ISSN: **3107-6513**

AI-Driven Intrusion Detection and Prevention Framework for Cloud-Fog-IoT Integrated systems: A Comprehensive Review and Future Research Directions

Chethana ganga N S
PhD Scholar, School of computer Science and Engineering
REVA UNIVERSITY, Bengaluru, India
nishachethu98@gmail.com

***Abstract*-The convergence of Cloud, Fog, and Internet of Things (IoT) technologies has enabled scalable, low-latency, and intelligent distributed systems. However, this integration has significantly expanded the attack surface, exposing systems to sophisticated cyber threats such as distributed denial-of-service (DDoS), botnets, and advanced persistent threats (APTs). Traditional intrusion detection systems (IDS) are inadequate due to their inability to handle dynamic, heterogeneous, and large-scale environments. This paper presents a comprehensive survey of Artificial Intelligence (AI)-driven Intrusion Detection and Prevention Systems (IDPS) in Cloud–Fog–IoT ecosystems. It critically analyzes deep learning, reinforcement learning, and federated learning-based approaches, identifies key limitations, and proposes a novel multi-layer AI-driven IDPS framework. The proposed architecture incorporates distributed intelligence, adaptive learning, and automated mitigation mechanisms to achieve enhanced security, scalability, and real-time responsiveness. Furthermore, this work introduces a hybrid AI model integrating CNN, LSTM, and Deep Reinforcement Learning (DRL), supported by federated learning for privacy preservation. Experimental considerations, research gaps, and future directions are also discussed.**

Keywords: AI Security, Intrusion Detection System, Intrusion Prevention System, Cloud Security, Fog Computing, IoT Security, Deep Learning, Federated Learning, Reinforcement Learning

I.INTRODUCTION

The rapid proliferation of IoT devices combined with cloud and fog computing paradigms has led to the emergence of complex distributed systems known as Cloud–Fog–IoT ecosystems. These systems enable efficient data processing, storage, and analytics but introduce significant security challenges due to their distributed nature, heterogeneous components, and resource constraints.

IoT devices often lack robust security mechanisms, making them vulnerable to attacks such as botnets and unauthorized access. Cloud computing provides centralized resources but suffers from latency and bandwidth limitations. Fog computing bridges this gap by enabling edge-level processing, thereby improving response time and reducing network congestion.

Conventional IDS approaches, including signature-based and anomaly-based methods, are insufficient in addressing modern cyber threats due to their static nature and inability to adapt to evolving attack patterns.

This literature review explores state-of-the-art AI-based intrusion detection approaches, focusing on deep learning models, multi-layer security frameworks, and explainable AI (XAI) techniques for Cloud–Fog–IoT ecosystems.

1.1 Intrusion Detection in Cloud–Fog–IoT Systems

Intrusion detection is a critical component in securing distributed systems. Existing approaches can be broadly categorized into signature-based and anomaly-based detection systems.

a. Machine Learning-Based IDS

Traditional machine learning techniques such as Support Vector Machines (SVM), Decision Trees, and Random Forests have been widely used for intrusion detection. Advantages of this security system includes that it is effective for known attack patterns and lower computational requirements. This method has a disadvantages like poor performance on zero-day attacks and requires manual feature engineering.

b. Deep Learning-Based IDS

Deep learning has significantly improved detection accuracy by automatically learning complex patterns from large-scale data. The major different models in this method includes, Convolutional Neural Network, Used for feature extraction and spatial pattern recognition in network traffic data. Recurrent Neural Network, Effective in capturing temporal dependencies in sequential network traffic. Autoencoders, Used for anomaly detection by reconstructing normal behavior and identifying deviations. Deep Belief Networks (DBNs): Capable of hierarchical feature learning for complex attack detection.

c. Hybrid and Ensemble Models

Recent research focuses on combining multiple models to improve robustness and accuracy. Combination of CNN and LSTM architectures is suitable for spatial-temporal learning. It

ensemble learning for reducing false positives and federated learning is suitable for distributed environments.

1.2 Intrusion Prevention Mechanisms

Beyond detection, prevention mechanisms are integrated to actively mitigate attacks. Automated response systems using reinforcement learning can be used. Software-defined networking (SDN)-based traffic control and Policy-based access control and dynamic firewalling .

Fog-Based Security Architectures

Fog computing acts as an intermediate layer between IoT devices and cloud systems. It enables low-latency threat detection , supports distributed IDS deployment and reduces burden on centralized cloud systems

II.COMPARITIVE ANALYSIS OF EXISTING METHOD

The literature on AI-driven intrusion detection and prevention systems highlights a significant evolution from traditional machine learning techniques to advanced deep learning approaches for securing Cloud–Fog–IoT environments.

Early studies such as [1] provide a comprehensive overview of machine learning and data mining methods for intrusion detection, emphasizing their effectiveness but also their limitations in handling dynamic and large-scale cyber threats. To address these issues, deep learning-based approaches have been introduced. For instance, [2] and [11] demonstrate that neural network-based models significantly improve detection accuracy by automatically learning complex attack patterns.

Sequential models like RNN and LSTM have been explored in [3] and [9], showing strong capability in capturing temporal dependencies in network traffic, which is essential for detecting sophisticated and evolving attacks. Additionally, anomaly detection techniques using autoencoders, as presented in [8], reduce reliance on manual feature engineering and enhance detection of unknown threats.

The availability of realistic datasets plays a crucial role in IDS development. The UNSW-NB15 dataset introduced in [4] addresses the limitations of earlier datasets and provides a more comprehensive benchmark for evaluating intrusion detection systems.

Real-time and IoT-specific intrusion detection has been explored in [6], where machine learning techniques are applied to detect DDoS attacks in IoT devices. Furthermore, [5] proposes an online deep learning-based IDS capable of continuous learning from streaming data, making it suitable for dynamic environments.

The integration of fog computing into security frameworks is highlighted in [7], which emphasizes distributed intrusion detection for reducing latency and improving scalability in fog-to-things environments.

Another emerging direction is the incorporation of Explainable AI (XAI), as discussed in [10], which addresses the lack of transparency in deep learning models and enhances trust in AI-based security systems.

Overall, the literature indicates that while deep learning techniques significantly improve detection accuracy and adaptability, challenges such as scalability, real-time processing, high false positives, and lack of explainability still persist. These gaps motivate the need for a unified, scalable, and explainable AI-driven intrusion detection and prevention framework for Cloud–Fog–IoT systems.

III.EMERGING TRENDS AND CHALLENGES-GAPS

a. Heterogeneity of IoT Devices
Gap: Diverse devices with varying capabilities and protocols complicate unified security implementation.
Impact: Difficulty in deploying standardized IDS models.
Potential Solutions: Lightweight AI models and protocol-aware detection systems.
b. Real-Time Threat Detection
Gap: Achieving low-latency detection in distributed environments remains challenging.
Impact: Delayed responses can lead to severe system compromise.
Potential Solutions: Edge and fog-based processing with optimized deep learning models.
c. Scalability Issues
Gap: Existing IDS frameworks struggle to scale across large IoT networks.
Impact: Performance degradation and increased false positives.
Potential Solutions: Distributed and hierarchical IDS architectures.
d. Data Privacy and Security
Gap: Centralized data processing raises privacy concerns.
Impact: Risk of sensitive data exposure.
Potential Solutions: Federated learning and privacy-preserving AI techniques.
e. Lack of Explainability (XAI)
Gap: Deep learning models operate as black boxes.
Impact: Difficult for security analysts to interpret decisions.
Potential Solutions: Integration of Explainable AI (XAI) techniques such as SHAP and LIME.

IV.OBJECTIVIES OF THE PROPOSED RESEARCH

4.1.DEVELOP INTELLIGENT DETECTION MODELS THAT OPERATE AT DIFFERENT LAYERS WITH VARYING COMPUTATIONAL CAPABILITIES.

Key Contributions

- IoT Layer: Lightweight anomaly detection models and Energy-efficient algorithms
- Fog Layer: Low-latency models (e.g., shallow CNN, Random Forest) and Real-time filtering and early attack detection

- Cloud Layer: Advanced deep learning models such as CNN (feature extraction) , LSTM (temporal analysis) , Autoencoders (anomaly detection) . Hybrid models includes CNN and LSTM.

4.2 DESIGN MULTI-LAYER THREAT DETECTION MODELS USING DEEP LEARNING TECHNIQUES ACROSS CLOUD, FOG, AND IOT LAYERS.

Key Contributions includes Create a multi-layer architecture:

- IoT Layer → Data collection
- Fog Layer → Real-time detection
- Cloud Layer → Deep analysis and intelligence

This technique includes interoperability across heterogeneous devices, Enable centralized monitoring with distributed intelligence

4.3 INTEGRATE EXPLAINABLE AI (XAI) MECHANISMS AND SCALABLE AI MODELS TO PROVIDE INTERPRETABLE AND TRANSPARENT DECISION-MAKING.

Key Contributions includes, Implement XAI techniques such as SHAP (Shapley Additive Explanations), LIME (Local Interpretable Model-Agnostic Explanations). It also includes Identify key features influencing attack detection, Develop visual dashboards for security analysts.

V.DETAILED METHODOLOGY FOR AI-DRIVEN IDPS IN CLOUD–FOG–IOT SYSTEMS

A. OVERALL RESEARCH DESIGN

The proposed methodology follows a multi-layer hierarchical architecture consisting of:

- IoT Layer → Data generation
- Fog Layer → Real-time lightweight detection
- Cloud Layer → Deep learning + explainability + global intelligence

The system integrates:

- Hybrid deep learning models
- Distributed detection
- Explainable AI (XAI)

B. METHODOLOGY ADDRESSING EACH RESEARCH GAP

Gap 1: Heterogeneity of IoT Devices

Problem: Different devices generate diverse data formats and protocols.

Methodology

Step 1: Unified Data Representation Layer

- Convert heterogeneous data into a common feature schema
- Use:
  - Protocol normalization
  - Feature standardization

Step 2: Feature Abstraction

- Apply embedding techniques:
  - Learned feature embeddings using neural networks
  - Protocol-independent feature extraction

Step 3: Lightweight Edge Models

Deploy device-specific micro-models

Use:

TinyML

Model quantization (8-bit/16-bit)

Gap 2: Real-Time Threat Detection

Problem: High latency reduces effectiveness.

Methodology

Step 1: Fog-Based Detection

- Deploy lightweight IDS at fog nodes
- Use: Shallow CNN / Random Forest

Step 2: Stream Processing

- Implement:

Sliding window analysis

- Online learning

Step 3: Early Filtering Mechanism

- Classify traffic into:
  - Benign → Forward
  - Suspicious → Escalate to cloud

Gap 3: Scalability Issues

Problem: System performance degrades with large-scale networks.

Methodology

Step 1: Distributed IDS Architecture

- Deploy IDS across:
  - Multiple fog nodes
  - Cloud clusters

Step 2: Load Balancing

Use:

- Traffic partitioning
- Distributed queues (Kafka-like models)

Step 3: Hierarchical Detection

- Tier 1: IoT filtering
- Tier 2: Fog detection
- Tier 3: Cloud analysis

Gap 4: Data Privacy and Security

Problem: Centralized data processing risks data exposure.

Methodology

Step 1: Federated Learning

- Train models locally at fog nodes
- Share only model updates (not raw data)

Step 2: Secure Aggregation

- Use encryption:
  - Homomorphic encryption
  - Secure multi-party computation

Step 3: Data Anonymization

- Remove:
  - IP identifiers
  - Sensitive payloads

Gap 5: Lack of Explainability (XAI)

Problem: Deep learning models are black boxes.

Methodology

Step 1: XAI Integration

- Apply:
  - SHAP (Shapley Additive Explanations)
  - LIME (Local Interpretable Model-Agnostic Explanations)

ISSN: **3107-6513**

Step 2: Feature Importance Ranking
- Identify:
  - Key attack indicators
  - Influential features

Step 3: Visualization Dashboard
- Display:
  - Decision explanations
  - Attack reasoning

Gap 6: Multi-Layer Security Integration
Problem: Lack of coordination across layers.
Methodology

Step 1: Unified IDPS Framework
- Integrate:
  - IoT + Fog + Cloud

Step 2: Cross-Layer Communication
- Share:
  - Alerts
  - Threat intelligence

Step 3: Global Threat Intelligence System
- Maintain centralized knowledge base

C. INTEGRATED SYSTEM WORKFLOW

1. Data collected from IoT devices
2. Preprocessed and normalized
3. Passed to Fog Layer for quick detection
4. Suspicious data forwarded to Cloud
5. Deep learning model performs classification
6. XAI module explains decisions
7. Prevention module executes actions
8. System updates knowledge base

D. EVALUATION METHODOLOGY

Performance Metrics
- Accuracy
- Precision
- Recall
- F1-Score
- ROC-AUC

System Metrics
- Latency
- Throughput
- Energy consumption

Security Metrics
- Detection rate
- False positive rate

E. EXPERIMENTAL SETUP

- Environment: Cloud–Fog simulation (e.g., iFogSim / EdgeSim)
- Hardware: GPU-enabled cloud + edge devices
- Tools**:** Python, TensorFlow, PyTorch

F. EXPECTED OUTCOMES

- Scalable multi-layer IDPS
- Real-time detection capability
- Reduced false positives
- Explainable security decisions
- Energy-efficient deployment

VI.CONCLUSION AND FUTURE WORK

The integration of Cloud, Fog, and IoT technologies has introduced new security challenges that traditional systems cannot effectively address. AI-driven intrusion detection and prevention systems have shown significant promise in enhancing security through intelligent, adaptive, and real-time threat detection.

Deep learning techniques such as CNNs, RNNs, and hybrid models have improved detection accuracy, while fog computing enables low-latency processing. However, challenges such as scalability, explainability, data privacy, and resource constraints remain critical research areas.

Future research should focus on developing unified, scalable, and explainable AI-based IDPS frameworks that can operate efficiently across distributed environments while ensuring robustness, transparency, and real-time performance.

REFERENCES

1. Buczak, A. L., & Guven, E. (2016). A survey of data mining and machine learning methods for cybersecurity intrusion detection. IEEE Communications Surveys & Tutorials.
2. Javaid, A., et al. (2016). A deep learning approach for network intrusion detection system. EAI ICST.
3. Yin, C., et al. (2017). A deep learning approach for intrusion detection using recurrent neural networks. IEEE Access.
4. Moustafa, N., & Slay, J. (2015). UNSW-NB15 dataset for network intrusion detection systems.
5. Alrawashdeh, K., & Purdy, C. (2016). Toward an online anomaly intrusion detection system based on deep learning.
6. Doshi, R., et al. (2018). Machine learning DDoS detection for consumer IoT devices.
7. Abeshu, A., & Chilamkurti, N. (2018). Deep learning: The frontier for distributed attack detection in fog-to-things computing.
8. Shone, N., et al. (2018). Deep learning-based IDS using autoencoders.
9. Kim, G., et al. (2016). LSTM-based system-call language modeling for anomaly detection.
10. Tjoa, E., & Guan, C. (2020). A survey on explainable artificial intelligence (XAI).
11. Zhang, Q., et al. (2019). Network intrusion detection using deep learning.
12. Ferrag, M. A., et al. (2020). Deep learning for cybersecurity intrusion detection in IoT systems.