Dydaktyka Informatyki 20(2025)
ISSN 2083-3156; e-ISSN 2543-9847
DOI: 10.15584/di.2025.20.15
https://www.journals.ur.edu.pl/di

Uniwersytet Rzeszowski

**Jacek WOŁOSZYN**[1], **Agnieszka MOLGA**[2]

[1] *ORCID: 0000-0003-4340-9853. Dr inż., Uniwersytet Radomski, Wydział Informatyki i Matematyki, Katedra Informatyki, ul. Malczewskiego 20A, 26-600 Radom, e-mail: jacek.woloszyn@uthrad.pl*
[2] *ORCID: 0000-0002-0857-5111. Dr, Uniwersytet Radomski, Wydział Transportu, Elektrotechniki i Informatyki, Katedra Informatyki, ul. Malczewskiego 29, 26-600 Radom, e-mail: agnieszka19216@wp.pl*

data złożenia tekstu do Redakcji DI: 18.05.2025; data wstępnej oceny artykułu: 27.05.2025

# ADVANCED ARTIFICIAL INTELLIGENCE METHODS IN CYBERSECURITY, THREAT AND ANOMALY DETECTION USING UNSUPERVISED LEARNING TECHNIQUES

# ZAAWANSOWANE METODY SZTUCZNEJ INTELIGENCJI W CYBERBEZPIECZEŃSTWIE, WYKRYWANIE ZAGROŻEŃ I ANOMALII Z WYKORZYSTANIEM TECHNIK UCZENIA BEZ NADZORU SZTUCZNEJ INTELIGENCJI

**Keywords:** cybersecurity, detection, anomalies, Python, implementations, artificial intelligence, machine learning.
**Słowa kluczowe:** cyberbezbieczeństwo, detekcja, anomalie, python, implementacje, sztuczna inteligencja, uczenie maszynowe.

**Abstract**

Artificial intelligence (AI) is playing an increasingly important role in cybersecurity, enabling faster and more effective detection and response to threats. One of them is the detection of threats and anomalies.

Machine learning algorithms process vast amounts of data in real time, detecting unusual patterns that may indicate potential attacks (e.g., DDoS attacks, intrusions, or network scanning attempts).

AI-based systems learn what behaviours are the norm for a given environment and then flag any deviations, which can help identify new, unknown threats. The first part discusses the use of machine learning algorithms in the environment of real data. The following parts discuss anomalies in network traffic and the possibilities of using ML techniques, as well as the initial process of data collection and preparation.

**Streszczenie**

Sztuczna inteligencja (AI) odgrywa coraz większą rolę w dziedzinie cyberbezpieczeństwa, umożliwiając szybsze i bardziej efektywne wykrywanie oraz reagowanie na zagrożenia. Jednym z nich jest wykrywanie zagrożeń i anomalii.

Algorytmy uczenia maszynowego przetwarzają ogromne ilości danych w czasie rzeczywistym, wykrywając nietypowe wzorce, które mogą wskazywać na potencjalne ataki (np. ataki DDoS, włamania lub próby skanowania sieci).

Systemy oparte na AI uczą się, jakie zachowania są normą dla danego środowiska, a następnie sygnalizują wszelkie odchylenia, co może pomóc w identyfikacji nowych, nieznanych zagrożeń. W rozdziale pierwszym poruszono wykorzystanie algorytmów uczenia maszynowego w środowisku rzeczywistych danych. W kolejnych rozdziałach omówiono anomalie w ruchu sieciowym i możliwości zastosowania technik ML oraz wstępny proces zbierania i przygotowania danych.

# Preface

In response to the increasing number of cyberattacks, organizations frequently leverage artificial intelligence (AI) and machine learning (ML) to detect emerging and sophisticated threats. A crucial aspect is threat and anomaly detection, which enables the rapid identification of unusual behavioral patterns within a network or system. In cases of DDoS attacks, intrusion attempts, or data breaches, swift action is essential, making real-time data processing solutions and deep learning models increasingly significant.

This article presents the key areas and methods for effective network traffic analysis and anomaly detection, including unsupervised learning techniques such as One-Class SVM and Isolation Forest.

# 1. Network Traffic Analysis

## 1.1. Real-Time Data Processing

The first step in network traffic analysis involves gathering detailed information about network activity, including packets, logs, and connection metadata. In practice, this is achieved using network monitoring systems such as Zeek (Bro) and Suricata, as well as log and event collection tools like Syslog and platforms such as the ELK Stack (Elasticsearch, Logstash, Kibana).

To detect threats in near real-time, Apache Kafka is employed for queuing incoming data and distributing it across different processing modules. Spark Streaming and Flink are used for real-time analysis, enabling the immediate detection of anomalous traffic patterns.

This approach allows the system to generate alerts and take preventive actions in cases of sudden spikes in request volume (e.g., a potential DDoS attack) before cybercriminals can cause significant damage.

### 1.2. Use of Machine Learning Algorithms

*Classification and Pattern Detection*

ML models (e.g., decision trees, random forests, or neural networks) are trained on historical data to recognize characteristic patterns associated with attacks.

DDoS attacks are characterized by sudden spikes in the number of packets or connections from multiple sources.

Intrusion attempts involve unusual login sequences that deviate from known behavior.

Systematic connections to multiple ports or IP addresses within a short time frame may indicate network scanning

Flow analysis utilizes statistics related to network flows[1] (number of packets, average packet size, session duration). ML models examine what values are typical for a given environment and signal deviations from the norm.

### 1.3. Advanced Deep Learning Techniques

Autoencoders are neural networks that learn to compress and reconstruct data, aiding in anomaly detection. If a significant reconstruction error occurs when processing network traffic, it may indicate activity that deviates from the "normal" traffic pattern.

Neural networks with regression (RNN, LSTM)[2] are highly effective in sequential analysis, where temporal dependencies are crucial, such as login sequences or packet order. They can help detect unusual event sequences in the case of complex attacks (APT).

## 2. Anomaly Detection

### 2.1. The Role of Normal Behavior Modeling

In anomaly detection, it is crucial to define what is considered "normal" within a given system. Models are built based on historical data that describe standard operations of users, applications, and devices.

---

[1] Zhou Zhi-Hua, *Ensemble Methods: Foundations and Algorithms*, Chapman and Hall/CRC, 2012; L. Sweeney, *k-Anonymity: A Model for Protecting Privacy*, "International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems", Vol. 10, No. 5, 2002.

[2] C. Althoff, *The Self-Taught Programmer: The Definitive Guide to Programming Professionally*, Independently published, 2017; R. Sommer, V. Paxson, *Outside the Closed World: On Using Machine Learning for Network Intrusion Detection*, IEEE Symposium on Security and Privacy (SP), 2010; Scikit-Learn Developers, *Scikit-Learn: Machine Learning in Python*, "Journal of Machine Learning Research" 2011, Vol. 12.

Network conditions often fluctuate (e.g., increased traffic in online stores during holiday seasons). To prevent excessive false alarms, models should dynamically adapt to changing conditions.

Since traditional signature-based systems struggle with new attack patterns, anomaly detection enables the identification of unusual behaviors, even if they have not been previously observed. This makes zero-day detection particularly important.

In cybersecurity, zero-day vulnerabilities (or zero-day exploits) refer to software weaknesses that are unknown to developers and have not yet been patched. The term "zero-day" means that developers have zero days to respond once the vulnerability is discovered before cybercriminals can exploit it.

### 2.2. Supervised vs. Unsupervised Approaches

Supervised learning requires labeled data (i.e., knowing which samples are attacks and which are not). This approach can be challenging because a comprehensive dataset of known attacks is not always available.

Unsupervised learning focuses solely on normal behavior patterns, treating any significant deviation as an anomaly. This method effectively detects unknown threats and zero-day attacks since it does not rely on predefined signatures.

## 3. Unsupervised Techniques

Unsupervised learning methods[3] are highly effective in cybersecurity, where labeled attack data is often scarce or difficult to obtain.

Below is a description of two popular algorithms.

### 3.1. One-Class SVM, Concept and Theoretical Foundations

A specialized variant of SVM (Support Vector Machine) that attempts to define a boundary for "normal" data. Anything outside this boundary is considered anomalous.

The model is trained on data representing only normal behavior.

New data points are evaluated against the defined boundary; those beyond it are classified as anomalies, leading to decision-making.

The nu parameter controls what proportion of data may be considered anomalies.

[3] I. Goodfellow, Y. Bengio, A. Courville, *Deep Learning*, MIT Press, 2016; M. Bishop Christopher, *Pattern Recognition and Machine Learning*, Springer, 2006.

*Advantages and Limitations*

Does not require labeled attack data, can model complex dependencies (using kernel functions).

Parameter selection (e.g., nu) can be challenging; computational cost increases with large and high-dimensional datasets.

### 3.2. Isolation Forest, Concept and Theoretical Foundations

This method assumes that anomalies can be easily "isolated" from the rest of the data, as they are rare and significantly different. The algorithm builds multiple random partitioning trees, where anomalies are isolated in fewer steps.

Each tree randomly splits the dataset into smaller fragments.

If an object is quickly separated from the rest (i.e., has a short path length in the tree), it is likely an anomaly.

The average isolation depth determines the final anomaly score.

*Advantages and Limitations*

Fast, scalable, easy to implement, and relatively robust to differences in data scale.

Random partitions may overlook subtle anomalies in highly complex datasets; selecting the number of trees and maximum depth requires testing.

## 4. Implementation Process and Practical Challenges

### 4.1. Data Collection and Preparation

Operational system data includes logs, network traffic metadata, and user activity. It is crucial to ensure that these datasets represent the widest possible cross-section of typical behavior.

Initial data preprocessing, such as data cleaning (removing duplicates, filling in missing values), normalization, and dimensionality reduction (e.g., PCA), helps obtain a clearer data representation.

### 4.2. Model Training and Validation

Parameter tuning is crucial in model development, allowing precise model optimization. In One-Class SVM, this includes setting the nu value and selecting the kernel parameter. In Isolation Forest, key parameters include the number of trees and maximum tree depth.

*Validation Methods*

Cross-validation (k-fold cross-validation) can help identify optimal parameters, even in anomaly detection scenarios.

In test environments, simulated attack events can be injected to verify whether the model detects them correctly.

*Performance Evaluation*

Metrics Precision, Recall, F1-score, and anomaly-specific indicators such as AUROC and AUPRC.

False positives, a high False Positive (FP) rate can overwhelm SOC teams and discourage automated response implementations.

### 4.3. Integration with Security Information and Event Management (SIEM) Systems and Response Mechanisms

Anomaly detection module outputs are forwarded to SIEM systems (e.g., Splunk, IBM QRadar) to correlate findings with other data sources, providing a broader security perspective.

Upon detecting a strong anomaly signal[4], the system may, block traffic from suspicious IP addresses.

Segment the network.

Alert the SOC team to initiate automated defense actions.

### 4.4. Example, DDoS Attack Scenario in a Corporate Environment

The system identifies a sudden increase in concurrent connections.

Models (e.g., Isolation Forest) detect an abnormal surge in unusual network flows.

This information is cross-referenced with firewall and IDS logs, triggering an alert. SIEM Correlation.

Response, the SOC team is notified, and the system automatically blocks suspicious traffic sources.

## Conclusion and Future Perspectives

Anomaly detection-based AI techniques are becoming the foundation of modern cybersecurity. Unsupervised methods such as One-Class SVM and Isolation Forest enable the detection of previously unknown attacks, particularly when labeled data is unavailable.

Reduced dependency on signature-based detection, which cannot keep up with emerging threats.

Scalable and effective tools for analyzing vast volumes of network traffic in real time.

With increasing network complexity and cybercriminal creativity, the future lies in hybrid solutions combining supervised and unsupervised learning, and

[4] V. Chandola, A. Banerjee, V. Kumar, *Anomaly Detection: A Survey*, "ACM Computing Surveys" 2009, Vol. 41, No. 3.

even reinforcement learning (RL) approaches. Growing attention is also directed toward federated learning, which enables organizations to share models without exchanging sensitive data.

However, false alarm costs and continuous model monitoring (model drift) must be considered when deploying such methods in production environments. Close collaboration between SOC teams, system administrators, and AI experts is essential.

Ultimately, integrating AI-driven anomaly detection with established security practices can significantly enhance network and system security, providing organizations with a critical edge in the constantly evolving battle against cyber threats.

## Bibliography


Althoff C., *The Self-Taught Programmer: The Definitive Guide to Programming Professionally*, Independently published, 2017.

Bishop Christopher M., *Pattern Recognition and Machine Learning*, Springer, 2006.

Chandola V., Banerjee A., Kumar V., *Anomaly Detection: A Survey*, "ACM Computing Surveys" 2009, Vol. 41, No. 3.

Goodfellow I., Bengio Y., Courville A., *Deep Learning*, MIT Press, 2016.

Scikit-Learn Developers, *Scikit-Learn: Machine Learning in Python*, "Journal of Machine Learning Research"2011, Vol. 12.

Sommer R., Paxson V., *Outside the Closed World: On Using Machine Learning for Network Intrusion Detection*, IEEE Symposium on Security and Privacy (SP), 2010.

Sweeney L., *k-Anonymity: A Model for Protecting Privacy*, "International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems" 2002, Vol. 10, No. 5.

Zhou Zhi-Hua, *Ensemble Methods: Foundations and Algorithms*, Chapman and Hall/CRC, 2012.