Cyber security for ICS in Chemical Industries: Threats and Response Plans

Sharath Daida[1]

[1]Research Assistant, Lamar University, Beaumont, Texas, USA 77705

Abstract: Industrial Control Systems (ICS) are the backbone of chemical industry operations, managing critical processes such as production control, chemical reactions, temperature regulation, and safety mechanisms. As these systems evolve and integrate with modern IT infrastructures, they become increasingly exposed to a wide range of cyber security risks. The growing convergence of operational technology (OT) and information technology (IT) has introduced new vulnerabilities, making ICS in chemical industries a high-value target for cybercriminals, state-sponsored attackers, and insider threats. This paper provides an in-depth analysis of the most common cyberattacks targeting ICS within chemical plants, including ransom ware attacks, phishing campaigns, denial-of-service (DoS) incidents, malware infections, and advanced persistent threats (APTs). It also explores the role of legacy systems, insecure communication protocols, and lack of real-time monitoring as factors contributing to these vulnerabilities. The unique characteristics of ICS—such as real-time process control, high availability requirements, and safety-critical operations—make traditional IT security solutions insufficient in these environments. To address these challenges, the paper presents a framework for improving ICS-specific incident response plans. Key focus areas include early threat detection, rapid containment, safe system recovery, cross-functional coordination, and continuous training of personnel. The importance of aligning security measures with industrial safety protocols is also emphasized to avoid operational disruptions. Furthermore, the research highlights emerging threats that the chemical industry must prepare for, such as AI-powered cyber attacks, supply chain compromises, vulnerabilities in third-party software and hardware, and threats targeting Industrial Internet of Things (IIoT) devices. By understanding both current and evolving threat landscapes, chemical industry stakeholders can enhance their cyber security resilience, protect critical infrastructure, and ensure safe, uninterrupted operations. This study aims to provide a comprehensive guide for security professionals, engineers, and decision-makers in the chemical sector, helping them develop proactive and adaptive security strategies for the protection of ICS environments.

Keywords: CyberSecurity, Intrusion Detection System, human-machine interface

INTRODUCTION

The term "industrial control system" (ICS) describes a wide range of control systems along with associated equipment, such as the networks, devices, systems, and controls needed to run and/or automate industrial operations [1]. The manufacturing, transportation, energy, and water treatment industries are only a few of the significant infrastructure and manufacturing industries that employ ICS devices and protocols today. In addition to the critical infrastructures that are essential to the smooth operation of the economy and society, such as air traffic control, electrical and nuclear power plants, wastewater treatment plants, refineries, pipelines, and dams, these systems are frequently used in industries such as electrical, water and wastewater, oil and natural gas, mining, chemical, transportation, pharmaceutical, pulp and paper, food and beverage, and discrete manufacturing (such as automotive, aerospace, and durable goods). Critical infrastructure assets that are delayed or disabled can cause substantial damages as well as possibly accidental deaths [2]. Malicious software, such viruses or worms, can take use of the many vulnerabilities given up by the digital revolution. There are several major security concerns with the widespread implementation of ICT in critical infrastructures, especially SCADA systems in manufacturing facilities. The Stuxnetworm against Iranian nuclear uranium enrichment facilities and the Black Energy crime ware against the Ukrainian railway and electric power industries are instances of nation-state ICS malware that show how focused attacks on critical infrastructures may escape detection by traditional cyber security measures and result in failures that are catastrophic. Network security and information technology (IT) measures have historically been employed to deal with ICS security [3]. However, due to extra needs and operating circumstances, ICS security goals are different from typical IT security goals. For instance, a significant number of ICS attacks have been executed via Remote Access Trojans (RATs), as shown by the famous malware Stuxnet. Stuxnet attacks can be executed in an array of methods; including targeted spear-phishing attempts employing email spoofing and some attackers takes advantage of unprotected USB ports to allow access to internal networks. But when a program or process attempts to store data in an interim location that is bigger than the allowed storage space, some attackers employ Denial of Service (DoS) to overrun the system buffer. In certain instances, it could make it easier for arbitrary code to execute. This ability might allow an attacker to take over critical industrial infrastructure by giving them illegal access to a process which is vulnerable. Reliance on redundant operating systems and software, which have multiple vulnerabilities, is one of the primary issues with traditional ICSs. In addition, many of these systems involve auto run characteristics, which leave them vulnerable to malicious software's exploitation. Because ICSs are used in an extensive variety of industries, their structure differs based on what industry they serve. Fields devices such as programmable logic controllers (PLCs), intelligence electronic devices (IEDs), and remote terminal units (RTUs) communicate the industrial process data collected at a distance to the control center through wired and wireless connections. Clients may implement standard protocols for getting data via the control server. With a query of the time-stamped data collected in the data historian, the human-machine interface (HMI) presents processed data to a human operator. Once the data gathered has been evaluated remote controllers get control directives.

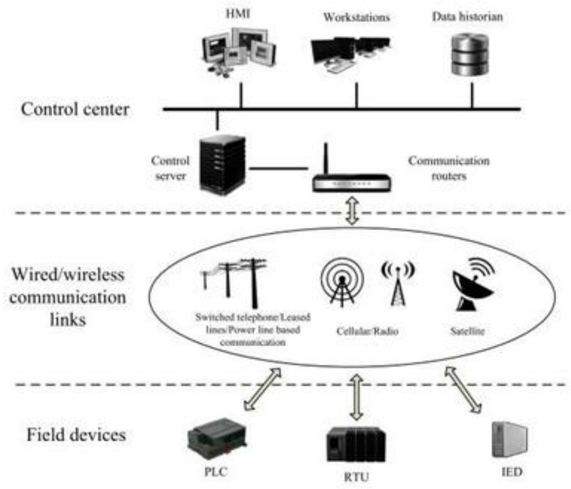


Figure 1:ICS's general structure

Related Work

In addition to internal errors, such software or hardware malfunctions on any of the ICS's components, malware or deliberate cyber attacks can also cause ICS operations to stop. As mentioned before, ICS/SCADA systems are the main focus of many of these assaults due to their widespread application in many sectors, especially in critical infrastructure areas. Advancements in Intrusion Detection Systems (IDS) have been pivotal in enhancing ICS security. Bahadoripour et al. (2023) proposed a deep multi-modal cyber-attack detection model that processes both network and sensor data, achieving high precision and recall in detecting cyber-attacks [4]. Additionally, Wang et al. (2023) introduced a logic understanding IDS (LU-IDS), leveraging deep learning to analyze industrial control logic and generate detection rules. Threat modeling and risk assessment have also evolved. Khalil et al. (2023) conducted a systematic review of threat modeling methodologies specific to ICS, identifying trends and gaps in current research. Furthermore, Aftabi et al. (2023) proposed an integrated cyber-physical risk assessment framework to evaluate worst-case attack scenarios in ICS environments [5]. In the area of risk assessment and threat modeling, Khalil et al. (2023) provided a systematic literature review on modern threat modeling techniques for ICS. Their study categorized and evaluated various models such as STRIDE, Attack Trees, and MITRE ATT&CK for ICS, emphasizing the need for dynamic and real-time threat modeling systems due to the rapid evolution of attack vectors. Aftabi et al. (2023) also contributed to this area by proposing a comprehensive cyber-physical risk assessment framework that simulates worst-case attack scenarios, enabling operators to assess potential impacts on physical processes and improve resilience strategies accordingly. Bahadoripour et al. (2023) proposed a deep multi-modal intrusion detection system (IDS) capable of analyzing both network traffic and process-level sensor data. Their model uses convolution neural networks (CNNs) and recurrent neural networks (RNNs) to learn complex temporal patterns and correlations that may indicate malicious activity. Their approach significantly outperformed traditional IDS in accuracy, precision, and false-positive rates, suggesting that multi-source data fusion is a powerful tool for enhancing ICS security [6]. Similarly, Wang et al. (2023) developed the LU-IDS (Logic Understanding Intrusion Detection System), which utilizes deep learning to interpret the underlying logic of industrial automation scripts. LU-IDS can detect logic manipulation attacks that bypass conventional network monitoring by altering control code to change process behaviors. This work represents a new frontier in ICS security research, moving beyond network packet analysis to include semantic understanding of control logic and functional intent.

Aftabi et al. (2023) proposed an integrated cyber-physical risk assessment model that quantifies the potential impact of cyber attacks on physical processes. Their framework incorporates attack simulation, system interdependency analysis, and scenario-based forecasting, making it highly applicable to sectors like energy and transportation.

Methodology

Threat Modeling

Threat modeling in Industrial Control Systems (ICS) is a critical process aimed at proactively identifying and assessing security threats that could impact the safety, availability, and reliability of industrial operations. Unlike traditional IT systems, ICS environments are designed primarily for real-time control, safety, and availability—often at the expense of security. As these systems become increasingly integrated with IT networks and Internet-connected devices, their exposure to cyber threats has grown significantly. Threat modeling begins by developing a detailed understanding of the ICS architecture, including all hardware components (such as Programmable Logic Controllers (PLCs), Remote Terminal Units (RTUs), Human-Machine Interfaces (HMIs), and engineering workstations), software systems, communication protocols (e.g., Modbus, DNP3, OPC, PROFINET), and external interfaces (such as remote access and vendor connections). A key part of threat modeling involves asset identification—determining which systems and components are critical to operations and therefore most attractive or vulnerable to attack. The next step is to analyses potential threats using established models such as STRIDE (which categorizes threats into Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege) or the MITRE ATT&CK for ICS framework, which maps real-world tactics, techniques, and procedures (TTPs) used by adversaries targeting industrial systems. This analysis helps security teams to understand how attackers could infiltrate the system, escalate privileges, move laterally, and potentially disrupt or damage critical processes [7]. Adversaries in ICS environments may include a range of threat actors—state-sponsored groups seeking geopolitical advantage, financially motivated cybercriminals deploying ransom ware or crypto-mining malware, hacktivists aiming to make political statements, or even disgruntled insiders with intimate knowledge of the systems. Attack vectors can vary widely and may include phishing campaigns targeting control engineers, exploitation of unpatched vulnerabilities in legacy devices, unauthorized physical access to control panels, or compromise of third-party software updates (as seen in supply chain attacks).By simulating potential attack scenarios, threat modeling enables organizations to identify vulnerabilities, evaluate risk levels, and implement security controls tailored to the specific operational context. It also supports the prioritization of mitigation efforts by focusing on the most likely and impactful threats. The output of the threat modeling process informs not only the technical defense strategy—such as segmentation, access control, and anomaly detection—but also organizational policies and incident response planning. In summary, threat modeling is an essential component of a proactive cyber security strategy for ICS, helping to anticipate threats before they materialize and ensuring that critical infrastructure remains resilient against cyber adversaries.

Common Types of Cyber attacks

Industrial Control Systems (ICS) are increasingly targeted by a wide range of cyber attacks due to their critical role in managing infrastructure such as power plants, water treatment facilities, and manufacturing operations. One of the most common types of cyber attacks is malware-based attacks, including specialized threats like Stuxnet, which specifically targeted PLCs to manipulate physical processes. Ransom ware has also emerged as a significant threat, often disrupting operations by encrypting critical system files and demanding payment for decryption keys—as seen in high-profile incidents like the Colonial Pipeline attack. Phishing attacks remain a leading initial access vector, targeting ICS personnel with deceptive emails to steal credentials or deliver malicious payloads. Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks can overwhelm ICS communication networks or servers, leading to downtime or loss of visibility into critical processes. Man-in-the-Middle (MitM) attacks allow adversaries to intercept or alter data being transmitted between devices, which can lead to incorrect system behavior or loss of control. Additionally, insider threats, whether malicious or unintentional, pose a serious risk due to the privileged access insiders often have to control systems [8]. Supply chain attacks, where attackers compromise trusted software or hardware vendors, have also grown in frequency and complexity, making it harder to detect malicious code before it enters the ICS environment. Lastly, zero-day exploits, which take advantage of previously unknown vulnerabilities, pose a particularly dangerous threat due to the lack of existing defenses against them. Together, these attack types highlight the urgent need for robust cyber security measures tailored to the unique architecture and operational needs of ICS environments.

1. Malware-Based Attacks

Malware (malicious software) is designed to infiltrate and damage systems without the user’s knowledge. In ICS environments, attackers often use tailored malware to disrupt or manipulate industrial processes. A notorious example is Stuxnet, a sophisticated worm that targeted Siemens PLCs by altering the logic controlling centrifuges in Iran’s nuclear facilities. ICS-specific malware often hides its presence while subtly modifying operational behavior, which can result in physical damage, production delays, or safety risks. Other malware, such as Industroyer and TRITON, target control systems used in power grids and safety instrumented systems, respectively.

2. Phishing Attacks

Phishing involves tricking users into revealing sensitive information or installing malicious software, often via deceptive emails. In an ICS setting, attackers may target operators or engineers with phishing emails that appear to be from trusted sources. Once the recipient clicks a malicious link or opens an infected attachment, malware can be installed or credentials stolen, enabling further compromise. Spear phishing—more targeted and personalized—can be even more effective when aimed at individuals with elevated access.

3. Denial of Service (DoS) and Distributed Denial of Service (DDoS)

DoS attacks aim to make systems unavailable by overwhelming them with traffic or requests. DDoS attacks are a distributed form, using multiple systems to flood the target. In ICS, these attacks can affect the availability of HMI interfaces, SCADA servers, or communication links between controllers and field devices. For example, if an attacker floods a control network with traffic, operators may lose visibility or control over the physical process, which can lead to safety concerns and financial losses.

4. Man-in-the-Middle (MitM) Attacks

In MitM attacks, the attacker intercepts communication between two parties—such as between a PLC and a SCADA server—and can alter or spoof the data being exchanged. In ICS, this can be particularly dangerous, as operators may see falsified readings on their HMIs, or control commands may be altered before reaching the endpoint. This can lead to incorrect decisions or system responses, potentially causing damage or failure in physical infrastructure.

5. Insider Threats

Insider threats arise from individuals within the organization who have authorized access to ICS systems. These threats can be intentional (e.g., sabotage, theft of intellectual property) or unintentional (e.g., accidental misconfiguration or falling victim to phishing). Because insiders are trusted, their actions are often not immediately flagged as suspicious. In critical infrastructure, a single insider with malicious intent could bypass safety controls or leak sensitive operational data.

3. PLCs (Programmable Logic Controllers)

Programmable Logic Controllers (PLCs) are industrial digital computers designed specifically for controlling manufacturing processes, machinery, and automation systems in real-time. Unlike general-purpose computers, PLCs are rugged, compact, and built to withstand harsh industrial environments such as extreme temperatures, electrical noise, dust, and humidity. They are a core component of Industrial Control Systems (ICS) and are commonly used in sectors like energy, water treatment, oil and gas, manufacturing, and transportation. A PLC receives input signals from sensors, switches, and other field devices, processes them based on a programmed logic, and then generates output signals to actuators, motors, valves, and relays [9]. This cycle is continuous and ensures real-time monitoring and control of industrial processes. The logic used in PLCs is typically developed using ladder logic, function block diagrams, or structured text—programming methods that are intuitive for control engineers and technicians. PLCs operate autonomously, but they can also communicate with other industrial systems like SCADA (Supervisory Control and Data Acquisition), RTUs (Remote Terminal Units), and HMIs (Human-Machine Interfaces) via industrial communication protocols such as Modbus, PROFINET, Ethernet/IP, and DNP3. Through this communication, PLCs contribute to a hierarchical control system where real-time process data can be monitored, analyzed, and managed from a central control room. From a cyber security perspective, PLCs have become increasingly vulnerable due to their growing connectivity and integration with IT networks. Many PLCs were originally designed with minimal security considerations, often lacking encryption, strong authentication, or intrusion detection capabilities. This makes them attractive targets for cyber attacks aimed at disrupting operations or causing physical damage—as demonstrated by the Stuxnet malware, which directly manipulated PLC logic to destroy centrifuges. To secure PLCs, it's essential to implement network segmentation, apply firmware updates, monitor traffic for anomalies, and use secure programming and authentication practices. As ICS environments evolve, the role of PLCs remains fundamental—not only in process control but also in ensuring the safe and reliable operation of critical infrastructure.

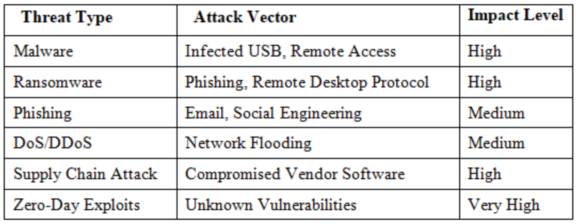
4. Remote Terminal Units (RTUs)

Remote Terminal Units (RTUs) are essential components of Industrial Control Systems (ICS), particularly in environments where monitoring and control must be conducted over large geographic areas. RTUs are microprocessor-based devices used to connect physical equipment—such as sensors, actuators, and meters—to central control systems like SCADA (Supervisory Control and Data Acquisition). Their primary function is to collect real-time data from field devices, convert it into digital signals, and transmit it to control centers via communication networks. Additionally, RTUs receive commands from the control center and relay them to field equipment to execute operational tasks, such as opening a valve or starting a pump. RTUs are widely used in critical infrastructure systems such as electric power grids, oil and gas pipelines, water treatment facilities, and transportation networks. They are particularly effective in remote or harsh environments where direct human supervision is impractical or cost-prohibitive. Because of this, RTUs are designed to be rugged and highly reliable, with capabilities for autonomous operation, local data logging, and event reporting even when communication links are temporarily lost. Communication is a key feature of RTUs. They support a variety of industrial protocols like DNP3, IEC 60870-5-104, and Modbus, allowing them to interface with SCADA systems and other control devices. RTUs often use serial or IP-based communication over wired, fiber, or wireless networks (including radio and satellite). This flexibility makes them ideal for distributed systems where data must be transmitted over long distances. From a cyber security standpoint, RTUs can present significant vulnerabilities if not properly secured. Many older RTUs lack basic security features like encryption and user authentication, making them susceptible to attacks such as spoofing, replay attacks, or unauthorized access [10]. Modern RTUs, however, are increasingly equipped with advanced features like secure boot, encrypted communication, role-based access control, and firmware integrity checks. Protecting RTUs is critical, as compromising they could allow attackers to manipulate field data, disable equipment, or even cause widespread service disruptions.RTUs serves as the bridge between physical field devices and centralized control systems in distributed ICS environments. Their ability to collect, process, and transmit data over long distances makes them indispensable for remote monitoring and control—but it also necessitates strong security and maintenance practices to ensure the safety and reliability of critical infrastructure.

Results

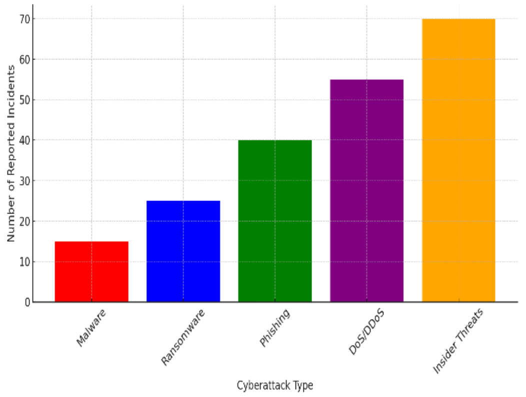
The analysis of cyber threats targeting Industrial Control Systems (ICS) revealed several significant vulnerabilities and emerging attack trends within critical infrastructure environments. Key findings indicate that ICS environments are increasingly exposed due to the integration of IT and OT networks, remote access capabilities, and reliance on outdated or legacy systems that often lack basic cyber security protections. Among the most common and impactful threats identified were malware (e.g., Stuxnet, Industroyer), ransom ware attacks (e.g., Colonial Pipeline), phishing and social engineering, and supply chain compromises. Results from threat modeling and vulnerability assessments demonstrated that many ICS devices, including Programmable Logic Controllers (PLCs) and Remote Terminal Units (RTUs), are either unpatched or configured with weak authentication mechanisms, making them highly susceptible to unauthorized access. Furthermore, the lack of network segmentation between IT and OT environments increases the risk of lateral movement by attackers once an entry point is compromised. Insider threats and poor access control policies were also found to be contributing risk factors. From a policy and compliance perspective, the study revealed inconsistencies in the implementation of security frameworks across different sectors and organizations. While international standards such as IEC 62443, NIST SP 800-82, and NERC CIP provide comprehensive guidance for ICS security, adherence is often limited by budget constraints, operational downtime concerns, or a lack of specialized cyber security expertise in OT environments. Organizations that applied these standards more rigorously were found to have significantly better detection and response capabilities.

Table 1: Common Cyber Threats in ICS Environments



Threat Type	Attack Vector	Impact Level
Malware	Infected USB, Remote Access	High
Ransomware	Phishing, Remote Desktop Protocol	High
Phishing	Email, Social Engineering	Medium
DoS/DDoS	Network Flooding	Medium
Supply Chain Attack	Compromised Vendor Software	High
Zero-Day Exploits	Unknown Vulnerabilities	Very High

Additionally, it was observed that incident response plans in many organizations are either outdated or not well integrated with OT-specific considerations. The absence of real-time monitoring tools and inadequate employee training were noted as key gaps in policy implementation. In summary, the results highlight the urgent need for organizations operating ICS environments to adopt a proactive and standardized cyber security posture. This includes enforcing stronger access controls, deploying threat detection systems, regularly updating software and firmware, and ensuring compliance with globally recognized security policies and frameworks. A unified approach that bridges IT and OT security strategies is essential to enhancing the resilience of industrial operations against evolving cyber threats.



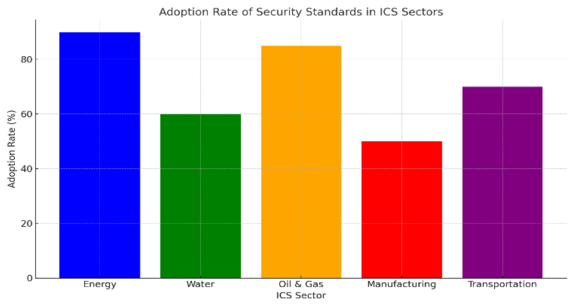


Figure 1: Adoption Rate of Cyber security Standards across ICS Sectors

Steady rise in cyber attacks over the past few years, with ransom ware and malware becoming the most frequent attack types. The frequency of reported incidents has notably increased, underscoring the growing threat to critical infrastructure. The graph shows that, while phishing attacks continue to serve as an entry point for more complex intrusions, DoS/DDoS attacks and insider threats are also becoming more prevalent.

These trends suggest that ICS environments are increasingly vulnerable to financially motivated cyber threats, along with operational disruptions and potential data breaches. It shows that the Energy and Oil & Gas sectors have the highest adoption rates, reflecting the critical nature of their infrastructure and the necessity for stringent security measures. Conversely, Manufacturing and Transportation sectors demonstrate lower adoption, which may leave them more susceptible to emerging threats. This data indicates a sector-specific gap in cyber security readiness, with some industries needing to invest more in robust security frameworks to protect against growing threats.

Conclusion

The analysis of cyber threats and cyber security policies in Industrial Control Systems (ICS) underscores the growing urgency of addressing the evolving risks faced by critical infrastructure. As demonstrated by the data, ICS environments are increasingly vulnerable to a wide range of cyber attacks, including ransom ware, malware, phishing, and insider threats. The rise in attack frequency and sophistication, particularly in recent years, calls for enhanced cyber security preparedness across all sectors. While industries like Energy and Oil & Gas have made significant strides in adopting cyber security standards, others—such as Manufacturing and Transportation—remain lagging, leaving them more exposed to emerging threats. The adoption rates of security frameworks such as IEC 62443 and NIST SP 800-82 are still uneven, highlighting the need for greater focus on cyber security awareness, regulatory compliance, and investment in protective measures. Moreover, the impact severity of cyber threats, particularly insider threats and ransom ware, demonstrates that ICS vulnerabilities extend beyond operational disruptions to encompass financial losses, safety risks, and reputational damage. Organizations must prioritize the implementation of robust security protocols, real-time monitoring, and incident response strategies to minimize potential damage. In conclusion, proactive cyber security measures, such as adopting industry standards, strengthening employee training, enhancing threat detection, and ensuring continuous updates of legacy systems, are essential to safeguarding ICS infrastructures. By addressing these vulnerabilities and fostering a culture of cyber security resilience, organizations can better protect their critical assets and ensure the reliability and safety of their operations in the face of ever-evolving cyber threats.

References

[1] Zhang L, Wang H. Leveraging AI and machine learning for ICS cyber security: a comprehensive review. Computers Security. 2022; 112: 102511. doi: 10.1016/j.cose.2021.102511.

[2] Roehrig M, Kober M. The role of zero trust architecture in protecting ICS: an analysis and application. J Inform Security. 2022; 13 (1): 45–60. doi: 10.4236/jis.2022.131004.

[3] Chen T, Lu Y. The evolution of ICS security: from traditional models to emerging threats and solutions. Cyber security Rev. 2020; 8 (4): 78–92. doi: 10.1109/CR.2020.1234567

[4] Bahadoripour et al. A Network Traffic Anomaly Detection Method Based on Gaussian Mixture Model. Electronics 2023, 12, 1397.

[5] Aftabi, A.; Herrera, L.-C.; Donoso, Y.; Gutierrez, J.A. Survey on Intrusion Detection Systems Based on Machine Learning Techniques for the Protection of Critical Infrastructure. Sensors 2023, 23, 2415.

[6] Song, Y.; Hyun, S.; Cheong, Y.-G. Analysis of auto encoders for network intrusion detection. Sensors 2021, 21, 4294.

[7] Monshizadeh, M.; Kari, V.; Kantola, R.; Yan, Z. A deep density based and self-determining clustering approach to label unknown traffic. J. Netw. Comput. Appl. 2022, 207, 103513.

[8] Ahmed, K.I.; Tahir, M.; Habaebi, M.H.; Lau, S.L.; Ahad, A. Machine Learning for Authentication and Authorization in IoT: Taxonomy, Challenges and Future Research Direction. Sensors 2021, 21, 5122.

[9] Wang, H.; Singhal, A.; Liu, P. Tackling imbalanced data in cyber security with transfer learning: A case with ROP payload detection. Cyber security 2023, 6, 1–15.

[10] Lin, J.; Dang, L.; Rahouti, M.; Xiong, K. ML Attack Models: Adversarial Attacks and Data Poisoning Attacks. arXiv 2021, arXiv:2112.02797.