ESP Journal of Engineering & Technology Advancements (ESP-JETA)
ISSN: 2583-2646
Special Issue: 2nd International Conference on Emerging Trends in Interdisciplinary Engineering Research (CETIMER 2026)

Original Article

Detecting Cyber Attacks in Real Time Using AI-Based Network Monitoring

Dr. Pradeep Mishra[1], Komal Verma[2]
[1]*Associate Professor, Department of Mathematics, Banaras Hindu University, Varanasi, India*
[2]*Data Scientist, Fractal Analytics, Mumbai, India*

Abstract: *Cyber-attacks are increasing rapidly in frequency, complexity, and sophistication, making traditional security systems insufficient for protecting modern networks. Conventional intrusion detection systems rely on predefined signatures and rules, which limits their ability to identify zero-day attacks, polymorphic malware, insider threats, and other unknown attack patterns. Artificial Intelligence (AI)-based network monitoring provides a more advanced solution by continuously analyzing large volumes of network traffic in real time and learning the normal behavior of users and devices. Machine learning techniques such as Random Forest, Support Vector Machine, and K-Means can classify traffic and detect anomalies, while deep learning models including Convolutional Neural Networks (CNN), Long Short-Term Memory (LSTM), and Autoencoders improve the detection of complex and evolving threats. By monitoring routers, servers, cloud systems, and IoT devices, AI-based systems can identify suspicious activities within seconds and reduce response time significantly. This research examines the role of AI in real-time cyber-attack detection, including system architecture, attack types, monitoring techniques, datasets, algorithms, advantages, challenges, and future developments. The study also compares different AI models and proposes an effective framework for implementing intelligent network monitoring systems in modern organizations.*

Keywords: *Cybersecurity, Artificial Intelligence, Network Monitoring, Intrusion Detection System, Machine Learning, Deep Learning, Real-Time Detection, Cyber Attacks.*

I. INTRODUCTION

The rapid digital transformation of modern society has significantly changed the way organizations operate and communicate. Businesses, governments, hospitals, banks, educational institutions, and industries increasingly depend on interconnected computer networks to perform daily activities. Cloud computing, online banking, e-commerce, remote working, digital classrooms, and smart healthcare systems have improved efficiency, accessibility, and communication. Organizations can now store large amounts of information, process transactions instantly, and provide services across the world through network-based technologies. However, this growing dependence on digital systems has also increased the exposure of networks to cyber threats. Every connected device, server, database, or cloud application becomes a potential entry point for attackers. As a result, the number and sophistication of cyber-attacks continue to rise each year.

Cybercriminals today use highly advanced methods to exploit vulnerabilities in computer networks. Common threats include phishing, ransomware, malware, Distributed Denial of Service (DDoS) attacks, insider attacks, botnets, and Advanced Persistent Threats (APTs). Phishing attacks trick users into revealing confidential information such as passwords, bank account details, or personal data through fake emails and websites. Ransomware attacks encrypt files and demand payment from victims before access is restored. Malware spreads through infected files, websites, or software and damages systems or steals information. DDoS attacks flood a network or website with massive amounts of traffic, making it unavailable to legitimate users. Insider attacks occur when employees or authorized users intentionally or unintentionally misuse their access privileges. Botnets are networks of compromised devices controlled remotely by attackers to launch large-scale attacks. APTs are long-term attacks in which attackers secretly remain inside a network for weeks or months to steal valuable information. These threats are becoming more dangerous because attackers constantly change their techniques to avoid detection.

Modern cyber-attacks occur extremely quickly. A ransomware attack can encrypt thousands of files within a few minutes, while a DDoS attack can disable an entire website or online service almost instantly. Attackers often automate their activities using malicious software, making it difficult for human analysts to respond in time. In large organizations, thousands or even millions of network packets travel through the system every second. Security teams cannot manually inspect such a huge amount of traffic. Consequently, by the time a suspicious activity is noticed, the attacker may have already stolen data, damaged systems, or spread across the entire network. The increasing speed and complexity of cyber-attacks highlight the urgent need for intelligent systems that can detect threats in real time.

Traditional cybersecurity tools such as firewalls, antivirus software, and rule-based Intrusion Detection Systems (IDS) have been widely used for many years. These systems are designed to identify attacks by comparing network activity with a

database of known signatures or predefined rules. For example, if a malicious program matches a known pattern stored in the system, the IDS can detect and block it. Although this method works well for previously identified threats, it has several limitations. Attackers frequently change the structure of malware, modify attack behavior, or create completely new techniques that do not match existing signatures. Such attacks are called zero-day attacks because they exploit vulnerabilities before security systems have time to update their databases. Rule-based systems also struggle to identify polymorphic malware, which changes its code repeatedly to avoid detection. As a result, traditional security approaches are often ineffective against modern threats.

Artificial Intelligence (AI)-based network monitoring has emerged as a powerful solution to overcome these limitations. AI systems can continuously observe and analyze network traffic from routers, servers, switches, cloud platforms, and user devices. Unlike traditional systems, AI does not depend only on fixed rules or signatures. Instead, it learns the normal behavior of a network by examining historical and real-time data. For example, the system can learn the usual login time of employees, the normal amount of traffic on a server, or the standard communication pattern between devices. When the AI system detects behavior that differs from the normal pattern, it can identify it as suspicious and generate an alert.

Machine learning and deep learning techniques play a major role in AI-based monitoring. Machine learning algorithms such as Random Forest, Support Vector Machine, and K-Means can classify traffic as normal or malicious. Deep learning models such as Convolutional Neural Networks (CNN), Long Short-Term Memory (LSTM), and Autoencoders are capable of analyzing more complex traffic patterns and identifying unknown attacks. These techniques allow the system to recognize subtle anomalies that may be difficult for humans or traditional tools to notice. For instance, if an employee account suddenly begins downloading large amounts of sensitive data late at night, the AI system can identify this as unusual behavior and warn the security team immediately.

Real-time AI-based monitoring provides several important benefits for organizations. It enables the immediate detection of cyber-attacks before they spread across the network. Faster detection reduces response time and allows organizations to take quick action, such as blocking malicious IP addresses, isolating infected devices, or shutting down suspicious connections. Early detection also minimizes financial losses, operational disruption, and damage to reputation. In addition, AI systems can identify previously unknown attack patterns, making them highly effective against zero-day threats and evolving malware. Therefore, AI-based network monitoring is becoming an essential component of modern cybersecurity strategies, helping organizations protect their data, systems, and digital infrastructure more effectively.

Figure 1. Ai-Based Network Monitoring Dashboard Detecting Cyber Attacks in Real Time

II. TIME CYBER ATTACK DETECTION

Cybersecurity incidents in modern networks develop at an extremely rapid speed. In many cases, an attack can cause significant damage within a few minutes or even seconds. For example, a ransomware attack can quickly encrypt thousands of files stored on servers, employee computers, and cloud platforms. Once the files are encrypted, the organization may lose access to important documents, customer records, and operational data. Similarly, a Distributed Denial of Service (DDoS) attack can flood a website or server with an enormous amount of traffic, causing the service to become unavailable almost instantly. When such incidents are not detected immediately, the consequences become more severe, leading to financial losses, business disruption, and damage to reputation.

One of the major reasons why real-time cyber-attack detection is necessary is that attackers increasingly use automated tools and artificial intelligence to launch attacks. Modern cybercriminals no longer depend only on manual hacking techniques. Instead, they use automated malware, attack scripts, and AI-powered tools that can scan networks, identify vulnerabilities, and exploit systems much faster than humans can respond. These tools can launch thousands of attacks simultaneously, target multiple systems at once, and continuously adapt to bypass security measures. Since attackers can operate at machine speed, organizations also require intelligent systems capable of responding in real time. Traditional security systems that depend on manual monitoring or delayed analysis are no longer sufficient in such an environment.

Another important factor is the enormous amount of traffic generated by modern networks. Large organizations may handle millions of data packets every second. Employees use email, cloud applications, online meetings, databases, mobile devices, and Internet of Things (IoT) systems throughout the day. This creates a huge amount of network activity that security analysts cannot inspect manually. Human experts may be able to review a limited number of alerts, but they cannot continuously analyze every packet, login attempt, file transfer, and communication occurring across the network. As a result, suspicious activities may remain unnoticed until it is too late. Real-time detection systems solve this problem by automatically analyzing large volumes of traffic and identifying malicious patterns immediately.

The increasing use of cloud computing and IoT devices has also created additional security challenges. Cloud platforms allow organizations to store data and run applications remotely, while IoT devices such as smart cameras, sensors, printers, and medical devices are becoming common in homes and businesses. Although these technologies improve convenience and efficiency, they also increase the number of endpoints connected to the network. Each connected device represents a potential vulnerability that attackers can exploit. Many IoT devices have weak security features, outdated software, or default passwords, making them easy targets for cybercriminals. If one vulnerable device is compromised, attackers may use it to gain access to other parts of the network. Therefore, organizations require continuous monitoring of all connected systems to identify suspicious behavior before the attack spreads.

Delayed detection allows attackers to move laterally within the network. After gaining access to one device or account, attackers often explore the network to identify more valuable targets. They may steal login credentials, access confidential databases, or move from one system to another without being noticed. This process is known as lateral movement. In many data breach incidents, attackers remain hidden inside the network for days, weeks, or even months before they are discovered. During this time, they can collect sensitive customer information, financial records, trade secrets, or intellectual property. The longer an attacker remains undetected, the greater the damage becomes. Real-time detection is therefore essential because it can identify unusual behavior at the earliest stage and stop attackers before they gain full control of the network.

The consequences of delayed detection can be extremely serious for organizations. In the case of ransomware, late detection may allow the malware to encrypt all important files, causing business operations to stop completely. Organizations may then be forced to pay a ransom or spend large amounts of money restoring their systems. DDoS attacks can make websites, banking systems, online shopping platforms, or government services unavailable to users, resulting in customer dissatisfaction and financial loss. Data breaches caused by delayed detection can expose confidential customer information, including personal details, passwords, and payment data. Such incidents often lead to legal penalties, loss of trust, and damage to the organization's reputation.

Insider attacks are another major concern. Employees or authorized users may intentionally or accidentally misuse their access privileges. If suspicious activity is not detected immediately, insiders may copy confidential documents, leak sensitive information, or damage important systems. Similarly, botnet infections can spread malware rapidly across multiple devices in the network. A single infected computer can communicate with other compromised devices and create a large botnet capable of launching attacks on other systems. Without real-time monitoring, such infections may continue spreading until the entire network is affected.

For these reasons, organizations require intelligent and automated systems that can detect malicious behavior the moment it occurs. Real-time cyber-attack detection enables security teams to respond immediately, isolate infected systems, block malicious traffic, and reduce the overall impact of an attack. It improves the ability of organizations to protect sensitive information, maintain service availability, and ensure business continuity in an increasingly complex digital environment.

III. AI-BASED NETWORK MONITORING

AI-based network monitoring refers to the use of artificial intelligence, machine learning, and deep learning techniques to observe, analyze, and secure computer networks. Unlike traditional monitoring systems that rely on fixed rules and previously known attack signatures, AI-based systems learn from historical and real-time network traffic. These systems

are capable of understanding the normal behavior of users, devices, and applications within a network. Once normal behavior is learned, the system can identify unusual activities that may indicate a cyber-attack.

The primary objective of AI-based network monitoring is to detect suspicious activity before it causes serious damage. In modern organizations, networks contain a large number of connected devices, including computers, mobile phones, servers, cloud systems, and Internet of Things devices. Every second, these devices generate huge amounts of traffic that cannot be manually analyzed by security teams. AI-based systems solve this problem by automatically collecting and examining the traffic data.

The monitoring process generally includes the following stages:

- Collection of network traffic from routers, servers, firewalls, cloud systems, and endpoints
- Cleaning and preprocessing of the collected data
- Extraction of important features such as IP address, port number, packet size, and protocol type
- Analysis of traffic patterns using AI algorithms
- Detection of suspicious or abnormal behavior
- Generation of alerts and automatic response to the attack

The first stage is the collection of traffic data. The system gathers information from different parts of the network, including routers, firewalls, switches, servers, cloud applications, and user devices. This traffic may include login records, packet details, communication between systems, and data transfer activities. Because large organizations may generate millions of packets every second, automated monitoring becomes necessary.

After collecting the traffic, the system preprocesses the data. Raw network traffic often contains repeated packets, incomplete records, unnecessary values, and missing information. If this raw data is analyzed directly, it can reduce the performance of the AI model. Therefore, preprocessing is performed to remove duplicate records, fill missing values, normalize the data, and convert text-based information into numerical form.

Once the data is prepared, the system extracts useful features from it. Feature extraction is important because not every detail in network traffic is useful for attack detection. The AI system selects only the information that can help identify suspicious behavior. For example, the system may examine the source IP address, destination IP address, port number, connection duration, packet size, and number of failed login attempts. These features help the system understand how the network normally behaves.

After feature extraction, machine learning and deep learning algorithms analyze the traffic. The AI model compares current activity with previously learned normal behavior. If the traffic pattern appears different from what is expected, the system marks it as suspicious. For example, if an employee who normally logs in during office hours suddenly accesses the system late at night and downloads a large amount of sensitive information, the AI system may identify this activity as an insider attack.

Different algorithms can be used for this analysis. Machine learning algorithms such as Decision Tree, Random Forest, Support Vector Machine, and K-Means are often used to classify network traffic as normal or malicious. Deep learning models such as Artificial Neural Networks, Convolutional Neural Networks, Long Short-Term Memory, and Autoencoders are more advanced and can identify complex attack patterns. These models are especially useful for detecting zero-day attacks and unknown threats that have never been seen before.

When suspicious activity is detected, the AI system immediately generates an alert. The alert is shown on a dashboard or sent to security administrators through email or mobile notifications. This allows the security team to respond quickly before the attack spreads across the network. In advanced systems, the response can be automatic. The AI system may block a malicious IP address, disconnect an infected device, stop unauthorized file transfers, or isolate a compromised system from the network. This automatic response reduces the time required to control the attack and prevents further damage.

An AI-based monitoring system contains several important components. The packet capture module records all incoming and outgoing traffic. The data preprocessing unit cleans the collected information. The feature extraction engine selects useful details from the traffic. The machine learning or deep learning model analyzes the behavior of the network. Finally, the alert and response mechanism informs administrators and takes necessary action.

AI-based network monitoring is more effective than traditional security systems because it can detect attacks quickly and accurately. It reduces the need for manual monitoring, provides continuous protection, and supports modern technologies such as cloud computing and IoT. As cyber threats continue to become more advanced, AI-based monitoring is becoming an essential part of network security in modern organizations.

IV . TYPES OF CYBER ATTACKS DETECTED BY AI SYSTEMS

A. Denial of Service (DoS) and Distributed Denial of Service (DDoS) Attacks

Denial of Service and Distributed Denial of Service attacks are among the most common forms of cyber-attacks detected by AI-based monitoring systems. In a DoS attack, a single system sends a large number of requests to a server in order to make it unavailable. In a DDoS attack, many infected devices from different locations send traffic to the target at the same time. As a result, the server becomes overloaded and cannot respond to legitimate users.

AI-based monitoring systems can quickly identify these attacks by examining traffic behavior. The system continuously observes the amount of traffic flowing through the network. If there is a sudden increase in traffic volume, repeated requests from multiple IP addresses, or unusual connection patterns, the AI model treats it as suspicious. Unlike traditional methods, AI can distinguish between normal high traffic and malicious traffic, which improves detection accuracy and reduces false alarms.

B. Malware and Ransomware

Malware is malicious software designed to damage systems, steal information, or gain unauthorized access. Ransomware is a type of malware that encrypts files and demands payment from the victim. Modern malware changes its code frequently to avoid detection, making traditional signature-based systems less effective.

AI systems detect malware and ransomware by analyzing behavior rather than only searching for known signatures. The system observes file activity, software execution, communication with external servers, and changes in system performance. If a device suddenly begins transferring unusual files, contacting suspicious websites, or encrypting many files within a short time, the AI system can identify the activity as malware or ransomware.

AI is especially useful for identifying unknown malware because it recognizes abnormal behavior patterns. Once the attack is detected, the system can isolate the infected device and prevent the malware from spreading across the network.

C. Phishing and Social Engineering

Phishing and social engineering attacks attempt to trick users into revealing passwords, bank details, or other confidential information. Attackers often send fake emails, messages, or websites that appear genuine. Since these attacks target human behavior, they are difficult to identify through traditional security tools.

AI-based monitoring systems can examine email traffic, sender information, URLs, and user actions to detect phishing attempts. For example, the system may identify suspicious email addresses, unusual subject lines, fake website links, or spelling mistakes commonly found in phishing emails. AI can also study user behavior. If a user suddenly clicks on a suspicious link or enters login credentials into an unknown website, the system can generate an alert.

AI helps reduce the success of phishing attacks by warning users before they provide confidential information to attackers.

D. Insider Threats

Insider threats occur when employees, contractors, or other authorized users misuse their access privileges. These threats may be intentional, such as stealing company data, or accidental, such as sending confidential information to the wrong person. Insider attacks are difficult to detect because the user already has legitimate access to the system.

AI-based monitoring systems study the normal behavior of each user. The system learns the usual login time, location, files accessed, and amount of data transferred by every employee. If a user behaves differently from normal, the AI system treats the activity as suspicious.

E. Advanced Persistent Threats (APT)

Advanced Persistent Threats are long-term and highly organized cyber-attacks. In an APT attack, the attacker enters the network and remains hidden for a long period. During this time, the attacker slowly collects information, steals sensitive data, and moves through different parts of the network without being noticed.

APT attacks are difficult to detect because the attacker behaves carefully and avoids obvious actions. Individual activities may appear harmless, but together they form a dangerous attack pattern. AI-based monitoring systems are highly effective in identifying these threats because they can connect multiple small anomalies.

V. MACHINE LEARNING TECHNIQUES USED IN CYBER ATTACK DETECTION M

Machine learning techniques are widely used in cyber-attack detection because they can examine large amounts of network traffic and identify suspicious behavior automatically. Unlike traditional security methods, machine learning models learn from traffic patterns and improve their performance over time. These techniques help security systems classify traffic

as normal or malicious, detect anomalies, and predict attacks before they cause major damage. Machine learning used in cybersecurity is generally divided into supervised learning, unsupervised learning, and reinforcement learning.

A. Supervised Learning

Supervised learning is the most common machine learning approach used in cyber-attack detection. In this method, the model is trained using labeled data. A labeled dataset contains examples of both normal network traffic and malicious traffic. During training, the model learns the difference between these two categories and uses this knowledge to classify new traffic.

A Decision Tree works by dividing the traffic into different branches based on conditions. It is simple and easy to understand. Random Forest improves accuracy by combining multiple decision trees. Support Vector Machine is effective when there is a clear separation between normal and malicious traffic. Naive Bayes uses probability to classify network activity, while Logistic Regression predicts whether a connection is safe or dangerous.

Supervised learning is very useful because it provides high accuracy when detecting known cyber-attacks. It can easily identify attacks such as phishing, malware, ransomware, and DDoS if these attack types are already present in the training data. Another advantage is that the training process becomes easier when a large labeled dataset is available.

However, supervised learning also has certain limitations. The model requires a large amount of labeled data, and preparing this data is often difficult and time-consuming. In addition, the system may fail to detect new or unknown attacks because it has never seen those attack patterns before. If attackers change their methods, the model may not recognize the new threat immediately.

B. Unsupervised Learning

Unsupervised learning is different because it does not require labeled data. Instead of learning from examples of attacks, the system studies the normal behavior of the network and identifies activities that appear unusual. This approach is very useful when labeled datasets are not available or when the organization wants to detect unknown attacks.

Unsupervised learning commonly uses techniques such as K-Means Clustering, DBSCAN, Isolation Forest, and Principal Component Analysis. K-Means groups similar traffic together and treats unusual traffic as suspicious. DBSCAN identifies groups of similar activities and recognizes anything outside the group as abnormal. Isolation Forest is designed to separate rare events from normal behavior, making it useful for detecting anomalies. Principal Component Analysis reduces unnecessary information and highlights the most important patterns in the traffic.

The main advantage of unsupervised learning is its ability to detect zero-day attacks and unknown threats. Since the model focuses on abnormal behavior instead of predefined attack signatures, it can identify attacks that have never appeared before. This makes it useful for detecting insider threats, unusual user behavior, and Advanced Persistent Threats.

Although unsupervised learning is effective, it may produce more false alarms. Because the system treats any unusual behavior as suspicious, it may sometimes classify normal activities as attacks. For example, if an employee works late at night or downloads many files for an urgent task, the system may incorrectly identify this behavior as malicious.

C. Reinforcement Learning

Reinforcement learning is another important machine learning technique used in cyber-attack detection. In this method, the system learns by receiving rewards and penalties. When the AI system takes the correct action, it receives a reward. When it takes the wrong action, it receives a penalty. Over time, the system learns the best way to respond to different situations.

Reinforcement learning is especially useful for adaptive cybersecurity systems. Instead of only detecting attacks, it can also learn how to respond automatically. For example, if the system successfully blocks malicious traffic or isolates an infected device, it receives a reward and learns that this response is effective. If the chosen response fails, the system changes its strategy in the future.

This method is highly useful in modern networks where cyber threats change continuously. Reinforcement learning allows security systems to adapt automatically and improve their performance without constant human supervision. It can be used in firewall management, network traffic control, automatic blocking of malicious users, and response to DDoS attacks. As cyber threats continue to evolve, reinforcement learning is becoming an important part of intelligent cybersecurity systems.

VI. DEEP LEARNING FOR REAL-TIME DETECTION

Deep learning is a branch of artificial intelligence that uses artificial neural networks with many layers to analyze and understand data. In cybersecurity, deep learning is very useful because modern network traffic is large, complex, and

continuously changing. Traditional security methods often fail to identify advanced cyber-attacks because they depend on predefined rules and known attack signatures. Deep learning models are more effective because they can automatically learn hidden relationships and patterns from network traffic. These models can identify suspicious activities in real time and improve the accuracy of cyber-attack detection.Deep learning is especially important for real-time detection because cyber-attacks often happen very quickly. Malware, ransomware, phishing, and insider threats can spread across a network within minutes. Deep learning models analyze large amounts of traffic and identify unusual behavior before serious damage occurs. They are also useful for detecting unknown attacks that have never appeared before.Artificial Neural Networks are the simplest type of deep learning model. They are designed to work in a way similar to the human brain. An ANN contains several layers of connected neurons. Each neuron receives information, processes it, and sends the result to the next layer. By using many layers, the model can learn complex relationships in the data.In cybersecurity, ANN models are mainly used for general classification of network traffic. They learn the difference between normal and malicious behavior by studying training data. After training, the model can examine new traffic and decide whether it is safe or dangerous. ANN models are commonly used for identifying malware, phishing attacks, unauthorized access, and unusual traffic patterns.

Although ANN models are useful, they are not always the best choice for highly complex attacks. They may struggle when the traffic contains complicated patterns or when the attack develops slowly over time. For this reason, more advanced deep learning models such as CNN, RNN, and LSTM are often preferred.Convolutional Neural Networks are deep learning models designed for pattern recognition. They are widely used in image analysis, but they can also be applied to network traffic. In cybersecurity, traffic data can be represented as matrices, allowing CNNs to examine the structure of the traffic in a similar way to an image.recognize specific patterns that are often associated with malicious behavior. For example, if a certain type of malware always generates a particular sequence of packets, the CNN model can learn this pattern and identify it immediately.CNN-based detection is especially useful because it can recognize complex attack signatures that traditional systems cannot detect. It is widely used for detecting malware patterns, DDoS attacks, and intrusion attempts. Since CNN models can process large amounts of traffic quickly, they are suitable for real-time monitoring systems.Recurrent Neural Networks are designed for analyzing sequential data. Unlike other deep learning models, an RNN can remember previous information and use it when analyzing new data. This makes RNNs useful in cybersecurity because network traffic often occurs as a sequence of events over time.

In cyber-attack detection, RNN models are used to study how traffic changes from one moment to another. For example, an attacker may attempt to log in repeatedly using different passwords. An RNN can observe this sequence and recognize the repeated attempts as suspicious behavior. Similarly, if a user suddenly accesses multiple systems in an unusual order, the model can identify the abnormal pattern.Long Short-Term Memory is a more advanced form of Recurrent Neural Network. LSTM models are designed to remember important information for a longer period of time. This makes them highly effective for detecting attacks that happen slowly or in multiple stages.Many cyber-attacks do not occur immediately. Advanced Persistent Threats, insider attacks, and ransomware often develop gradually. An attacker may remain inside the network for several days or weeks before causing damage. LSTM models can remember earlier network activity and compare it with later behavior. If the sequence appears suspicious, the model can identify the attack.For example, an employee account may log in at unusual times over several days and slowly transfer confidential information. A normal system may not notice this behavior, but an LSTM model can observe the pattern across time and recognize it as an insider threat. LSTM models are therefore very useful for detecting Advanced Persistent Threats, ransomware, and long-term suspicious behavior.

Autoencoders are deep learning models mainly used for anomaly detection. An autoencoder first learns what normal network behavior looks like. After learning the normal pattern, the model tries to reproduce it. If the new traffic is very different from the learned behavior, the system identifies it as suspicious.Autoencoders are particularly useful because they do not need labeled attack data. Instead of learning examples of attacks, they focus only on normal traffic. Any major deviation from normal behavior is treated as a possible cyber threat. This makes autoencoders highly effective for detecting unknown attacks and zero-day threats.For example, if a network suddenly begins showing unusual login activity, suspicious file transfers, or unexpected communication with external servers, the autoencoder can detect that the behavior is different from normal traffic. The system then generates an alert for the security team. Autoencoders are also useful for reducing the size of traffic data, making it easier and faster to analyze large networks. Because of their ability to detect previously unknown attacks, autoencoders play an important role in modern AI-based cybersecurity systems.

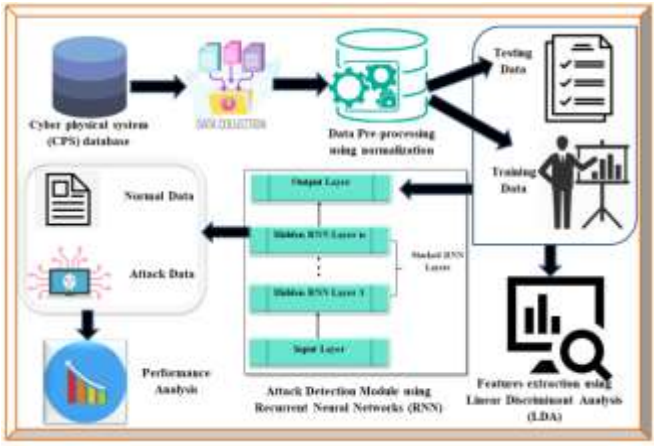

Figure 2.Deep learning model architecture for cyber attack detection

VII. DATASETS USED FOR AI-BASED NETWORK MONITORING A

AI-based network monitoring systems require high-quality datasets for training and testing. A dataset is a collection of network traffic records that includes both normal behavior and malicious activity. These datasets are used to teach machine learning and deep learning models how to recognize cyber-attacks. Without proper datasets, the AI system cannot learn the difference between safe traffic and harmful traffic.

Dataset	Description	Common Use
KDD Cup 1999	One of the earliest intrusion detection datasets containing normal and attack traffic	Basic machine learning training
NSL-KDD	Improved version of KDD Cup 1999 with fewer duplicate records and better quality	Classification research
CICIDS2017	Contains modern network traffic and recent cyber-attacks	Realistic intrusion detection testing
UNSW-NB15	Includes both normal and malicious traffic with modern attack categories	Deep learning research
Bot-IoT	Dataset focused on attacks against IoT devices	IoT security research
ToN-IoT	Includes IoT traffic, network traffic, and telemetry data	Real-time monitoring research

Cybersecurity datasets usually contain information such as source IP address, destination IP address, port number, packet size, protocol type, connection duration, and attack category. Some datasets contain only traditional attacks, while others include modern threats such as ransomware, botnets, DDoS attacks, phishing, and insider attacks. Researchers use these datasets to evaluate the performance of AI models and compare different algorithms.

The KDD Cup 1999 dataset is one of the oldest and most widely known cybersecurity datasets. It was created to support intrusion detection research and contains a large number of traffic records. The dataset includes several categories of attacks, such as Denial of Service, Probe attacks, Remote-to-Local attacks, and User-to-Root attacks. Since it is one of the earliest datasets, many machine learning studies still use it for basic training and performance comparison. However, the dataset has several limitations because it contains duplicate records and outdated attack patterns. As a result, it is not very useful for detecting modern cyber threats.

To solve the problems found in KDD Cup 1999, researchers developed the NSL-KDD dataset. NSL-KDD is an improved version that removes duplicate records and provides a more balanced distribution of data. Because of these improvements, NSL-KDD is widely used for machine learning classification research. The dataset contains examples of both normal traffic and malicious traffic, allowing researchers to train algorithms such as Decision Tree, Random Forest, and Support Vector Machine. Although NSL-KDD is better than KDD Cup 1999, it still does not include the latest cyber-attacks found in modern networks.

CICIDS2017 is one of the most important datasets used in current cybersecurity research. It was developed to represent real-world network traffic and includes both normal activity and modern attacks. The dataset contains various attack categories, including DDoS, brute force attacks, botnets, infiltration, ransomware, and web attacks. CICIDS2017 is considered realistic because the traffic was generated in an environment similar to a real organization. It also includes detailed information about user behavior and attack patterns. Because of these features, CICIDS2017 is widely used for testing intrusion detection systems and evaluating deep learning models.

Another widely used dataset is UNSW-NB15. This dataset was created to overcome the limitations of older datasets and provide a more modern collection of network traffic. UNSW-NB15 contains both normal traffic and multiple attack categories, such as worms, shellcode, backdoors, reconnaissance, and exploits. The dataset includes many useful features that help machine learning and deep learning models identify cyber threats more accurately. UNSW-NB15 is especially popular in deep learning research because it contains more realistic traffic patterns and better represents current cyber-attacks.

The growth of Internet of Things technology has created the need for specialized datasets. Many organizations now use smart devices, sensors, cameras, and connected machines, which can also become targets for attackers. Bot-IoT is a dataset designed specifically for IoT security research. It contains network traffic generated by botnet attacks, DDoS attacks, scanning attacks, and data theft in IoT environments. Researchers use Bot-IoT to train AI models that can detect attacks against smart devices.

ToN-IoT is another important dataset for IoT-based monitoring. It includes information from IoT devices, network traffic, operating systems, and sensor data. Unlike many other datasets, ToN-IoT combines different types of information in one dataset. This makes it useful for real-time monitoring and for detecting attacks in complex environments where IoT devices are connected to larger networks.

Among all these datasets, CICIDS2017 and UNSW-NB15 are the most widely used in modern research. They are preferred because they include recent attack categories, realistic traffic patterns, and a large number of useful features. These datasets help AI models perform better in real-world situations and improve the accuracy of cyber-attack detection systems.

VIII. PROPOSED AI-BASED REAL-TIME MONITORING FRAMEWORK

An AI-based real-time monitoring framework is designed to identify cyber-attacks immediately after they appear inside an enterprise network. The framework continuously monitors the movement of data across the organization and analyzes traffic in real time. Unlike traditional monitoring systems that depend mainly on fixed rules and manual observation, this framework uses artificial intelligence to learn the normal behavior of the network and identify unusual activities automatically. Because modern cyber-attacks can spread within a few minutes, a real-time monitoring framework is necessary to reduce damage and improve security.

The first stage of the framework is data collection. The system continuously gathers network packets and traffic information from multiple sources within the organization. These sources include firewalls, routers, cloud servers, end-user devices, and Internet of Things sensors. Firewalls provide information about incoming and outgoing connections. Routers show how data travels through the network. Cloud servers generate information related to online applications and storage systems. End-user devices such as computers, laptops, and mobile phones provide login details and user activity. IoT sensors contribute additional information from smart devices and connected machines.

The purpose of data collection is to ensure that every activity inside the network is observed. Since cyber-attacks can happen at any time, the collection process must operate continuously. Large organizations may generate millions of packets every second, making it impossible for humans to inspect every connection manually. Therefore, automatic collection is an essential part of the framework.

After collecting the traffic, the next stage is data preprocessing. Raw network traffic often contains repeated packets, missing values, incomplete records, and unnecessary information. If this data is used directly, the AI model may produce incorrect or inaccurate results. Therefore, the data must first be cleaned and prepared before analysis begins.

During preprocessing, duplicate packets are removed so that the same activity is not counted multiple times. Missing values are corrected or replaced to make the data complete. Text-based information such as protocol names and service types is converted into numerical form because machine learning algorithms can only process numbers. The data is also normalized so that all values are represented on a similar scale. This step improves the quality of the data and increases the accuracy of the monitoring system.

Once the traffic is cleaned, the system performs feature extraction. Feature extraction means selecting the most important details from the network traffic. Not every piece of information is useful for attack detection. Therefore, the framework focuses only on those features that can help distinguish between normal behavior and malicious behavior.

The most important features usually include source IP address, destination IP address, packet size, port number, protocol type, number of failed login attempts, and session duration. The source and destination IP addresses help identify where the communication begins and where it ends. Packet size may reveal whether an unusually large amount of

information is being transferred. Port numbers indicate which services are being accessed. The number of failed login attempts may indicate a password attack, while session duration can help identify unusual long-term connections.

After feature extraction, the next stage is AI model training. In this step, the selected machine learning or deep learning model learns the difference between normal traffic and malicious traffic. The system is trained using cybersecurity datasets that contain examples of different attack types and normal network activity. Some datasets are labeled, meaning that the type of traffic is already known. Other datasets are unlabeled, requiring the model to discover patterns on its own.

The framework may use machine learning algorithms such as Decision Tree, Random Forest, and Support Vector Machine. It may also use deep learning models such as Convolutional Neural Network, Long Short-Term Memory, and Autoencoder. During training, the model studies the patterns present in the data and gradually learns how different attacks behave. After sufficient training, the model becomes capable of recognizing suspicious activity in real time.

The next stage is real-time detection. Every new packet or activity entering the network is immediately compared with the patterns learned during training. If the traffic matches normal behavior, it is treated as safe. If the activity appears unusual, the system classifies it as suspicious. If the activity clearly represents a cyber-attack, it is classified as malicious.

The system usually places the traffic into three categories: normal, suspicious, and malicious. Normal traffic represents ordinary user activity and requires no action. Suspicious traffic includes unusual behavior that may need further investigation. Malicious traffic indicates a clear attack and requires an immediate response. For example, if a user suddenly logs in from an unusual location and accesses confidential files, the system may classify the activity as suspicious. If the user then downloads a large amount of sensitive information, the system may classify the activity as malicious.

The final stage of the framework is automated response. Once malicious activity is detected, the system immediately takes action to reduce the impact of the attack. In traditional security systems, administrators must examine the alert and then decide how to respond. This process can take several minutes or hours. However, many modern attacks spread very quickly, so a delayed response can increase the damage.

The AI-based monitoring system can automatically block malicious IP addresses, disconnect compromised devices, notify administrators, and create incident reports. Blocking the IP address prevents the attacker from continuing the attack. Disconnecting infected devices stops malware from spreading to other systems. Notifications allow administrators to investigate the event, while incident reports provide detailed information about the attack.

This proposed framework provides faster detection, quicker response, and better protection than traditional monitoring methods. It helps organizations reduce financial loss, protect confidential information, and maintain secure operation of the network.

IX. COMPARATIVE ANALYSIS OF AI ALGORITHMS

Different AI algorithms are used in cyber-attack detection because each algorithm has its own strengths and weaknesses. Some algorithms are faster and easier to use, while others provide higher accuracy and better detection of unknown attacks. Choosing the correct algorithm is important because network environments are different. A small organization may require a fast and simple model, while a large enterprise may need a more complex model capable of detecting advanced cyber threats.

The comparison of AI algorithms is usually based on four factors: accuracy, speed, ability to detect unknown attacks, and complexity. Accuracy refers to how correctly the algorithm identifies malicious traffic. Speed indicates how quickly the algorithm can process the traffic. Suitability for unknown attacks shows whether the algorithm can detect new threats that were not present in the training data. Complexity describes how difficult the algorithm is to train and implement.

Algorithm	Accuracy	Speed	Suitable for Unknown Attacks	Complexity
Decision Tree	Medium	Fast	Low	Low
Random Forest	High	Medium	Medium	Medium
Support Vector Machine (SVM)	High	Medium	Medium	High
K-Means	Medium	Fast	High	Low
Convolutional Neural Network (CNN)	Very High	Medium	Medium	High
Long Short-Term Memory (LSTM)	Very High	Slow	High	Very High
Autoencoder	High	Fast	Very High	Medium

Table 1. Comparison of Major AI Algorithms

Decision Tree is one of the simplest machine learning algorithms used in cyber-attack detection. It works by dividing the traffic into different branches according to certain conditions. Decision Tree is easy to understand and can process data

very quickly. Because of its low complexity, it is suitable for small and medium-sized networks.However, the accuracy of Decision Tree is only moderate. It works well when the attack patterns are simple and already known. The model is less effective for unknown attacks because it depends mainly on patterns that have already been learned.Random Forest is an improved version of the Decision Tree algorithm. Instead of using a single tree, it combines many trees and then makes a final decision based on the combined result. This improves the accuracy of the system and reduces errors.

Random Forest provides high accuracy and is commonly used in cybersecurity research. It can detect known attacks more effectively than Decision Tree and can also identify some unknown attacks. However, because it uses many trees, it is more complex and slower than a single Decision Tree.Support Vector Machine is a machine learning algorithm that separates normal traffic and malicious traffic using a boundary. It is highly accurate and works well when there is a clear difference between safe and dangerous network behavior.SVM performs better than many simple algorithms because it can handle complex traffic patterns. However, it is more difficult to train and requires more computational power. It is also less suitable for very large datasets because the processing speed becomes slower as the amount of traffic increases.K-Means is an unsupervised learning algorithm. Unlike supervised methods, it does not require labeled data. The algorithm groups similar traffic into clusters and identifies unusual traffic as suspicious.

K-Means is very useful for detecting unknown and zero-day attacks because it focuses on unusual behavior instead of known attack signatures. It is also fast and has low complexity. However, its accuracy is not as high as deep learning models because it may incorrectly classify some normal traffic as malicious.Convolutional Neural Networks are deep learning models used for recognizing complex patterns in data. CNNs are highly effective for analyzing network traffic because they can identify hidden relationships and intrusion signatures.CNN provides very high accuracy and is especially useful for detecting malware, DDoS attacks, and unusual traffic patterns. Although it is more powerful than traditional machine learning algorithms, it also requires more computational resources and takes longer to train.LSTM is one of the most advanced deep learning models used in cybersecurity. It is designed to remember previous traffic behavior and analyze long sequences of network activity. Because of this, it is highly effective for detecting attacks that happen over time, such as insider threats and Advanced Persistent Threats.

LSTM provides very high accuracy and can detect unknown attacks better than most other algorithms. However, it is slow and has very high complexity. Training an LSTM model requires large datasets and powerful hardware.Autoencoder is another deep learning model mainly used for anomaly detection. It learns the normal behavior of the network and identifies any activity that differs from that pattern. Because of this, it is highly effective for detecting unknown attacks and zero-day threats.Autoencoder provides high accuracy and very good performance for anomaly detection. It is faster than LSTM and less complex, making it a practical choice for many organizations. Among all the algorithms, Autoencoder is considered one of the best choices for identifying unknown cyber threats.The comparison shows that deep learning models such as CNN, LSTM, and Autoencoder provide the highest accuracy in cyber-attack detection. Among them, LSTM is the most effective for time-based attacks, while Autoencoder is the best for unknown threats. Traditional machine learning algorithms such as Decision Tree and Random Forest are easier to use and faster, but they are less effective against advanced attacks. Unsupervised techniques such as K-Means and Autoencoder are more suitable for detecting zero-day attacks because they focus on unusual behavior rather than known signatures.

X . ADVANTAGES OF AI-BASED CYBER ATTACK DETECTION

AI-based cyber-attack detection systems provide many advantages compared with traditional security methods. Traditional monitoring systems usually depend on fixed rules and known attack signatures. These systems can detect only previously identified threats and often fail when attackers use new techniques. AI-based systems are more effective because they learn from network behavior and adapt automatically to changing attack patterns.

cyber-attacks can spread across a network within minutes. Ransomware can encrypt files quickly, and DDoS attacks can make websites unavailable almost instantly. AI systems analyze traffic in real time and detect suspicious activity immediately. This allows organizations to respond before the attack causes major damage.

Another major benefit is the ability to detect zero-day and unknown attacks. Traditional systems depend on attack signatures that are already stored in their databases. If a new type of malware or attack appears, the traditional system may not recognize it. AI-based monitoring solves this problem by examining behavior instead of relying only on signatures. If the system notices unusual traffic, abnormal login activity, or unexpected file transfers, it can identify the behavior as suspicious even if the attack has never been seen before.

AI systems also reduce the need for manual monitoring. Large organizations generate huge amounts of network traffic every second. Human analysts cannot inspect every packet, login attempt, or file transfer. AI-based monitoring

automatically analyzes this information and highlights only the most important threats. This reduces the workload of security teams and allows them to focus on serious incidents.

Continuous surveillance is another important advantage. Unlike human analysts, AI systems can monitor the network every hour of the day without interruption. This is especially important because cyber-attacks may occur at any time, including nights, weekends, and holidays. Continuous monitoring improves the chances of detecting attacks early.

AI-based systems are also capable of processing very large amounts of data. Modern enterprise networks include cloud platforms, mobile devices, and IoT sensors, all of which generate large volumes of traffic. AI can analyze this traffic much faster than traditional methods

XI. CONCLUSION

Detecting cyber-attacks in real time has become one of the most important requirements in the modern digital environment. Organizations today depend heavily on computer networks, cloud services, mobile devices, and Internet of Things technologies for their daily operations. Businesses, banks, hospitals, governments, and educational institutions store large amounts of sensitive information in digital form. As the use of these technologies continues to increase, the risk of cyber-attacks also becomes greater. Attackers now use advanced tools, automation, and artificial intelligence to launch attacks more quickly and more effectively than ever before. Because of this, traditional security systems are no longer sufficient to protect modern networks.

Conventional security methods such as firewalls, antivirus software, and signature-based intrusion detection systems were designed mainly to identify known threats. These systems compare network activity with a database of previously identified attack signatures. Although this approach is useful for detecting common attacks, it has many limitations. Modern attackers constantly change their methods and create new forms of malware, phishing techniques, ransomware, and network intrusions. Zero-day attacks and polymorphic malware can easily avoid traditional detection systems because their behavior is different from known attack signatures. Therefore, relying only on conventional security methods creates a major weakness in the protection of modern networks.

AI-based network monitoring provides a more powerful and intelligent solution. Instead of depending only on fixed rules, AI systems continuously observe network behavior and learn what is normal within the organization. The system collects information from routers, firewalls, cloud servers, user devices, and IoT sensors. By studying this information, the AI model learns the usual behavior of users and devices. If any activity appears unusual, the system immediately identifies it as suspicious.

One of the greatest strengths of AI-based monitoring is its ability to detect both known and unknown attacks. Machine learning algorithms such as Decision Tree, Random Forest, Support Vector Machine, and K-Means help classify network traffic and identify malicious behavior. Deep learning models such as Convolutional Neural Network, Long Short-Term Memory, and Autoencoder provide even greater accuracy. These models can recognize hidden patterns in traffic and detect threats that may not be visible to traditional systems.

Random Forest is effective for identifying known attacks because it provides high accuracy and good performance with structured data. CNN models are useful for recognizing complex malware patterns and unusual traffic structures. LSTM models are especially important because they can remember previous network behavior and detect attacks that develop over time. For example, insider threats and Advanced Persistent Threats may continue for days or weeks before causing visible damage. LSTM models can identify these long-term attack patterns. Autoencoders are useful for detecting zero-day attacks because they learn normal behavior and identify anything that differs from it.

Another important advantage of AI-based cyber-attack detection is the reduction in response time. Traditional systems often require human analysts to examine alerts and decide what action should be taken. This process may take several minutes or even hours. During this time, the attacker may continue spreading malware, stealing data, or damaging systems. AI-based systems reduce this delay by detecting suspicious behavior in real time and responding automatically. The system can block malicious IP addresses, disconnect infected devices, stop suspicious file transfers, and notify administrators immediately. Faster response significantly reduces financial loss and limits the spread of the attack.

Despite these advantages, AI-based cybersecurity still faces several challenges. One major problem is the possibility of false positives. Sometimes the system may identify normal behavior as suspicious. For example, an employee working late at night or downloading many files for a project may be incorrectly treated as a threat. Too many false alarms can reduce the trust of security teams and increase their workload.

Privacy is another important concern. AI-based monitoring systems collect large amounts of information about users, devices, and communication. If this information is not protected properly, it may create privacy risks. Organizations must ensure that monitoring systems follow legal and ethical standards while protecting sensitive information.

The computational cost of AI systems is also high. Deep learning models such as CNN and LSTM require powerful computers, large datasets, and significant processing time. Small organizations may find it difficult to afford such systems. In addition, cybercriminals may try to attack the AI model itself by providing false data and misleading the system.

Even with these challenges, the future of AI-based cybersecurity remains very promising. New developments such as Explainable AI are making the decisions of AI systems easier to understand. Federated learning allows organizations to train AI models without sharing sensitive data, improving privacy. Autonomous response systems are becoming more advanced and can react to attacks without human involvement.

In the future, organizations will increasingly depend on intelligent monitoring systems to protect their networks. AI-based cyber-attack detection will continue to improve in accuracy, speed, and reliability. As cyber threats become more sophisticated, AI-based network monitoring will become an essential part of modern cybersecurity and will play a major role in protecting valuable data, systems, and digital infrastructure.

XII. REFERENCES

[1] Ahmad, Z., Khan, A. S., Shiang, C. W., Abdullah, J., & Ahmad, F. (2021). Network intrusion detection system: A systematic study of machine learning and deep learning approaches. *Transactions on Emerging Telecommunications Technologies*, 32(1), e4150.

[2] Sharma, V., & Kumar, M. (2025). Improving intrusion detection with hybrid deep learning models: A study on CIC-IDS2017, UNSW-NB15, and KDD CUP 99. *Journal of Information Systems Engineering and Management*, 10(11s).

[3] Kilincer, I. F., et al. (2025). Explainable AI supported hybrid deep learning method for intrusion detection using the CL2-IDS dataset. *Alexandria Engineering Journal*.

[4] Waghmode, P., et al. (2025). Intrusion detection system based on machine learning using NSL-KDD, CICIDS2017, and UNSW-NB15 datasets. *Scientific Reports*.

[5] Pinto, D., et al. (2025). A review on intrusion detection datasets: Tools, processes, and future trends. *Computer Networks*.

[6] Sajid, M., et al. (2024). Enhancing intrusion detection: A hybrid machine and deep learning approach. *Journal of Cloud Computing*, 13(1).

[7] Yogesh, et al. (2024). Deep learning based network intrusion detection system: A review and future directions. *International Journal of Information Security*.

[8] Wu, Y., et al. (2024). Current status, challenges and future trends of deep learning based intrusion detection systems. *Journal of Imaging*, 10(10), 254.

[9] Buyuktanir, B., et al. (2025). Federated learning in intrusion detection: Advancements, challenges, and opportunities. *Cluster Computing*.

[10] Rahmati, M. (2025). Towards explainable and lightweight AI for real-time cyber threat hunting in edge networks. *arXiv preprint arXiv:2504.16118*.

[11] Muhammad, A. E., Yow, K. C., Bacanin-Dzakula, N., & Khan, M. A. (2025). L-XAIDS: A LIME-based explainable AI framework for intrusion detection systems. *arXiv preprint arXiv:2508.17244*.

[12] Corea, P. M., Liu, Y., Wang, J., Niu, S., & Song, H. (2024). Explainable AI for comparative analysis of intrusion detection models. *arXiv preprint arXiv:2406.09684*.

[13] Sinha, P., et al. (2025). An efficient data driven framework for intrusion detection in cyber security datasets. *PeerJ Computer Science*.

[14] Han, L. (2023). A comparative study of intrusion detection using deep learning techniques. Technical Report, Universiti Kebangsaan Malaysia.

[15] Chowdhury, M. (2024). Advances in intrusion detection systems using machine learning and deep learning. *International Journal of Computer Applications*.

[16] Canadian Institute for Cybersecurity. (2017). CICIDS2017 dataset. University of New Brunswick.

[17] Tavallaee, M., Bagheri, E., Lu, W., & Ghorbani, A. A. (2009). A detailed analysis of the KDD CUP 99 dataset. *Proceedings of the IEEE Symposium on Computational Intelligence for Security and Defense Applications*.

[18] Moustafa, N., & Slay, J. (2015). UNSW-NB15: A comprehensive data set for network intrusion detection systems. *Military Communications and Information Systems Conference*, 1–6.

[19] Sharafaldin, I., Lashkari, A. H., & Ghorbani, A. A. (2018). Toward generating a new intrusion detection dataset and intrusion traffic characterization. *Proceedings of the 4th International Conference on Information Systems Security and Privacy*, 108–116.

[20] Koroniotis, N., Moustafa, N., Sitnikova, E., & Turnbull, B. (2019). Towards the development of realistic botnet dataset in the Internet of Things for network forensic analytics: Bot-IoT dataset. *Future Generation Computer Systems*, 100, 779–796.

[21] Moustafa, N. (2021). ToN-IoT telemetry dataset: A new generation dataset of IoT and IIoT attacks. *IEEE Access*, 9, 165130–165150.

[22] Denning, D. E. (1987). An intrusion-detection model. *IEEE Transactions on Software Engineering*, 13(2), 222–232.

[23] Bace, R., & Mell, P. (2001). Intrusion Detection Systems. National Institute of Standards and Technology.

[24] Biggio, B., Fumera, G., & Roli, F. (2014). Security evaluation of pattern classifiers under attack. *IEEE Transactions on Knowledge and Data Engineering*.

[25] Biggio, B., Corona, I., Nelson, B., Rubinstein, B. I. P., Maiorca, D., Fumera, G., & Roli, F. (2014). Evasion attacks against machine learning at test time. *Machine Learning and Knowledge Discovery in Databases*, 387–402.
[26] Goodfellow, I., Bengio, Y., & Courville, A. (2016). *Deep Learning*. MIT Press.
[27] Chollet, F. (2018). *Deep Learning with Python*. Manning Publications.
[28] Géron, A. (2022). *Hands-On Machine Learning with Scikit-Learn, Keras, and TensorFlow* (3rd ed.). O'Reilly Media.
[29] Bishop, C. M. (2006). *Pattern Recognition and Machine Learning*. Springer.
[30] Anderson, J. P. (1980). Computer security threat monitoring and surveillance. James P. Anderson Co.