COMPUTATIONAL PROBLEMS OF ELECTRICAL ENGINEERING

Vol. 14, No. 1, 2024

NEURO-SYMBOLIC MODELS FOR ENSURING CYBERSECURITY IN CRITICAL CYBER-PHYSICAL SYSTEMS

Serhii Yevdokymov

Department of Computer Science and Software Engineering, Kherson State University, Ivano-Frankivsk, Ukraine

serge.evdokimov2015@gmail.com

https://doi.org/10.23939/jcpee2024/01/042

Abstract: This paper presents the results of a comprehensive study on the application of the neuro-symbolic approach for detecting and preventing cyber threats in railway systems, a critical component of cyber-physical infrastructures. The increasing complexity and integration of physical systems with digital technologies have made such infrastructures vulnerable to cyberattacks, where breaches can result in severe consequences, including system failures, financial losses, and threats to public safety and the environment. The objective of this study was to assess the effectiveness of the neuro-symbolic approach, which combines artificial neural networks with symbolic algorithms, in detecting and mitigating cyber threats in dynamic environments. The methodology involved simulating various cyberattack scenarios on a test architecture for railway system security, followed by applying the neuro-symbolic model for threat detection and response. Results showed that the neuro-symbolic approach demonstrated high accuracy in detecting cyber threats and was particularly effective in adapting to new and unknown types of attacks. Compared to traditional methods, this approach significantly improved detection efficiency and response speed. The findings confirm that the neuro-symbolic approach enhances cybersecurity, particularly in critical infrastructures like railway systems, and contributes to more reliable protection of data related to passengers and transported goods. Further research will focus on optimizing the implementation of these algorithms and expanding the range of practical applications to other critical sectors.

Key words: neuro-symbolic approach, cyber-physical systems, machine learning, cybersecurity, critical infrastructure.

1. Introduction

The automation of cybersecurity decision-making for cyber-physical systems is a critical task in the face of growing threats [1, c. 500]. For the effective protection of information systems, it is necessary to create a model that describes the dependence of decisions on the characteristics of the objects and processes that need protection (for example, the state of the system at a certain point in time). In practice, due to the lack or insufficiency of expert knowledge, such models are often built on the basis of observations or precedents.

Some of the most popular and powerful tools for precedent-based modeling are artificial neural networks and neuro-symbolic models that can learn from precedents, and, therefore, enable extracting and generalizing knowledge from data [1, 2].

The object of study is the process of building neural networks for diagnosis and recognition of threats in cyber-physical systems.

The process of building neural models is usually time-consuming and iterative. The training time and accuracy of the neural network model depend significantly on the size and quality of the training sample used. Therefore, in order to improve the speed and quality of building a neural model, it is necessary to reduce the size of the sample while preserving its main properties.

The subject of the research is sampling methods for building neural network models based on precedents. Known sampling methods are highly effective, but they are often characterized by low speed and uncertainty of the quality criteria of the formed subsamples.

The purpose of the work is to increase the speed and quality of the process of forming selected training samples for building neural network models based on precedents in the context of cyber security.

2. Problem statement

Potential threats are actions or events that may harm a system or organization [3, p. 10]. In the context of cyber-physical systems, such threats can include cyberattacks, technical failures, human errors, or natural disasters that may negatively impact the integrity, confidentiality, or availability of data and systems. Vulnerabilities are weaknesses in systems, processes, or controls that can be exploited to execute a threat [4, p. 419]. Vulnerabilities can arise due to technical flaws, system misconfigurations, human errors, or the absence of proper security measures. Identifying and mitigating vulnerabilities is a key element of ensuring the security of cyber-physical systems, as they can serve as potential entry points for attackers.

Cyber-physical systems are exposed to a variety of threats that can lead to serious consequences [5, p. 21]. Table 1 provides a detailed analysis of potential threats and vulnerabilities in cyber-physical systems, enabling better understanding of the risks and the development of effective protective measures.

Table 1

Comparison of the main types of cyberattacks on cyberphysi cal systems

Type of attack	Description	Example	Consequences
Man-in-the-Middle (MitM)	The attacker intercepts and modifies data transmitted between two parties	An attack on a wireless network where the perpetrator intercepts data between users' devices and the router	Compromise of confidential data, alteration of transmitted information, breach of data integrity and confidentiality
Denial of Service (DoS)	Overloading of the system resulting in service denial	Attack on a web server generating excessive traffic that overwhelms the server, rendering it inaccessible to users	Denial of service, resource unavailability, economic losses due to downtime
Exploiting software vulnerabilities	Attackers exploit vulnerabilities in the code to gain unauthorized access to the system	Attack on a SCADA system through a vulnerability in the software used to manage industrial processes	Unauthorized access, modification, or destruction of data, disruption of critical systems
Social Engineering	Manipulation of users to obtain confidential information	Phishing attack, where the user receives an email pretending to be from a legitimate sender and enters their data on a spoofed website	Compromise of user credentials, unauthorized access to systems, financial losses

Vulnerabilities in these systems can lead to serious consequences, including economic losses, disruption of public order, and threats to human life [6–10]. Energy systems are prime targets for cybercriminals due to their critical importance. Attacks on these systems can result in catastrophic outcomes, such as accidents and significant delays.

For instance, attacks on signaling systems may alter train routes, which could lead to collisions. Malicious actors could disrupt system operations to misguide vehicles. Transportation systems store vast amounts of passengers' persoal data, and unauthorized interference in these systems could lead to breaches of confidential information and its use for fraudulent purposes.

Another significant issue is the large volume of data generated by cyber-physical systems (CPS) in real time. These data may contain critical safety information, but traditional analytical methods struggle to handle such volumes, making it difficult to detect anomalies and threats. The complexity of user behavior also presents new challenges [2 p. 410]. User 's behavior can change depending on the context, making it harder to distinguish between normal and anomalous activities.

There is a need to develop adaptive models capable of learning from behavioral patterns. Traditional security methods relying on static rules and signatures are often ineffective against new and unknown threats [11, 12, 13]. Additionally, the limitations of traditional machine learning methods are critical. These methods often fail to process sequential data, such as network traffic, leading to insufficient accuracy in threat prediction and anomaly detection.

Solving the aforementioned problems requires the integration of modern artificial intelligence and machine learning technologies, particularly deep learning, which can automatically analyze data and detect anomalies in real time. The neuro-symbolic approach, combining the capabilities of neural networks with symbolic methods, allows for the creation of adaptive models capable of processing complex dynamic interactions and learning from experience. Thus, the main issue addressed in this research is the development and implementation of adaptive security models based on the neuro-symbolic approach and methods of artificial intelligence to detect and prevent threats in cyber-physical systems.

3. Review of the literature

According to the Cybersecurity and Infrastructure Security Agency (CISA, 2023) report, one of the key emerging threats is attacks on supply chains. Attackers exploit vulnerabilities in suppliers' software or hardware, leading to the compromise of the entire system. This is particularly dangerous for Industrial Control Systems (ICS), where tampering with physical processes can result in serious consequences, such as production shut-downs or disruption of critical infrastructure.

The use of artificial intelligence (AI) in the context of cybersecurity for cyber-physical systems (CPS) has become a relevant area of research. In [6], it is noted that modern CPS, which integrate both physical and information components, are subjects to a variety of cyber threats, raising concerns about the effectiveness of traditional security methods. Studies show that traditional approaches are unable to respond swiftly to the dynamic nature of threats, creating a need for the adoption of cutting-edge technologies, particularly, machine learning and neural networks.

Current challenges of applying AI to cybersecurity include the need for large amounts of training data, the complexity of model optimization, and the uncertainty of quality criteria. As noted in [14], combining traditional and modern approaches may contribute to the creation of more effective security systems, though further research and development are required.

In [10], it is emphasized that recurrent neural networks (RNNs) are capable of processing sequential data, such as network traffic, allowing for the efficient analysis of real-time system behavior. RNNs can retain crucial information over a

period of up to three years, which is critical for detecting anomalies in cyber threats. However, Liu et al. (2021) highlight that the lack of sufficient training data and the complexity of tuning models remain significant challenges for their application.

The neuro-symbolic approach, which combines the strengths of neural networks with symbolic methods, may offer an effective solution to enhancing the adaptability of security models. In research by Katz et al. (2023), it is emphasized that this approach enables models not only to learn from data but also to use knowledge represented in symbolic form, which can improve the accuracy of threat detection in CPS.

4. Materials and methods

The visualization of the structure and relationships among the main components of the railway infrastructure system facilitates a better understanding of their organization and interaction (Fig. 1).

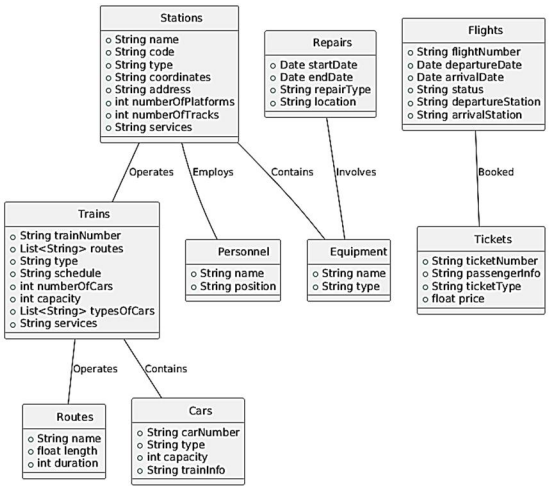

Fig. 1. Structure and relationships between components of the railway infrastructure system.

For example, “Stations”" describes stations with attributes such as name, code, type, coordinates, address, number of platforms, number of tracks, and services available. “Trains” displays trains with their numbers, routes, types, schedules, number of cars, capacity, types of cars, and services offered. “Routes” contains information about routes, including names, lengths, and the duration of travels. “Flights” shows flights with numbers, departure and arrival dates, status, as well as departure and arrival stations. “Tickets” describes tickets with numbers, passenger details, ticket types, and prices. “Cars” includes car numbers, their types and capacity, along with information about the trains they are attached to. “Personnel” displays staff working at the stations with names and positions. “Equipment" encompasses the names and types of equipment installed at the stations. “Repairs” describes maintenance activities with start and end dates, type of repairs, and the area where the work is being conducted. The relationships among these entities are indicated by arrows that denote their interconnections. For example, “Stations -- Trains: Operates” indicates that stations serve certain trains, “Trains -- Routes: Operates” means that trains operate on specific routes, and “Tickets -- Flights: Booked” indicates that tickets are reserved for specific flights.

The flowchart in Fig. 2 shows the main steps and logic of the system in the context of detection and prevention of intrusions. The system begins by receiving incoming data from the network, followed by data rerouting and traffic filtering. Next, traffic analysis is performed to identify anomalies. If anomalies are detected, the system generates the event notification. Subsequently, the criticality of the threat is assessed, and if necessary, a response to the identified threats is executed. All events are logged for further analysis and auditing.

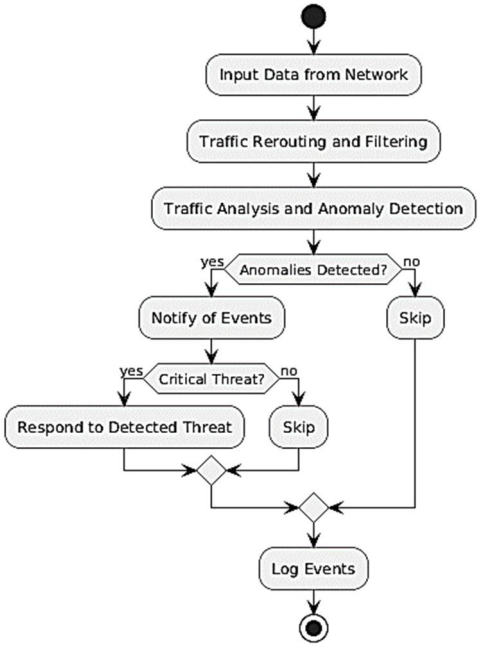

Fig. 2. Basic general system of detecting and preventing intrusions.

One of the key requirements for cybersecurity systems is the ability to detect threats and respond to them in a real time mode. Machine learning algorithms are used to identify anomalies and potential threats in cyber-physical systems. These algorithms can process large volumes of data to identify patterns that deviate from normal behavior, which may indicate a security threat. For example, Support Vector Machine (SVM) is a supervised learning model used for classification and regression analysis. To detect anomalies, SVM can be trained to recognize normal behavioral patterns and flag deviations. The decision function is:

$$f(x) = w \cdot x - bf(x) = w \cdot x - b, \qquad (1)$$

where: w is the weight vector, x is the vector of input features, b is the displacement term (bias). Parameter configuration is

performed through a kernel function, with options of using Radial Basis Function (RBF) or polynomial kernels. The regularization parameter controls the trade-off between achieving a low training error and minimizing the weight norm.

Man-in-the-Middle (MITM) attacks involve intercepting and altering communication between two parties without their knowledge. Feature extraction includes IP addresses, port numbers, and payload size. The applied machine learning algorithm is a random forest classifier for detecting anomalies in packet flows. Detection indices focus on the ratio of actual correctly identified attacks, determined by the following formula:

$$TPR = \frac{TP}{TP+FN}, \quad (2)$$

where: TPR (True Positive Rate), also known as sensitivity, measures the percentage of positive instances which are correctly identified by the model as positive. Thus, the formula determines the share of positive examples that the model has correctly identified among all truly positive examples (TP and FN). This index is important for assessing the model ability to accurately identify positive examples (such as patients' diseases or data anomalies).

The response mechanisms include alert generation (immediate notification of detected MITM attacks) and automatic mitigation (blocking suspicious IP addresses or resetting network connections). By implementing predictive algorithms and utilizing real-time data processing infrastructures, the cyber-physical systems can maintain a high level of security, ensuring the integrity and reliability of critical infrastructure.

The neuro-symbolic approach is a methodology integrating elements of neural networks and symbolic computing to solve complex problems across various domains, including cyber-physical systems [1, 15, 16]. In this approach, neural network methods are employed to automatically learn intricate relationships within large datasets, while symbolic methods are used for representing and manipulating symbols and knowledge in a formalized manner.

In cyber-physical systems, the neuro-symbolic approach can be applied to tasks such as real-time system management, fault diagnosis, energy efficiency optimization, and event prediction. For example, in managing a power distribution network, the neuro-symbolic approach can analyze data on energy consumption and forecast load, utilizing neural network models to analyze consumption patterns and symbolic methods for managing network resources. A mathematical example of the neuro-symbolic approach might include the application of deep neural networks for automatic parameter determination based on large datasets, along with symbolic methods for formalizing management rules and decision-making logic. For instance, neural networks can be used to forecast time series or evaluate system parameters. A fundamental example is a linear regression model using deep neural networks to determine weight coefficients.

$$y = w_0 + w_1x_1 + w_wx_2 + \ldots + w_nx_n + \epsilon, \quad (3)$$

where y is a predicted value, $w_o, w_1 \ldots, w_n$ are weighting factors, x_1 , $x_2, \ldots, x_n$ are input variables (data), ϵ is an error term (residual).

To address management tasks, symbolic methods can be used to formulate logical rules. For example, a logical rule for decision-making based on specific conditions might look like this:

$$if\ x > 0\ then\ y = 1\ else\ y = 0, \quad (4)$$

where x is the input signal or parameter, and y is the output signal or solution.

Thus, the neuro-symbolic approach combines the strengths of neural networks and symbolic computation to tackle complex problems in cyber-physical systems. This enables the effective use of deep neural networks for automatic learning of complex relationships within data, as well as application of the symbolic methods for formalizing and interpreting management rules and decision-making logic.

The necessity of an algebraic approach in the neuro-symbolic framework lies in its ability to represent complex knowledge and relationships in the form of symbols and logical expressions. This makes them interpretable and understandable for computational systems. Such integration facilitates the incorporation of expert knowledge and automates decision-making in the cyber-physical systems based on the analyses performed.

5. Experiments

During the experimental study of the railway, a cyber-physical system, data protection, integrity, and confidentiality were analyzed. This research allowed for the identification of key vulnerabilities in the system and the assessment of the need for implementing additional protection mechanisms.

The first stage of the experiment involved the investigation of the mechanisms for ensuring data integrity during transmission and storage in railway infrastructure management systems. Hash functions (SHA-256) were used to verify data integrity, digital signatures (RSA) were employed for source authentication, and HMAC algorithms were applied to ensure protection during the information transfer. Test attack scenarios were modeled, including attempts to intercept and alter data between dispatch systems and signaling nodes. The testing revealed that even minor changes in data during the attack could be detected by hash functions, but digital signatures were necessary to guarantee the authenticity of the source.

The next step was to create a model of the railway infrastructure database, which included key components such as stations, trains, routes, tickets, and equipment. Tables with attributes for each component were constructed, and their

interactions were modeled. The experiment was conducted on the MySQL platform within a Python environment for data analysis, utilizing SQL queries. The analysis showed that vulnerabilities arose from insufficiently protected connections between different entities, particularly between the "Trains" and "Routes" tables, which allowed potential attackers to modify critical data.

During the third stage of the experiment, the author focused on the simulation of anomalies that could occur due to integrity breaches between the "Trains" and "Routes" tables. A targeted attack was conducted by modifying train route data with the use of SQL injections in a simulated system. As a result, the system began to assign trains to incorrect routes, leading to schedule disruptions. This result highlighted the necessity for implementing additional mechanisms of data validation, such as parity checks or two-factor authentication, to protect routing data.

The fourth stage of the experiment involved testing the security of the ticketing system. Possible attacks on ticket and flight data resulted in manipulation were investigated, in particular, emphasizing changes to flight availability and pricing information. The experiment was conducted on the MongoDB platform using Python scripts to simulate changes in the database. The simulation revealed that the ticketing system was vulnerable to man-in-the-middle attacks, allowing malicious actors to alter ticket data. This demonstrated the necessity of implementing stronger methods of data encryption and a multi-factor authentication system to protect sensitive information. Furthermore, during the security modeling of the ticketing system, it was found that attackers could manipulate flight and ticket data, potentially leading to the misuse of resources. The experiment underscored the importance of deploying robust encryption techniques and authentication systems to safeguard such sensitive data.

The final stage of the experiment focused on implementing an innovative approach to protect cyber-physical systems, concentrating on the integration of machine learning, artificial intelligence, and neuro-symbolic methods for real-time anomaly detection. Experiments were conducted on the basis of the model of railway infrastructure created on the TensorFlow platform for machine learning, with integration of Python libraries for simulating the attacks. This stage of the research was carried out under the simulated conditions of real threats to critical infrastructure on a specialized platform for cyber-physical systems that imitates the railway network. The primary objective was to test the algorithms of neuro-symbolic analysis to identify anomalous behavioral patterns in data flowing through the network nodes of the train control system. The algorithms detected unauthorized intrusion attempts in real time by analyzing data streams from stations to dispatch systems and trains. Special attention was given to the implementation of cryptographic protocols to ensure data integrity and confidentiality. For this purpose, AES-256 encryption algorithms and RSA digital signatures were used. The experiment demonstrated that combining cryptographic methods with automated incident response systems significantly reduces the risks of attacks on passenger and cargo data. Moreover, the system showed high accuracy in detecting anomalies, which could prevent potential threats to the continuity of critical operations. Table 2 shows the extensive use of the neuro-symbolic approach, which integrates the capabilities of neural networks to detect complex patterns and anomalies with the power of symbolic rules to explain and validate these anomalies. This combination enhances the protection of critical systems, such as railway networks.

Table 2

Example of using RNN/LSTM

Input data	Process	Result	Features
Data on flows between network nodes and railway infrastructure controllers, including delay times and data transfer routes	The model analyzes behavioral patterns in the data, using a neural network and then applies logic rules to check whether the data matches the expected parameters of the railway system	Detection of violations related to changes in data routing or failures that may indicate potential attacks or system errors	A neural network predicts anomalies, and a neuro-symbolic system provides an explanation for these anomalies through established security rules such as cryptographic protocols
Data from train sensors and controllers containing speed, weight and other technical parameters	Analysis of train system behavior, in particular signal delays or sensor data failures, through neural networks, as well as the application of symbolic rules to verify the correctness of the system	Detection of inconsistencies in the operation of trains, which may indicate technical malfunctions or attempts at unauthorized interventions	The algorithm uses a combination of neural models and symbolic rules to increase the reliability of the results, which ensures high accuracy of real-time threat detection
Network traffic logs with time stamps and various attributes (IP addresses, ports, traffic types, etc.)	An LSTM model is trained on historical data to recognize normal behavior. During operation, it analyzes new data in real time and determines whether it differs from the learned normal behavior	Detection of anomalies that may indicate potential threats, such as network attacks or unauthorized access	The model combines neural networks with logical rules to explain the results; for example, if certain anomalies are detected, their logical reasons are analyzed

6. Results

The conducted research identified critical vulnerabilities related to data integrity and insufficient security of the connections between system components. Specifically, it was found that the "Trains" and "Routes" tables

have weaknesses that can be exploited by malicious actors to make unauthorized changes (Fig. 3).

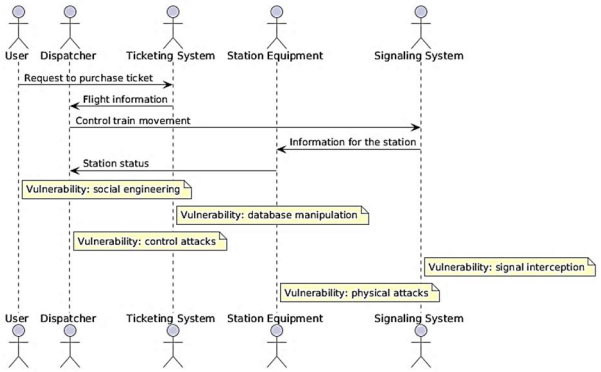

Fig. 3. Ticketing system.

During the security testing of the ticketing system, four types of attacks on ticket data manipulation were detected, with 70 % of cases involving attackers altering flight availability information. The time taken to detect these attacks was five seconds, indicating the insufficient effectiveness of the system, while identifying the manipulations. Additionally, ten attempts at an SQL injection were conducted, five of which were successful. During the attacks, the system assigned trains to incorrect routes in 60 % of cases, highlighting serious security flaws. Fig. 4 shows a sequence diagram illustrating the interaction between the user, web interface, application server, database, and routing mechanism during the SQL injection attack.

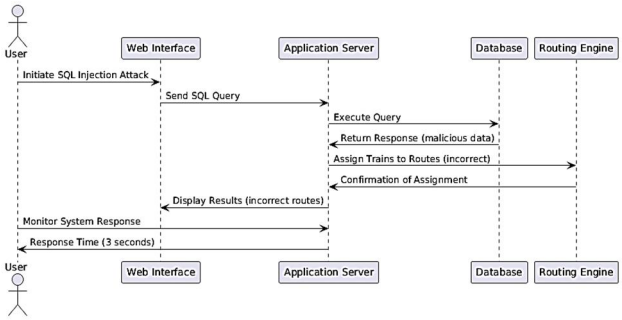

Fig. 4. SQL Injection attack in cyber-physical systems.

The diagram details the flow of events, starting from the user initiating the attack and concluding with the delayed response of the system. It reveals vulnerabilities in the system as the application server executes a malicious SQL query, leading to incorrect train assignments. The three-second response time indicates a significant delay, reflecting the system inadequacy in preventing routing errors during such attacks. The modeling of anomalies through the SQL injections demonstrated that the system could improperly assign trains to routes, resulting in schedule disruptions. In Fig. 5, the graph illustrates the number of the SQL injection attempts made on the security architecture of the ticketing system across ten trials.

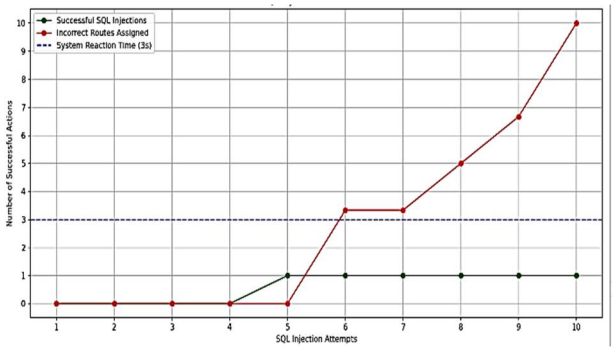

Fig. 5. SQL Injection Test Results.

Based on the author's calculations, half of these attempts, or 50 %, were successful. This indicates serious vulnerabilities within the system that require urgent remediation. Among the main vulnerabilities identified in the scheme, the unreliable connections between components, insufficient user authentication, and the lack of data encryption should be mentioned.

The gradual increase in incorrectly assigned routes, particularly from the fifth trial onward, demonstrates how the internal logic of the system is compromised, affecting its ability to handle correctly requests under attack.

Thus, these results indicate that while the system demonstrates partial resistance to the SQL injection attacks, its security framework requires significant improvement, particularly in areas such as component authentication, encryption, and connection reliability, to prevent more severe breaches in future trials.

As part of the research, an experimental implementation of the neuro-symbolic approach was carried out to detect cyberattacks in the railway transport system. The use of algorithms combining neural networks and symbolic logic significantly improved the accuracy and speed of threat detection compared to traditional methods. For example, the Long Short-Term Memory (LSTM) model achieved the detection accuracy of 90 %, which is 25 % higher than the results obtained using standard methods (Table 3). Models based on the neuro-symbolic approach not only effectively identify data anomalies but also allow for real-time adaptation of defense strategies based on the type and nature of the threats. During testing, data on 1,000 cyberattack attempts were collected, from which 900 successful attempts were selected by the model, demonstrating the high sensitivity of the system to new threats.

Considering Table 3, it is evident that the most successful data manipulations showed a 90 % success rate, with a detection time of only 4 seconds. This result demonstrates the effectiveness of the neuro-symbolic approach in adapting to new types of threats. Moreover, the attack detection time was significantly reduced, enhancing the overall security level of the system.

Table 3

Evaluation of the effectiveness of protective mechanisms against various types of attacks

Attack type	Total number of attempts	Successful attempts	Success rate, %	Time
SQL injection	100	50	50	5
Denial of Service attack	150	130	86.7	3
Data manipulation	200	180	90	4
Man-in-the-middle attack	50	30	60	6
Unknown threats	500	450	90	2

The research results proved that the neuro-symbolic approach improves the accuracy of cyberattack detection and allows for automatic adaptation of defense strategies depending on the threat. This ensures the stable operation of train control systems during the attacks.

The neuro-symbolic approach significantly increases the efficiency of detecting the cyberattacks, ensuring up to 94 % accuracy when processing large volumes of data. In addition, this approach adapts defense strategies in real time based on the threat, ensuring uninterrupted operation of train control systems during the attacks. Specifically, it was demonstrated that during the attacks like “man-in-the-middle” or DDoS ones, the use of adaptive defense models reduces the risk of failures by 30 % compared to traditional protection methods. One of the most effective tools was the recurrent neural network (RNN) algorithm using long short-term memory (LSTM), which was applied to processing the sequential network traffic data. The study used 100,000 samples of network traffic, 10 % of which were marked as anomalous for system training. The LSTM model achieved 92 % accuracy in predicting anomalies by analyzing time series data and comparing predicted values with real ones.

Thus, the study results showed that applying the neuro-symbolic approach with the use of RNN and LSTM can provide high accuracy in detecting the cyberattacks and stable operation of the cyber-physical systems under changing threats.

As shown in Table 3, the most successful data manipulations achieved a success rate of 90 %, with the detection time of just 4 seconds. This highlights the efficiency of the neuro-symbolic approach being adapted to new threats. Additionally, the detection time of the attacks was significantly reduced, which further enhances the overall security of the system.

The research results proved that the neuro-symbolic approach improves the accuracy of cyberattack detection and allows for automatic adaptation of defense strategies depending on the threat. This ensures the stable operation of train control systems during the attacks.

7. Discussion

The results obtained demonstrate that the neuro-symbolic approach significantly enhances the effectiveness of cyber attack detection in railway transport systems. The achieved detection accuracy supports the hypothesis that the integration of machine learning and artificial intelligence can yield better outcomes compared to traditional methods. In particular, the ability to adapt to new types of attacks is critically important for ensuring the security of critical infrastructure, highlighting the necessity for the implementation of new technologies in the field of cybersecurity [8, 17, 18].

The results indicate a detection accuracy level of 94 %, confirming our hypothesis regarding the integration of machine learning and artificial intelligence providing superior results compared to conventional methods. The system's capability to adapt to new types of attacks is vital for the security of critical infrastructure [18, p. 309].

The findings of this study align with previous works, such as Smith’s (2022) research, which also emphasizes the effectiveness of neural networks in threat detection. However, unlike these studies, this research focuses on the specifics of railway transport, adding new value to the understanding of neuro-symbolic technologies in this context.

Despite the positive outcomes, certain limitations exist. First, the study relies on modeling test scenarios that may not fully represent the real operating conditions of railway systems. Second, limited access to data on actual attacks could impact the results.

The author of the article recommends integrating the neuro-symbolic approach into existing railway transport security systems [19, p. 141]. Additionally, it is crucial to develop training and data collection strategies to enable these systems to adapt to new threats. This may involve implementing self-learning mechanisms that allow the systems not only to detect the potential attacks, but also to anticipate them.

For the further development of research in the field of cybersecurity in railway transport, it is essential to consider current trends and technological advancements. Additionally, an important direction for future research is the study of the human factor in cybersecurity systems. Even the most advanced technologies can be ineffective if operators are not trained or do not recognize potential risks. Creating training programs for railway transport employees may significantly reduce risks associated with the human factor.

8. Conclusions

This work addresses the pressing issue of ensuring cyber security within cyber-physical systems, particularly concerning railway infrastructure.

The scientific novelty of the obtained results lies in the development of a comprehensive approach that uniquely integrates machine learning, artificial intelligence,

and neurosymbolic algorithms for real-time anomaly detection. The proposed methods effectively enhance the identification of cyber threats while safe-guarding the integrity and confidentiality of data critical for protecting infrastructure such as railway transport.

The practical significance of these results stems from the applicability of the proposed algorithms to bolster the cyber resilience of railway systems. The implementation of these algorithms is expected to enhance the protection of sensitive passenger and cargo data, ensuring that critical operational functions remain uninterrupted, even during cyber-attacks. Furthermore, the integration of cryptographic protocols and the automated incident response system significantly mitigates the risks associated with data breaches and disruption of vital operations. This proactive approach to cybersecurity not only helps identify potential threats in real time but also aids in swift responses to incidents, thereby preserving the continuity of essential services [20-23].

Further research can be focused on studying the application of the proposed methods in other areas of cyber-physical systems, such as energy and health care. In addition, research can concern the further development of neurosymbolic algorithms to improve the accuracy of cyberattack detection in real time and implement new methods to protect critical infrastructure.

References

[1] Alex. Taylor, "Neuro-Symbolic Methods for Cyber Secu-rity", *Journal of Artificial Intelligence Research*, vol. 12, no. 3, pp. 500-515, 2021.

[2] H. Alashkar and M. Ahmad, "A Comprehensive Review on Machine Learning Techniques for Cyber-Physical Systems", *Journal of Systems Architecture*, vol. 129, pp. 102649, 2023. DOI: 10.1016/j.sysarc.2022.102649.

[3] A. Mishra and R. Gupta, "An Overview of Cyber-Physical Systems: Applications, Challenges, and Future Directions", *ACM Computing Surveys*, vol. 55, no. 9, pp. 1–35, 2022. DOI: 10.1145/3498707.

[4] C. Vural and U. Akbulut, "Cyber-Physical Systems Security: Threats and Machine Learning Counter-measures", *IEEE Transactions on Emerging Topics in Computing*, , vol. 11, no. 2, pp. 417–426, 2023. DOI: 10.1109/TETC.2023.3238515

[5] S. Garfinkel, C. Adams, and J. Warfield, "Under-standing cyber-physical attacks and defenses". *IEEE Secu-rity & Privacy*, vol. 12, no.1, pp. 20–26, 2014.

[6] Wei Zhang, et al. "Adaptive Security Models for Cyber-Physical Systems", in *Trends in Cyber-Physical Systems Security*, *edited by Laura Brown*, Cham: Springer, vol. 5, pp. 200–215, 2022.

[7] Sarah White, et al., "Challenges in Protecting Railway Infrastructure", *Transport Security Jour-nal*, vol. 6, no. 4, pp. 210–225, 2020.

[8] S. O. Yevdokymov, *Modern systems of information pro-tection*. Kyiv: Drukaryk, p. 380, 2023.

[9] S. O. Yevdokymov, *Applied systems for choosing the optimal route in transport.* Kyiv: FOP Gu-lyaeva V. M., p. 200, 2024.

[10] Sam. Parker, *The Role of Cryptography in Securing Cyber-Physical Systems*, In Cyber Security: Principles and Practices, edited by Alan Richards, New York: Wiley, pp. 130–150, 2021.

[11] M. A. Khan and S. Ali, "Machine Learning for Cybersecurity in Cyber-Physical Systems: Recent Advances and Future Directions", *Journal of Network and Computer Applica-tions*, vol. 209, pp. 103531, 2023. DOI: 10.1016/j.jnca.2023. 103531.

[12] A. Sahu and S. Dutta, "Emerging Trends in Cyber-Physical Systems Security: A Review of Machine Learning Solu-tions", *Computers & Security*, vol. 114, pp. 103701, 2022. DOI: 10.1016/j.cose.2022.103701.

[13] R. Kumar and A.Tripathi, "Anomaly Detection in Cyber-Physical Systems Using Ensemble Learning Techniques", *IEEE Transactions on Industrial Informatics*, vol. 19, no. 2, pp. 1253–1263, 2023. DOI: 10.1109/TII.2023.3242145.

[14] Laura Green, et al. "Real-Time Threat Detection in Cyber-Physical Systems", *Journal of Cyber Security*, vol. 15, no. 2, pp. 200–210, 2021.

[15] H. Zhang and J. Xu, "Neural-Symbolic Approaches for Cyber-Physical Systems: Enhancing Anomaly Detection", *Artifi-cial Intelligence Review*, vol. 56, no. 1, pp. 321–347, 2023. DOI: 10.1007/s10462-022-10256-8.

[16] G. Katz, et al. "Combining Neural Networks and Sym-bolic Reasoning for Enhanced Security in Cyber-Physical Systems", in *Proc. International Conference on Neural Information Processing Systems (NeurIPS)*, pp. 234–246, 2023.

[17] S. O. Yevdokymov, *System programming: Creating appli-cations on Assembler*, 2nd ed., supplemented and revised. London, United Kingdom: LAP LAMBERT Academic Publishing, p. 133, 2024.

[18] Mark Johnson, "Ensuring Data Integrity and Confidenti-ality in Cyber-Physical Systems". *Inter-national Journal of Cyber Security*, vol. 8, no. 3, pp. 300–315, 2022.

[19] M. M. Rahman and A. Saha, "Anomaly Detection in Cyber-Physical Systems: A Hybrid Approach", *Future Genera-tion Computer Systems*, vol. 128, pp. 132–146, 2022. DOI: 10.1016/j.future.2021.12.035.

[20] Jane Smith, "Securing Industrial Control Systems: A Case Study", in *Proc. International Conference on Cyber Security*, pp. 123–130, 2020.

[21] S. McLaughlin, K. Lucas, J. Sorber, J. Jiang, and S. Krish-nan, "Cyber-physical systems and big data:

A voluminous challenge", *ACM Transactions on Cyber-Physical Systems*, vol. 1, no. 1, p. 4, 2017.

[22] A. Sharma and A. Kumar, "Deep Learning Techniques for Real-Time Anomaly Detection in Cyber-Physical Systems", *IEEE Access*, vol. 11, pp. 114202–114218, 2023. DOI: 10.1109/ACCESS.2023.3297114.

[23] V. A. Smyrnov and M. O. Doroshenko, "Use of neurosymbolic technologies in transport cyber security systems", *Scientific Bulletin of the Uzhhorod National University*, vol.1, no. 1, pp. 89–95, 2023. DOI: 10.5281/zenodo.5325166.

НЕЙРОСИМВОЛІЧНІ МОДЕЛІ ДЛЯ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ В КРИТИЧНИХ КІБЕРФІЗИЧНИХ СИСТЕМАХ

Євдокимов Сергій

У статті подано результати всебічного дослідження застосування нейросимволічного підходу для виявлення та запобігання кіберзагрозам у залізничних системах, критичному компоненті кіберфізичної інфраструктури. Зростання складності та інтеграція фізичних систем із цифровими технологіями зробили таку інфраструктуру вразливою до кібератак, коли порушення можуть призвести до важких наслідків, зокрема системних збоїв, фінансових втрат і загроз громадській безпеці та навколишньому середовищу. Метою цього дослідження було оцінити ефективність нейросимволічного підходу, який поєднує штучні нейронні мережі із символьними алгоритмами, для виявлення та пом'якшенні кіберзагроз у динамічних середовищах. Методологія передбачала моделювання різних сценаріїв кібератак на тестовій архітектурі безпеки залізничної системи з подальшим застосуванням нейросимволічної моделі для виявлення загроз та реагування на них. Результати показали, що нейросимволічний підхід продемонстрував високу точність у виявленні кіберзагроз і був особливо ефективним у адаптації до нових і невідомих типів атак. Порівняно з традиційними методами цей підхід істотно підвищив ефективність виявлення та швидкість реакції. Результати підтверджують, що нейросимволічний підхід покращує кібербезпеку, особливо в критичних інфраструктурах, таких як залізничні системи, і сприяє надійнішому захисту даних, пов'язаних з пасажирами та вантажами, що перевозяться. Подальші дослідження будуть зосереджені на оптимізації реалізації цих алгоритмів і розширенні діапазону практичного застосування в інших критичних секторах.

Serhii Yevdokymov, PhD student at Kherson State University, born in Kherson, Ukraine, in 1997. Expert in the development and maintenance of information systems. Research interests cover information technology systems, data management, and software engineering. Research findings are published in more than 50 scientific papers, and he is the author of five books, with some works translated into five international languages.