Encrypted Flow Intelligence: A Literature Review of AI Models for Traffic-Based Threat Detection

Prof.Sahana Sharma M
Dayananda Sagar Academy of Technology and Management, Bangalore.

Charitha K R
Dayananda Sagar Academy of Technology and Management, Bangalore.

Deeksha B Poojary
Dayananda Sagar Academy of Technology and Management, Bangalore.

Soujanya V
Dayananda Sagar Academy of Technology and Management, Bangalore.

Pragati Sanjay Hubballi
Dayananda Sagar Academy of Technology and Management, Bangalore.

Abstract

The growth of encrypted online communication has strengthened user privacy but also introduced major obstacles for threat detection systems. Since traditionally intrusion detection relies heavily on inspecting readable data, these systems often fail when faced with encrypted traffic. To address this issue, recent studies have turned toward artificial intelligence, particularly approaches using machine and deep learning, which can infer suspicious behavior without decrypting data. This review consolidates findings from recent literature, evaluating model architectures, training techniques, and detection effectiveness. Emphasis is placed on models that can be deployed in real-world environments while maintaining performance and protecting data confidentiality.

Keywords: Systematic review; encrypted traffic; intrusion detection; deep learning; machine learning; network security.

1. INTRODUCTION

The transformation of digital communication and cloud technologies has fundamentally reshaped how online services are accessed and secured. With the mainstream adoption of encryption standards like HTTPS, SSL/TLS, and VPNs, digital privacy has significantly improved. However, these same protective mechanisms have inadvertently made it more difficult for network defense systems to detect harmful activity. Cybercriminals now exploit encrypted channels to conduct operations such as data theft, malware deployment, and covert attacks, all while remaining hidden from conventional monitoring tools. As a result, the exponential growth in encrypted traffic—commonly labeled as cyber big data—has overwhelmed traditional intrusion detection systems (IDS), which rely on visibility into plaintext data packets [1][2].

One of the main tactics employed by threat actors involves using encrypted tunnels to disguise their malicious actions, effectively bypassing IDS that are based on signature-matching and payload scanning techniques [3]. As these rule-based tools struggle to cope with fast, high-volume encrypted data streams, they are quickly becoming obsolete. This shift has driven research toward the use of intelligent, learning-based methods that can detect suspicious patterns without accessing the content of the traffic. Among these, artificial intelligence (AI)—and more specifically, machine learning (ML) and deep learning (DL)—has emerged as a promising alternative for developing next-generation IDS capable of adaptive, private, and scalable detection [4][5].AI-driven systems are now being trained to detect threats by analyzing traffic behavior and flow patterns, rather than inspecting packet contents. These systems are capable of identifying anomalies using features such as flow timing, sequence behaviors, and connection metadata [6]. Convolutional neural networks (CNNs) are frequently used to capture spatial traffic characteristics, while long short-term memory (LSTM) models are effective at recognizing temporal dependencies. Attention-based models further enhance precision by selectively focusing on important input segments [7][8]. Techniques such as combining Bi-LSTM and CNN layers, or applying 1D-CNNs in end-to-end architectures, have demonstrated strong detection performance even without access to payload data [5][9].

In a way similar to how natural language processing interprets emotion from text, these AI-enhanced IDS tools learn to infer threat behavior based on indirect traffic signals. They are often able to flag subtle indicators of compromise—such as minor deviations in session timing or flow consistency—that may escape traditional systems [4]. Modern intrusion detection research has also expanded to include multi-class attack identification, allowing for classification of attacks like Denial of Service (DoS), Probe, Remote to Local (R2L), and User to Root (U2R), using well-known datasets such as NSL-KDD and UNSW-NB15 [2][6].On a methodological level, encrypted traffic analysis typically falls into two categories: statistical feature-based evaluation and machine learning algorithms. The first approach focuses on metrics like flow entropy, duration, and packet variation. The second relies on predictive models such as Support Vector Machines (SVM), Decision Trees, and ensemble classifiers including Random Forest [4][6]. More recent studies have emphasized unsupervised and semi-supervised learning to address the issue of limited labeled datasets for encrypted traffic. Deep architectures such as CNN-LSTM and stacked autoencoders have shown notable promise in identifying hidden patterns in complex traffic flows [7].

2. RELATED WORK

To counter these challenges, researchers have adopted AI-based solutions, particularly ML and DL, that assess metadata and network flow behavior without decrypting the content. Initial research proposed hybrid architectures such as LSTM-ANN to detect anomalies while maintaining computational efficiency. Advanced deep learning models, including CNN-LSTM frameworks, have demonstrated strong performance across binary as well as multiclass classification scenarios, highlighting their effectiveness in encrypted network environments. Although Random Forest shows reliable results in general use cases, its accuracy notably decreases when applied to encrypted traffic. Various optimization strategies—such as Particle Swarm Optimization and Correlation-Based Feature Selection—have been explored to enhance these models, though they still encounter difficulties in processing encrypted data. End-to-end solutions like 1D-CNN and multi-layered architectures such as Deep-Full-Range (which integrate CNN, LSTM, and autoencoders) have proven effective when trained on raw traffic. Despite offering flexibility and higher detection accuracy, these deep models demand high computational power and access to accurately labeled datasets. Recent studies have emphasized flow-level anomaly detection as a key strategy to overcome the challenge of effectively overcoming encryption-induced obfuscation.

3.OBJECTIVE

This study aims to deliver a comprehensive and organized evaluation of how AI-driven technologies are being applied to intrusion detection within encrypted networks. The research is structured to achieve the following goals:

1. To investigate the shortcomings of legacy Intrusion Detection Systems (IDS), particularly those that rely heavily on analyzing raw packet content and static pattern matching for threat identification.
2. To explore the potential of intelligent, automated detection mechanisms that use learning algorithms to detect unusual behavior in encrypted streams without the need for decryption.
3. To classify and critically compare a range of artificial intelligence models—such as convolutional and recurrent neural networks, support vector machines, ensemble methods, and hybrid combinations—using performance benchmarks like detection rate, error tolerance, adaptability, and resource usage.
4. To uncover the main technical barriers that limit the deployment of AI-based IDS in encrypted settings, including issues related to dataset availability, privacy protection, and processing power.
5. To shed light on cutting-edge developments such as collaborative learning, adaptive feedback systems, and privacy-preserving model designs that aim to make future IDS more robust and efficient.
6. To support decision-makers and researchers by offering a strategic synthesis of the current literature and by identifying promising methods for building secure, intelligent intrusion detection systems suited for modern, encrypted communication networks.

4. PROPOSED METHODOLOGY

This section outlines a systematic framework designed to assess AI methodologies that address intrusion detection in encrypted data environments. Unlike conventional IDS that rely on inspecting content within packets, this review shifts focus toward models capable of detecting threats by examining external traffic attributes and behavioral markers such as flow sequences, timing intervals, and statistical irregularities.

Rather than processing raw payloads, this approach analyzes network behavior using metrics such as connection patterns and distribution of flow features. These insights are then used to evaluate and contrast a broad spectrum of learning-based systems. Emphasis is placed on adaptive algorithms that include various types of neural networks and hybrid models, with performance evaluated against criteria such as real-time responsiveness, scalability, accuracy, and the ability to minimize false alarms.

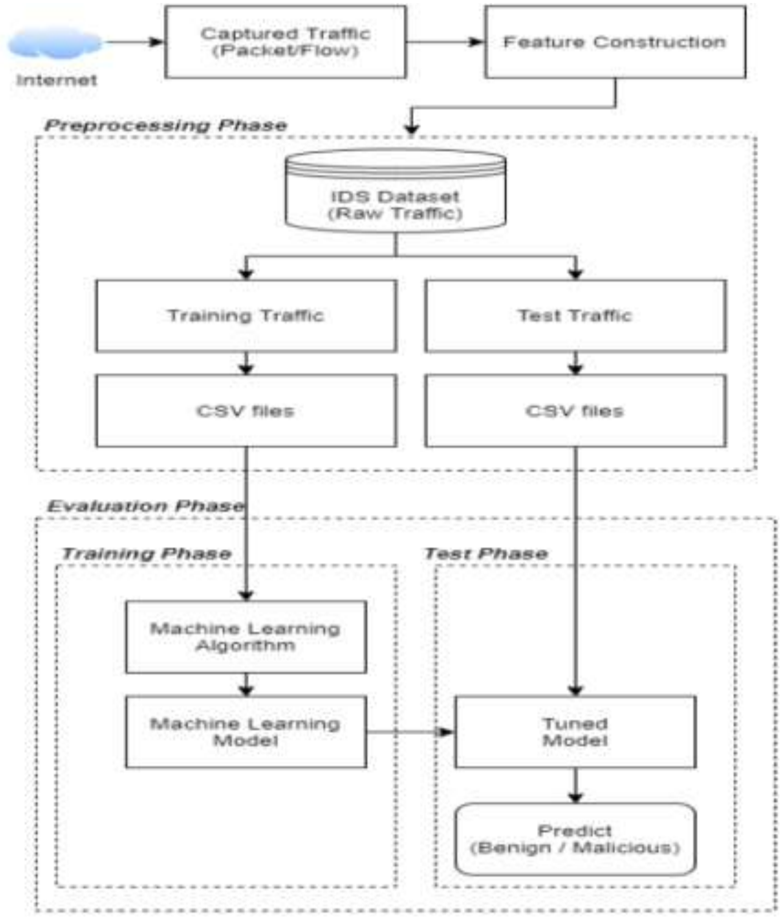
A. Research Scope and Objectives

- Investigate AI-centric frameworks for encrypted traffic analysis that do not require decryption.
- Examine the structural design of models, including supervised, unsupervised, and hybrid learning methods.
- Evaluate and compare how well different models perform across diverse datasets and assessment criteria.
- Highlight recurring issues, such as traffic obfuscation through encryption, limited labeled data, and latency or scalability concerns during real-time processing.

B. Literature Identification and Selection Criteria

- The review includes peer-reviewed articles published between 2017 and 2024.
- Selected works must address encrypted traffic detection using AI methodologies—either ML or DL-based.
- Studies must be validated using widely accepted benchmark datasets like NSL-KDD, UNSW-NB15, ISCX VPN-nonVPN, and CICIDS2017.
- Papers must include or analyze hybrid approaches such as CNN-LSTM, ANN-LSTM, or Bi-LSTM.

The ten most relevant publications, primarily sourced from the IEEE Xplore digital library, were chosen for in-depth analysis based on these criteria [1][10].



The reviewed AI-powered intrusion detection systems were classified into four core categories, reflecting their underlying architecture and learning methodology:

C. Model Categorization Framework

1. **Classical Machine Learning Models**
This group includes algorithms such as Random Forest, Decision Tree classifiers, Support Vector Machines, and Naive Bayes. These models typically rely on predefined statistical attributes and use supervised learning techniques for classification tasks [3][4][6].
2. **Integrated Deep Learning Structures**
This category features designs where Convolutional Neural Networks (CNNs) are paired with LSTM units, or where feedforward networks are coupled with sequence-based models like LSTM. These hybrids are capable of capturing both structural and temporal dynamics in encrypted traffic [1][2][5].
3. **Composite Neural Network Architectures**
Here, layered models—such as CNNs fused with LSTM networks or LSTM-enhanced artificial neural networks—work in tandem to process time-dependent and spatial properties within encrypted streams [1][2][5].
4. **End-to-End Learning and Self-Adaptive Models**
These systems bypass the need for handcrafted input features by processing raw traffic directly using 1D convolutional layers or autoencoders. They allow automatic classification by extracting features internally through deep learning pipelines [8][9].

D. Evaluation Criteria

Each selected detection model was evaluated using the following performance indicators:

- **Accuracy of Threat Detection (%):** Reflects how precisely the model identifies attacks.
- **False Alarm Rate (FPR):** Measures the tendency to wrongly flag legitimate traffic as malicious.
- **Precision, Recall, and F1-Score:** Metrics that assess a model’s balance between completeness and correctness.
- **Responsiveness to Real-Time Threats:** Ability to function efficiently in live traffic conditions.

- **Scalability and Resource Usage:** Evaluates whether the model can scale across devices and traffic loads while minimizing resource consumption.
- **Effectiveness on Encrypted Data:** Indicates robustness when deployed in environments with secure traffic formats.

E. Proposed Review Approach

The review process is structured into several phases to ensure a thorough and unbiased examination of current literature on AI-based encrypted intrusion detection:

1. **Information Retrieval**
Gather essential details from selected studies, including dataset characteristics, the type of models used, nature of extracted features (e.g., flow-level attributes or packet metadata), training configurations, and reported performance metrics.
2. **Comparative Benchmarking**
Conduct side-by-side evaluations of different models applied to identical or closely matched datasets to provide an objective basis for performance comparison.
3. **Performance Pattern Discovery**
Identify recurring advancements—such as the effectiveness of integrating CNN with LSTM layers, or improvements offered by autoencoder-based unsupervised anomaly detection models.
4. **Literature Gap Identification**
Pinpoint missing elements in existing research, such as:
   - Minimal real-world testing and deployment scenarios.
   - Lack of robust solutions for adversarial or encrypted traffic manipulation.
   - Limited incorporation of decentralized, privacy-aware learning frameworks like federated learning.

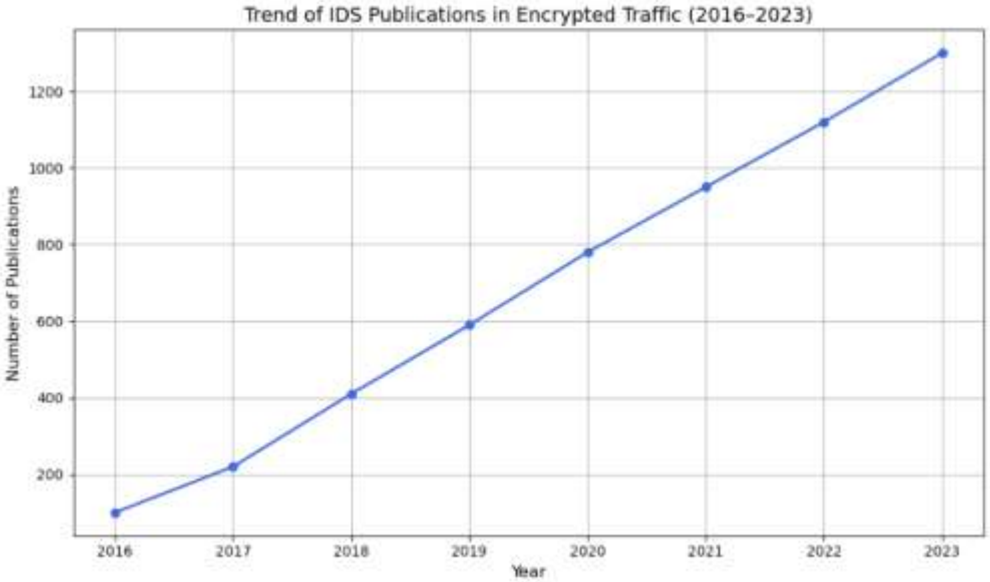
5. Challenges in AI-Based Intrusion Detection for Encrypted Traffic

While artificial intelligence has shown promise in detecting sophisticated threats, encrypted environments introduce a distinct set of hurdles that affect detection accuracy and system deployment.

1. **Absence of Content Visibility**
Encryption masks the payload content of data packets, making traditional signature-based approaches ineffective. Detection must rely solely on observable metadata and statistical flow patterns.
2. **Complex Feature Derivation**
Extracting informative patterns from encrypted communication is inherently challenging. Manual feature crafting often lacks reliability, and although deep learning methods offer improved capability, they demand large volumes of training data and significant computational power.
3. **Skewed Class Distribution**
Public intrusion datasets tend to contain far more examples of normal activity than of actual attacks. This imbalance skews training, reducing the ability of AI models to recognize rare, high-risk threats.
4. **Deficiency of Labeled Traffic**
Labeling encrypted traffic accurately is both labor-intensive and technically difficult. As a result, most datasets lack high-quality labels, limiting model evaluation and reducing training reliability.
5. **Limitations in Real-Time Execution**
Achieving rapid detection with low-latency is critical for operational use. However, deep learning models often have high processing demands that can be impractical in environments with limited resources, such as edge computing or IoT networks.

6.Result and Discussion

Intrusion Detection Systems (IDS) are essential for network security, but traditional systems struggle with encrypted traffic due to the obfuscation of packet content. The rise of encryption techniques like TLS/SSL and IPsec has made it difficult for signature-based or anomaly-based IDS to detect attacks effectively. To address this, AI-based techniques have emerged as a promising solution to monitor encrypted traffic and detect malicious activities.



This section presents the outcome of the data retrieval and analysis process conducted through a Systematic Literature Review (SLR). As mentioned in the methodology, the primary databases consulted are Scopus and Google Scholar. The initial keyword search produced approximately 7,212 documents from the Scopus database and over 1,100,000 documents from Google Scholar, totaling more than 1.1 million entries.These filters reduced the dataset to 3,176 publications, of which a further 1,505 were excluded through a fast-review process of abstracts and conclusions. Out of these, 980 were discarded because they focused on traditional (unencrypted) traffic. An additional 658 papers did not use any specific or relevant detection technique for encrypted traffic, or lacked experimental validation. Finally, 33 papers remained that directly addressed the Research Questions (RQ) and were considered suitable for final analysis. Among them, 6 highly relevant papers were selected based on the depth of evaluation, technical rigor, and relevance to our RQs. These are analyzed in the sections below

7.Conclusion

The widespread adoption of encryption protocols like TLS/SSL and IPsec has made traditional IDS less effective due to the inability to inspect encrypted payloads. AI-based intrusion detection, using models such as CNNs, RNNs, SVMs, and Decision Trees, provides a viable solution by analyzing metadata like packet size and flow behavior without decryption. Reinforcement learning further adds adaptability by enabling dynamic response to evolving threats.

However, challenges remain, including limited labeled datasets, high computational requirements, and privacy concerns related to encrypted data. Future advancements should focus on hybrid models, federated learning for privacy preservation, and techniques like transfer and adversarial learning to improve robustness and adaptability.

AI-powered IDS represent a promising approach to safeguarding encrypted network environments, offering enhanced threat detection without compromising user privacy.

References

1. M. Shadeja, A. Prakash, and S. Singh, “Deep Defense: A Hybrid LSTM-ANN Architecture for Intelligent Intrusion Detection System,” *Ajay Kumar Garg Engineering College*, Ghaziabad, Uttar Pradesh, India, [n.d.].
2. S. S. Kanumalli, S. P., L. K., T. M., and R. A., “Design of a Scalable Intrusion Detection Framework Integrating Bi-LSTM and CNN Models,” presented at the *3rd International Conference on Artificial Intelligence and Smart Energy (ICAIS)*, 2023.
3. M. S. Rahman, W. T. Islam, and M. R. A. Khan, “Investigating Machine Learning Approaches for Improving Network Security,” presented at the *2024 IEEE 3rd International Conference on Robotics, Automation, Artificial Intelligence, and Internet of Things (RAAICON)*, Dhaka, Bangladesh, Nov. 2024.A. Kiran, B. A. Kumar, T. Sameeratmaja, S. W. Prakash, Likhitha, and U. S. S. R. Charan, “Applying Machine Learning Approaches for Intrusion Detection in Networks,” in *Proc. of the 2023 Int. Conf. on Computer Communication and Informatics (ICCCI)*, 2023.
4. Z. T. Pear, “Enhanced Network Intrusion Detection Using a Hybrid CNN-LSTM Approach on the UNSW-NB15 Dataset,” *IEEE*, 2024.
5. A. A. Yilmaz, “Intrusion Detection in Computer Networks using Optimized Machine Learning Algorithms,” in *Proc. 2022 3rd Int. Informatics and Software Engineering Conf. (IISEC)*, 2022.
6. J. A. Abraham and B. V. R., “Intrusion Detection and Prevention in Networks Using Machine Learning and Deep Learning Approaches: A Review,” *Int. J. of Eng. Research & Technology*, vol. 10, no. 9, pp. 1–6, 2021.
7. W. Wang, M. Zhu, X. Zeng, and Z. Yang, *Encrypted Traffic Classification Using One-Dimensional CNNs*, University of Science and Technology of China, unpublished manuscript, [n.d.].
8. Y. Li, Z. Zhang, H. Guo, T. Jiang, J. Hou, and Z. Liu, “A Survey of Encrypted Malicious Traffic Detection,” in *Proc. 2021 Int. Conf. on Communications, Computing, Cybersecurity, and Informatics (CCCI)*, 2021.
9. Y. Zeng, H. Gu, W. Wei, and A. Guo, “Deep-Full-Range: A Unified Deep Learning Framework for Encrypted Traffic Classification and Intrusion Detection,” presented at the *IEEE Conference on Network Security and Traffic Analysis*, 2019.