CYBER ATTACK DETECTION AND MONITORING SYSTEM FOR COMPUTER NETWORKS BASED ON ARTIFICIAL INTELLIGENCE

associate professor Uzoqov Farkhod G'afforovich, Namangan state technical university
Phone: +998(94) 301 01 81 Email: farxodjonuzoqov@gmail.com

Abstract: This article discusses the detection and countermeasures of cyber threats in modern computer networks. It discusses a system for detecting and monitoring network attacks based on artificial intelligence technologies.

Keywords: Cybersecurity, artificial intelligence, intrusion detection system (IDS), network monitoring, data analytics, machine learning, normal and abnormal activity, threat prediction, network traffic.

Introduction

With the development of modern information and communication technologies, cybersecurity problems are becoming increasingly complex and widespread. Millions of cyberattacks are recorded worldwide every year, leading to serious financial losses and data privacy breaches. Since traditional security systems - firewalls, antivirus programs and signature-based intrusion detection systems - are limited in their effectiveness against unknown and emerging attacks, the development of artificial intelligence-based solutions is becoming an urgent task.

Artificial intelligence, especially machine learning and deep learning, provides the ability to automatically detect anomalies in network traffic, classify various attacks, and even predict emerging threats. These technologies have the ability to study complex patterns of network activity, identify the boundaries between normal and abnormal activity, and respond to threats in real time. Traditional protection mechanisms currently available cannot fully respond to the dynamics of increasing cyber threats. Therefore, the development of a system for detecting and monitoring network attacks based on artificial intelligence is one of the most promising areas of ensuring modern information security.

Asosiy qism

The aim of the project is to develop a system that effectively detects and monitors cyberattacks on computer networks based on artificial intelligence technologies. These are as follows:

- Conducting an analysis of modern threats in the field of network security;
- Developing methods for collecting and preparing data to detect network attacks;
- Creating an attack detection model based on machine learning algorithms;
- Experimentally evaluating the effectiveness of the developed system.

Modern analysis of network security threats

Currently, cyberattacks are becoming increasingly complex, and their types are constantly being updated. The main threats include:

DDoS attacks: Stopping the operation of a target server or network by overloading its resources.

Botnets: Armed attacks through networks consisting of many infected devices.

Phishing and execution attacks: Enticing users to disclose confidential information or forcing them to execute malicious code.

Data theft: Stealing significant data through illegal access.

Ransomware: Encrypting data and demanding a ransom to restore it.

Data collection and preparation

The CICIDS2017 dataset was used in the experimental part of the study. This dataset contains about 2.5 million records with more than 80 features reflecting real network traffic. The following steps were performed during the data preparation stage:

- ✓ Data cleaning: Duplicates, dotted lines, and invalid values were removed.
- ✓ Normalization: Numeric features were scaled, text data was converted to a numeric format.
- ✓ Feature selection: The most important features such as "Source Port", "Destination Port", "Protocol", "Packet Length", "Flow Duration" were extracted.

Classification of network attacks. In the study, network attacks were divided into the following main categories: Normal traffic, DDoS attacks, Port scanning, Botnet activity, Web attacks.

Machine Learning Model Creation

A variety of machine learning algorithms were compared and their performance was evaluated:

Decision Trees: Simple to understand and produced fast results, but had a high risk of overfitting.

Random Forest: Combined multiple decision trees to produce more accurate and consistent results.

Support Vector Machines (SVM): Demonstrated high accuracy on small datasets, but decreased performance on larger datasets.

Artificial Neural Networks (ANN): Highly capable of learning complex patterns, but computationally demanding.

The best results were achieved using the Random Forest algorithm, which achieved an accuracy rate of 96.5%.

System Architecture: The developed system consists of the following main modules:

1. Data Collection Module: Collects and processes network traffic.
2. Feature Extraction Module: Extracts traffic features.
3. Detection Module: Detects attacks using a machine learning model.
4. Monitoring and Reporting Module: Provides information about detected threats and generates reports.

Experimental results:

Various metrics were used to evaluate the reliability and effectiveness of the system: Accuracy: 96.5%, Precision: 95.8%, Recall: 96.2%, F1-Score: 96.0%

The results showed that the developed system has a much higher level of accuracy and reliability than traditional methods.

The CICIDS2017 dataset is used as the main source, a comparative analysis of various machine learning algorithms (Random Forest, SVM, CNN, LSTM) is performed, and the accuracy, reliability, and real-time performance of the system are evaluated. The results of the work can be practically applied in ensuring the security of corporate network infrastructure, data centers, and other critical infrastructure facilities.

Conclusion

In conclusion, it can be said that the network attack detection and monitoring system based on artificial intelligence offers an effective solution to modern cybersecurity problems and has the potential for widespread application in practice.

REFERENCES USED

1. Abdullayev, R. (2021). *Zamonaviy Axborot Xavfsizligi*. Toshkent: O'zbekiston Milliy Universiteti Nashriyoti.
2. Tanenbaum, A. S., & Wetherall, D. J. (2021). *Computer Networks*. 6th Edition. Pearson Education.

3. Goodfellow, I., Bengio, Y., & Courville, A. (2020). *Deep Learning*. MIT Press.

4. **Abdullayev, A. (2021). "Virtual reallik asoslari" o'quv qo'llanma**

5. **Karimov, S. (2022). "Kengaytirilgan reallik texnologiyalari" o'quv qo'llanma**

Online resources

1. Cisco Systems. (2023). Network Security Fundamentals. https://www.cisco.com/security

2. SANS Institute. (2023). Information Security Resources. https://www.sans.org

3. O'zbekiston Raqamli Texnologiyalar Vazirligi. (2023). Kiberxavfsizlik bo'yicha metodik qo'llanma. https://dtm.uz/cybersecurity