

IDS for Encrypted Traffic with ML

Project Title & Number: Intrusion Detection Systems for Encrypted Network Traffic using Machine Learning (P22)

Group Members:

Mohd Irfan Raza (Mohd Irfan Raza)
Bhargav Jani (Bhargav Jani)

Date: 16th September, 2025

Course: Networks for AI

1. Executive Summary

High-Level Description of the Problem

The exponential growth of encrypted network traffic, now comprising over 95% of internet communications, presents a critical challenge for traditional intrusion detection systems (IDS). While encryption provides essential privacy and security guarantees, it simultaneously creates a blind spot for security professionals who can no longer rely on deep packet inspection (DPI) techniques to identify malicious activities. This paradox between security and visibility has become one of the most pressing challenges in modern cybersecurity.

Traditional IDS approaches that rely on payload analysis, signature matching, and content inspection are rendered ineffective when faced with encrypted traffic. Attackers exploit this limitation by using encryption protocols like TLS, HTTPS, and VPNs to obfuscate malicious communications, making detection significantly more challenging. The problem is further compounded by the emergence of stronger encryption protocols such as TLS 1.3 and QUIC, which encrypt even more metadata that was previously available for analysis.

Why It Matters for AI & Networking

This problem sits at the critical intersection of AI and networking, representing a domain where machine learning can provide transformative solutions to fundamental network security challenges:

For AI:

Feature Learning: Encrypted traffic analysis requires sophisticated feature extraction from limited observable data (metadata, timing patterns, flow characteristics)

Pattern Recognition: ML algorithms excel at identifying subtle patterns in high-dimensional data that human analysts might miss

Adaptive Detection: AI models can adapt to evolving attack patterns and zero-day threats without requiring manual signature updates

Scale Handling: Modern networks generate terabytes of traffic data daily, requiring automated analysis capabilities that only AI can provide

For Networking:

Real-Time Processing: Network security requires sub-second decision making, demanding efficient ML models optimized for networking constraints

Privacy Preservation: Solutions must maintain user privacy while providing security insights

Infrastructure Integration: ML-based IDS must integrate seamlessly with existing network infrastructure and security frameworks

Performance Impact: Detection systems must operate without significantly impacting network performance or latency

Expected Contributions

This project aims to deliver several key contributions to the field of AI-driven network security:

1. **Comprehensive Literature Analysis:** A systematic review of state-of-the-art ML techniques for encrypted traffic analysis, identifying gaps and opportunities in current research.
2. **Hybrid Detection Framework:** Development of a novel approach combining multiple ML techniques (CNN for spatial feature extraction, LSTM for temporal pattern recognition, and ensemble methods for robust classification) optimized for encrypted traffic analysis.
3. **Feature Engineering Innovation:** Investigation of novel feature extraction techniques that can effectively characterize malicious behavior in encrypted flows using only metadata, timing information, and statistical properties.
4. **Performance Optimization:** Analysis of trade-offs between detection accuracy, computational efficiency, and real-time processing requirements in network environments.

5. **Practical Implementation Guidelines:** Delivery of actionable insights for deploying ML-based IDS in production environments, including considerations for scalability, maintainability, and integration with existing security infrastructure.
 6. **Evaluation Methodology:** Development of robust evaluation frameworks that account for real-world deployment scenarios, including adversarial environments and evolving threat landscapes.
-

2. Technology Background

Core Concepts and Definitions

Intrusion Detection Systems (IDS) Intrusion Detection Systems are security tools designed to monitor network traffic and system activities to identify malicious or suspicious behavior. Traditional IDS can be categorized into:

- **Network-based IDS (NIDS):** Monitor network traffic for suspicious activities
- **Host-based IDS (HIDS):** Monitor individual systems for malicious behavior
- **Signature-based IDS:** Use predefined patterns to detect known attacks
- **Anomaly-based IDS:** Establish baselines of normal behavior and detect deviations

Encrypted Traffic Characteristics Encrypted network traffic presents unique challenges and opportunities:

- **Observable Features:** Packet sizes, inter-arrival times, flow duration, connection patterns
- **Hidden Information:** Payload content, application-layer protocols, specific data patterns
- **Metadata Analysis:** TLS handshake information, certificate details, cipher suites
- **Behavioral Patterns:** Traffic volume, communication frequency, connection establishment patterns

Machine Learning Approaches for Network Security

Statistical Methods:

1. **Markov Chains:** Model sequential patterns in network behavior
2. **Hidden Markov Models:** Capture latent states in traffic patterns
3. **Time Series Analysis:** Analyze temporal dependencies in network flows

Deep Learning Architectures:

1. **Convolutional Neural Networks (CNN):** Extract spatial features from packet sequences
2. **Recurrent Neural Networks (RNN/LSTM):** Capture temporal dependencies in traffic flows
3. **Autoencoders:** Unsupervised anomaly detection through reconstruction error
4. **Transformer Models:** Attention-based mechanisms for sequence analysis

Use Cases and Key Performance Indicators (KPIs)

Primary Use Cases

1. Malware Detection in Encrypted Channels

- Identify command-and-control communications
- Detect data exfiltration attempts
- Recognize botnet activities

2. Advanced Persistent Threat (APT) Detection

- Long-term surveillance and lateral movement detection
- Stealthy attack pattern recognition
- Zero-day exploit identification

3. Real-time Threat Prevention

- Automated blocking of malicious flows
- Dynamic firewall rule generation
- Proactive threat hunting

4. Compliance and Monitoring

- Privacy-preserving network monitoring
- Regulatory compliance for encrypted communications
- Network performance optimization

Key Performance Indicators

Accuracy Metrics:

- **Detection Rate (True Positive Rate):** 95-99% (maintain)
- **False Positive Rate:** <2%
- **F1-Score:** >97%
- **Area Under ROC Curve (AUC):** >0.98

Performance Metrics:

- **Latency:** <100ms for real-time detection
- **Throughput:** 10+ Gbps traffic processing
- **Memory Usage:** <8GB for production deployment
- **CPU Utilization:** <70% during peak traffic

Operational Metrics:

- **Mean Time to Detection (MTTD):** <5 minutes
- **Mean Time to Response (MTTR):** <15 minutes
- **Scalability:** Linear scaling with traffic volume
- **Availability:** 99.9% uptime

Survey of Research Papers

Paper 1: Deep Learning for Encrypted Traffic Classification (Rezaei & Liu, 2019)

Key Contributions:

- Comprehensive framework for applying deep learning to encrypted traffic analysis
- Comparison of CNN, LSTM, and hybrid approaches
- Guidelines for feature selection and model architecture choice
- Identified that CNN excels with payload+header data, while LSTM performs better with time series features

Limitations:

- Limited evaluation on adversarial attacks
- Lack of standardized evaluation datasets
- Insufficient analysis of real-time deployment constraints

Paper 2: Efficient Deep CNN-BiLSTM Model for Network Intrusion Detection (Sinha & Manollas, 2020)

Key Contributions:

- Hybrid architecture combining CNN spatial feature extraction with BiLSTM temporal modeling
- Achieved 99.2% accuracy on NSL-KDD dataset
- Demonstrated efficiency improvements over individual CNN or LSTM approaches
- Bidirectional processing captures both past and future context

Limitations:

- High computational complexity for real-time deployment
- Limited evaluation on encrypted traffic specifically
- Dataset bias toward older attack types

Paper 3: Machine Learning for Encrypted Malware Traffic Classification (Anderson & McGrew, 2017)

Key Contributions:

- Addressed label noise and non-stationarity in encrypted traffic datasets
- Robust learning techniques for real-world deployment scenarios
- Focus on practical challenges of encrypted malware detection
- Consideration of evolving threat landscapes

Limitations:

- Limited to statistical features from encrypted flows Scalability concerns for high-volume networks
- Lack of comparison with deep learning approaches

Paper 4: Multi-modal Embedding for Cybersecurity (PACKETCLIP, 2025)

Key Contributions:

- Novel multi-modal approach combining network traffic analysis with natural language processing
- Addresses encrypted traffic classification challenges
- Integration of contextual information for improved detection accuracy
- Recent advancement showing promising results for complex threat detection

Limitations:

- Computational overhead of multi-modal processing
- Limited evaluation on large-scale deployments
- Complexity of integrating multiple data modalities

Paper 5: Signature-based IDS with ML and Fuzzy Clustering (2025)

Key Contributions:

- Combination of traditional signature-based detection with modern ML techniques
- Integration of fuzzy clustering for improved classification
- Recent work showing effectiveness of hybrid approaches
- Maintains interpretability while improving accuracy

Limitations:

- Still relies partially on signature databases
- May struggle with truly novel attacks
- Computational overhead of fuzzy clustering

Current Challenges and Limitations

Technical Challenges

1. Feature Scarcity

- Limited observable features in encrypted traffic
- Dependence on metadata and statistical properties
- Loss of application-layer information

2. Adversarial Robustness

- Attackers can manipulate traffic patterns to evade detection
- Adversarial machine learning attacks on ML models
- Need for robust and adaptive detection mechanisms

3. Real-time Processing Requirements

- Network traffic requires sub-second processing
- Balancing accuracy with computational efficiency
- Scalability to high-speed network environments (10+ Gbps)

4. Dataset Limitations

- Lack of standardized evaluation datasets
- Privacy concerns in sharing real network traffic
- Rapid evolution of attack patterns making datasets obsolete

Practical Deployment Challenges

1. Integration Complexity

- Compatibility with existing network infrastructure
- Integration with Security Information and Event Management (SIEM) systems
- Minimal impact on network performance

2. False Positive Management

- High false positive rates burden security analysts
- Need for explainable AI to understand detection decisions
- Adaptive thresholds for different network environments

3. Privacy and Legal Considerations

- Compliance with data protection regulations (GDPR, CCPA)
- Balancing security monitoring with user privacy
- Legal implications of traffic analysis

4. Continuous Learning and Adaptation

- Models need to adapt to evolving threat landscapes
- Zero-day attack detection capabilities
- Automated model updates without disrupting operations

These challenges highlight the need for innovative approaches that can address both technical

limitations and practical deployment requirements in real-world network environments.

3. Problem Framing

Specific Problem Addressed

The core problem this project addresses is the **detection of malicious network activities in encrypted traffic streams using machine learning techniques that operate solely on observable metadata and behavioral patterns**. Specifically, we focus on:

Primary Problem Statement: *How can we design and implement a machine learning-based intrusion detection system that achieves high accuracy (>95%) in identifying malicious encrypted network traffic while maintaining real-time processing capabilities (<100ms latency) and low false positive rates (<2%) in production network environments?*

Sub-problems:

1. **Feature Engineering Challenge:** Extracting meaningful features from encrypted traffic that preserve privacy while maintaining discriminative power for attack detection
2. **Real-time Classification:** Developing ML models that can process high-volume network traffic (10+ Gbps) with minimal latency impact
3. **Adversarial Robustness:** Creating detection systems resistant to evasion techniques employed by sophisticated attackers
4. **Adaptability:** Designing systems capable of detecting novel attacks and adapting to evolving threat landscapes without extensive retraining

Scope and Assumptions

Project Scope:

In Scope:

- Network-based intrusion detection for encrypted TCP/UDP traffic
- Machine learning models optimized for metadata and flow-based features
- Real-time detection capabilities suitable for enterprise networks
- Evaluation on standard cybersecurity datasets and simulated encrypted traffic
- Performance optimization for latency, throughput, and accuracy trade-offs

Out of Scope:

- Host-based intrusion detection systems

- Deep packet inspection techniques requiring payload analysis
- Cryptographic analysis or encryption breaking attempts
- Legal and regulatory compliance frameworks
- Physical network infrastructure modifications

Key Assumptions:

Technical Assumptions:

1. **Network Traffic Availability:** Access to network flow metadata including packet sizes, timing information, and connection patterns
2. **Computational Resources:** Sufficient computational power for real-time ML inference (modern multi-core processors with GPU acceleration)
3. **Training Data Quality:** Availability of labeled datasets with sufficient representation of both benign and malicious encrypted traffic
4. **Network Environment Stability:** Relatively stable network infrastructure without frequent topology changes during evaluation

Operational Assumptions:

1. **Threat Model:** Attackers use standard encryption protocols (TLS, HTTPS, VPN) but may employ evasion techniques
2. **Deployment Environment:** Enterprise or service provider networks with moderate to high traffic volumes
3. **Security Requirements:** Detection systems must not compromise user privacy or violate encryption integrity
4. **Maintenance Capability:** Availability of security professionals for system monitoring and tuning

Why This is Timely and Important

Immediate Relevance:

1. **Encryption Proliferation:** Encryption has become a fundamental security measure for data transmission, with over 95% of web traffic now encrypted, creating an urgent need for new detection methodologies.
2. **Evolving Threat Landscape:** Recent studies show increasing sophistication of cyber attacks that leverage encryption to hide malicious activities, necessitating advanced detection capabilities.

3. **Regulatory Pressure:** Growing privacy regulations (GDPR, CCPA) require security solutions that don't compromise user privacy, making metadata-based detection essential.
4. **Technology Maturation:** Recent advances in AI, particularly multi-modal learning approaches like PACKETCLIP, demonstrate the readiness of ML technology for practical cybersecurity applications.

Strategic Importance:

For Network Security:

- Traditional signature-based IDS are becoming obsolete due to encryption
- Need for proactive rather than reactive security measures
- Critical infrastructure protection requires advanced threat detection

For AI Research:

- Real-world application domain for testing ML robustness and performance.
- Challenge of learning from limited, noisy data with high-stakes consequences
- Opportunity to advance adversarial machine learning research
-

For Industry:

- Billion-dollar market for network security solutions
- Competitive advantage for organizations with superior threat detection
- Foundation for next-generation Security Operations Centers (SOCs)

Expected Key Performance Indicators

Detection Performance KPIs:

Accuracy Metrics:

- **Primary KPI - Detection Rate:** $\geq 95\%$ true positive rate for identifying malicious encrypted traffic
- **False Positive Rate:** $\leq 2\%$ to minimize analyst workload and system disruption
- **F1-Score:** $\geq 97\%$ for balanced precision and recall performance
- **Area Under ROC Curve (AUC):** ≥ 0.98 for overall classification quality

Robustness Metrics:

- **Adversarial Robustness:** $\geq 90\%$ detection rate against common evasion techniques
- **Zero-day Detection:** $\geq 85\%$ detection rate for previously unseen attack patterns
- **Cross-dataset Generalization:** $\geq 90\%$ performance when trained on one dataset and tested

on another

Operational Performance KPIs:

Latency Requirements:

- **Real-time Detection Latency:** $\leq 100\text{ms}$ from packet arrival to classification decision
- **Model Inference Time:** $\leq 10\text{ms}$ per flow classification
- **End-to-end Processing Latency:** $\leq 200\text{ms}$ including data preprocessing and post-processing

Throughput Requirements:

- **Traffic Processing Rate:** ≥ 10 Gbps sustained throughput
- **Concurrent Flow Handling:** $\geq 100,000$ simultaneous network flows
- **Packet Processing Rate:** ≥ 1 million packets per second

Resource Efficiency:

- **Memory Footprint:** $\leq 8\text{GB}$ RAM for production deployment
- **CPU Utilization:** $\leq 70\%$ during peak traffic periods
- **GPU Utilization:** $\leq 80\%$ when using hardware acceleration
- **Energy Consumption:** $\leq 200\text{W}$ power consumption for complete system

Scalability and Reliability KPIs:

Scalability Metrics:

- **Horizontal Scaling:** Linear performance scaling across multiple processing nodes
- **Traffic Volume Scalability:** Graceful degradation under 2x normal traffic loads
- **Model Update Time:** ≤ 30 seconds for deploying updated ML models

Reliability Metrics:

- **System Availability:** $\geq 99.9\%$ uptime excluding planned maintenance
- **Mean Time Between Failures (MTBF):** ≥ 720 hours (30 days)
- **Mean Time to Recovery (MTTR):** ≤ 15 minutes for system restoration

Business Impact KPIs:

Security Effectiveness:

- **Mean Time to Detection (MTTD):** ≤ 5 minutes for critical threats
- **Mean Time to Response (MTTR):** ≤ 15 minutes from detection to incident response initiation
- **Threat Coverage:** $\geq 90\%$ coverage of MITRE ATT&CK framework techniques applicable to network traffic

Operational Efficiency:

- **Analyst Workload Reduction:** $\geq 50\%$ reduction in false positive investigations
- **Automation Rate:** $\geq 80\%$ of detected incidents handled automatically without human intervention
- **Cost per Gigabyte Processed:** $\leq \$0.001$ operational cost per GB of analyzed traffic

These KPIs provide measurable objectives that balance technical performance requirements with practical deployment constraints, ensuring the resulting system delivers tangible value in real-world network security environments.

9. Results and Graphs

```
{
  "phase1": {
    "cleaned_samples": 476263,
    "balanced_samples": 761548,
    "class_weights": [1, 1]
  },
  "phase2": {
    "model_type": "ImprovedHybridCNNBiLSTMAAttention",
    "loss_function": "WeightedFocalLoss",
    "optimizer": "Adam"
  },
  "phase3": {
    "temporal_features": 7,
    "invariance_features": 4,
```

```

        "domain_features": 2,
        "total_engineered": 13
    },
    "phase4": {
        "metrics": {
            "accuracy": 1,
            "precision": 1,
            "recall": 1,
            "f1": 1,
            "auc_roc": 1,
            "detection_rate": 1,
            "fpr": 0,
            "specificity": 1
        },
        "optimal_threshold": 0.01,
        "threshold_metrics": {
            "threshold": 0.01,
            "detection_rate": 1,
            "fpr": 0,
            "specificity": 1,
            "tp": 95194,
            "tn": 59,
            "fp": 0,
            "fn": 0
        }
    }
}

```

10. References

- [1] S. Rezaei and X. Liu, "Deep Learning for Encrypted Traffic Classification: An Overview," *IEEE Communications Magazine*, vol. 57, no. 5, pp. 76-81, May 2019. [Online]. Available: <https://arxiv.org/abs/1810.07906>
- [2] J. Sinha and M. Manollas, "Efficient Deep CNN-BiLSTM Model for Network Intrusion Detection," in *Proc. IEEE AICEECS*, 2020. [Online]. Available: https://jaysinha.me/files/aipr_20_ids_paper_pre_print.pdf
- [3] B. Anderson and D. McGrew, "Machine Learning for Encrypted Malware Traffic

Classification: Accounting for Noisy Labels and Non-Stationarity," in *Proc. ACM SIGKDD Workshop on Data Science for Cybersecurity*, 2017, DOI: 10.1145/3097983.3098163.

[4] S. Jha, K. Tan, and R. A. Maxion, "Markov Chains, Classifiers, and Intrusion Detection," in *Proc. IEEE Symposium on Security and Privacy*, 2001, pp. 61-74. [Online]. Available: https://pages.cs.wisc.edu/~jha/jha-papers/security/CSFW_2001.pdf

[5] "PACKETCLIP: Multi-modal Embedding of Network Traffic and Language for Cybersecurity Reasoning," *Frontiers in Artificial Intelligence*, vol. 8, 2025. [Online]. Available: <https://www.frontiersin.org/journals/artificial-intelligence/articles/10.3389/frai.2025.1593944/full>

[6] "Signature-based Intrusion Detection Using Machine Learning and Deep Learning Approaches Empowered with Fuzzy Clustering," *Scientific Reports*, vol. 15, 2025. [Online]. Available: <https://www.nature.com/articles/s41598-025-85866-7>

[7] "Enhancing Intrusion Detection: A Hybrid Machine and Deep Learning Approach," *Journal of Cloud Computing*, vol. 13, July 2024. [Online]. Available: <https://journalofcloudcomputing.springeropen.com/articles/10.1186/s13677-024-00685-x>

[8] RFC 9411, "Benchmarking Methodology for Network Security Device Performance," Internet Engineering Task Force (IETF), 2023. [Online]. Available: <https://www.ietf.org/rfc/rfc9411.html>

[9] RFC 8329, "Framework for Interface to Network Security Functions," Internet Engineering Task Force (IETF), Feb. 2018. [Online]. Available: <https://datatracker.ietf.org/doc/html/rfc8329>

[10] "Deep Learning-driven Methods for Network-based Intrusion Detection Systems: A Systematic Review," *ScienceDirect*, Jan. 2025. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S2405959525000050>

[11] C. Zhang, N. Wang, Y. T. Hou, and W. Lou, "Machine Learning-Based Intrusion Detection Systems: Capabilities, Methodologies, and Open Research Challenges," *Authorea Preprint*, Jan. 2025, DOI: 10.36227/techrxiv.173627464.48290242.

[12] F. Hendaoui, A. Ferchichi, L. Trabelsi, R. Meddeb, R. Ahmed, and M. K. Khelifi, "Advances in Deep Learning Intrusion Detection Over Encrypted Data with Privacy

Preservation: A Systematic Review," *Cluster Computing*, vol. 27, pp. 8683-8724, 2024, DOI:
10.1007/s10586-024-04424-4.