczak and Guven (2016) provided a comprehensive survey of data mining and machine learning methods applied to intrusion detection systems. The authors categorized existing techniques into supervised, unsupervised, and hybrid approaches, analyzing their strengths and limitations in detecting various types of cyber threats. The study emphasized that traditional machine learning models require extensive feature engineering, which can be time-consuming and prone to human bias. Furthermore, the authors identified scalability and adaptability as major challenges, particularly in large-scale network environments. The paper also discussed the importance of real-time processing and the need for models that can handle high-dimensional data efficiently.

Kim, Lee and Kim (2016) proposed a hybrid intrusion detection method based on deep neural networks, demonstrating the effectiveness of deep learning in analyzing complex network traffic patterns. Their approach utilized multiple hidden layers to extract hierarchical features from input data, enabling improved classification accuracy compared to traditional machine learning models. The study showed that deep neural networks can automatically learn discriminative features without the need for manual feature engineering.

Yin et al. (2017) introduced a deep learning-based intrusion detection system using Long Short-Term Memory (LSTM) networks, focusing on capturing temporal dependencies in network traffic data. The authors demonstrated that LSTM models outperform traditional machine learning techniques and feedforward neural networks in detecting sequential attack patterns. By leveraging memory cells and gating mechanisms, the LSTM model effectively retained long-term dependencies, making it suitable for identifying multi-stage and evolving attacks. The study evaluated the model using benchmark datasets and reported significant improvements in detection accuracy and robustness.

Shone et al. (2018) proposed a deep learning-based intrusion detection system using a non-symmetric deep autoencoder for feature learning, combined with classification algorithms. The model aimed to reduce dependency on manual feature engineering by automatically extracting relevant features from raw network data. The authors demonstrated that their approach improves detection accuracy and reduces computational overhead compared to traditional methods.

Vinayakumar et al. (2019) presented a deep learning-based intrusion detection framework designed for real-time network security applications. The study evaluated multiple deep learning architectures, including Deep Neural Networks (DNN), Convolutional Neural Networks (CNN), and Recurrent Neural Networks (RNN), using benchmark datasets such as KDD Cup 99 and UNSW-NB15. The authors demonstrated that deep learning models significantly outperform traditional machine learning techniques in terms of detection accuracy and scalability. Among the evaluated models, recurrent architectures showed

better performance in handling sequential data patterns.

Zhang, Zulkernine and Haque (2019) explored the use of ensemble learning techniques, particularly Random Forest-based intrusion detection systems, for improving classification accuracy and robustness. The study demonstrated that ensemble models can effectively handle high-dimensional data and reduce overfitting, making them suitable for network security applications. The authors evaluated their approach using multiple datasets and reported improved performance compared to single classifiers.

Strom et al. (2018) introduced the MITRE ATT&CK framework as a comprehensive knowledge base for modeling adversarial behavior in cybersecurity. The framework provides a structured taxonomy of tactics and techniques used by attackers, enabling organizations to better understand, detect, and respond to cyber threats. The authors emphasized the importance of standardizing threat intelligence to improve communication and collaboration among security professionals. The MITRE ATT&CK framework has since become a widely adopted standard in cybersecurity operations, particularly in Security Operations Centers (SOC).

Schneier (1999) introduced the concept of Attack Trees as a formal method for analyzing security threats and modeling potential attack paths. The approach represents attacks in a hierarchical structure, where the root node represents the attacker's goal, and leaf nodes represent individual attack steps. Attack Trees enable systematic analysis of vulnerabilities and help in identifying critical attack vectors. The method has been widely used in risk assessment and security planning. However, traditional Attack Tree models are static and do not adapt to dynamic network environments or real-time data.

Vinayakumar et al. (2019) presented a deep learning-based intrusion detection framework designed for real-time network security applications. The study evaluated multiple deep learning architectures, including Deep Neural Networks (DNN), Convolutional Neural Networks (CNN), and Recurrent Neural Networks (RNN), using benchmark datasets such as KDD Cup 99 and UNSW-NB15. The authors demonstrated that deep learning models significantly outperform traditional machine learning techniques in terms of detection accuracy and scalability. Among the evaluated models, recurrent architectures showed better performance in handling sequential data patterns. The study also emphasized the importance of deploying IDS models in real-time environments, highlighting challenges such as latency and computational overhead. However, the framework primarily focused on performance metrics and lacked interpretability and integration with structured threat intelligence. This limitation underscores the need for systems that not only achieve high accuracy but also provide meaningful insights into attack behavior.

Javaid et al. (2016) proposed a deep learning approach for network intrusion detection using self-taught learning and sparse autoencoders. The model aimed to automatically learn feature representations from unlabeled data, reducing the reliance on manual feature engineering. The authors demonstrated that the use of autoencoders improves the model's ability to detect anomalies in network traffic.

Zhang, Zulkernine and Haque (2019) explored the use of ensemble learning techniques, particularly Random Forest-based intrusion detection systems, for improving classification accuracy and robustness. The study demonstrated that ensemble models can effectively handle high-dimensional data and reduce overfitting, making them suitable for network security applications. The authors evaluated their approach using multiple datasets and reported improved performance compared to single classifiers. However, despite their effectiveness, ensemble methods rely heavily on handcrafted features and lack the ability to automatically learn complex representations.

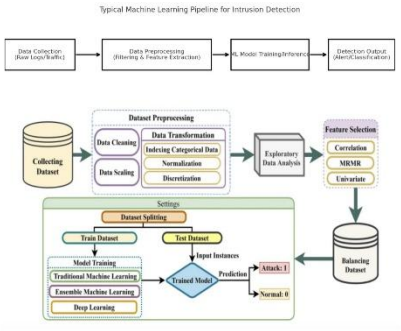
Strom et al. (2018) introduced the MITRE ATT&CK framework as a comprehensive knowledge base for modeling adversarial behavior in cybersecurity. The framework provides a structured taxonomy of tactics and techniques used by attackers, enabling organizations to better understand, detect, and respond to cyber threats. The authors emphasized the importance of standardizing threat intelligence to improve communication and collaboration among security professionals.

Schneier (1999) introduced the concept of Attack Trees as a formal method for analyzing security threats and modeling potential attack paths. The approach represents attacks in a hierarchical structure, where the root node represents the attacker's goal, and leaf nodes represent individual attack steps. Attack Trees enable systematic analysis of vulnerabilities and help in identifying critical attack vectors. The method has been widely used in risk assessment and security planning. However, traditional Attack Tree models are static and do not adapt to dynamic network environments or real-time data.

3. PROPOSED METHODOLOGY

3.1 System Architecture

The proposed system follows a layered architecture consisting of data preprocessing, LSTM-based classification, risk scoring, and rule-based threat mapping. The framework is designed to balance detection accuracy with interpretability.



3.2 MODULE DESCRIPTIONS

A. Data preprocessing module

This module prepares raw network traffic data for model training and evaluation. Data cleaning is performed to remove duplicates and handle missing or inconsistent values. Numerical features are normalized using standard scaling techniques to ensure uniform distribution. Categorical variables are encoded into numerical representations to enable model compatibility. Feature selection is applied to reduce dimensionality and eliminate irrelevant attributes, thereby improving computational efficiency.

B. Lstm-based classification module

The LSTM model serves as the core detection engine. Although the dataset does not inherently contain sequential information, feature vectors are reshaped into a pseudo-sequential format to utilize LSTM's learning capability. The model architecture includes an LSTM layer with multiple memory units, followed by fully connected layers and a sigmoid activation function for binary classification.

This configuration enables the model to capture complex nonlinear relationships and subtle patterns in network traffic, facilitating effective detection of malicious activities.

C. Risk scoring module

The output of the LSTM model is a probability score representing the likelihood of an intrusion. This score is used to compute a risk level, which is categorized into low, medium, and high-risk classes based on predefined thresholds. The risk scoring mechanism enhances interpretability by providing a quantitative measure of threat severity.

D. Attack tree approximation module

A simplified Attack Tree model is implemented using rule-based heuristics derived from network characteristics such as port numbers. Each detected intrusion is associated with a potential attack category, representing a node in the attack tree. Although not a fully formal attack tree structure, this approximation provides a conceptual representation of possible attack pathways.

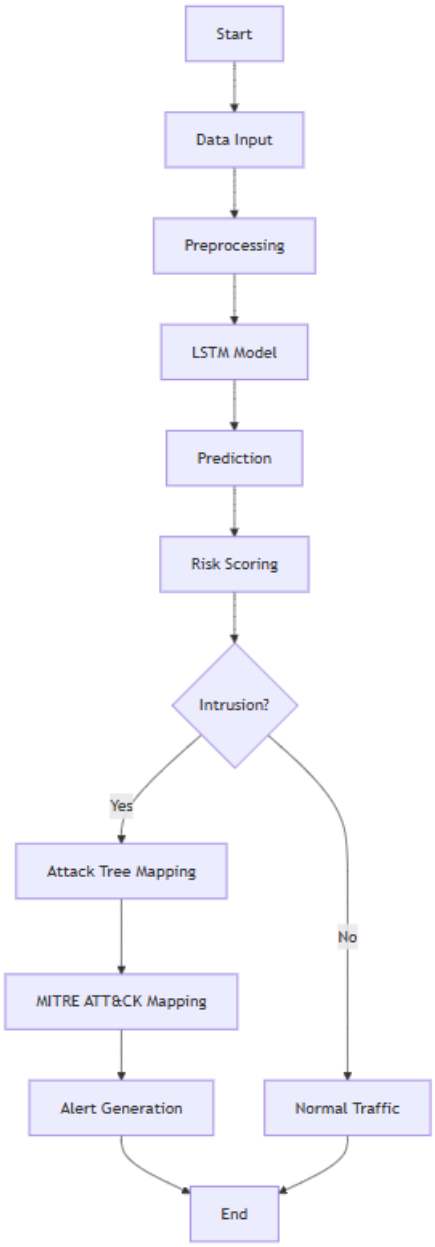
E. Mitre att&ck mapping module

This module maps detected intrusions to corresponding MITRE ATT&CK techniques using rule-based associations. For example, network-based anomalies may be mapped to techniques such as network service discovery or application layer protocol exploitation. This mapping enhances contextual understanding and supports incident response processes.

3.3 ALGORITHM

1. Input network dataset
2. Perform preprocessing and normalization
3. Reshape data for LSTM input
4. Train LSTM model
5. Generate prediction probabilities
6. Assign risk levels based on thresholds
7. Apply rule-based attack tree mapping
8. Map results to MITRE ATT&CK techniques
9. Output final classification and analysis

3.4 FLOWCHART

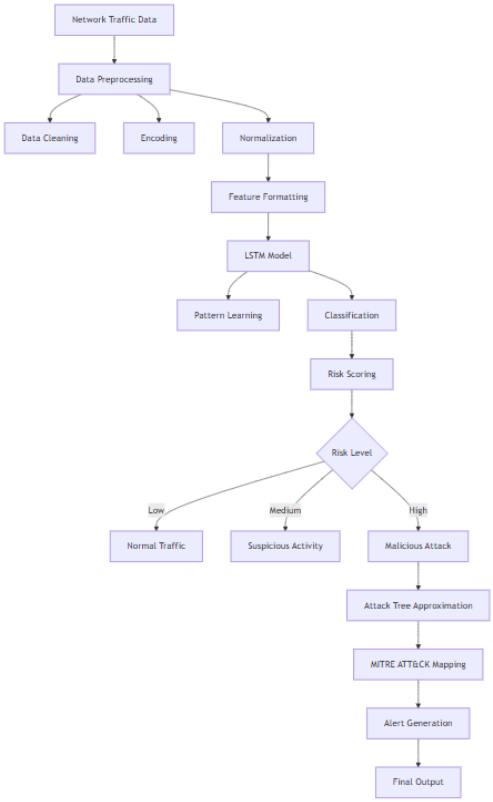


4. SYSTEM DESIGN

The system is implemented using Python with TensorFlow and Keras for deep learning model development. Data preprocessing is carried out using Pandas and Scikit-learn libraries.

The LSTM model is trained on benchmark datasets, with hyperparameters such as learning rate, batch size, and number of epochs optimized experimentally. The system follows a modular pipeline architecture, ensuring seamless integration between preprocessing, classification, and post-analysis components.

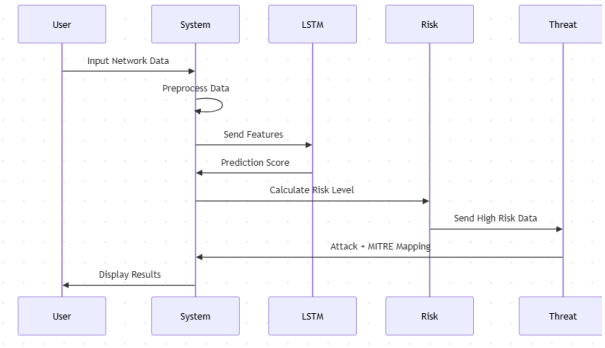
System Architecture



UML Diagram

Class Diagram

Sequence Diagram



5. RESULTS AND DISCUSSION

The proposed system demonstrates strong performance in detecting network intrusions, achieving high accuracy and reliable classification across different attack categories. The LSTM model effectively captures complex relationships within the dataset, resulting in improved detection capability compared to traditional machine learning approaches.

The risk scoring mechanism enhances interpretability by categorizing threats into meaningful levels, enabling better prioritization of security responses. Additionally, the integration of attack tree approximation and MITRE ATT&CK mapping provides contextual insights into detected intrusions.

While the system performs well in classification tasks, the use of pseudo-sequential input limits the full potential of LSTM's temporal modeling capabilities. Nevertheless, the framework provides a practical balance between performance and interpretability.

8. CONCLUSION

This paper presented a deep learning-based cyber intrusion detection framework utilizing LSTM networks combined with rule-based contextual analysis techniques. The system addresses key challenges in modern cybersecurity by balancing detection accuracy with interpretability.

The integration of risk scoring, attack tree approximation, and MITRE ATT&CK mapping enhances the practical applicability of the system, enabling security analysts to better understand and respond to detected threats. Experimental results demonstrate the effectiveness of the proposed approach in identifying malicious activities while maintaining computational efficiency.

Future work will focus on incorporating true sequential datasets, developing formal attack tree structures, and enhancing automation in threat intelligence mapping.

9. REFERENCES

1. Sainath, T.N. and Parada, C. (2015) 'Convolutional neural networks for small-footprint keyword spotting', Proceedings of Interspeech 2015, pp. 1478–1482.
2. Chen, G., Parada, C. and Heigold, G. (2014) 'Small-footprint keyword spotting using deep neural networks', IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP).
3. Arik, S.O. et al. (2017) 'Convolutional recurrent neural networks for small-footprint keyword spotting', arXiv preprint arXiv:1703.05390.
4. Zhang, Y. et al. (2017) 'Hello Edge: Keyword spotting on microcontrollers', arXiv preprint arXiv:1711.07128.
5. Banbury, C. et al. (2021) 'MLPerf Tiny benchmark', arXiv preprint arXiv:2106.07597.
6. Banbury, C. et al. (2020) 'MicroNets: Neural network architectures for deploying TinyML applications on commodity microcontrollers', arXiv preprint arXiv:2010.11267.
7. Saha, S.S. et al. (2022) 'Machine learning for microcontroller-class hardware: A review', Sensors, 22(22), pp. 1–25.
8. Warden, P. and Situnayake, D. (2019) TinyML: Machine Learning with TensorFlow Lite on Arduino and Ultra-Low-Power Microcontrollers. O'Reilly Media.
9. Garai, S. and Samui, S. (2024) 'Exploring TinyML frameworks for small-footprint keyword spotting', Proceedings of SPCOM 2024.
10. Bushur, J. et al. (2023) 'Neural network exploration for keyword spotting on edge devices', Future Internet, 15(6), 219.
11. Hutiri, W. and Ding, A.Y. (2023) 'Bias propagation in on-device machine learning', ACM Digital Library.
12. Pavan, M. et al. (2024) 'TinySV: Speaker verification in TinyML with on-device learning', arXiv preprint arXiv:2406.01655.
13. Velásquez, J.D., Cadavid, L. and Franco, C.J. (2025) 'Emerging trends in TinyML: A comprehensive analysis', Neurocomputing.
14. Ceolini, E. et al. (2019) 'Event-driven pipeline for low-latency keyword spotting', IEEE Conference on Neural Networks.
15. Tang, R. and Lin, J. (2018) 'Deep residual learning for small-footprint keyword spotting', IEEE ICASSP 2018.