International Research Journal of Studies in Computer Science and Engineering
Volume: 01, Issue: 01, August 2026 | ISSN: XXXX.XXXX

AI-Driven Adaptive Cybersecurity Framework for Real-Time Threat Detection in Intelligent Computing Networks

Yizheng Chen
Assistant Professor
Department of Computer Science
D.Y.A. International University, USA

Abstract

The rapid expansion of intelligent computing networks, Internet of Things devices, cloud infrastructures, edge computing and interconnected digital services has significantly increased the complexity of modern cybersecurity environments. Conventional security mechanisms that rely primarily on predefined signatures and static rules are increasingly challenged by zero-day attacks, polymorphic malware, insider threats and rapidly evolving network behaviours. Artificial intelligence (AI) and machine learning (ML) provide opportunities to develop adaptive cybersecurity systems capable of continuously analysing network behaviour, identifying anomalous activities and supporting real-time threat mitigation. This paper proposes an AI-driven adaptive cybersecurity framework that integrates network monitoring, feature extraction, machine-learning-based anomaly detection, threat classification, risk assessment and automated response. The proposed architecture combines supervised and unsupervised learning to detect both known and previously unseen threats. A feedback mechanism enables the framework to learn from new security events and dynamically update its detection strategies. The study further considers challenges associated with false positives, adversarial attacks, data imbalance, model drift, explainability, computational overhead and privacy. The proposed framework is designed to support intelligent computing networks by providing continuous monitoring and adaptive defence while maintaining human oversight for high-risk security decisions. The framework demonstrates how AI can transform cybersecurity from a predominantly reactive model into a proactive, context-aware and continuously adaptive security paradigm.

Keywords: Artificial Intelligence, Cybersecurity, Machine Learning, Anomaly Detection, Network Security, Threat Detection, Adaptive Security, Intelligent Computing Networks, Real-Time Security, Intrusion Detection.

International Research Journal of Studies in Computer Science and Engineering
Volume: 01, Issue: 01, August 2026 | ISSN: XXXX.XXXX

1. Introduction

Modern computing environments are increasingly interconnected through:

- Cloud computing.
- Edge computing.
- Internet of Things (IoT).
- 5G and advanced communication networks.
- Distributed applications.
- Smart infrastructure.
- Industrial networks.

This connectivity provides significant operational benefits but also creates a larger attack surface.

Attackers increasingly employ:

- Zero-day exploits.
- Distributed denial-of-service attacks.
- Credential attacks.
- Malware.
- Ransomware.
- Botnets.
- Data exfiltration.
- Advanced persistent threats.

Traditional cybersecurity systems frequently depend on predefined signatures and rules. Although effective against known threats, these approaches can struggle with previously unseen attack patterns.

AI-driven cybersecurity provides an alternative by learning patterns of normal and malicious network behaviour.

2. Evolution of Network Security

Network security has progressively evolved through several stages:

Signature-Based Security

↓

Rule-Based Detection

↓

Statistical Anomaly Detection

International Research Journal of Studies in Computer Science and Engineering
Volume: 01, Issue: 01, August 2026 | ISSN: XXXX.XXXX

↓

Machine Learning

↓

Deep Learning

↓

Adaptive AI Security

The latest stage aims to continuously learn from changing network environments.

3. Problem Statement

The primary challenge is the detection of emerging network threats in environments where:

- Network traffic changes continuously.
- Attack behaviour evolves rapidly.
- Devices have different security profiles.
- Data volumes are extremely large.
- Threat signatures may not yet exist.
- False positives can overwhelm security teams.

Therefore, cybersecurity systems require mechanisms capable of detecting deviations from normal behaviour and adapting to new attack patterns.

4. Research Motivation

The motivation for this study is based on five major requirements:

1. Real-time threat detection.
2. Identification of unknown attacks.
3. Continuous model adaptation.
4. Automated threat response.
5. Reduced dependence on manually defined rules.

AI can provide the computational foundation for these capabilities.

5. Research Objectives

The study aims to:

1. Develop an adaptive AI-based cybersecurity architecture.
2. Detect anomalous network behaviour in real time.
3. Classify potential cyber threats.
4. Develop dynamic risk-scoring mechanisms.
5. Enable automated response to detected threats.

International Research Journal of Studies in Computer Science and Engineering
Volume: 01, Issue: 01, August 2026 | ISSN: XXXX.XXXX

6. Reduce false-positive rates.
7. Establish a feedback mechanism for continuous learning.
8. Improve resilience against emerging attacks.

6. Literature Review

6.1 Traditional Intrusion Detection

Intrusion detection systems traditionally use signatures and predefined rules.

Their main advantages are:

- Fast detection.
- Simple implementation.
- High accuracy for known attacks.

However, they can struggle with novel attacks.

6.2 Machine Learning for Cybersecurity

Machine learning allows security systems to learn relationships from historical network data.

Common algorithms include:

- Decision Trees.
- Random Forest.
- Support Vector Machines.
- Logistic Regression.
- k-Nearest Neighbours.
- Gradient Boosting.

6.3 Unsupervised Learning

Unsupervised learning is particularly useful where labelled attack data are limited.

Techniques include:

- Clustering.
- Autoencoders.
- Isolation Forest.
- One-Class SVM.

These models can identify deviations from established behavioural patterns.

6.4 Deep Learning

Deep neural networks can process complex and high-dimensional network data.

Potential applications include:

- Traffic classification.

- Malware detection.
- Behavioural analysis.
- Intrusion detection.

7. Research Gap

Existing cybersecurity approaches often focus on individual detection techniques rather than integrating:

Detection + Risk Assessment + Adaptation + Automated Response

into a single framework.

Major gaps include:

- Limited adaptation to model drift.
- High false-positive rates.
- Insufficient explainability.
- Limited integration of edge and cloud environments.
- Vulnerability to adversarial manipulation.
- Limited real-time feedback mechanisms.

8. Proposed Framework

The proposed architecture consists of eight primary layers:

1. Network Data Acquisition.
2. Data Preprocessing.
3. Feature Engineering.
4. AI-Based Detection.
5. Threat Classification.
6. Risk Assessment.
7. Adaptive Response.
8. Continuous Learning.

9. Network Data Acquisition

The first layer collects security-relevant information from:

- Network packets.
- Flow records.
- Firewall logs.
- Authentication events.
- DNS requests.

- Endpoint activity.
- Cloud logs.
- IoT devices.

The resulting data stream forms the input for subsequent analysis.

10. Data Preprocessing

Raw network data may contain:

- Missing values.
- Duplicate records.
- Noise.
- Irrelevant variables.

Preprocessing may therefore include:

- Data cleaning.
- Normalisation.
- Encoding.
- Noise reduction.
- Feature selection.

11. Feature Engineering

Potential features include:

Feature Category	Examples
Network	Packet rate, flow duration
Traffic	Bytes transmitted, packet size
Protocol	TCP, UDP, HTTP, DNS
Behaviour	Connection frequency
Authentication	Failed login attempts
Endpoint	Process activity
Temporal	Time between events

Feature engineering significantly affects detection performance.

International Research Journal of Studies in Computer Science and Engineering
Volume: 01, Issue: 01, August 2026 | ISSN: XXXX.XXXX

12. AI-Based Threat Detection

The detection layer combines multiple approaches.

Supervised Detection

Used for known attack categories.

Unsupervised Detection

Used for previously unknown anomalies.

Hybrid Detection

Combines both approaches.

The hybrid model is particularly appropriate for evolving network environments.

13. Anomaly Detection

The system first establishes a representation of normal behaviour.

When incoming traffic deviates significantly from this representation, an anomaly score is generated.

Conceptually:

Normal Behaviour → Low Anomaly Score

Abnormal Behaviour → High Anomaly Score

14. Threat Classification

Detected anomalies can be classified into categories such as:

- Denial-of-service.
- Malware activity.
- Credential attacks.
- Scanning.
- Data exfiltration.
- Privilege escalation.
- Botnet behaviour.

Classification enables targeted response strategies.

15. Risk Assessment

Not every anomaly represents an equally serious threat.

The proposed framework calculates a dynamic risk score using factors such as:

- Anomaly severity.
- Asset importance.
- Attack confidence.

International Research Journal of Studies in Computer Science and Engineering
Volume: 01, Issue: 01, August 2026 | ISSN: XXXX.XXXX

- Potential impact.
- Historical behaviour.
- Threat intelligence.

A conceptual model is:

Risk Score = Threat Probability × Potential Impact × Asset Criticality

16. Adaptive Response

Based on risk level, the framework can recommend or execute different responses.

Risk Level	Example Response
Low	Continue monitoring
Moderate	Increase monitoring
High	Isolate suspicious endpoint
Critical	Block traffic and alert security team

High-impact actions should remain subject to appropriate human and organisational controls.

17. Continuous Learning

The proposed architecture includes a feedback loop.

Detection

↓

Security Analyst Validation

↓

Response Outcome

↓

New Training Data

↓

Model Update

↓

Improved Detection

This allows the system to adapt as threats evolve.

International Research Journal of Studies in Computer Science and Engineering
Volume: 01, Issue: 01, August 2026 | ISSN: XXXX.XXXX

18. Conceptual Architecture

Network / IoT / Cloud Data

↓

Data Collection

↓

Preprocessing

↓

Feature Extraction

↓

AI Detection Engine

↓

Anomaly Detection

↓

Threat Classification

↓

Risk Scoring

↓

Adaptive Response

↓

Security Analyst

↓

Feedback & Model Updating

19. Real-Time Detection Pipeline

The framework operates continuously:

Incoming Traffic

→ Feature Extraction

→ AI Analysis

→ Anomaly Score

→ Threat Classification

→ Risk Assessment

→ Response

The objective is to minimise the time between attack initiation and defensive action.

20. Edge-Based Threat Detection

Edge computing can reduce latency by processing security information closer to devices.

Benefits include:

- Faster detection.
- Lower bandwidth consumption.
- Reduced cloud dependency.
- Localised security responses.

This is especially useful for IoT and industrial networks.

21. Cloud-Based Security Intelligence

Cloud infrastructure can provide:

- Large-scale model training.
- Centralised threat intelligence.
- Historical data storage.
- Cross-network analytics.

The proposed framework therefore supports a hybrid:

Edge Detection + Cloud Intelligence

architecture.

22. Federated Learning

Federated learning can allow multiple organisations or network nodes to collaboratively improve models without necessarily centralising raw data.

Conceptually:

Local Training

→ Model Update

→ Central Aggregation

→ Updated Global Model

This can help address privacy and data-sharing challenges.

23. Adversarial Machine Learning

AI security systems themselves may become targets.

Attackers can attempt to:

- Manipulate input data.
- Evade detection.

- Poison training datasets.
- Exploit model weaknesses.

Therefore, cybersecurity AI must itself be protected.

24. Model Drift

Network behaviour changes over time.

For example:

- New applications are deployed.
- New devices appear.
- Traffic patterns change.
- Attack strategies evolve.

A model trained on historical data may therefore gradually lose accuracy.

Continuous monitoring and retraining are required.

25. False Positives

Excessive false alarms can overwhelm security teams.

The framework can reduce false positives by combining:

- Multiple detection models.
- Contextual information.
- Historical behaviour.
- Risk scoring.
- Analyst feedback.

26. Explainable AI

Security analysts need to understand why an alert was generated.

An explainable system could identify:

- Important network features.
- Behavioural deviations.
- Attack indicators.
- Confidence levels.

This improves trust and facilitates investigation.

27. Human-in-the-Loop Security

The framework adopts a human–AI collaboration model.

AI

- Monitors.

- Detects.
- Prioritises.
- Recommends.

Human Analyst

- Validates.
- Investigates.
- Authorises high-risk actions.
- Provides feedback.

This balances automation and accountability.

28. Threat Intelligence Integration

External threat intelligence can provide information about:

- Malicious IP addresses.
- Domains.
- Malware indicators.
- Attack campaigns.
- Known vulnerabilities.

Combining threat intelligence with behavioural AI can strengthen detection.

29. Zero-Trust Integration

The proposed framework can support zero-trust principles by continuously evaluating:

- Identity.
- Device behaviour.
- Network activity.
- Access patterns.
- Risk.

Access decisions can therefore become context-aware rather than permanently trusted.

30. Intelligent Endpoint Security

AI can monitor endpoint behaviour including:

- Process execution.
- File modifications.
- Network connections.
- Privilege changes.

Unexpected combinations of behaviours can trigger alerts.

International Research Journal of Studies in Computer Science and Engineering
Volume: 01, Issue: 01, August 2026 | ISSN: XXXX.XXXX

31. IoT Security

IoT environments often contain large numbers of heterogeneous devices.

AI can establish individual behavioural profiles.

For example:

Normal Device Profile

→ Expected communication

→ Expected frequency

→ Expected destinations

A deviation may indicate compromise.

32. Cloud Security

Cloud environments generate large volumes of logs and events.

AI can correlate:

- Authentication events.
- API calls.
- Resource access.
- Network traffic.

This can identify suspicious cloud activity.

33. Performance Evaluation Framework

The proposed framework should be evaluated using:

Metric	Purpose
Accuracy	Overall classification performance
Precision	Correctness of positive detections
Recall	Ability to detect attacks
F1-score	Balance between precision and recall
False-positive rate	Unnecessary alerts
Detection latency	Speed of detection
Throughput	Processing capacity
Adaptation time	Speed of learning new threats

International Research Journal of Studies in Computer Science and Engineering
Volume: 01, Issue: 01, August 2026 | ISSN: XXXX.XXXX

34. Experimental Design

A potential experimental study could compare:

Model A

Traditional signature-based IDS.

Model B

Single machine-learning classifier.

Model C

Unsupervised anomaly detector.

Model D

Proposed adaptive hybrid AI framework.

The models can be evaluated using identical datasets and testing conditions.

35. Dataset Strategy

An experimental implementation may use combinations of:

- Network-flow datasets.
- Intrusion-detection datasets.
- IoT security datasets.
- Enterprise traffic records.
- Synthetic attack environments.

Data should be separated into:

Training → Validation → Testing

to prevent evaluation bias.

36. Ablation Analysis

The proposed framework can be tested by removing individual components.

For example:

- Without anomaly detection.
- Without adaptive learning.
- Without risk scoring.
- Without threat intelligence.
- Without feedback.

This helps determine which components contribute most to performance.

37. Expected Results

The proposed framework is expected to provide:

- Improved detection of emerging threats.
- Reduced false positives.
- Faster threat identification.
- Improved prioritisation.
- Greater adaptability.
- Better support for distributed networks.

Actual performance should be established through empirical experimentation rather than assumed.

38. Security and Privacy Considerations

AI-based cybersecurity systems process potentially sensitive network information.

Important safeguards include:

- Data minimisation.
- Encryption.
- Access control.
- Secure model storage.
- Privacy-preserving learning.
- Audit logging.

39. Challenges

Major implementation challenges include:

1. High computational requirements.
2. Data-quality problems.
3. Class imbalance.
4. Adversarial attacks.
5. Model drift.
6. Explainability.
7. False positives.
8. Privacy concerns.
9. Integration with legacy systems.
10. Regulatory requirements.

40. Research Contributions

The proposed study contributes:

Contribution 1

An integrated AI-driven cybersecurity architecture.

Contribution 2

Hybrid detection combining known-threat classification and anomaly detection.

Contribution 3

Dynamic risk assessment.

Contribution 4

Adaptive response mechanisms.

Contribution 5

Continuous learning through analyst feedback.

Contribution 6

Integration of edge, cloud and intelligent network environments.

41. Future Research Directions

Future work should explore:

- Large-scale security foundation models.
- Autonomous security agents.
- Explainable threat detection.
- Federated cybersecurity intelligence.
- Quantum-resistant security analytics.
- AI-powered deception systems.
- Privacy-preserving anomaly detection.
- Self-healing networks.
- Adversarially robust machine learning.
- Collaborative threat intelligence.

42. Discussion

The proposed framework represents a shift from static cybersecurity toward adaptive defence.

Traditional systems often ask:

"Does this activity match a known attack?"

An adaptive AI system can additionally ask:

"Is this behaviour unusual for this environment?"

and:

International Research Journal of Studies in Computer Science and Engineering
Volume: 01, Issue: 01, August 2026 | ISSN: XXXX.XXXX

"How risky is this deviation?"

and:

"What response is appropriate?"

This broader perspective is particularly important in intelligent computing networks where devices, applications and traffic patterns continuously change.

The most important feature of the framework is its feedback loop. Threat detection should not be treated as a one-time prediction problem. Security environments evolve continuously, requiring models to learn from new observations.

However, complete autonomous cybersecurity also introduces risks. Incorrect automated decisions could disrupt legitimate services. Therefore, the most appropriate architecture is likely to combine automated low-risk responses with human oversight for high-impact decisions.

43. Conclusion

AI-driven adaptive cybersecurity provides a promising approach for protecting increasingly complex intelligent computing networks. The proposed framework combines network monitoring, data preprocessing, machine-learning-based anomaly detection, threat classification, dynamic risk assessment and adaptive response within a continuous learning architecture.

Unlike purely signature-based systems, the framework is designed to identify behavioural deviations and emerging threats even when explicit attack signatures are unavailable. The integration of edge and cloud intelligence further supports low-latency detection while enabling large-scale model training and threat-intelligence analysis.

Nevertheless, AI does not eliminate cybersecurity challenges. Model drift, adversarial attacks, false positives, data scarcity, explainability and privacy remain important concerns. Consequently, future cybersecurity systems should emphasise robust AI, continuous validation and human-centred security operations.

Ultimately, the evolution of cybersecurity is likely to move toward adaptive, context-aware and continuously learning defence systems. By combining machine intelligence with security expertise and carefully controlled automation, AI can contribute to more resilient computing networks capable of responding to increasingly sophisticated and rapidly changing cyber threats.

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. Sommer, R., & Paxson, V. (2010). Outside the closed world: On using machine learning for network intrusion detection. 2010. IEEE Symposium on Security and Privacy, 305–316.
3. Shone, N., Ngoc, T. N., Phai, V. D., & Shi, Q. (2018). A deep learning approach to network intrusion detection. IEEE Transactions on Emerging Topics in Computational Intelligence, 2(1), 41–50.
4. Chandola, V., Banerjee, A., & Kumar, V. (2009). Anomaly detection: A survey. ACM Computing Surveys, 41(3), 1–58.
5. Liao, H.-J., Lin, C.-H. R., Lin, Y.-C., & Tung, K.-Y. (2013). Intrusion detection system: A comprehensive review. Journal of Network and Computer Applications, 36(1), 16–24.
6. Garcia-Teodoro, P., Diaz-Verdejo, J., Maciá-Fernández, G., & Vázquez, E. (2009). Anomaly-based network intrusion detection: Techniques, systems and challenges. Computers & Security, 28(1–2), 18–28.
7. Sommer, R., & Paxson, V. (2010). Outside the closed world: On using machine learning for network intrusion detection. 2010. IEEE Symposium on Security and Privacy, 305–316.
8. Apruzzese, G., Colajanni, M., Ferretti, L., Guido, A., & Marchetti, M. (2018). On the effectiveness of machine and deep learning for cyber security. 2018 10th International Conference on Cyber Conflict, 371–390.
9. Khraisat, A., Gondal, I., Vamplew, P., & Kamruzzaman, J. (2019). Survey of intrusion detection systems: Techniques, datasets and challenges. Cybersecurity, 2, 20.
10. Ring, M., Wunderlich, S., Grüdl, D., Landes, D., & Hotho, A. (2019). A survey of network-based intrusion detection data sets. Computers & Security, 86, 147–167.
11. Tufan, E., Kaya, T., & Alhajj, R. (2021). A survey on adversarial machine learning for cybersecurity. ACM Computing Surveys.
12. Biggio, B., & Roli, F. (2018). Wild patterns: Ten years after the rise of adversarial machine learning. Pattern Recognition, 84, 317–331.
13. McMahan, B., Moore, E., Ramage, D., Hampson, S., & y Arcas, B. A. (2017). Communication-efficient learning of deep networks from decentralised data. Proceedings of AISTATS, 1273–1282.

14. Shokri, R., & Shmatikov, V. (2015). Privacy-preserving deep learning. Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security, 1310–1321.
15. Ferrag, M. A., Maglaras, L., Moschoyiannis, S., & Janicke, H. (2020). Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study. Journal of Information Security and Applications, 50, 102419.