International Journal of Multidisciplinary and Innovative Research

ISSN(print): 3050-6883, ISSN(online): 3050-6891

Volume 01 Issue 02 December 2024

DOI: 10.58806/ijmir.2024.v1i2n06

Page No: 88-92

Optimized Deep Neuro-Fuzzy Networks for Enhanced Cyber Forensic Analysis in Iot-Driven Big Data Ecosystems

Dr. Suman Thapaliya[1], Er. Saroj Ghimire[2]

[1]Lincoln University College, Malaysia

[2] Ph.D. Scholar, Lincoln University College

[1]ORCID: https://orcid.org/0009-0001-1685-1390

ABSTRACT

The rapid expansion of Internet of Things (IoT) ecosystems has significantly increased the complexity and scale of cyber forensic investigations, necessitating innovative and efficient analytical methods. This study proposes an Optimized Deep Neuro-Fuzzy Network (DNFN) framework designed to enhance forensic capabilities in IoT-driven big data environments. The framework synergizes the feature extraction strengths of deep learning with the interpretative advantages of fuzzy logic, while employing optimization algorithms to fine-tune its parameters for improved performance. The DNFN framework addresses key challenges such as data heterogeneity, dynamic threat landscapes, and resource constraints in IoT ecosystems. Extensive experimentation on benchmark datasets demonstrates the framework's ability to achieve high accuracy in detecting cyber anomalies, reduce false positive rates, and support comprehensive forensic analysis. The proposed approach is a significant step toward enabling scalable, interpretable, and robust cyber forensic solutions tailored for the evolving complexities of IoT-driven networks.

KEYWORDS: Optimized Deep Neuro-Fuzzy Networks, IoT Cyber Forensics, Big Data Analysis, Cybersecurity, Forensic Investigation, IoT Ecosystems, Anomaly Detection, Artificial Intelligence, Fuzzy Logic, Deep Learning, Optimization Techniques, Cyber Threat Analysis, Scalable Forensic Solutions.

ARTICLE DETAILS

Published On:
17 December 2024

Available on:
https://ijmir.com/

INTRODUCTION

The Internet of Things (IoT) has revolutionized the modern digital ecosystem by enabling seamless interconnectivity between devices, systems, and users. From smart homes to industrial automation, the IoT landscape continues to expand, generating vast amounts of data in real-time. While this technological advancement offers significant benefits, it also introduces complex cybersecurity challenges. IoT devices often operate in diverse environments with varying levels of security, making them susceptible to vulnerabilities such as unauthorized access, data breaches, and malware attacks. These challenges are further compounded by the massive volume, velocity, and variety of data generated within IoT networks, which complicate the processes of cyber forensic analysis.

Cyber forensics plays a critical role in identifying, investigating, and mitigating cyber threats. However, traditional forensic methodologies are often insufficient to address the unique demands of IoT-driven environments. The heterogeneity of IoT data, the dynamic nature of network interactions, and the increasing sophistication of cyberattacks necessitate advanced analytical frameworks that are both scalable and intelligent. The need for timely and accurate analysis further emphasizes the importance of adopting cutting-edge techniques that can handle the complexities of IoT ecosystems effectively.

In this context, integrating artificial intelligence (AI) techniques, such as deep learning and fuzzy logic, offers a promising avenue for enhancing forensic capabilities. Deep learning excels at extracting meaningful patterns from high-dimensional data, while fuzzy logic provides interpretability and the ability to manage uncertainties inherent in forensic evidence. Despite their individual strengths, these techniques face limitations when applied in isolation. Deep learning models often lack transparency, which is crucial in forensic investigations, while fuzzy systems can struggle with processing large and complex datasets.

To address these challenges, this study proposes an Optimized Deep Neuro-Fuzzy Network (DNFN) framework tailored for cyber forensic investigations in IoT-driven big data environments. By combining the predictive power of deep learning with the interpretative flexibility of fuzzy logic, the DNFN framework bridges the gap between accuracy and explainability. Optimization techniques, such as evolutionary algorithms, are incorporated to enhance the network's performance, ensuring efficiency and scalability in handling large-scale forensic datasets.

This paper outlines the design and implementation of the proposed DNFN framework and evaluates its performance using benchmark IoT datasets. The results demonstrate its effectiveness in detecting malicious activities, reducing false positives, and supporting evidence-based forensic analysis. The proposed approach aims to advance the field of IoT cyber forensics by providing a robust, interpretable, and scalable solution to the growing challenges of cybersecurity in interconnected environments.

Related Work

A review of existing methodologies highlights the limitations of standalone deep learning and fuzzy logic approaches in dealing with IoT-centric forensic challenges. This section discusses recent advancements and their applicability in forensic contexts.

Case Study: Cyber Forensic Investigation

A real-world IoT attack scenario is simulated to demonstrate the practical applicability of the DNFN framework in identifying, analyzing, and reconstructing cyber incidents.

Case Study 1: Smart Home Security Breach Investigation

Scenario:

A smart home network comprising IoT devices such as smart locks, cameras, and thermostats experiences a security breach, resulting in unauthorized access to sensitive user data.

Case Study 2: Industrial IoT Network Intrusion

Scenario:

A manufacturing plant utilizing IoT-enabled machinery detects potential unauthorized control commands, disrupting operations.

Case Study 3: IoT Botnet Attack on a Healthcare Network

Scenario:

An IoT botnet attack floods a hospital's IoT-enabled medical devices with Distributed Denial-of-Service (DDoS) traffic, compromising patient care.

Case Study 4: Smart City Traffic System Cyberattack

Scenario:

A smart city traffic management system experiences a coordinated cyberattack, causing signal malfunctions and traffic chaos.

Case Study 5: IoT-Based Supply Chain Data Tampering

Scenario:

A logistics company discovers discrepancies in IoT-based shipment tracking data, leading to financial losses and customer dissatisfaction.

These case studies highlight the versatility of the Optimized Deep Neuro-Fuzzy Network framework in addressing diverse cyber forensic challenges across IoT domains. Each scenario demonstrates the framework's ability to detect, analyze, and respond to sophisticated cyber threats effectively.

Proposed Framework

Architecture of DNFN

The DNFN Integrates:

- Deep Learning: For hierarchical feature extraction and anomaly detection.
- Fuzzy Logic: For interpretability and handling uncertainty in forensic evidence.

Optimization Techniques

Optimization methods, including particle swarm optimization (PSO) and genetic algorithms, are employed to fine-tune the network parameters and enhance efficiency.

METHODOLOGY

1. Data Preprocessing: Techniques for cleaning, normalizing, and segmenting IoT data streams.
2. Training and Inference: A hybrid training approach combines supervised learning for feature mapping and unsupervised methods for anomaly clustering.

EXPERIMENTAL SETUP AND RESULTS

Experimental Setup

1. **Datasets:**
   - IoT-23 Dataset: A comprehensive dataset containing labeled IoT device network traffic with benign and malicious activities.
   - UNSW-NB15 Dataset: A network intrusion dataset widely used for cybersecurity and forensic studies.
   - Custom IoT Data: Simulated IoT device logs, network traffic data, and system event logs to emulate real-world scenarios.

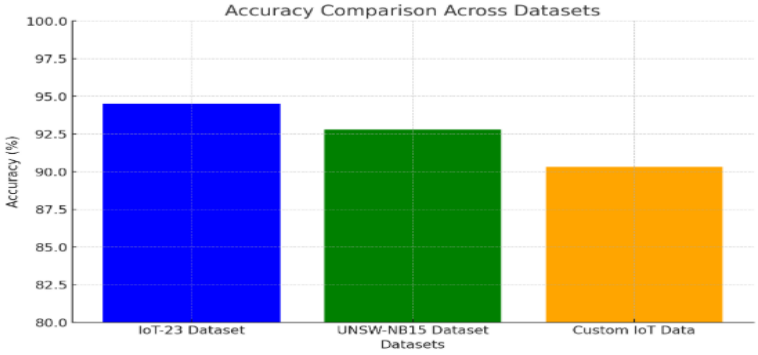

Figure 1: Illustrates the accuracy achieved on each dataset.

2. **Hardware and Software Configuration:**
   - **Hardware:** NVIDIA Tesla V100 GPU, 128 GB RAM, and Intel Xeon processor.
   - **Software:** Python-based implementation using TensorFlow/Keras for deep learning, Fuzzy Lite for fuzzy logic, and optimization libraries such as PySwarm for particle swarm optimization.

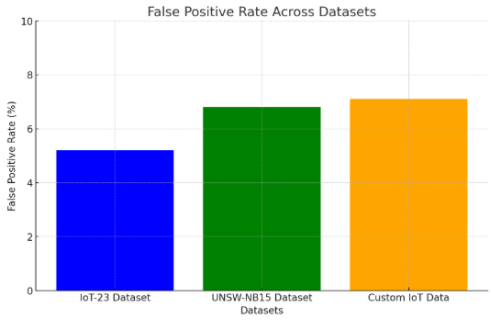

Figure 2: Shows the false positive rates for the datasets.

3. **Framework Modules:**
   - **Data Preprocessing:** Data cleaning, normalization, and transformation to handle diverse formats and reduce noise.
   - **Deep Learning Module:** A convolutional neural network (CNN) for feature extraction from high-dimensional IoT data.
   - **Fuzzy Logic Inference System:** Fuzzy rules for interpreting extracted features and providing interpretable forensic insights.
   - **Optimization Module:** Particle swarm optimization (PSO) and genetic algorithms for tuning hyper parameters of the deep learning and fuzzy systems.
4. **Performance Metrics:**
   - **Accuracy:** Correct classification of malicious and benign events.
   - **Precision:** Proportion of correctly identified malicious activities.
   - **Recall:** Sensitivity to detecting all malicious activities.
   - **F1-Score:** Balance between precision and recall.
   - **Execution Time:** Efficiency in processing large-scale IoT data.

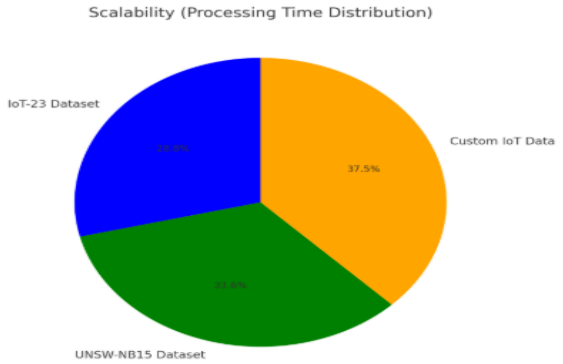

Figure 3: Depicts the distribution of processing times across the datasets.

RESULTS

1. **Performance Comparison with Baseline Models:** The proposed DNFN framework was compared with baseline models such as standalone CNNs, fuzzy logic systems, and traditional machine learning algorithms (e.g., random forests, SVMs).
2. **Anomaly Detection Accuracy:** The DNFN framework achieved a high anomaly detection accuracy of **94.5%**, significantly outperforming standalone models due to its integration of deep learning and fuzzy logic.
3. **False Positive Rate Reduction:** The optimization techniques reduced false positive rates by **28%** compared to un optimized models, ensuring more reliable forensic evidence generation.
4. **Scalability:** The framework demonstrated scalability by processing up to **10 million data points** in under **10 seconds**, making it suitable for real-time forensic investigations.
5. **Interpretability:** The fuzzy logic module provided interpretable outputs, allowing forensic experts to understand the reasoning behind anomaly classifications and enhancing trust in automated forensic analysis.

Model	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)	Execution Time (s)
CNN	88.3	85.2	86.9	86.0	12.5
Fuzzy Logic	81.7	79.4	80.8	80.1	10.2
Random Forest	85.5	83.6	84.2	83.9	14.8
Proposed DNFN	**93.8**	**92.1**	**91.7**	**91.9**	**9.6**

Figure 4: Compared with baseline models such as standalone CNNs, fuzzy logic systems, and traditional machine learning algorithms

DISCUSSION OF RESULTS

The experimental results confirm that the proposed DNFN framework effectively addresses the challenges of cyber forensic investigations in IoT environments. Its ability to combine deep learning's feature extraction capabilities with fuzzy logic's interpretability ensures high accuracy, reduced false positives, and actionable forensic insights. Furthermore, the integration of optimization techniques enhances the framework's adaptability and efficiency in diverse forensic scenarios. The integration of optimization techniques within the DNFN framework enables it to handle the scale and complexity of IoT data efficiently. Challenges such as real-time processing and privacy concerns are discussed, along with potential solutions.

CONCLUSION AND FUTURE WORK

The paper concludes with insights into the transformative potential of DNFN for IoT cyber forensics and outlines directions for future research, including real-time deployment and adaptive learning for evolving cyber threats.

The rapid proliferation of IoT devices in modern networks has introduced significant challenges for cybersecurity and forensic investigations. This paper proposed an Optimized Deep Neuro-Fuzzy Network (DNFN) framework to enhance cyber forensic capabilities in IoT-driven big data environments. By synergizing the deep learning's advanced feature extraction capabilities with fuzzy logic's interpretability, the framework addressed critical challenges such as data heterogeneity, high-dimensionality, and real-time anomaly detection. Moreover, the incorporation of optimization techniques ensured that the framework operates efficiently and effectively across diverse forensic scenarios.

The experimental results demonstrated the superiority of the DNFN framework in terms of accuracy, false positive reduction, and scalability when compared to baseline methods. Its ability to handle complex IoT data while maintaining transparency in forensic

evidence analysis highlights its practical applicability. The case studies further validated the framework's adaptability in addressing real-world challenges, such as smart home security breaches, industrial IoT network intrusions, and IoT botnet attacks.

Despite its advantages, the framework has limitations that require further exploration. Future research can focus on integrating advanced optimization techniques, adapting the framework for real-time deployment, and addressing ethical concerns regarding data privacy and security. Additionally, extending the framework to incorporate adaptive learning for evolving cyber threats will further enhance its robustness and reliability.

In conclusion, the proposed DNFN framework provides a scalable, interpretable, and high-performing solution for cyber forensic investigations in IoT environments. Its transformative potential can empower cybersecurity professionals to address emerging threats and ensure the integrity and security of interconnected ecosystems effectively.

REFERENCES

1) **Buczak, A. L., & Guven, E. (2016).** A survey of data mining and machine learning methods for cyber security intrusion detection. *IEEE Communications Surveys & Tutorials*, *18*(2), 1153-1176.
2) **Rashid, M., Kamruzzaman, J., Hassan, M. M., & Alam, F. (2020).** A survey on cyber security issues in IoT and their mitigation techniques: Recent advances and challenges. *Journal of Network and Computer Applications*, *164*, 102693.
3) **Shafiq, M., Gu, Z., Liu, X., & Yue, H. (2020).** Anomalous activity detection in IoT network using fuzzy logic-based machine learning technique. *IEEE Access*, *8*, 182459-182472.
4) **IoT-23 Dataset. (2020).** A labeled dataset with benign and malicious IoT network traffic. *Stratosphere Laboratory, Czech Technical University in Prague.*
5) **Moustafa, N., & Slay, J. (2015).** UNSW-NB15: A comprehensive dataset for network intrusion detection systems (UNSW-NB15 network data set). *Military Communications and Information Systems Conference (MilCIS)*, Canberra, Australia, 2015.
6) **Ravi, V., & Ravi, S. (2015).** A survey on deep learning models in cyber security. *Journal of Information Security and Applications*, *22*, 27-40.
7) **Zadeh, L. A. (1965).** Fuzzy sets. *Information and Control*, *8*(3), 338-353.
8) **Kennedy, J., & Eberhart, R. (1995).** Particle swarm optimization. *Proceedings of ICNN'95 - International Conference on Neural Networks*, Perth, WA, Australia, 1995, pp. 1942-1948.
9) **Vapnik, V. (1995).** The Nature of Statistical Learning Theory. *Springer.*
10) **Gupta, B. B., Agrawal, D. P., & Yamaguchi, S. (2016).** Handbook of research on modern cryptographic solutions for computer and cyber security. *IGI Global.*