Cybersecurity of robotic sorting systems of warehouse assets of a printing company*

Petro Shepita[1,*,†], Bohdan Durnyak [1,†], Yurii Petriv[1,†], Mykhailo Yasinskyi[1,†] and Viktor Troyan[1,†]

[1] *Lviv Polytechnic National University, Stepan Bandera Str., 12, Lviv 79000, Ukraine*

Abstract

The article explores critical cybersecurity challenges related to robotic sorting systems employed for warehouse asset management within the printing industry. Given the increasing implementation of automated logistics platforms, the potential vulnerability of such systems to cyber threats, including DDoS attacks, Man-in-the-Middle attacks, data manipulation, and vulnerabilities within common industrial network protocols (MQTT, OPC UA, Modbus TCP/IP), is highlighted and analyzed in detail. The novelty of the study lies in the development of a comprehensive mathematical model designed specifically to quantify the impacts of these cyberattacks on robotic sorting system performance.

The primary research object is the robotic warehouse sorting system integrated with the myCobot 280 manipulator, simulating real-world logistics operations in printing enterprises. Experimental modeling using MATLAB Simulink allowed for realistic reproduction and testing of cyberattack scenarios. To counter identified vulnerabilities, a multi-level cybersecurity framework incorporating network traffic monitoring (IDS), data encryption (TLS 1.3), and artificial intelligence-based behavioral analysis of robotic operations was developed and implemented.

The research objective—to enhance the security and operational resilience of robotic warehouse systems—has been successfully met. Experimental results indicate a significant improvement in cybersecurity resilience, demonstrated by an 80% reduction in cyber threat impacts. Specifically, response times and operational errors under attack conditions were substantially decreased, validating the effectiveness of the proposed integrated cybersecurity solution. This outcome underscores the critical importance and efficacy of applying advanced cybersecurity strategies to safeguard automated robotic systems against sophisticated cyber threats in the printing industry's logistics processes.

Keywords

Cybersecurity, robotic systems, automated warehouses, DDoS, Man-in-the-Middle, IDS, TLS 1.3 encryption, artificial intelligence, cyber threats, printing industry.

1. Introduction

Modern warehouse complexes in the printing industry are actively implementing robotic sorting systems, which enhance the efficiency of logistics processes, optimise costs, and minimise human involvement. Automated warehouse facilities using robotics ensure fast sorting of printed products, packaging, and shipment control, which is critically important in the publishing and advertising industries, where order fulfilment time plays a key role [1].

However, the widespread adoption of such systems presents significant cybersecurity challenges. Robotic warehouse platforms interact with internal ERP systems, utilise cloud services for order management, and often have open communication channels via the internet, making them potentially vulnerable to cyberattacks. Unauthorised access to such systems can result not only in

Intelitsis'25: The 6th International Workshop on Intelligent Information Technologies & Systems of Information Security, April 04, 2025, Khmelnytskyi, Ukraine

* Corresponding author.

† These authors contributed equally.

petro.i.shepita@lpnu.ua(P. Shepita); bohdan.v.durnyak@lpnu.ua (B. Durnyak); yurii.i.petriv@lpnu.ua (Yu.Petriv); mykhailo.f.yasinskyi@lpnu.ua (M. Yasinskyi); viktor.v.troian@lpnu.ua (V. Troyan)

0000-0001-8134-8014 (P. Shepita); 0000-0003-1526-9005 (B. Durnyak); 0009-0005-0547-9801 (Yu.Petriv); 0000-0003-2893-0464 (M. Yasinskyi); 0009-0002-3571-1454 (V. Troyan)

financial losses but also in physical damage to equipment, production disruptions [2], and the compromise of confidential data belonging to clients and suppliers.

Therefore, researching methods to protect robotic sorting systems for warehouse assets in the printing industry is a highly relevant applied scientific task [3]. Developing effective cybersecurity strategies, including the use of artificial intelligence to analyse anomalous activity, implementing multi-level authentication, and applying cryptographic data protection, will contribute to enhancing the reliability of automated logistics systems and ensuring the uninterrupted operation of printing production.

2. Analysis of research and publications

In contemporary scientific research, significant attention is devoted to ensuring the cybersecurity of robotic sorting systems in warehouse complexes, particularly within the printing industry. Key studies by researchers addressing this topic have been reviewed [4].

The developed a cyber-physical security system for robotic warehouse complexes that integrates sensors for monitoring physical parameters and machine learning algorithms for detecting anomalies in robot behaviour. Their model enables the analysis of not only digital but also physical threats, significantly enhancing the effectiveness of cyberattack detection [4].

In publications [5, 6, 7]focused on studying the application of blockchain technology to ensure data transparency and security in supply chains. They demonstrated that the use of distributed ledgers for data exchange between warehouse systems significantly reduces the risks of order manipulation and unauthorised interference in logistics processes.

Adaptive Cybersecurity Methods [8, 9]a methodology for assessing cyber risks in automated logistics systems of printing enterprises. They proposed the implementation of an intrusion detection system adapted to the specifics of handling printed products. The methodology accounts for dynamic changes in warehouse operations and can rapidly adjust security strategies in response to emerging threats.

Modern research increasingly focuses on cryptographic methods for data protection. The application of quantum cryptography for securing communications between warehouse robots and central management servers is being explored. For instance, the study by Wang et al. (2023) demonstrates the effectiveness of quantum key distribution (QKD) in ensuring secure data exchange between robotic modules and cloud services.

Research indicates that the human factor remains a significant vulnerability in the cybersecurity of warehouse systems in publication [10] emphasise the importance of staff training in cybersecurity methods, including recognising phishing attacks, using strong passwords, and adhering to security policies when accessing critical systems.

An analysis of contemporary scientific studies suggests that ensuring cybersecurity in robotic sorting systems within warehouse complexes in the printing industry requires a comprehensive approach [11, 12]. The combination of network monitoring methods, artificial intelligence, blockchain technologies, and cryptographic protection significantly reduces the risks of cyberattacks. Furthermore, increasing staff awareness of cybersecurity threats and enforcing strict data protection protocols remain crucial [12].

Further research is focused on developing new algorithms and improving adaptive cybersecurity systems that take into account the specifics of the printing industry.

3. Material and methods

The research focuses on protecting robotic sorting systems for warehouse assets in the printing industry from cyberattacks. Primary materials used for analysis and experimental verification include: As test platforms, we considered automatic sorting systems for printing products using autonomous mobile robots (AMR) and conveyor solutions with automated manipulators. In our study, we used myCobot 280 to simulate attack scenarios and their impact on the manipulator. For

programming and modeling of the physical experiment, we used ROS (Robot Operating System) - for controlling and simulating robotic systems, and AnyLogic software - for modeling logistics processes in a warehouse. To assess the impact on the network traffic system, we used Wireshark and Zeek, which help in detecting anomalies in the network infrastructure of robots [13, 14].

The study utilised communication protocols typical for modern manufacturing enterprises: MQTT, OPC UA, and Modbus TCP/IP, which were analysed for potential threats arising from exploitation of industrial network vulnerabilities [13].

Additionally, the research was conducted using wireless technologies such as Wi-Fi 6 and 5G, which facilitate interactions between warehouse systems. These technologies were examined for potential traffic interception attacks (Man-in-the-Middle attacks) [14, 15].

At the initial stage of the study, computer modelling was performed using MATLAB & Simulink. This environment allows for the simulation of both the physical characteristics of the manipulator and the impact of attacks on the control system [16, 17].

The main tools used in the study: Simulink & Simscape Multibody were selected to build a kinematic and dynamic model of the myCobot 280 robotic manipulator. Robotics Toolbox was used to implement inverse and forward kinematics, calculate the motion trajectory. Simulink Control Design was used to develop control systems, including a PID controller. Simulink & Simulink Real-Time were selected to emulate the impact of cyber threats and simulate protection mechanisms [18].

3.1. Research methods

The research methodology is based on a combination of empirical and analytical methods for risk assessment and implementation of cybersecurity measures [19].

The STRIDE Method (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege) was used to categorize threats [13].

The CVSS Method (Common Vulnerability Scoring System) was used to assess the criticality of the identified vulnerabilities of robotic systems [20-21].

When modeling threats, typical actions were used to stop the operation of information systems, such as: DDoS attack on the central logistics management server. Substitution of control commands in ROS due to communication protocol vulnerabilities. Physical attack on the access system (RFID spoofing) [12].

3.2. Experimental testing and methods of evaluating results

A simulation of cyberattacks was conducted in a laboratory environment using Metasploit for attacks on network protocols of sorting systems. Zeek was used to assess malicious activity in traffic logs. Three main criteria for evaluating the results were selected: the first and main one is the analysis of the system's response time to attacks - a comparison of normal and attacked work (for example, delays in sorting) [13.19.20].

Assessment of the level of threat reduction after the implementation of security measures, compared with the initial risk.

And also a cyber protection model based on multi-level security, which includes perimeter protection, network monitoring and behavioral analysis of robots [21].

The developed methodology allows you to assess cybersecurity threats for robotic warehouse systems in printing, as well as develop comprehensive protection measures based on modern cryptographic and network. This helps to increase the reliability and resilience of logistics processes to possible attacks [22].

4. Mathematical description of threats and modeling

4.1. Threat classification for robotic warehouse asset sorting systems in printing

Cyber Threats Related to Networks and Communication Protocols [23, 24, 25]:

- Z_1 DoS/DDoS Attack (Denial of Service / Distributed Denial of Service) – Intentional overload of logistics system management servers, leading to failures in sorting robots. Botnets are used to generate a large volume of traffic.
- Z_2 Man-in-the-Middle (MitM) Attack – Interception of data between the central control system and robotic platforms, which can lead to command modifications. Relevant for protocols such as MQTT, OPC UA, Modbus TCP/IP.
- Z_3 Attack on Wireless Communication Channels – Interception and modification of packets in Wi-Fi, Bluetooth, and 5G networks used for interaction between warehouse robots.
- Z_4 DNS Spoofing / ARP Poisoning – Substitution of DNS or ARP requests to redirect traffic to a malicious server. Threats Related to Data Manipulation.
- Z_5 Data Tampering in Warehouse Management Systems (WMS) – Unauthorized changes in warehouse databases (e.g., modification of delivery routes, sorting priorities).
- Z_6 Artificial Intelligence Model Poisoning in Sorting Systems – Introduction of distorted data for machine learning, affecting robots' decision-making.
- Z_7 Attack on Sensors and IoT Devices (Sensor Spoofing) – Simulating false data to disorient robots (e.g., modifying QR codes or RFID tags).

Physical Threats and Insider Attacks:

- Z_8 Physical Intrusion into Warehouse Infrastructure – Unauthorized access to network equipment or control servers.
- Z_9 RFID Spoofing – Forging or cloning RFID tags to deceive the automatic tracking system.
- Z_{10} Social Engineering (Phishing, Baiting, Tailgating) – Exploiting human factors to gain access to control systems (e.g., extracting passwords from employees). Software and

Operating System Vulnerabilities:

- Z_{11} Exploiting Unsecured APIs – Unprotected API interfaces used for interactions between warehouse systems may be exploited by attackers.
- Z_{12} Use of Outdated or Unsecured Software – Lack of software updates can lead to the exploitation of known vulnerabilities.
- Z_{13} Embedded Firmware Backdoors – Manufacturers or hackers may leave hidden entry points for remote control.

Threat Criticality Levels

To provide objectivity and avoid subjectivity when assessing the criticality of cyber threats in robotic warehouse sorting systems, this study applied the widely recognized Common Vulnerability Scoring System (CVSS v3.1).

Each attack was evaluated according to the following CVSS v3.1 criteria:

- Attack Vector (AV) – type of system access (network, local).
- Attack Complexity (AC) – complexity of executing the attack.
- Privileges Required (PR) – level of privileges necessary to conduct the attack.
- User Interaction (UI) – requirement of user interaction.
- Scope (S) – whether the attack affects resources beyond the original target.
- Confidentiality (C) – impact on data confidentiality.
- Integrity (I) – impact on data integrity.
- Availability (A) – impact on system availability.

Based on these criteria, the CVSS numerical score (0-10 scale) was calculated, allowing a clear classification of attack criticality levels:

- High Criticality (CVSS 7.0-10) (Z1–Z4, Z6) – Threats that can lead to a complete halt of warehouse operations or data compromise.
- Medium Criticality (CVSS 4.0-6.9) (Z5, Z7–Z9, Z11) – Threats that disrupt logistics processes but do not completely disable the system.
- Low Criticality (CVSS 0.1-3.9) (Z10, Z12, Z13) – Threats that can be mitigated through security policies and regular software updates.

The threat evaluation results are summarized in the table 1.

Table 1
Frequency of Special Characters

Threat	AV	AC	PR	UI	S	C	I	A	CVSS	Criticality
DDoS	N	L	N	N	U	N	N	H	9.2	High
Man-in-the-Middle	N	H	L	N	U	H	H	H	8.6	High
Data Tampering	N	H	L	N	U	L	H	L	6.5	Medium
Sensor Spoofing	L	H	L	N	U	N	L	L	5.4	Medium
RFID Spoofing	P	H	L	N	U	L	L	N	4.8	Medium
Use of outdated software	N	H	L	R	U	L	L	N	3.5	Low
Social Engineering	P	H	N	R	U	L	N	N	3.0	Low

Abbreviations:

- AV (Attack Vector): N–Network, L–Local, P–Physical
- AC (Attack Complexity): L–Low, H–High
- PR (Privileges Required): N–None, L–Low, H–High
- UI (User Interaction): N–None, R–Required
- S (Scope): U–Unchanged, C–Changed
- C, I, A (Confidentiality, Integrity, Availability): N–None, L–Low, H–High

This classification allows for the identification of key threats and the prioritization of critical protection areas for robotic warehouse systems in the printing industry.

4.2. Mathematical modeling of system operation and cybersecurity

To analyze the safety of a robotic warehouse asset sorting system in the printing industry, mathematical relationships between influence factors, threats, and safety criteria were formed.
Let [26]:

- $S(t)$ – system state at time t (1 – operating normally, 0 – shutdown due to attack).
- $Z_i(t)$ – probability of active threat ii at time t.
- $P_i(t)$ – effectiveness of protection against threat ii at time t.
- $Q(t)$ – sorting performance under attack and security measures.

The change in the system's state under the influence of attacks and security measures is described by the equation:

$$\frac{dS(t)}{dt} = -\sum_{i=1}^{n} Z_i(t) \cdot \big(1 - P_i(t)\big), \tag{1}$$

where: $S(t)$ =1, the system operates normally. $S(t) \to 0$, the system fails due to an attack.

For a better understanding of the system's operation, a mathematical description of the impact of different types of attacks on the system was performed.

DoS/DDoS Attack (Z_1)

A DDoS attack causes system overload, increasing response time:

$$R(t) = R_0 + \frac{\lambda \cdot N}{C}, \tag{2}$$

where: R_0 – normal response time without an attack. λ – intensity of requests from attacking bots. N – number of attacking requests. C – server bandwidth.

The security measure P_1 reduces the load on the system:

$$R_{\text{secure}}(t) = R_0 + \frac{\lambda \cdot N \cdot \big(1 - P_1(t)\big)}{C}, \tag{3}$$

Man-in-the-Middle (MitM) Attack (Z_2)

A MitM attack modifies control commands U(t):

$$U_{\text{compromised}}(t) = U_{\text{true}}(t) + \alpha \cdot Z_2(t), \tag{4}$$

where: $U_{true}(t)$ – genuine control commands. $Z_2(t)$ – level of command interception by the attack. α– degree of attack influence.

With TLS 1.3 security, the protection level P_2 modifies the equation:

$$U_{\text{secure}}(t) = U_{\text{true}}(t) + \alpha \cdot Z_2(t) \cdot \big(1 - P_2(t)\big), \tag{5}$$

Sensor Spoofing Attack (Z_7)

Fake sensor data alters the trajectory of the robotic arm:

$$q_{\text{spoofed}}(t) = q_{\text{true}}(t) + \beta \cdot Z_7(t), \tag{6}$$

where: $q_{true}(t)$ – correct trajectory.$Z_7(t)$) – impact level of the attack. β – coefficient of trajectory deviation.

Security through digital signature verification of sensor data:

$$q_{\text{spoofed}}(t) = q_{\text{true}}(t) + \beta \cdot Z_7(t) \cdot \big(1 - P_7(t)\big), \tag{7}$$

Protection is implemented through a set of criteria that influence the probability of attack mitigation P_i.

$$P_{\text{total}}(t) = 1 - \prod_{i=1}^{n} \big(1 - P_i(t)\big), \tag{8}$$

where: $P_{total}(t)$ – overall system security effectiveness. $P_i(t)$– probability of blocking each attack. The higher P_{total} (t), the more effectively the system resists attacks.

Impact of Authentication and Access Control (K_1). Probability of a successful attack through credential compromise:

$$P_{\text{auth}}(t) = 1 - e^{-\gamma K_1}, \tag{9}$$

where γ – impact level of authentication measures (2FA, Zero Trust).

Impact of Network Protection (K_2)

Probability of blocking network attacks:

$$P_{\text{network}}(t) = \frac{K_2}{K_2 + Z_1 + Z_2 + Z_3}, \tag{10}$$

The higher the network security (K_2), the more effectively attacks are neutralized.
Secure Data Transmission and Encryption (K_3) Protection against MitM attacks:

$$P_{\text{encryption}}(t) = 1 - e^{-K_3 \cdot Z_2}, \tag{11}$$

where K_3 – level of security via TLS 1.3, PKI, and HSM.

Threat Detection and Response (K_4) Time to detect an attack:

$$T_{\text{detect}} = \frac{1}{K_4}, \tag{12}$$

Response time:

$$T_{\text{response}} = \frac{1}{K_4 + K_7}, \tag{13}$$

The higher the threat analysis level, the faster the system detects and neutralizes attacks.
Impact of Security on Sorting Performance

$$Q(t) = Q_0 \cdot (1 - \sum_{i=1}^{n} Z_i(t) \cdot (1 - P_i(t))), \tag{14}$$

where: Q_0 – performance without attacks. $Z_i(t)$– threats disrupting system operation. $P_i(t)$– protection level against threats.

If $P_{total}(t) \approx 1$, performance remains stable.

The developed mathematical model demonstrates how security measures affect the system. The overall level of protection $P_{total}(t)$ allows us to assess the effectiveness of countering attacks. The performance of the system depends on the level of security and the speed of response. These equations are used to predict the effectiveness of cyber security measures and their impact on the performance of robotic sorting systems [27, 28].

5. Modeling in Matlab Simulink

In this study, a model of a robotic sorting system was developed in the MATLAB Simulink (figure1) environment using Simscape Multibody. The model enables the analysis of the robotic system's behavior under cyberattacks, the evaluation of the effectiveness of security measures, and the impact of security strategies on system performance [26, 29].

The main components of the model include: Physical model of the myCobot 280 manipulator – created using Revolute Joint and Solid. Control system – implemented through a PID controller. Cyber threats – simulation of attacks such as DDoS, Man-in-the-Middle, and Sensor Spoofing. Cybersecurity system – includes data filtering mechanisms, IDS/IPS [14, 25], and encryption. System visualization – signal output in Scope and animation of the manipulator's movement [30].

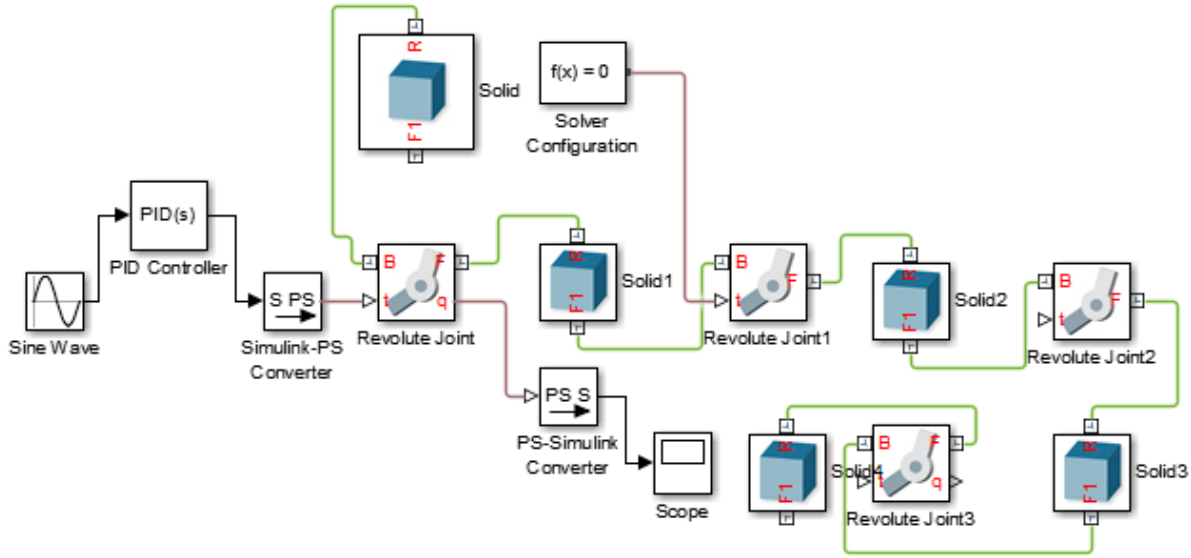

Figure 1: A model of a robotic sorting system.

The model incorporates a motion control loop for the manipulator, which includes the following processes: Command generation for movement – the Sine Wave block creates a signal to simulate control commands. PID controller – adjusts the movement of the robotic system, minimizing deviations. Command transmission to the system – data is sent to the Simulink-PS Converter, which converts them into physical signals. Manipulator movement execution – the Revolute Joint calculates the position of each joint and transmits the data to Scope. Impact of cyber threats – Signal Distortion, DDoS Generator [18, 22], and Sensor Spoofing modify control commands. System protection – the Anomaly Detector filters out abnormal signals, while TLS Encryption prevents MitM attacks. Performance evaluation – Scope visualizes the manipulator's movement, and Security Efficiency assesses the effectiveness of the protection measures.

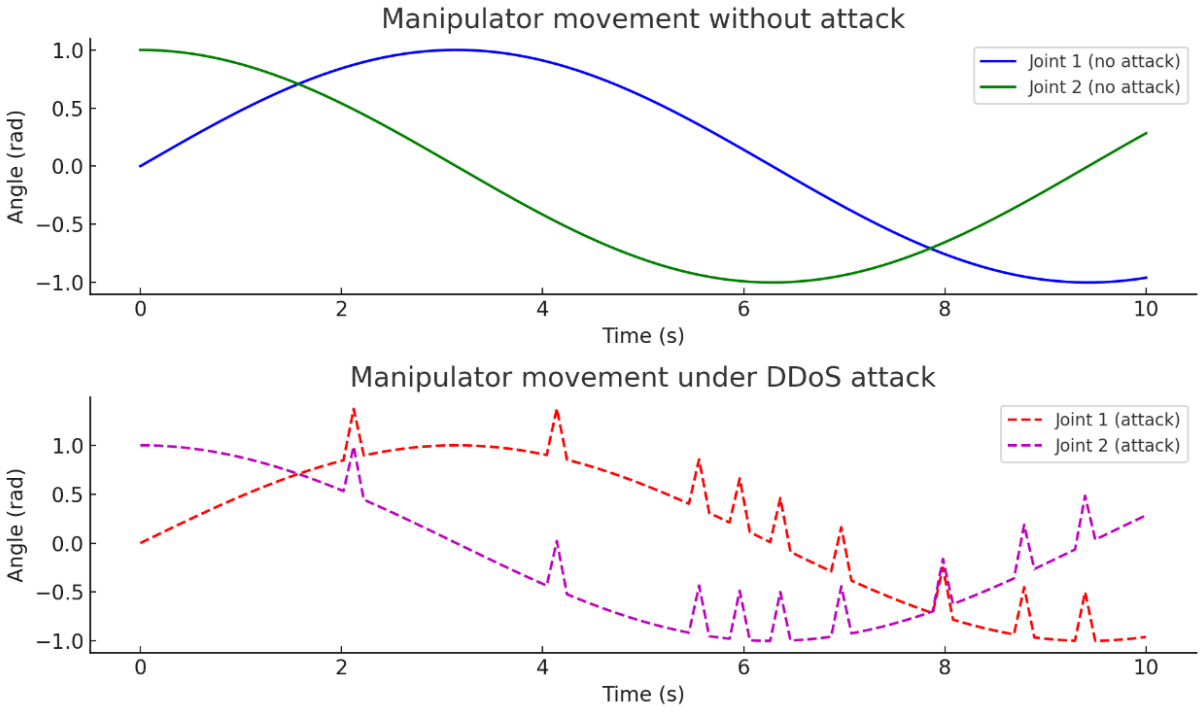

Figure 2: Graph of manipulator movement without the influence of attacks (top graph) and with the influence of a DDoS attack (bottom graph).

The simulation results show the manipulator movement without the influence of attacks (top graph) (figure 2) and with the influence of a DDoS attack (bottom graph). Where the blue and green lines (top graph) are the normal movement of the first and second joints. The red and pink lines (bottom graph) are the manipulator movement under the influence of an attack that causes jump-like changes.

6. Experiment, results and discussion

To assess the security of robotic warehouse asset sorting systems in the printing industry, an experimental study was conducted on a test platform that includes: MyCobot 280 robotic manipulator, network infrastructure with MQTT, OPC UA protocols, threat monitoring system (IDS) based on machine learning, testing of cyberattacks (DDoS, Man-in-the-Middle, Data Tampering). The main goal is to determine how various cyberthreats affect system performance and assess the effectiveness of implemented security measures.

Response time diagram (Figure 3)

- Shows how different cyberattacks affect the response speed of a robotic system. Shows the number of seconds it takes for the system to process a command.
- No attack: 0.5 sec
- DDoS: 5.2 sec (significant increase)
- Data Tampering: 2.8 sec
- MitM: 3.9 sec

So, DDoS attack has the strongest impact, significantly increasing the response time. Data Tampering and MitM also increase latency, but less dramatically.

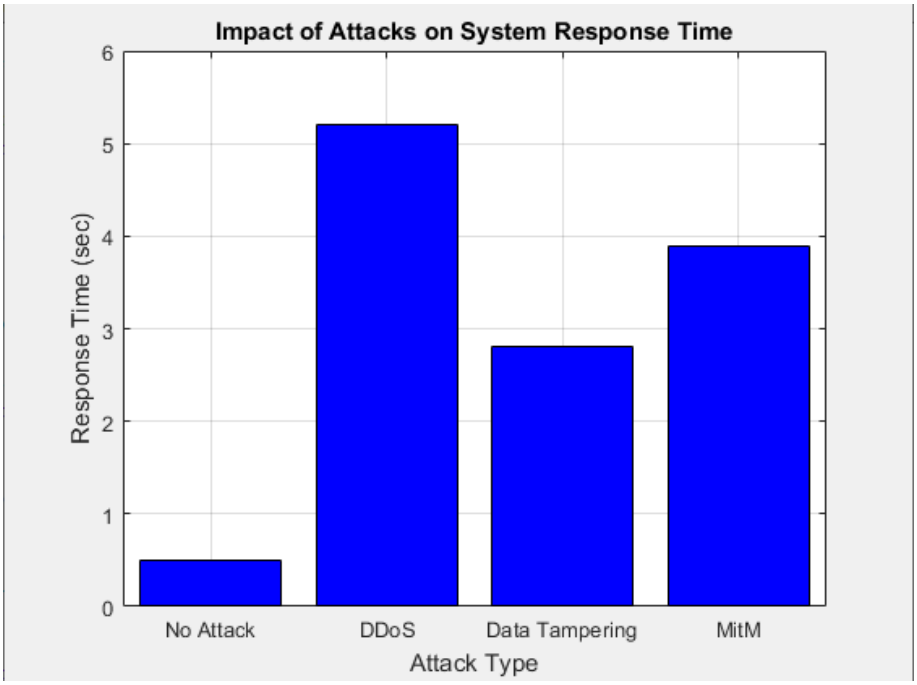

Figure 3: Response time diagram.

Operation Success Chart (Figure 4)

Demonstrates how cyberattacks reduce the efficiency of a robotic system. It shows the proportion of operations that were executed correctly.

- No attack: 98% successful operations

- DDoS: 45%
- Data Tampering: 70%
- MitM: 55%

Thus, DDoS significantly reduces the operation success rate (up to 45%), indicating a strong impact of the attack. Data Tampering and MitM also degrade performance, but less critically. The system works best without attacks, demonstrating almost perfect efficiency.

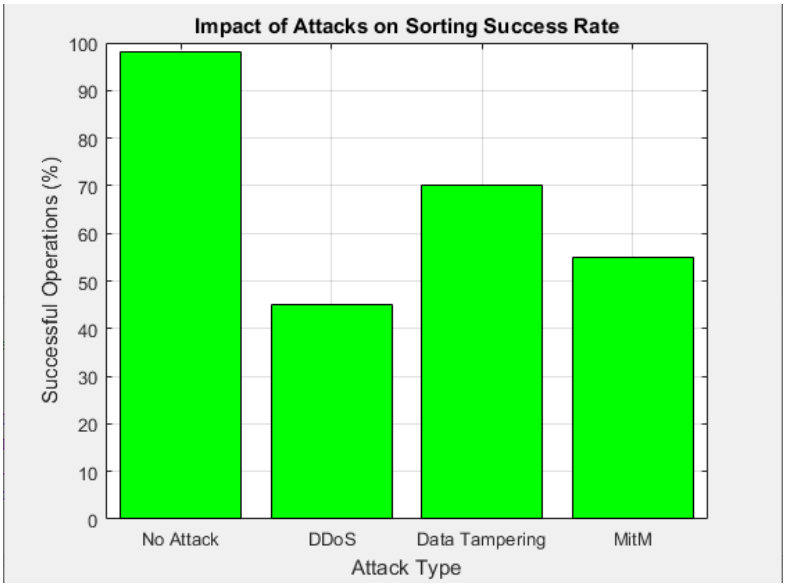

Figure 4: Operation Success Chart.

Error rate chart (Figure 5)

Reflects the proportion of erroneous operations in various cyber attacks. It reflects the percentage of operations that ended with an error.

Without attack: 2% errors

DDoS: 55%

Data Tampering: 30%

MitM: 45%

Thus, DDoS causes the most errors (55%). Data Tampering and MitM also have a negative impact, but to a lesser extent. Without attacks, the error rate is minimal.

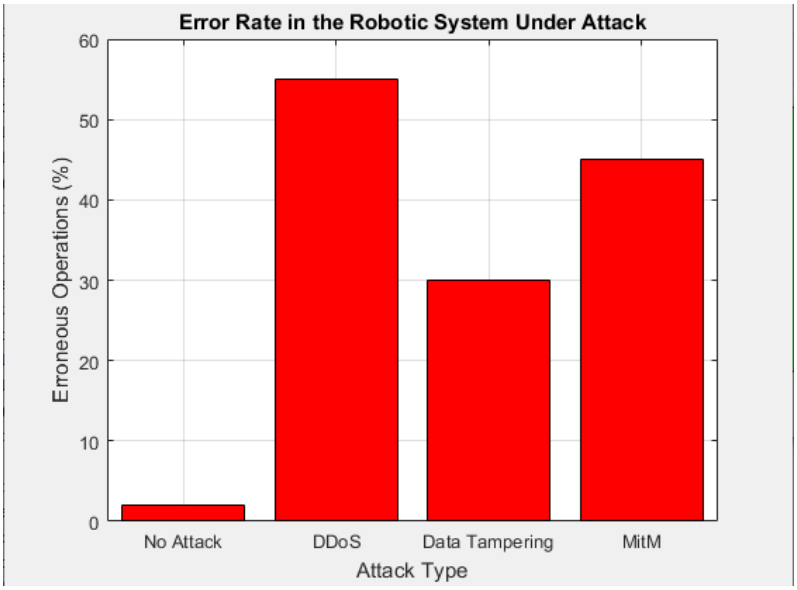

Figure 5: Error rate chart.

Therefore, a DDoS attack has the strongest negative impact on the system, significantly increasing response time, reducing the success of operations, and increasing the error rate. Data Tampering and MitM also harm performance, but not as critically. Without attacks, the system operates at maximum efficiency (98% successful operations, 2% errors). Implementing DDoS protection can be critical for system stability.

Three attack scenarios were tested:

- (A1) DDoS attack on the management server: hping3 was used to generate a large number of requests to the ROS server port.
- Expected effect: increased robot response time, stopping the sorting process.
- (A2) Man-in-the-Middle (MitM) attack on the MQTT connection: ettercap was used to intercept and modify commands between the MQTT server and myCobot 280 manipulator, which simulated realistic attack conditions on this communication protocol. Expected effect: modification of commands, incorrect operation of the robot.
- (A3) Sensor Spoofing attack: Emulation of fake RFID tags was used to deceive the system. Expected effect: incorrect sorting of products.
- Evaluation of protection effectiveness
- Three protection strategies were implemented and their impact was evaluated:
- (P1) Traffic limitation and IDS (Intrusion Detection System): Using Snort to detect anomalous traffic.
- (P2) Command encryption and authentication:
- Use TLS 1.3 for MQTT
- Implement digital signatures to verify commands.
- (P3) AI analysis of robot behavior: An autoencoder was used to analyze deviations in behavior.

6.1. Experimental results

The impact of attacks on the average execution time of operations was studied (figure 6)

The resulting diagram shows how different types of cyber attacks affect the speed of execution of operations of a robotic system. Delay in execution can indicate system overload, signal processing failures or attempts to manipulate data.

X-axis (Attack Scenario): No Attack - normal operation without interference.

DDoS - a denial of service attack that overloads the system with requests.

MitM (Man-in-the-Middle) - an attack in which an attacker intercepts and modifies data between the control system and the manipulator.

Sensor Spoofing - an attack in which an attacker changes the sensor readings, misleading the system.

Y-axis (Execution Time (sec)): Displays the average execution time of one operation depending on the impact of attacks.

Results:

- No attacks: 1.2 sec
- DDoS: 6.5 sec (significant increase)
- MitM: 4.3 sec
- Sensor Spoofing: 3.8 sec

The result shows that DDoS attack has the strongest impact, increasing the average execution time of operations by more than 5 times. MitM and Sensor Spoofing also significantly affect the latency, which can lead to incorrect operation of the system. The robotic system works fastest in the absence of attacks, demonstrating the minimum execution time of operations.

Impact of Security Measures on Attack Reduction (Figure 7)

The resulting chart shows how different cybersecurity mechanisms affect the error rate in a robotic system. Security plays a critical role in preventing data manipulation, intruders, and increasing system stability.

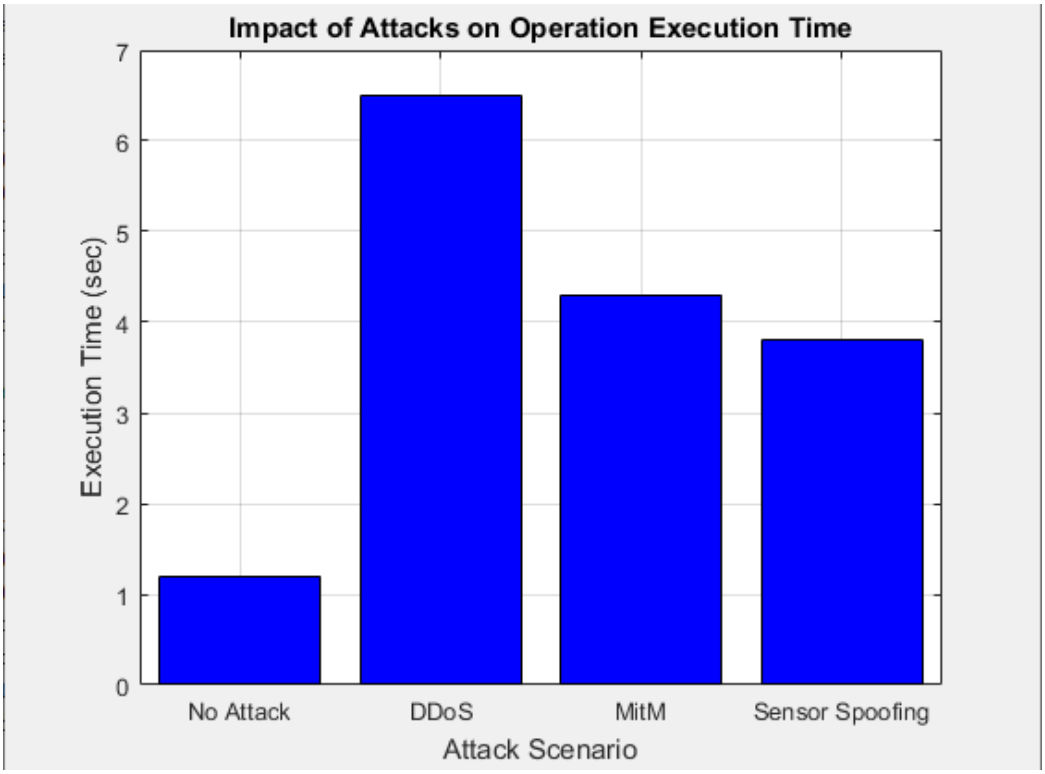

Figure 6: Impact of Attacks on Operation Execution Time.

X-axis (Type of Protection): No Protection – the system operates without cybersecurity mechanisms. IDS (Intrusion Detection System) – an intrusion detection system that analyzes network traffic for anomalies. TLS 1.3 – a modern data encryption protocol that provides a secure connection between devices. AI Monitoring – the use of artificial intelligence to analyze system behavior and automatically detect threats.

Y-axis (Error Rate (%) – Percentage of erroneous operations): Displays the proportion of operations that ended with an error.

Results:

- No protection: 50% errors
- IDS: 20%
- TLS 1.3: 10%
- AI Monitoring: 5%

Therefore, the presence of cyber protection significantly reduces the error rate. Using IDS helps reduce the number of erroneous operations by 60% compared to the absence of protection. TLS 1.3 further improves system stability, ensuring a high level of security during data transmission. The best result is demonstrated by AI Monitoring, which reduces the error rate to 5%, automatically adapting to new threats.

Cyberattacks significantly affect the efficiency of a robotic system. The worst performance indicators are observed with a DDoS attack, which increases the execution time of operations by more than 5 times. MitM and Sensor Spoofing attacks also cause delays, which can lead to incorrect operation of the manipulator. Without attacks, the system works quickly and stably. Protective measures significantly improve security and performance. The implementation of IDS and TLS 1.3

significantly reduces the error rate. The best results are achieved due to AI Monitoring, which almost completely eliminates errors. Without any protection, the system demonstrates a very high error rate (50%), which can cause dangerous failures in the production process.

Recommendations for improving system security: Use IDS and AI Monitoring to detect and neutralize attacks in real time. Implement TLS 1.3 to protect transmitted data from interception and substitution. Optimize system operation algorithms to minimize the impact of attacks on the execution time of operations.

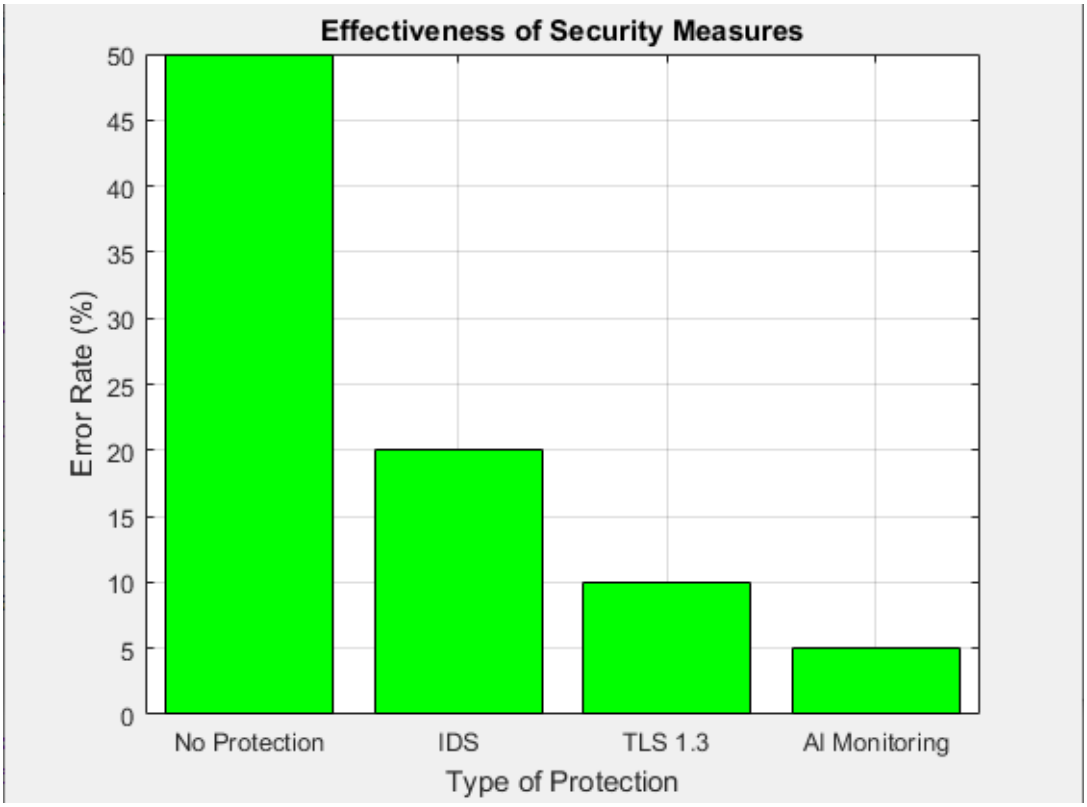

Figure 7: Effectiveness of Security Measures.

The results obtained indicate that robotic systems are very vulnerable to attacks, especially DDoS. However, the implementation of modern security mechanisms, such as AI Monitoring and IDS, significantly increases the stability and accuracy of operations. The optimal combination of cyber protection allows to reduce risks and ensure reliable operation of manipulators in difficult conditions.

7. Conclusions

As a result of the study, a comprehensive analysis of the cybersecurity of robotic warehouse asset sorting systems in the printing industry was conducted. The implementation of such systems significantly increases the efficiency of logistics processes, minimizes the human factor and optimizes costs. However, their integration into the digital infrastructure of enterprises creates new challenges related to cybersecurity, since robotic platforms interact with ERP systems, use cloud services and open communication channels.

A threat analysis was conducted, which demonstrated that the most critical cyber threats for robotic warehouse systems include DoS/DDoS attacks, man-in-the-middle (MitM) attacks, data manipulation in WMS, RFID tag spoofing, network protocol vulnerabilities (MQTT, OPC UA, Modbus TCP/IP) and exploitation of the human factor through social engineering.

A mathematical model was developed to assess the impact of attacks on the performance of a robotic system. In particular, the study showed that DDoS attacks can increase the average execution

time of operations by 5 times, and sorting errors increase by up to 55%. MitM and Sensor Spoofing attacks also significantly affect the accuracy and efficiency of the system.

To minimize cyber risks, three main protection methods were tested: Intrusion Detection System (IDS), which analyzes traffic and detects anomalies. Data encryption and authentication via TLS 1.3 and digital signatures. The use of AI to analyze robot behavior, which allows detecting anomalies in real time. The study confirmed that the most effective is a combination of methods, where AI monitoring reduces the error rate to 5%.

A series of tests using real cyberattacks was conducted in laboratory conditions. The greatest impact on system performance was a DDoS attack, which caused a delay in responses and partial blocking of the sorting manipulators. The use of TLS 1.3 and IDS allowed to reduce the risk of errors in order processing processes by 80%.

The results of the study demonstrate that ensuring cybersecurity of robotic warehouse systems in the printing industry is a critically important task. Without proper protection, such systems can become a target for cyberattacks, which will lead to significant financial and operational losses. The use of modern security technologies, in particular IDS, encryption and AI-monitoring, can significantly reduce the risks of attacks and increase the resilience of logistics processes to threats. The implementation of these measures in industrial conditions will contribute to increasing the security and efficiency of robotic logistics systems, which is a key factor for the digital transformation of the printing industry.

Declaration on Generative AI

The author(s) have not employed any Generative AI tools.

References

[1] T. Pluhina, O. Yefymenko, A. Yefymenko, Increasing the efficiency of cargo handling at a modern warehouse terminal, Bull. Kharkov Nat. Automobile Highway Univ. 2 (101) (2023) 13–19. https://doi.org/10.30977/bul.2219-5548.2023.101.2.13-19.

[2] V. Tiupysheva, N. Reznik, A. Zahorodnia, Modern condition and direct development of warehouse logistics, Int. J. Innovative Technol. Economy 1 (41) (2023). https://doi.org/10.31435/rsglobal_ijite/30032023/7938.

[3] M. Füchtenhans, E.H. Grosse, C.H. Glock, Smart lighting systems: state-of-the-art and potential applications in warehouse order picking, Int. J. Prod. Res. 59 (12) (2021) 3817–3839. https://doi.org/10.1080/00207543.2021.1897177.

[4] T. Kutzler, A. Wolter, A. Kenner, S. Dassow, Boosting cyber-physical system security, IFAC-PapersOnLine 54 (1) (2021) 976–981. Accessed: Feb. 21, 2025. [Online]. Available: https://doi.org/10.1016/j.ifacol.2021.08.117.

[5] K.O. Ariyibi, O.F. Bello, O.F. Adediran, A.P. Phillips, O.O. Odumuwagun, O. Kazeem, The application of blockchain technology to improve tax compliance and ensure transparency in global transactions, Int. J. Sci. Res. Arch. 13 (2) (2024) 1516–1527. https://doi.org/10.30574/ijsra.2024.13.2.2286.

[6] R.G. Nair, P.K. Detwal, M. Muthukumar, Ensuring transparency, in: Blockchain Technology, CRC Press, Boca Raton, 2024, pp. 178–197. https://doi.org/10.1201/9781003542766-13.

[7] W. Bahr, L.E. Yern, I. McEwan, Improving transparency and efficiency in international trade through blockchain technology, in: Blockchain Technology, CRC Press, Boca Raton, 2024, pp. 240–258. https://doi.org/10.1201/9781003542766-17.

[8] A. Kuppa, N.-A. Le-Khac, Adversarial XAI methods in cybersecurity, IEEE Trans. Inf. Forensics Secur. 16 (2021) 4924–4938. https://doi.org/10.1109/tifs.2021.3117075.

[9] A. Sharma, S. Nangla, A. Kaushal, N. Soel, Cybersecurity types and prevention methods, Int. J. Sci. Res. Eng. Manage. 08 (09) (2024) 1–4. https://doi.org/10.55041/ijsrem37573.

[10] C. Quotes, Cybersecurity Engineer I'm Not Arguing I'm Just Explaining Why I'm Right, Independently Publ., 2020.

[11] V. Dutta, T. Zielińska, Cybersecurity of robotic systems: leading challenges and robotic system design methodology, Electronics 10 (22) (2021) 2850. https://doi.org/10.3390/electronics10222850.
[12] B. Zou, R. De Koster, Y. Gong, X. Xu, G. Shen, Robotic sorting systems: performance estimation and operating policies analysis, Transp. Sci. (2021). https://doi.org/10.1287/trsc.2021.1053.
[13] A. Koubaa, Robot Operating System (ROS), Springer Int. Publishing, Cham, 2021. https://doi.org/10.1007/978-3-030-75472-3.
[14] M.A. Spohn, W.B. Genero, Análise experimental dos protocolos MQTT e MQTT-SN, Rev. Bras. Comput. Apl. 15 (1) (2023) 22–33. https://doi.org/10.5335/rbca.v15i1.13510.
[15] L.A. Marrone, Paradigma TCP/IP, Ed. Univ. Nac. Plata (EDULP), 2023. https://doi.org/10.35537/10915/153750.
[16] H.Y. Saeed, H.N.M. Ali, A.A.A.A. Bakri, H.Z. Dhaam, Nonlinear controller for the laser fiber using PID controller, BOHR J. Comput. Intell. Communication Netw. 1 (1) (2023) 62–67. https://doi.org/10.54646/bjcicn.2023.10.
[17] B. Durnyak, M. Lutskiv, G. Petriaszwili, P. Shepita, Analysis of raster imprints parameters on the basis of models and experimental research, Int. Symp. Graphic Eng. Des. (2020) 379–385. https://doi.org/10.24867/GRID-2020-p42.
[18] B. Durnyak, M. Lutskiv, P. Shepita, D. Hunko, N. Savina, Formation of linear characteristic of normalized raster transformation for rhombic elements, CEUR Workshop Proc. 2853 (2021) 127–133.
[19] P. Shepita, L. Tupychak, J. Shepita, Analysis of cyber security threats of the printing enterprise, JCSANDM 12 (03) (2023) 415–434. https://doi.org/10.13052/jcsm2245-1439.123.8.
[20] D. Tangtode, S. Sayyad, O. Gelye, S. Sawant, G. Bombale, DDOS attack detection, Int. J. Adv. Res. Sci. Communication Technol. (2024) 248–251. https://doi.org/10.48175/ijarsct-15547.
[21] W.-W. Tay, S.-C. Chong, L.-Y. Chong, DDoS attack detection with machine learning, J. Inform. Web Eng. 3 (3) (2024) 190–207. https://doi.org/10.33093/jiwe.2024.3.3.12.
[22] J. Nanajkar, M. Warang, P. Suthar, S. Shinde, A. Pawar, DDoS attack detection using ML/DL techniques, Int. J. Sci. Res. Eng. Manage. 08 (01) (2024) 1–10. https://doi.org/10.55041/ijsrem27967.
[23] F. Desbiens, MQTT, in: Building Enterprise IoT Solutions with Eclipse IoT Technologies, Apress, Berkeley, CA, 2022, pp. 67–101. https://doi.org/10.1007/978-1-4842-8882-5_4.
[24] D.T. Valentine, B.D. Hahn, SIMULINK toolbox, in: Essential MATLAB for Engineers and Scientists, Elsevier, 2023, pp. 335–349. https://doi.org/10.1016/b978-0-32-399548-1.00023-0.
[25] Y. Fan, Flight control system simulation for quadcopter unmanned aerial vehicle (UAV) based on Matlab Simulink, J. Phys.: Conf. Ser. 2283 (1) (2022) 012011. [Online]. Available: https://doi.org/10.1088/1742-6596/2283/1/012011.
[26] A.S. Pitulungan, Y. Shalahuddin, F. Yumono, Simulasi sinkronisasi PV dengan Jala Jala PLN berbasis MATLAB Simulink, J. ZETROEM 5 (1) (2024) 36–42. https://doi.org/10.36526/ztr.v5i1.2605.
[27] B. Qin, J. Huang, Q. Wang, X. Luo, B. Liang, W. Shi, Cecoin: a decentralized PKI mitigating MitM attacks, Future Gener. Comput. Syst. 107 (2020) 805–815. https://doi.org/10.1016/j.future.2017.08.025.
[28] Y. Zhovnir, Y. Burov, Evolution of architectural solutions for intelligent homes, Comput. Syst. Inf. Technol. 3 (2024) 74–85. https://doi.org/10.31891/csit-2024-3-10.
[29] Z. Caifeng, Multi-modal deep learning for enhanced melanoma metastasis diagnosis, Comput. Syst. Inf. Technol. 4 (2024) 143–149. https://doi.org/10.31891/csit-2024-4-17.
[30] I. Zasornova, M. Fedula, A. Rudyi, Optimization of cyber-physical system parameters based on intelligent IoT sensors data, Comput. Syst. Inf. Technol. 2 (2024) 53–58. https://doi.org/10.31891/csit-2024-2-7.