ALFA BK UNIVERSITY
FACULTY OF INFORMATION TECHNOLOGY
FACULTY OF MATHEMATICS AND COMPUTER SCIENCE
ALFATECH Journal

UDK: 711.45:004.78::004.8
DOI: https://doi.org/10.46793/AlfaTech1.3.01V
Original scientific paper

The role of artificial intelligence in malware detection in smart cities

Milica Varšandan[1], Čaba Varšandan[2], Veselinka Lejić[3]

Abstract: Smart cities have a complex structure and generate a large amount of data. This is precisely why the presence of artificial intelligence is necessary to effectively detect and neutralize any malware. Artificial intelligence enables not only detection but also an attack, but also to improve the entire smart city protection system. Combining available protection solutions with constant improvements and reacting at the right time are of most importance. This paper serves as a survey and tutorial on the application of artificial intelligence for malware detection in smart cities. The focus is placed on smart city domains such as the Internet of Things, Operational Technology, traffic management, utilities, and public safety systems. Areas outside the smart city context, such as personal cybersecurity or general IT infrastructure, are not covered in this study. The main contributions of this paper include: providing a comprehensive overview of how Artificial intelligence supports malware detection and prevention through advanced technologies and analytical methods, identifying key challenges and limitations in applying Artificial intelligence to urban cybersecurity, and outlining future directions for improving system resilience and adaptive protection. Artificial intelligence has a large number of algorithms and methods, which are helping to monitor and analyze the system behavior. In addition to identifying threats, it is possible to adapt to new forms of malicious software. There are certain challenges in implementing artificial intelligence for malicious software detection, as well as strategies for improving protection.

Keywords: artificial intelligence, detection, malware, smart cities

1 INTRODUCTION

The rapid development of digital technologies and urban infrastructures has led to the emergence of smart cities - complex systems in which information technologies, sensors, and Internet of Things (IoT) devices are interconnected to improve citizens' quality of life and the efficiency of resource management. However, in parallel with the connectivity increases, the exposure of these systems to various types of cyber threats increases, too. The most concerning are the malware attacks, malicious software designed to compromise system security, including data theft, or disrupt critical infrastructure operations.

In this regard, artificial intelligence (AI) has become a crucial help in combating modern cyberattacks. Using machine learning methods, big data analysis, and automatic anomaly detection, AI supports quick, accurate, and adaptive protection for smart cities. These clever systems are able to react instantly, foresee dangers, and learn from past mistakes.

The goal of the paper is to analyze the role of AI in detecting and preventing malware within a smart city environment. The methods employed in this process have received particular attention, ranging from machine learning and natural language processing (NLP) to more sophisticated strategies like graph neural networks (GNN) and hybrid approaches. The paper discusses different challenges and limitations associated with implementing these technologies. After conducting a literature review and finalizing the paper, the future development directions were outlined what could further enhance the cybersecurity of urban environments.

By looking at both theoretical frameworks and practical applications, the study aims to close the gap between research and real-world applications. Finally, it emphasizes how AI-driven cybersecurity solutions serve as the foundation for building safer, more resilient, and sustainable smart cities.

2 UNDERSTANDING THE CONTEX OF SMART CITIES

The development of smart cities brings great benefits such as efficiency and sustainability. The devices become increasingly connected to system automations, and as a result they are more exposed to cyber threats, and they include malware – malicious software that compromises security, uses or steals data or even to disable critical infrastructures.

Artificial intelligence plays a key role in identifying, analyzing, and neutralizing malware in smart cities. Using different methods from machine learning [1], big data processing [2], and automatic anomaly detection, AI enables quick and accurate system protection, as a direct result of it, it is reducing the risk of potential attacks. This paper explores how AI is applied in malicious software detection [3] and prevention in smart cities, analyzing the advantages of it, challenges with it, and future development perspectives.

Smart cities are urban environments that use advanced technologies, sensors, IoT devices, and data analytics to improve the efficiency of resource management, traffic control, and the safety and quality of life of the citizens. They operate based on networked systems that enable automatic data exchange and the real-time decision-making.

Smart cities bring numerous benefits, but their complexity and connectivity also create new security challenges. The large amount of generated and transferred data between different systems can be a target of cyberattacks, in the form of malware. Malicious software can compromise the operation of critical systems such as energy networks, transportation, or public safety systems, and could have major consequences for citizens and infrastructures if confidential information is stolen.

The implementation of advanced AI-based solutions is becoming essential for detecting and neutralizing malware in smart cities. The AI solutions enable automated monitoring of network traffic, analysis of behavioral patterns, and identification of potential threats at an early stage. This results in an increase in the security and resilience of the system to cyberattacks.

3 THREAT MODEL FOR SMART CITIES

A precise definition of the underlying threat model is necessary to build a thorough understanding of cybersecurity in smart cities. The primary assets that need to be safeguarded, the possible adversaries who might try to compromise them, the primary attack surfaces where threats can appear, and the common behaviors displayed by malicious software in these settings are all identified by this model. Putting this foundation in place makes it easier to understand how artificial intelligence will be used in later defense and detection systems.

3.1 Assets

Smart cities rely on a diverse set of a wide range interrelated resources that collectively enable their functionality. Communication infrastructures that link subsystems, control systems in charge of transportation, energy, and water distribution, centralized or edge-based data platforms that store, process, and analyze data, and Internet of Things nodes like environmental sensors, security cameras, and smart meters are a few examples. The confidentiality, availability, and integrity of these assets are critical to maintaining public safety and service reliability.

3.2 Adversaries

The spectrum of potential adversaries targeting smart cities is broad. It motivates individual hackers seeking financial gain, organized cybercriminal networks motivated by profit or disruption, insider threats with privileged access, and state-sponsored entities pursuing geopolitical or strategic objectives. These attackers look for weak spots in both technology and human behavior to break in, take control, or cause damage to digital systems.

3.3 Attack Surfaces

Intelligent urban systems present numerous, often overlapping vulnerabilities due to their interconnected nature. IoT nodes serve as frequent targets for attackers due to their minimal processing capabilities and absence of security measures. Inadequate authentication or outdated firmware can lead to the breach of controllers and gateways. A different high-risk vector is data pipelines, which transfer information among IoT devices, analytics platforms, and control systems. This is particularly accurate when data integrity or encryption protections are inadequate. Additionally, cloud interfaces and public communication networks heighten the risk of potential intrusions.

3.4 Typical Malware Behaviors

Malware that targets the infrastructure of smart cities can take many different forms. These include tampering with sensor readings to create false situational awareness, illegal system control, data exfiltration, and service interruption. To get around detection systems, more sophisticated malware may use covert strategies like code obfuscation, polymorphism, or delayed activation. Ransomware and botnet attacks continue to be common in critical infrastructures because they have the ability to stop vital services or incorporate compromised devices into massively coordinated attacks.

This threat model establishes the analytical framework for the subsequent sections of this paper, where artificial intelligence-based techniques for detecting, classifying, and mitigating these threats will be systematically explored

4 HOW ARTIFICAL INTELLIGENCE HELPS IN MALICIOUS SOFTWARE DETECTION

Artificial intelligence plays a key role in malware detection using advanced analytical methods that enable fast and accurate detection of threats in digital systems.

Machine learning methods are one of the most powerful tools in malware detection [5] because they allow systems to automatically learn from data and improve their detection capabilities without explicit programming. They analyze patterns and anomalies in network traffic, software behavior, and the structure of the malicious code. How machine learning contributes to malware detection:

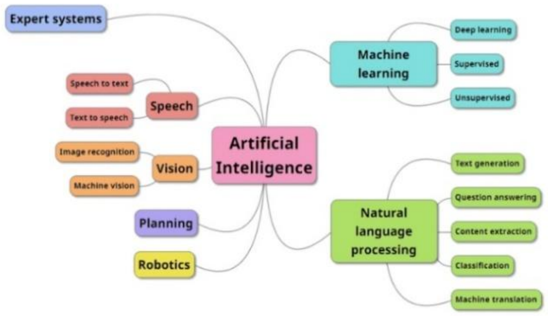

Figure 1 Types and uses of AI [4]

1) Data collection and feature extraction

Data collection: The system collects big data from many different sources, for example system logs, network traffic, application behavior, and user activity

Feature extraction: The relevant information is extracted, such as file access, communication frequency, unusual data flows, and code structure. These features serve as input for machine learning models.

2) Supervised learning

Training on labeled data: Pre-labeled data is used (the malware is clearly marked here), and the models are trained to distinguish between bad and good behavior.

Classification algorithms: Support Vector Machine (SVM), Random Forest, or neural networks learn how to classify new, unknown examples based on previously learned patterns.

Prediction: After the training is complete, the model can recognize and flag potential malicious activity in real time.

3) Unsupervised learning

Anomaly detection: In situations where pre-labeled data is not available or the malware is new and unknown, unsupervised algorithms identify unusual patterns that deviate from normal behavior.

Identification of new threats: Allows the detection of new or evolving malware that may not yet be documented/recognized in existing databases.

4) Automation of the analysis

Fast data processing: Machine learning models can analyze huge amounts of data in real time, significantly reducing the time to detect potential threats.

Continuous learning: As new threats emerge, the models will be regularly updated and improved, allowing the systems to adapt to changes and remain effective against new malware.

5) Threat detection and prevention

Identification of behavioral patterns: Machine learning allows the identification of suspicious patterns in system behavior, and this may include some unusual access to network resources or changes in application performance.

Automated responses: In combination with other systems, machine learning models can automatically trigger defensive measures, such as isolating an infected device or blocking suspicious activities, thereby preventing the spread of malware.

Figure 2 Traffic lights from TechCrunch [6]

Usage examples in smart cities:

In traffic [6]: if AI notices that traffic lights are behaving unusually, for example, if they all turn green at the same time, this could indicate an attack.

Public utilities [7]: sudden increase in energy consumption in a certain part of the city may indicate a cyberattack on the electricity distribution network or resource hijacking for mining purposes.

IoT devices [8]: if a sensor starts sending data to unknown servers, or irregular data or data types, AI can recognize the compromise and block it.

5 SPECIFIC ARTIFICAL INTELLIGENCE TECHNOLOGIES FOR MALWARE DETECTION

Artificial intelligence uses various technologies and approaches to improve malware detection and analysis.

These techniques enable faster, more accurate, and automated threat identification in digital environments, including smart cities. The combination of the mentioned technologies provides a powerful and effective malware protection system in smart city ecosystems.

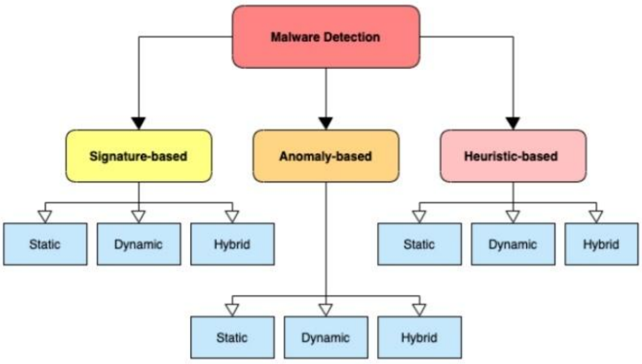

Figure 3 Classification of Malware Detection Techniques [4]

1) Natural Language Processing

NLP technology is used to analyze text data to identify malicious activity. The focus is on phishing messages, malicious emails, and fraudulent requests that often precede attacks.

Techniques used for malware detection:

Sentiment Analysis [9]: Can identify manipulative language in phishing emails, scams, and social engineering. For example, an email that uses the warning „Your account will be closed“ may be flagged as suspicious content.

Named Entity Recognition (NER) [10]: The algorithm recognizes keywords and phrases, such as bank names, user details, links, and phrases used in phishing emails. For example, if an email claims to be from „Paypal“, but the link leads to a suspicious domain, NLP can detect a discrepancy.

Parsing and Semantics Analysis [11]: NLP models analyze grammatical structure and detect anomalies that may indicate fraudulent emails generated using automated tools.

Tokenization and n-gram analysis [12]: Models are trained on known phishing emails to detect patterns in the text that indicate malicious messages.
An antivirus software can use NLP to analyze incoming emails in real time and block phishing attacks before they reach users.

2) Data classification and clustering

These techniques allow the analysis of large amounts of data and the automatic grouping of malware based on their behavior or structure.

Supervised Learning: Models trained on labeled data, i.e., known malware and files. Algorithms such as SVM, Random Forest, and Convolutional Neural Networks (CNN) are used here.

Unsupervised Learning – Clustering: Used when there are no predefined labels, for example, when new malware is discovered. Algorithms such as: K-Means, Density-Based Spatial Clustering (DBSCAN), and Principal Component Analysis (PCA).

Feature Extraction: Artificial intelligence analyzes malware characteristics such as: behavior patterns, the system it uses (Windows, Linux), and type of API call.

When unknown software or malicious software is detected on the network, the AI system can group it with similar threats and suggest appropriate defenses.

3) Reinforcement Learning (RL)

RL makes it possible for an AI model to continuously learn through interaction with its environment. Instead of passively analyzing data, RL allows AI systems to actively explore and adapt their strategies to combat malware.

Methods used for malware detection:

Q-Learning: This model learns from feedback and adapts to detect new attacks.

Deep Q Networks: A combination of deep learning and Q-Learning allows AI models to recognize complex attack patterns.

Policy Gradient Methods: Allow models to predict an attacker's next moves and take proactive protective measures.

The RL-based system can simulate various cyberattacks and train AI to recognize and block suspicious activities in real time.

4) Graph Neural Networks

Smart cities are built on large network infrastructures with thousands of connected devices. GNN helps analyze relationships between devices to identify potential cyberattacks..

GNN methods in malware detection:

Graph Embeddings: Represent devices and their interactions as a graph with nodes and links. Allows models to detect unusual connections that may indicate a hacker attack.

Anomalous Subgraph Detection: Identifies small parts of the network where suspicious activity is occurring.

Graph Convolutional Networks: Analysis enables the detection of dynamic relationships in the network and the identification of potential chain attacks.

If the AI model catches an unknown device attempting to establish unauthorized communication with smart city systems, it can immediately block it.

6 HYBRID METHODS

Hybrid methods in cybersecurity combine traditional malware detection techniques with modern AI models to provide more accurate, efficient, and adaptive protection. These methods enable the detection of both old and new threats. Some of the more notable hybrid methods are:

Static analysis: Relies upon traditional methods to recognize suspicious patterns in data. Here, heuristic analysis (examines suspicious behavior of files and applications based on previous patterns), frequency analysis (analyzes the frequency of certain operations associated with malware), and mathematical modeling (uses probabilistic models to predict threats).

By integrating AI models, traditional statistical analysis becomes much more accurate. Machine learning is used to analyze big data, recognize patterns, and identify anomalies. Deep Learning improves the detection of more complex threats by analyzing raw data such as network traffic and system calls. Automatic rule tuning adjusts detection thresholds, reducing false positives.

Antivirus software can use statistical analysis to detect suspicious network behavior, while AI models further evaluate patterns and make more accurate decisions based on real-world data.

Signature-Based detection [13]: Is one of the oldest and most widely used methods for identifying malware. This method works by using the libraries of known malware signatures and comparing them to analyzed files or network traffic.

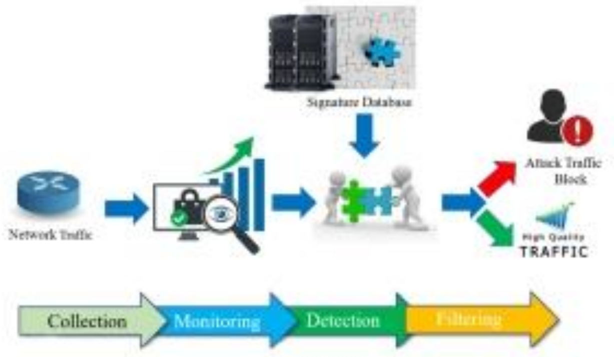

Figure 4 Methodology used in Signature-Based IDS [13]

It provides fast and efficient detection of known malware and has a low false positive rate. On the other hand, its major drawback is that it cannot recognize new and unknown threats and cannot easily adapt to polymorphic and metamorphic malware, which change their code to avoid detection.

AI improves Signature-Based Detection by detecting new threats, improving analysis of polymorphic malware, and reducing false positive detections.

A modern antivirus solution can use signature-based analysis to identify known malware, while an AI model analyzes suspicious files in parallel and assesses whether they represent a new threat.

7 AI BASED TOOLS FOR MALEWARE DETECTION

AI technologies play an increasingly important role in enhancing cybersecurity in complex infrastructures such as smart cities and IoT networks. These systems rely on machine learning, deep learning, and behavioral analysis to detect threats, analyze patterns, and respond to potential attacks. Combining multiple AI approaches can improve the resilience of smart city networks by addressing different types of malware and anomalies.

Several AI-based tools are widely studied in the literature for malware and network threat detection. These tools vary in terms of inputs, detection methodology, deployment requirements, and known limitations. Independent studies indicate that the choice of tool should be aligned with the specific environment and threat landscape, rather than relying solely on vendor-provided claims.

Table 1 Overview of AI-Based Malware Detection Tools

Tool	Inputs	Detection Style	Deployment Footprint
Darktrace	Network traffic, system telemetry	Behavioral anomaly detection	Enterprise network sensors
Cylance	Endpoint file and process data	Predictive machine learning	Lightweight on endpoints
Deep Instinct	Endpoint and file-level data	Deep learning (pre-execution)	Endpoint agents
Vectra	Network traffic, identity telemetry	AI-driven NDR/MXDR detection	Network and cloud-integrated sensors

Notes on Tool Limitations:

Darktrace: May produce higher false positives in dynamic environments [15] and relies heavily on network telemetry; endpoint coverage is limited.

Cylance: Focuses on endpoints and does not directly monitor network [16] or Operational Technology (OT)/IoT infrastructure; some zero-day malware may evade detection.

Deep Instinct: Limited independent long-term evaluations; primarily tested in controlled environments [17]; may require frequent model updates.

Vectra: May require extensive tuning for IoT/OT environments; fewer independent tests are available; primarily network-focused detection [18].

This overview emphasizes the practical capabilities and limitations of AI-based malware detection tools, providing a neutral, evidence-based perspective suitable for research purposes. By understanding the strengths and weaknesses of each approach, cybersecurity teams can design more robust and adaptive defense strategies for smart cities and IoT infrastructures.

8 CHALLENGES IN IMPLEMENTING AI FOR MALEWARE DETECTION

While AI technologies significantly improve malware detection and prevention, their implementation comes with numerous challenges. These challenges can make it difficult to effectively protect systems and require additional strategies to overcome them.

False positive and false negative results [14]: AI systems sometimes misidentify legitimate activities as threats (false positives), and on the other hand, they can miss malicious activities because they do not recognize them as threats (false negatives). In smart cities, false positives can cause unnecessary system outages, while false negatives can allow attackers to access critical infrastructure.

Let’s describe it with an example. AI can block legitimate network traffic because it thinks it is an attack. While some advanced malware may look like a regular file, the AI does not recognize it as a threat. This can be addressed by combining statistical analysis with AI to reduce the error rate, implementing hybrid methods that include expert supervision, and continuously optimizing the AI model to improve the malware databases.

Complexity of the algorithm: The problem here is that AI models for malware detection often use more complex algorithms, such as neural networks and graph analysis, and this requires a lot of computing power. Organizations have limited resources and may have trouble implementing these solutions, and devices in IoT networks and smart cities may not be able to execute complex AI algorithms in real time.

Let’s use this example. Large AI models require graphics processing units (GPU) or specialized processors and can be expensive. While real-time data processing can be delayed, this can lead to delays in attack detection. This can be addressed by using Cloud AI solutions where analysis is performed on remote servers, optimizing models to use fewer resources, such as the portable version of neural networks, and combining AI with edge computing technologies to reduce the load on local devices.

Lack of data for training the AI models: AI relies on a large amount of data and data sets to learn to recognize patterns in malware behavior. If an AI model is not trained on a wide enough range of threats, it may have trouble recognizing new and rare malware. Also, limited access to real malware samples can reduce the system's effectiveness. Imagine that like a sommelier without much experience. Would you rely on his/her suggestions?

New malware emerges every day, but there is not enough data to recognize them immediately. AI models can be over-adapted to known threats and fail to recognize zero-day attacks. This can be addressed by using synthetic data and simulation to train models. What is very important is to collaborate with researchers to collect new malware and apply unsupervised learning to recognize anomalies even in unknown malware.

Malware evolution: Attackers are using AI to develop more advanced and resilient malware. Malware can use automated methods of concealment, such as polymorphic and metamorphic techniques that change their code to avoid detection. Generative neural networks allow attackers to create malware that dynamically adapts to defense systems.

Malware can use AI to detect antivirus software and adapt its code to bypass it. Attacks like deepfake phishing use AI to generate convincing fake messages or even fake voices and videos. This is addressed by applying adversarial learning techniques, i.e., AI is trained against advanced malware to become more resilient to new threats. Then, by combining heuristic analysis and machine learning to recognize attack patterns that do not rely only on known malware, and constantly updating AI models through continuous learning and collaborative threat databases.

Data privacy: AI malware detection tools often analyze large amounts of data to identify threats. This data can contain sensitive user information, raising privacy and data protection concerns. Regulations such as GDPR (Europe) and CCPA (California) restrict how organizations can use user data.

An AI system can analyze emails and recognize phishing attacks, but at the same time, it can have access to users' private messages. Using a Cloud AI solution can mean that data is sent to third parties, which increases the risk of misuse. To prevent this, it is necessary to implement differential privacy, where AI can learn from data without direct access to user identities, to use local analytics (on-device AI) to keep data on the user's device, and to comply with legal regulations through data encryption and transparency in information processing.

9 CONTRIBUTIONS

This paper contributes to the field of smart city cybersecurity by providing a comprehensive analysis of how AI enhances malware detection and prevention within complex urban infrastructures. The study integrates theoretical insights with practical applications, demonstrating how AI-based methods such as machine learning, NLP, and GNN's can be used to better withstand against changing cyberthreats. The paper critically analyzes current issues with data limitations, algorithmic complexity, and privacy protection in addition to describing the technical workings of these approaches. It provides an informed viewpoint on the practical implications of these approaches, emphasizing the importance of balancing technological innovation with ethical considerations and regulatory compliance.

By synthesizing the capabilities and constraints of various AI-driven systems, the research underscores the necessity of developing adaptive and hybrid defense architectures capable of responding dynamically to new forms of malicious software. The findings aim to support further academic inquiry and guide practitioners in designing secure, intelligent, and sustainable digital environments for smart cities, while also pointing toward future research directions such as explainable AI, federated learningm and the integration of quantum computing for enhanced resilience.

10 CONCLUSION

The integration of AI within smart city infrastructures represents a key factor in achieving advanced and reliable cybersecurity. As the number of connected devices and data exchanges increases, so does the exposure to cyber threats, particularly malware. AI provides an essential advantage by enabling systems to independently detect, analyze, and respond to attacks in real time. Through the use of technologies such as machine learning, NLP, reinforcement learning, and GNN, AI can identify both existing and previously unknown types of malware, adapt to their evolving patterns, and react with exceptional speed and precision compared to traditional protection systems.

Despite its great potential, implementing AI in malware detection faces several challenges. Problems such as false alerts, complex algorithms that require significant computing power, insufficient training datasets, and privacy concerns can affect the overall efficiency of the system. In addition, the continuous evolution of malicious software - often enhanced by AI itself-demands constant adaptation and improvement of protection models. The best results are achieved by combining conventional security methods with AI-driven analytical approaches, creating a balanced and adaptive defense strategy.

Ultimately, the future of cybersecurity in smart cities depends on the intelligent application of artificial intelligence and ongoing innovation. By fostering collaboration between technology, research, and ethical data management, AI will not only strengthen digital defenses but also anticipate and prevent future cyber risks-ensuring a safer, more resilient, and sustainable urban ecosystem.

11 Reference

[1] Xiaoning Dou, Weijing Chen, Lei Zhu, Yingmei Bai, Yan Li, Xiaoxiao Wu (2023), Machine Learning for Smart Cities: A Comprehensive Review of Applications and Opportunities, (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 14, No. 9 DOI:10.14569/IJACSA.2023.01409104

[2] Ibrahim Abaker Targio Hashem, Victor Chang , Nor Badrul Anuar, Kayode Adewole, Ibrar Yaqoob, Abdullah Gani, Ejaz Ahmed, Haruna Chiroma (October 2016), The Role of Big Data in Smart City, International Journal of Information Management DOI:10.1016/j.ijinfomgt.2016.05.002

[3] Mustafa J.M. Alhamdi, Jose Manuel Lopez-Guede, Jafar AlQaryouti,
Javad Rahebi,Ekaitz Zulueta,Unai Fernandez-Gamiz (January 2025), AI-based malware detection in IoT networks within smart cities: A survey, Computer Communications,
DOI:https://doi.org/10.1016/j.comcom.2025.108055

[4] Md Jobair Hossain Faruk, Hossain Shahriar, Maria Valero, Farhat Lamia Barsha, Shahriar Sobhan, Md Abdullah Khan, Michael Whitman, Alfredo Cuzzocreak, Dan Lo, Akond Rahman and Fan Wu (December 2021), Malware Detection and Prevention using Artificial Intelligence Techniques, Conference: 2021 IEEE International Conference on Big Data
DOI:10.1109/BigData52589.2021.9671434

[5] Kaspersky, Machine Learning for Malware Detection, 2021

[6] Lorenzo Franceschi-Bicchierai, Hackers could create traffic jams thanks to flaw in traffic light controller, researcher says, July 18, 2024

[7] Vetrivel Subramaniam Rajkumar (Student Member, IEEE), Alexandru Ştefanov (Member, IEEE), Alfan Presekal (Student Member, IEEE), Peter Palensky (Senior Member, IEEE), and José Luis Rueda Torres (Senior Member, IEEE) (January 2023), Cyber Attacks on Power Grids: Causes and Propagation of Cascading Failures
DOI:10.1109/ACCESS.2023.3317695

[8] Anurag Tiwari, Akhilesh A. Waoo,
IoT based Smart Home Cyber-Attack Detection and Defense, August 2023

[9] Elastic Search AI Platform (2025), What is sentiment analysis?
www.elastic.co/what-is/sentiment-analysis

[10] Pavlos Evangelatos, Christos Iliou, Thanassis Mavropoulos, Konstantinos Apostolou, Theodora Tsikrika, Stefanos Vrochidis, Named Entity Recognition in Cyber Threat Intelligence Using Transformer-based Models, DOI: 10.1109/CSR51186.2021.9527981, July 2021

[11] Shabina Dhuria, Natural Language Processing: An approach to Parsing and Semantic Analysis, International Journal of New Innovations in Engineering and Technology, ISSN : 2319-6319

[12] Matthieu Jimenez, Cordy Maxime, Yves Le Traon, Mike Papadakis, On the Impact of Tokenizer and Parameters on N-Gram Based Code Analysis, 2018 IEEE International Conference on Software Maintenance and Evolution (ICSME), DOI: 10.1109/ICSME.2018.00053

[13] S. Jyoti, A. Bhandari, V. Baggan, M. Snehi, and Ritu, Diverse Methods for Signature based Intrusion Detection Schemes Adopted, International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878 (Online), Volume-9 Issue-2, July 2020
DOI:10.35940/ijrte.A2791.079220

[14] Omobolaji Olufunmilayo Olateju, Samuel Ufom Okon, Udochukwu ThankGod Ikechukwu Igwenagu, Abidemi Ayodotun Salami, Tunbosun Oyewale Oladoyinbo and Oluwaseun Oladeji Olaniyi, Combating the Challenges of False Positives in AI-Driven Anomaly Detection Systems and Enhancing Data Security in the Cloud, Asian Journal of Research in Computer Science Volume 17, Issue 6, Page 264-292, 2024; Article no.AJRCOS.118126 ISSN: 2581-8260,
DOI:https://doi.org/10.9734/ajrcos/2024/v17i6472

[15] Sontan, Adewale & Samuel, Segun. (2024). The intersection of Artificial Intelligence and cybersecurity: Challenges and opportunities. World Journal of Advanced Research and Reviews. 21. 1720-1736. DOI:10.30574/wjarr.2024.21.2.0607.

[16] Karantzas, George & Patsakis, Constantinos. (2021). An Empirical Assessment of Endpoint Security Systems Against Advanced Persistent Threats Attack Vectors.
DOI:10.48550/arXiv.2108.10422.

[17] Vähäkainu, Petri & Lehto, Martti. (2019). Artificial intelligence in the cyber security environment Artificial intelligence in the cyber security environment. Proceedings of the 14th International Conference on Cyber Warfare and Security ICCWS2019, 28 February - 1 March 2019, Stellenbosch University, South Africa, pages 431-440 https://www.researchgate.net/publication/338223306_Artificial_intelligence_in_the_cyber_security_environment_Artificial_intelligence_in_the_cyber_security_environment

[18] Abdiukov, Tim. (2025). AI-powered threat hunting: Designing real-time predictive security frameworks for professional cloud environments. Global Journal of Engineering and Technology Advances. 24. 014-024. DOI:10.30574/gjeta.2025.24.2.0232.

Contact information:

Milica VARŠANDAN,
Dr Lazar Vrkatic Faculty of Law and Business Studies, Novi Sad, Serbia
milicamarjanovic89@gmail.com

Čaba VARŠANDAN,
HTEC Group, Belgrade, Serbia
varsandancaba@gmail.com

Veselika LEJIĆ
Technical Faculty „Mihajlo Pupin„ Zrenjanin
veselinka89@gmail.com