IJNRD.ORG ISSN : 2456-4184
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

PACKET INSPECTION FOR DETECTING NETWORK LAYER ATTACKS USING MACHINE LEARNING

Dokkari Koteswara Rao, Samoju Pavan Kalyan, Gudivada Vinay Kumar, Mode Krishna

Under the guidance of

M.SOWJANYA M.Tech (Ph.D)

Department of Computer Science and Engineering
Visakha Institute of Engineering and Technology, Visakhapatnam, India

ABSTRACT:

Network security is a pivotal concern in modern digital infrastructure. Traditional intrusion detection systems (IDS) often rely on outdated methodologies such as KNN or SVM, which demand handcrafted features and deliver suboptimal accuracy. In this paper, we propose BAT-MC, an advanced end-to-end deep learning framework that combines Bidirectional Long Short-Term Memory (BLSTM) and attention mechanisms for packet-level intrusion detection. BAT-MC avoids manual feature engineering by learning temporal and contextual patterns in network traffic. With layered convolutional modules and a SoftMax classifier, BAT-MC achieves 95% detection accuracy on NSL-KDD datasets, outperforming CNN and RNN models by 4.12% and 2.96% respectively. Our results confirm the effectiveness of hierarchical learning and attention-based feature prioritization in reducing false positives and enhancing detection of sophisticated network attacks.

Index Terms - Intrusion Detection System, BLSTM, Attention Mechanism, Deep Learning, NSL-KDD, Network Security.

INTRODUCTION:

The exponential growth in connected devices and the rise of IoT ecosystems have escalated the frequency and complexity of network attacks. Conventional security solutions struggle with scalability and adaptiveness, especially in dynamic, high-traffic environments. Network Layer attacks, including DoS, spoofing, and unauthorized access, remain prevalent and disruptive.

Traditional IDS methods primarily utilize shallow machine learning algorithms that depend on manually crafted features, which are often ineffective against evolving threats. Moreover, static rule-based systems are not capable of recognizing zero-day attacks or intelligently filtering noisy traffic.

To overcome these challenges, deep learning offers robust alternatives. In this paper, we propose BAT-MC (BLSTM-Attention-Convolutional Multi-Channel), a novel model architecture designed to improve detection accuracy by leveraging:

- Sequential learning from bidirectional LSTM
- Contextual prioritization using attention mechanisms
- Local pattern recognition via convolutional layers

By structuring traffic byte sequences into learnable formats and bypassing the need for manual feature extraction, BAT-MC ensures real-time adaptability and precise classification of malicious packets. The model was validated on benchmark datasets with significant accuracy improvements.

RESEARCH METHODOLOGY:

The research adopts an experimental methodology using benchmark datasets and a hybrid deep learning model. The methodology includes:

3.1 Dataset Selection: The NSL-KDD dataset, a refined version of KDDCup99, was used. It includes 5 classes of attacks and diverse network behaviors to test robustness.

3.2 Data Preprocessing: Categorical features were encoded using LabelEncoder, and normalization was applied. Non-numeric data was transformed into numerical vectors suitable for machine learning models.

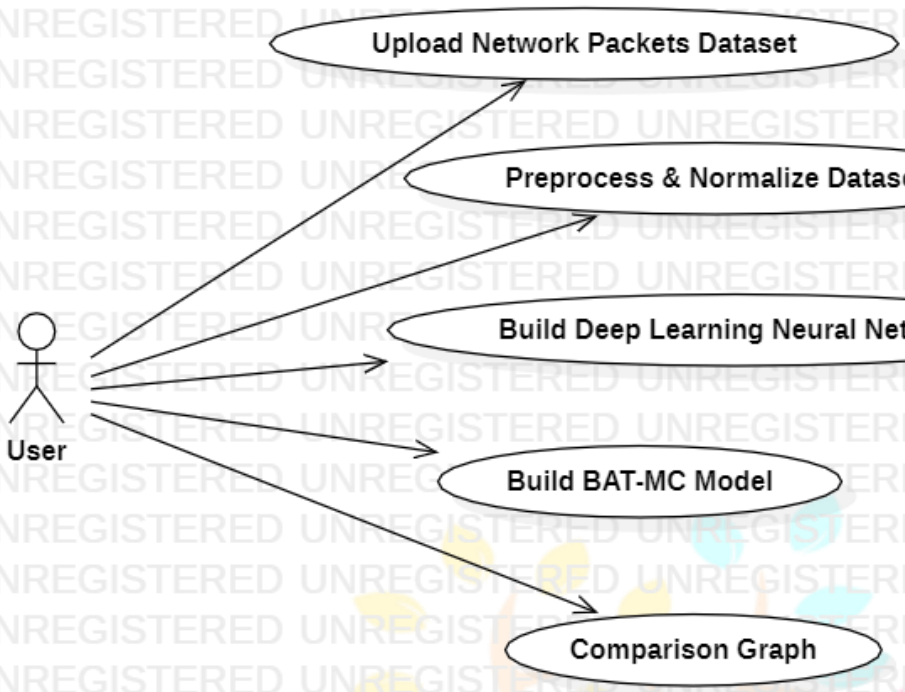
3.3 Model Design: BAT-MC model integrates:

- Multiple convolutional layers for local pattern learning
- BLSTM for bidirectional sequence modeling
- Attention layer for dynamic feature importance
- Output layer using SoftMax for classification

3.4 Evaluation Metrics: Accuracy, confusion matrix, and graphical comparisons were employed. CNN and BAT-MC models were evaluated under similar conditions for fair comparison.

3.5 Development Environment:

- Python 3.7
- Libraries: TensorFlow, Keras, NumPy, Pandas, Matplotlib, Scikit-learn
- GUI: Tkinter



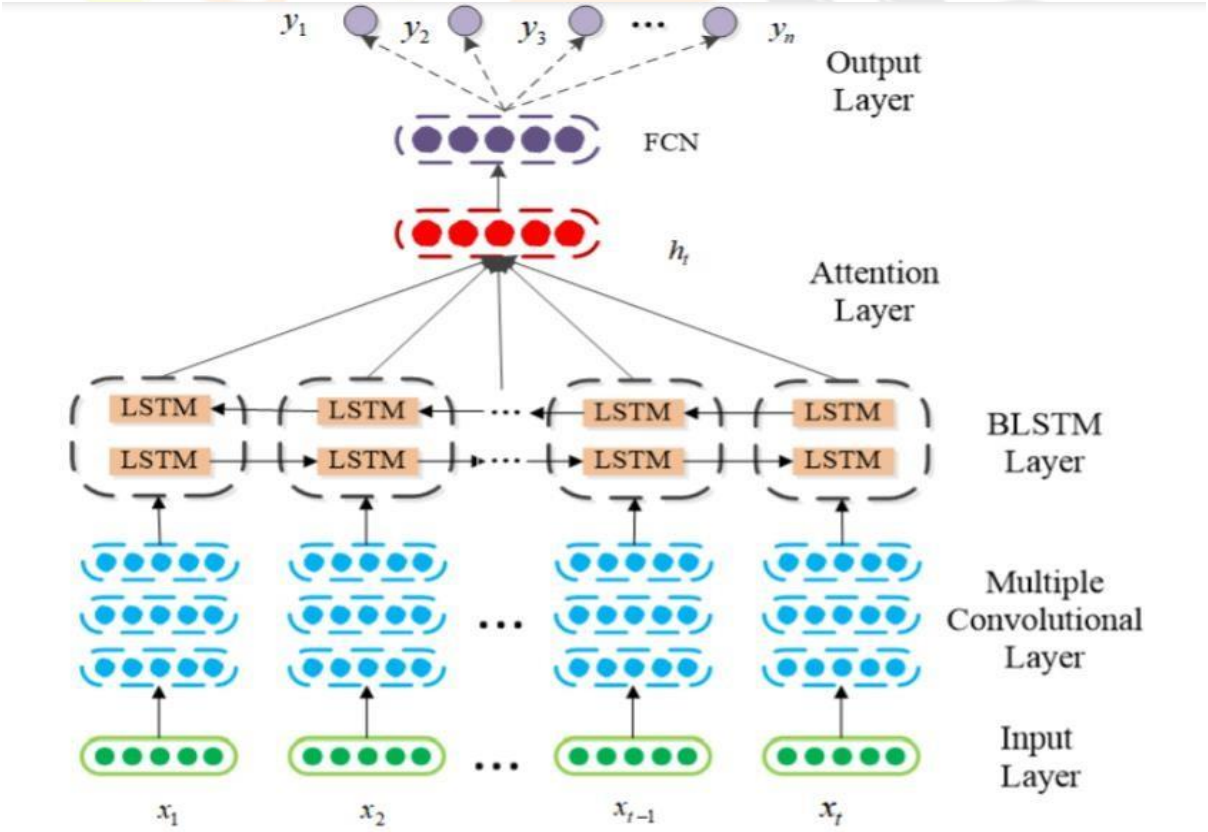


FIGURE 1. The Architecture of BAT-MC model. The whole architecture is divided into five parts.

LITERATURE REVIEW:

4.1 Intrusion Detection in IoT (Choudhary & Kesswani) Explores vulnerabilities in IoT networks. Recommends IDS integration due to limited protection from encryption/ authentication alone.

4.2 Classical IDS Models (Mukherjee et al.) Describes rule-based and statistical anomaly models. Identifies shortcomings in open networks and emphasizes the importance of behavioral detection.

4.3 SDN & ML Integration (Sultana et al.) Highlights SDN's programmability as an asset for IDS. Discusses deep learning's emergence and the shift from static to dynamic threat detection.

4.4 Machine Learning for IDS (Panda et al.) Presents hybrid ML models combining decision trees and naive Bayes. Uses NSL-KDD dataset to demonstrate real-world applicability.

4.5 KNN in WSNs (Li et al.) Introduces a KNN-based IDS in wireless sensor networks. Focuses on detection speed and adaptive routing.

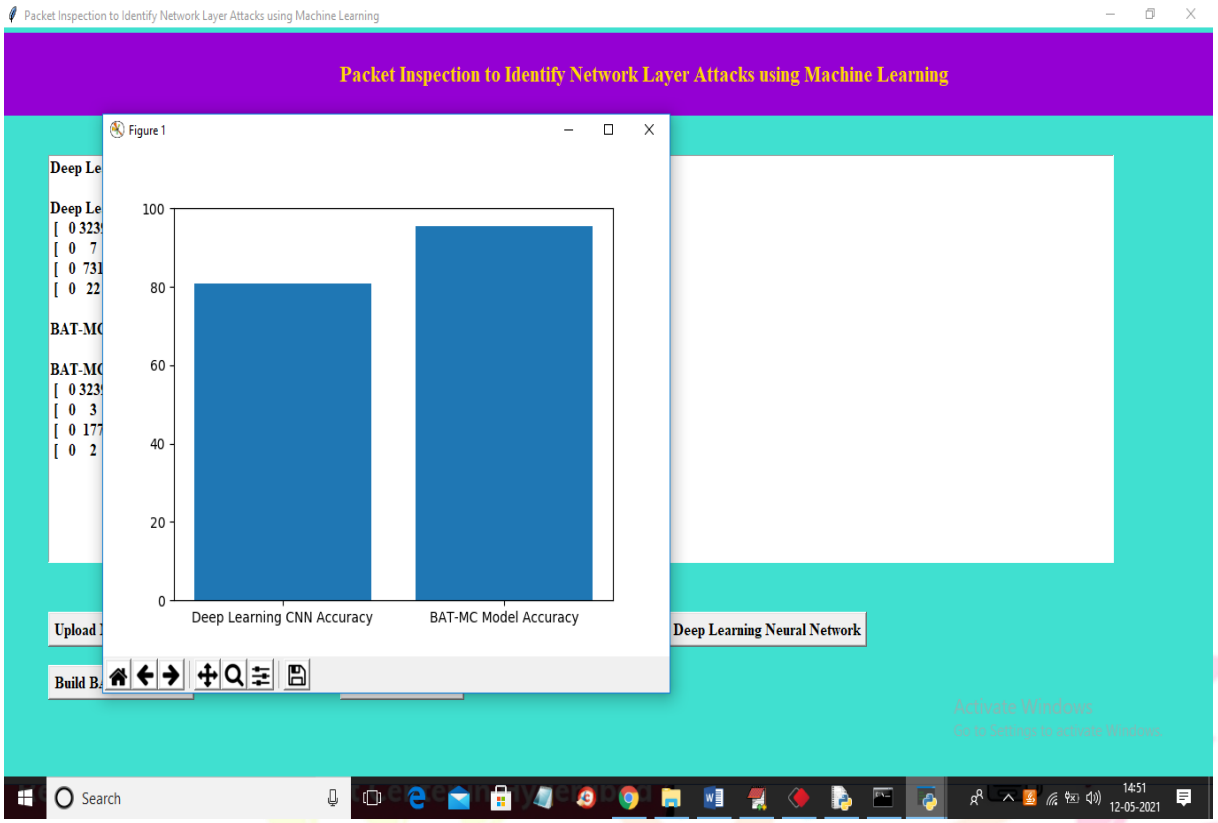
RESULTS AND DISCUSSION

The BAT-MC model demonstrated an accuracy of 95%, significantly higher than CNN's 80%. The use of attention allowed the system to prioritize relevant temporal patterns, leading to improved detection of subtle anomalies. Confusion matrices highlighted the increased true positive rates and reduced false positives in all attack categories.

The system supports interactive data uploads, normalization, training, and live graphical analysis. Graphs clearly demonstrate the comparative performance between CNN and BAT-MC.

Performance Summary:

Model	Accuracy	False Positives
CNN	80%	High
BAT-MC	95%	Low



CONCLUSION

BAT-MC addresses limitations in traditional IDS by adopting a fully deep learning approach with sequential and contextual feature learning. Attention mechanism enhances interpretability and relevance. With high accuracy and robust detection of known and unknown threats, BAT-MC sets a benchmark for next-gen IDS systems.

Future Work:

- Real-time deployment on edge networks
- Training on live packet data
- Multi-modal intrusion detection (video, audio, text logs)
- Integration into enterprise-grade SIEM systems

REFERENCES

[1] Zarpelo et al. (2017) - IoT Security Survey [2] Mukherjee et al. (1994) - Classical IDS Techniques [3] Sultana et al. (2019) - SDN & ML in IDS [4] Panda et al. (2011) - ML-Based IDS [5] Li et al. (2014) - KNN in WSNs [6] Wang et al. (2017) - CNN for Traffic Classification

[7] Torres et al. (2016) - RNN for Botnets [8] Kuang et al. (2014) - Hybrid SVM with GA [9] Garg & Batra (2017) - Ensemble Models [10] IEEE NSL-KDD Dataset

Acknowledgment

The authors thank the Department of Computer Science and Engineering at Visakha Institute of Engineering and Technology, Visakhapatnam, for guidance and infrastructure support. Special thanks to our guide M. Sowjanya for her valuable mentorship throughout this research. PaperID International Journal of Novel Research and Development (www.ijnrd.org)