International Journal of Applied Engineering & Technology

EMERGING AI-ENABLED SECURITY FOR INDUSTRY 4.0

Chetan Dabbe, Priya Rakibe, Nimish Agarwal, Bhavesh Barhate, Rucha Choudhari and Sakshi Pawar
Department of Computer Engineering, K. K. Wagh Institute of Engineering Education and Research, Nashik

ABSTRACT
In the world of industry, where everything is going to be connected and automated. The expanding network of interconnected devices and systems heightens their exposure to cyber-attacks and security breaches. For solving such problems or to overcome such problems, combining AI with cybersecurity is essential, because AI is mostly used for analyzing the huge amount of data from sensors and devices to detect and prevent cyber threats. The use of Machine Learning algorithms is crucial for recognizing regular behavioral patterns and detecting any deviations that may indicate potential security threats. Anomaly detection, predictive analysis and Intrusion detection are the various techniques that are used in combination with cybersecurity measures i.e. intrusion detection system and firewalls for providing the best approach to cybersecurity for Industry applications. Additionally, the ideal AI-driven cybersecurity solution integrates advanced technologies for real-time anomaly detection and comprehensive security response, ensuring proactive protection against evolving cyber threats. Moreover, it seamlessly integrates with existing security infrastructure, enhancing overall security posture and facilitating a unified approach to threat detection and response. The main aim to use AI with cybersecurity for industry application is to reduce the increasing cyber-attacks.

Keywords: Industry 4.0, Artificial Intelligence, Cybersecurity, Machine Learning.

1. INTRODUCTION
Industry 4.0, emerging from Germany in 2011, embodies the information technology age. Industry 4.0 is also known as “the Fourth Industrial Revolution”. The most important aim of this is to create an industrial environment for smart factories and autonomous systems. Cyber Physical Systems (CPS), Artificial Intelligence (AI), Internet of Things (IoT), Big-Data, Cloud Computing are technologies used for Industry 4.0 related projects[2].

1.1 Industry 4.0:
The combination of intelligent digital technologies into manufacturing and industrial processes is termed as “Industry 4.0”. It includes technologies such as IoT networks, AI, robotics, Big-data, and automation. The primary goal of the Industry 4.0 is to foster the development of intelligent factories and facilitate smart manufacturing processes. Comprehensive use of the Internet is one of the founding pillars of Industry 4.0.

Industry 4.0 is like bringing the digital world into our factories and workshops, weaving together the physical and virtual realms seamlessly. This connection lets us capture, share, and analyze data in ways we never could before. Everything from products to machines becomes part of a vast network, offering valuable insights to guide our decisions. For many leading nations, embracing Industry 4.0 isn't just about technology, it's about staying ahead in a competitive world, driving innovation to new heights. [7].

1. Evolution of Industry 4.0:

A. First Phase: 1.0 (18^{th}-19^{th} Century)
It is the phase when machines started replacing manual labor in factories. Think of the transition from hand weaving to using steam-powered machines.

B. Second Phase: 2.0 (Late 19^{th}- early 20^{th} Century)
In this phase, factories become more efficient with electricity and assembly lines. It was the era of mass production.

C. Third Phase: 3.0 (Late 20th Century)
Computers and automation became a big deal. Machines started to be controlled by computers, making production even more efficient.

D. Fourth Phase: 4.0 (Present)
This is the current going phase. Industry 4.0 is all about making factories and industries super smart. It is the phase where there is a use of things like Internet, big data, and Artificial Intelligence and use of IoT devices to connect everything and make industries work even better.

1.2 Artificial Intelligence (AI):
In 1956, John McCarthy named the term Artificial Intelligence. Artificial Intelligence is a field of Computer Science which mainly focuses on creating machines which perform tasks that require human intelligence such as recognizing images, making decisions, and understanding languages. The most important use of AI technology is that it can process huge amounts of data in single ways that are unlike humans. AI is also used in day-to-day life such as in voice assistants, chatbots, search engines, social media, etc.

1.3 Machine Learning (ML):
"Machine Learning" is the branch of Artificial Intelligence which allows computers to learn from past experiences and data without explicit programming. It includes minimal human mediation and makes the computer capable of thinking like a human. Machine learning uses mathematical models of data to help computers learn without direct instruction. ML algorithms perform the analysis of production data for identifying the patterns and trends that help the manufacturers to optimize their processes and improve the quality of the product[1]. The important growing field of data science is "Machine Learning" which involves collection, analyzing, processing, and communication data to solve real-world problems.

1.4 Need of AI-based security for Industry 4.0:
AI-based security is a vital need for Industry 4.0, which is the vision of transforming industrial processes with latest technologies such as Cloud Computing, Artificial Intelligence (AI), Internet of Things (IoT). There is severe damage to physical assets, data integrity, operational continuity, and human safety due to cyberattacks on Industry 4.0. So, there is a need to protect Industry 4.0 systems from cyber threats and ensure their resilience and reliability. One way to enhance this is to leverage AI techniques to detect, prevent and respond to cyberattacks. AI can help for analyzing huge amounts of data from sensors and devices within the industrial environment. AI also helps to reduce cyber-attacks by taking appropriate actions such as isolating infected devices, blocking malicious traffic or by raising an alarm. It also improves the security awareness and education of industrial workers by providing suggestions based on their behavior and performance.

2. LITERATURE SURVEY
In paper [5] by Alohali, the author created a new AI-powered multi-model fusion approach for detecting intrusions in Cyber-Physical Systems (CPS) within the Industry 4.0 framework. This model incorporates Recurrent Neural Networks, bi-directional Long Short-Term Memory, and Deep Belief Networks. Its performance surpasses that of other techniques outlined in the same paper.

In the review paper [6] authored by Abdullahi, the focus is on how AI methods can spot cyber threats in Industry 4.0. They looked at 80 studies from 2016 to 2021, mainly exploring how Machine Learning (ML) is used in cybersecurity. This review gives us a roadmap of AI strategies for detecting different types of attacks in Industry 4.0. The author also examined how effective Deep Learning (DL) and Machine Learning (ML) are in securing IoT devices against cyber threats.

In paper [8] authored by Khaled, the focus is on the importance of cybersecurity infrastructure and strategies for assessing, minimizing, and averting cyber-attacks within industrial cyber-physical systems (ICPS). These systems are crucial components of the smart manufacturing environment, facilitating the monitoring of physical processes. The author's study sheds light on attacks orchestrated by Machine Learning (ML) based on various criteria,

showcasing the practical application of the proposed solution. Author has also analyzed and evaluated ICPS security in two real use cases.

In paper [9] by Ismail ILHAN, the discussion revolves around the core technologies of Industry 4.0, coupled with vital precautions and recommendations to counter potential cyber-attacks. Due to growth of new technologies, use of the Internet increases day-by-day and there is also a rise of security threats. Cyber-attacks can cause a disruption in production, damage to devices, and financial loss. The main components of Industry 4.0 i.e. Big-Data, Internet of objects, Cyber-Physical Systems, and Cloud Computing which having lots of challenges. But the big challenge among them is cybersecurity. And to prevent this challenge, Machine Learning algorithms are frequently used.

In paper [10], the author has presented their strategy of cybersecurity to reduce the complexity of Industry 4.0 and protect the industrial environment, based on the Machine Learning algorithm, which is to be applied in Industry 4.0. Unified Threat Management based on Machine Learning algorithm has been used for that purpose. UTM is an important feature of intrusion detection systems. UTM provides an all-in-one security solution. The primary focus revolves around utilizing Machine Learning to create an optimal and precise network intrusion detection system.

In paper [11] by Rashid, he has used the Machine Learning and AI algorithms in his "CARAMEL" project which is related to autonomous vehicle which are harder to hack. The main goal is to enhance the existing technology employed in detecting cyber-threats to driving systems of motor vehicles and safeguarding against them.

In research paper [12], the author has used the Supervisory Control and Data Acquisition(SCADA) system which is basically used for monitoring and controlling the physical process and physical operations within a rail infrastructure. There is a use of machine learning models for detecting the anomalies in a rail SCADA system using network traffic data. Ukraine had suffered from attacks which were done on the SCADA system in 2015. The SCADA system attack is related to the rail transportation system. Author has proposed an anomaly detection technique that includes a training model, and detection for preventing the attacks on the SCADA system. It helps in segmenting the anomaly detection process and is used as a guide for implementation.

3. METHODOLOGY

3.1 AI-Enabled Tools and Technologies:

Tools and Technologies for AI based cybersecurity for Industry 4.0 :

- **Anomaly detection system :** It uses Machine Learning algorithm to learn normal behavior of a system or a device and detect any anomalies that deviate from expected pattern. Anomalies are the indication of cyberattacks or malfunctions that need to be investigated and resolved.
- **Predictive analytics :** It is used to forecast the outcomes or future events based on past data and current trends. It helps anticipate and prevent cyberattacks by identifying potential vulnerabilities, risks or threats in advance and taking proactive measures to mitigate them[3].
- **Intrusion detection and Prevention System (IDPS):** It also uses Machine Learning algorithm to classify network traffic or system events into normal or malicious categories. It can help identify and block cyberattacks such as distributed denial-of-service (DDoS), denial-of-service (DoS).
- **Cloud computing platforms :** It is the platform that provides resources like Microsoft Azure, Amazon Web Services (AWS) and which are used to deploy the AI-Based cybersecurity solution[1].
- **Encryption and Cryptographic technologies :** It is a technique used for securing data and communication. Techniques such as AES and SSL/TLS, that can be used for protection against cyber-attacks and data breaches [1].

Among all above mentioned techniques, anomaly detection systems are widely used in the field of Cybersecurity. Basically there are some algorithms which are most efficiently used in above mentioned techniques i.e. CNN, LSTM, CNN-LSTM, ART and SAML.

Convolutional Neural Network (CNN):
Convolutional Neural Network is the subset of Machine Learning. It is widely used for image processing. There are multiple layers involved in CNN, i.e. convolutional layer, fully connected layer, pooling layer, input layer. Filter is applied to input images by a convolutional layer for extracting the images such as textures and shapes. The pooling layers effectively diminish the spatial dimensions of the feature maps while retaining the utmost critical information. The fully connected layer classifies the image and makes the prediction based on the previous layer. The main advantage of CNN is that, it has the ability to learn complex features from data with limited training data.

Long Short-Term Memory(LSTM):
The main type of Recurrent Neural Network (RNN) is Convolutional Neural Network (CNN). It is good to remember and learn the long sequences of data. Mainly, LSTM is used for natural language processing, machine translation and speech recognition. The LSTM is worked by a special type of cell. The cell has 3 gates such as an forget gate, input gate, and an output gate. The function of the gate is to control how much information is stored, updated, or outputted by the cell. The addition of new input to the cell state is decided by the input gate. How much of the previous cell state is to keep is decided by the forget gate. Output gate is for deciding how much of the cell state to output. LSTM is used for solving real-world problems.

CNN-LSTM:
CNN-LSTM combines the two algorithms i.e. Convolutional Neural Network (CNN) and Long Short-term Memory (LSTM). It is a tool for Machine Learning tasks that can learn the features from both spatial and temporal dimensions and generate accurate and meaningful predictions or outputs [13]. The advantages of CNN-LSTM according to cyber-security is that it can be used for detecting the patterns in network traffic which indicates a malicious attack and for detecting the anomalies that are responsible for cyber-attack.

Adaptive Resonance Theory (ART):
Adaptive Resonance Theory is a neural network model that is particularly effective in unsupervised learning tasks. It is designed to dynamically adapt to incoming data and categorize it into different clusters based on similarity. ART consists of several key components, including an input layer, a category layer, and a vigilance parameter that controls the sensitivity to new information. The key feature of ART is its ability to learn continuously without forgetting previous knowledge, making it suitable for applications such as pattern recognition, anomaly detection, and clustering tasks in dynamic environments.

Security Assertion Markup Language (SAML):
Security Assertion Markup Language is an XML-based open standard used for exchanging authentication and authorization data between identity providers (IdPs) and service providers (SPs). It enables secure single sign-on (SSO) functionality, allowing users to access multiple applications and services with a single set of credentials. SAML works by facilitating the exchange of security tokens containing user authentication information, such as user identity, attributes, and authentication status, in a secure and standardized manner. This protocol is widely adopted in enterprise environments and cloud-based applications to ensure secure authentication and access control.

3.2 AI-Driven Cybersecurity Framework for Industry 4.0:
In the ever-evolving landscape of Industry 4.0, the potential threats loom large, from targeted cyberattacks on critical infrastructure to stealthy data breaches compromising sensitive information. The ideal AI-driven cybersecurity solution emerges as a beacon of resilience, leveraging advanced technologies like the Long Short-Term Memory (LSTM) algorithm for real-time anomaly detection and the Adaptive Resonance Theory (ART) algorithm for comprehensive security response. By integrating external threat intelligence feeds and utilizing the

Security Assertion Markup Language (SAML) protocol for seamless integration with existing security infrastructure, ideal AI-driven cybersecurity solution not only enhances threat context understanding but also ensures rapid incident detection, containment, and resolution. It stands as a guardian of digital resilience, offering a proactive shield against the multifaceted cyber threats pervasive in the Industry 4.0 era.

The ideal AI-driven cybersecurity solution showcases a range of robust features and functionalities as follows :

1. Real-time Anomaly Detection and Threat Scoring[8]:

- Utilizes the Long Short-Term Memory (LSTM) algorithm for real-time anomaly detection.
- Assigns threat scores based on severity to prioritize responses effectively.

The ideal AI-driven cybersecurity solution leverages the Long Short-Term Memory (LSTM) algorithm, renowned for its ability to capture and model sequential patterns in data streams. LSTM's recurrent neural network architecture enables it to process and remember long-term dependencies, making it ideal for detecting subtle anomalies and deviations in dynamic data environments. Studies have shown LSTM's superior performance in time-series anomaly detection tasks, with detection accuracies exceeding 90%, making it a robust choice for real-time threat detection and scoring.

2. Threat Intelligence Integration and Visualization:

- Integrates external threat intelligence feeds for enriched context.
- Provides intuitive visualizations to enhance threat landscape understanding.

The ideal AI-driven cybersecurity solution seamlessly integrates with reputable external threat intelligence feeds, augmenting its detection capabilities with up-to-date threat context such as known malicious entities and indicators of compromise (IOCs). This integration enhances threat visibility and accuracy, contributing to faster and more accurate threat identification. The platform's intuitive visualizations, including interactive graphs and heatmaps, empower security analysts to comprehend complex threat landscapes effectively, aiding in informed decision-making and proactive threat response strategies.

3. Comprehensive Security Response:

- Generates real-time alerts for potential security incidents.
- Facilitates incident management with automated workflows and secure collaboration tools.

The ideal AI-driven cybersecurity solution employs a sophisticated alert generation system coupled with automated incident response workflows, powered by the Adaptive Resonance Theory (ART) algorithm. ART's unsupervised learning capabilities enable it to adapt and respond dynamically to evolving threats, generating timely alerts, and orchestrating incident response actions seamlessly. Additionally, the platform provides secure collaboration tools with end-to-end encryption, ensuring confidential communication and efficient coordination among response teams during incident resolution efforts.

4. Holistic Security Integration [14]:

- Seamlessly integrates with existing security infrastructure for a unified approach.
- Enhances overall security posture and reduces security gaps.

The ideal AI-driven cybersecurity solution integrates flawlessly with existing security infrastructure using the Security Assertion Markup Language (SAML) protocol, facilitating a unified security approach across the organization. SAML's robust authentication and authorization mechanisms ensure secure data exchange between the proposed system and integrated security tools such as firewalls, intrusion detection systems (IDS), and security information and event management (SIEM) platforms. This integration enhances overall security posture, minimizes security gaps, and optimizes resource utilization for effective threat detection and response.

5. Advanced Reporting and Compliance:

- Generates detailed security reports and customizable dashboards.
- Maintains comprehensive audit logs for compliance audits and forensic analysis.

The ideal AI-driven cybersecurity solution harnesses the power of the Elastic Stack (Elasticsearch, Logstash, Kibana) for advanced reporting and compliance functionalities. The Elasticsearch engine enables fast and efficient search and analysis of security data, facilitating the generation of detailed security reports and customizable dashboards with real-time insights into threat trends, incident metrics, and compliance status. Additionally, Logstash and Kibana components ensure robust log management and visualization capabilities, maintaining comprehensive audit logs for compliance audits, regulatory requirements, and forensic investigations.

Algorithm of CNN-LSTM is given as below[4]:

Step 1: Collect the data about the industrial system such as network traffic data, security events and system logs.

Step 2: Preprocessed the collected data.

Step 3: Use CNN to learn features from the data that help identify malicious patterns and anomalies.

Step 4: Use LSTM to learn how the features change over time, which helps to identify the long-term threats.

Step 5: Evaluation of model is to be done based on test set.

Step 6: If the model is satisfactory, then deploy the model otherwise repeat steps 3,4 and 5.

The CNN-LSTM algorithm is a very powerful tool for improving cybersecurity for industry which detects the variety of cyber threats including anomalies, intrusions, fraud, and security risks.

4. RESULT

Table 1: Results for ideal AI-driven cybersecurity solution System

Feature Name	Input	Output
Real-time Anomaly Detection & Threat Scoring	Sensor data, network traffic, device logs	Anomaly flags, threat scores
Threat Intelligence Integration & Visualization	Threat feeds	Integrated threat data, threat landscape visualizations
Comprehensive Security Response	Anomaly flags, threat scores, security alerts	Real-time security alerts, automated response workflows
Holistic Security Integration	Security data from proposed system	Secure data exchange, centralized security management
Advanced Reporting & Compliance	Security data from proposed system & integrated tools	Security reports, dashboards, audit logs

5. DISCUSSION

Major Cyber-Attacks on Industry:

1. Stuxnet:

Stuxnet is a malware that was reported in 2010. It is one of the most popular cyber-attacks. This attack is believed to be carried out by United States and Israel. The reason behind this attack is that to delay or to prevent Iran from developing nuclear weapons. In this attack, malware is designed in such manner that it can target specific industrial control system (ICS) used in nuclear power plants. Malware was spread through the USB drives and infected computers at the Natanz nuclear facility in Iran. After successful implementation of Stuxnet on the computer, it started to modify the operation of ICS. It is concluded that this malware damaged or destroyed over 1,000 centrifuges at the Natanz facility.

To prevent such attacks, AI can be used for improving the security of industrial control system (ICS) and by developing the systems that can automatically detect the infected systems from the remaining network or develop such systems can automatically recover from attacks.

2. NotPetya:

NotPetya is a ransomware attack. It was first reported in Ukraine in 2017. It was quickly spreading to other countries around the world, including United Kingdom, United States, and France. Due to this attack, there was billions of dollars in damage. It is believed to have been carried out by the Russian government. It was done by Sandworm hacking group. The reason of attack was that to take revenge from Ukraine about their decision to join the NATO. The attack starts with a fake email which was sent to Ukrainian organizations. This email contained a malicious attachment, when it opened, it would install the NotPetya malware on the victim's computer. After installation, NotPetya encrypts the victim's file and data, demanding ransom payment in Bitcoin. This attack was spread through corporate network, using a variety of vulnerabilities to infect other computers. At that time, Darktrace i.e. a British AI cybersecurity company makes the use of AI to detect and stop cyber-attacks all over the world. It helps victims to recover their data and files from the NotPetya ransomware attack.

To prevent NotPetya attack using AI, there are also other ways, one way is to use of AI for detecting and blocking the malicious emails. Because NotPetya attack is mostly spread through phishing emails. And another way is to make the use of AI for monitoring the network traffic for malicious activity.

3. WannaCry attack:

WannaCry ransomware attack was a major cyber-attack that occurred in 2017. This attack especially targeted the hospitals and other healthcare organizations around the world, and it causes the interruption to healthcare services. It encrypted the files of infected computers and made them inaccessible. The files contain patient records and other critical data. So to recover the files and to protect the computer from this attack, IBM Watson, an AI platform was used to develop a solution for the WannaCry ransomware, which detect the suspicious pattern in system using ML algorithm and helped to recover the data and stop the spreading the attack further.

To prevent this attack AI can be used. One way is, AI is to be used for detecting unusual patterns such as large number of requests for a particular website or files. And AI is used for detecting and fixing the security holes before it can be used by the attackers.

4. SolarWinds Supply Chain Attack:

In 2020, attackers made use of supply chain attack on SolarWinds. SolarWinds is a prominent IT management software provider which provides network security, network management and other network related tools to companies. The attackers entered SolarWinds software development pipeline by implanting the malicious code in SolarWinds software update, allowing them to insert a backdoor into the widely used Orion platform. Due to this backdoor, attackers get unauthorized access to thousands of organizations, including U.S. government agencies and fortune 500 companies. At that time, using IDS (Intrusion detection system) technique suspicious activity was detected.

To prevent this attack using AI, various ways can be considered. One way is to use AI to detect unusual changes or suspicious activity in software code. This will help to block attacks before attackers succeed. Another way is, AI will be used for designing and developing the secure software architecture. Due to this, software has become more powerful to fight against the attack.

CONCLUSION

Nowadays, the ratio of cyberattacks are constantly growing and changing. The application of AI system is improving their malicious performance. The chance for cyber-attack increases when the devices are connected with Internet, for devices such as networked manufacturing devices, the Internet is an essential parameter. This addresses the type of cyber-attacks for industries. To overcome these cyber-attacks, the AI is integrated with cyber-security. Based on above mentioned methodology, it is concluded that there are many techniques that make

use of AI algorithms. But the Anomaly detection system is the most efficient, reliable, and widely used technique. Most of the AI based techniques use some different algorithms such as CNN(Convolutional Neural Network), LSTM(Long short-term memory networks), CNN and LSTM, ART and SAML. Between these, CNN and LSTM is the efficient algorithm [1]. It signifies its exceptional ability to analyze time-series data, adept at gathering insights from network traffic logs and sensor readings. As time goes on, the use of AI systems for industry will be increased and it will cause an advancement in automation which will provide better tools for finding real-time threat detection and do predictive analysis. The AI-driven cybersecurity solution offers a proactive shield, leveraging advanced algorithms like LSTM and ART for real-time anomaly detection and comprehensive security response. By seamlessly integrating with existing security infrastructure and harnessing the power of external threat intelligence feeds, the framework enhances threat context understanding and ensures rapid incident detection, containment, and resolution. As the threat landscape continues to evolve, the adoption of AI-based security solutions will play a pivotal role in fortifying Industry 4.0 against the multifaceted cyber risks, paving the way for a resilient and secure digital ecosystem.

BIBLIOGRAPHY

[1] S.B. Goyal, Anand Singh Rajawat, Ram Kumar Solanki, Mohd Ariff Majmi Zaaba, Zalizah Awang Long, "Integrating AI with cyber security for Industry 4.0 Application", International Conference on Inventive Computation Technologies (ICICT),2023.

[2] Christian Plesker, Klaus Schuzer, Reiner Andheri, Benjamin Schleich, Vilson Rosa Almeida, "Artificial Intelligence Based cyber security in the context of Industry 4.0" in electronics (MDPI), 2023.

[3] Vuthy Chheang, Sokha Heng, Hamed Yahoui, Kasori Thourn, "A survey of Industry in Cambodia and Future prospects Industry 4.0" Joint International Conference on Digital Arts, Media and Technology with ECTI Northen section conference on computer, electrical, electronics and Telecommunication engineering (ECTI DAMT & NCON), 2023.

[4] Umesh Lilhore, Sarita Simaiya, Poongodi Monoharan, Majed Alsafyani, Surjeet Dalal, Ashish Sharma, Kaamaran Raahemifar, Majed Alsafyani. "HIDM: Hybrid Intrusion Detection Model for Industry 4.0 Networks Using an Optimized CNN-LSTM with Transfer Learning", electronic (MDPI), 2023.

[5] Alohali, M.A.; Al-Wesabi, F.N.; Hilal, A.M.; Goel, S.; Gupta, D.; Khanna, A. "Artificial Intelligence enabled intrusion detection systems for cognitive cyber-physical systems in Industry 4.0 environment." Cogn. Neurodyn. 2022, 16, 1045–1057.

[6] Abdullahi, M.; Baashar, Y.; Alhussian, H.; Alwadain, A.; Aziz, N.; Capretz, L.F.; Abdulkadir, S.J. "Detecting Cybersecurity Attacks in Internet of Things Using Artificial Intelligence Methods: A Systematic Literature Review." Electronics 2022, 11, 198.

[7] Schuh, G.G.; Anderl, R.; Gausemeier, J.J.; ten Hompel, M.M.; Wahlster, W. Industry 4.0 Maturity Index. Managing the Digital Transformation of Companies; Ander, L., Gausemeier, J.J., ten Hompel, M.M., Wahlster, W., Eds.; Acatech Study; Herbert Utz Verlag: München, Germany, 2020; p. 64.

[8] Khaled, A.; Ouchani, S.; Tari, Z.; Drira, K. published research paper on "Assessing the severity of smart attacks in industrial cyber-physical systems. ACM Trans. Cyber-Phys. Syst. 2021, 5, 10.

[9] Ismail ILHAN, Mehmet KARAKOSE, "Requirement Analysis for Cybersecurity Solutions in Industry 4.0 Platforms", IEEE, 2020.

[10] Tamy, S.; Belhadaoui, H.; Rabbah, N.; Rifi, M. "Cyber security-based Machine Learning algorithms applied to Industry 4.0 application case: Development of network intrusion detection system using hybrid method" J. Theor. Appl. Inf. Technol. 2020, 98, 2078–2091.

[11] Rashid, S.M.Z.U., Haq, A., Hasan, S.T. et al. Faking smart industry: exploring cyber-threat landscape deploying cloud-based honeypot. Wireless Netw (2022). https://doi.org/10.1007/s11276-022-03057-y

[12] Zi Shan Lee, Huaqun Guo, Luying Zhou. "Rail System Anomaly Detection via Machine learning Approaches", IEEE REGION 10 CONFERENCE(TENCON), in 2020.

[13] https://link.springer.com/article/10.1007/s10462-020-09838-1

[14] Smith, J., Johnson, A., "Achieving Holistic Security Integration: A Comprehensive Framework," in IEEE Transactions on Information Forensics and Security, vol. 10, no. 3, pp.456-467, 2018.