

(RESEARCH ARTICLE)



AI-powered ransomware prediction and prevention for industrial control systems (ICS)

Luqman Ali *

Cybersecurity Specialist, Hitachi Cyber.

World Journal of Advanced Engineering Technology and Sciences, 2026, 19(03), 214-226

Publication history: Received on 11 May 2026; revised on 19 June 2026; accepted on 22 June 2026

Article DOI: <https://doi.org/10.30574/wjaets.2026.19.3.0330>

Abstract

Ransomware attacks are becoming more common against ICS that control critical infrastructure like power plants, oil and gas operations, water treatment plants, and manufacturing facilities. Unlike a typical IT environment, a disruption in ICS operations can result in physical damage, safety issues, and widespread service outages. In this study, the researchers have concentrated on creating an AI-based framework that can predict and prevent ransomware attacks in ICS systems. The approach proposed combines anomaly detection, real-time network traffic monitoring and automated system isolation to detect the initial stages of a malicious activity before the full-scale infection. Abnormal behaviors of the sensors and abnormal communication patterns in the industrial network are detected using the machine learning method. The anticipated benefits of such an approach are better early detection, less downtime of systems and better operational safety. In conclusion, the study provides valuable insights into enhancing cybersecurity resilience in critical infrastructure systems by implementing intelligent and proactive defense strategies.

Keywords: Ransomware Detection; Industrial Control; Anomaly Detection; Machine Learning; SCADA Security; Cybersecurity Framework

1. Introduction

Industrial Control Systems (ICS) are a critical part of the operation of critical infrastructure, such as electricity generation, water treatment, manufacturing processes, oil and gas production systems and more. These systems are tasked to control and monitor physical processes in real time and are crucial to the maintenance of societal and economic stability. Supervisory Control and Data Acquisition (SCADA) systems, Programmable Logic Controllers (PLCs), and distributed control systems are some of the main elements of ICS that are designed to ensure uninterrupted industrial operation. Recent progresses have resulted in greater IT and OT network integration for efficiency, but it has also given rise to a larger attack surface for cyber intrusions. This convergence has made cyber attacks even more dangerous, especially ransomware attacks that may impact not only electronic processes, but industrial processes as well. Another difference between ICS and traditional IT environments is that ICS generally employ legacy systems that typically have fewer security updates, making them more susceptible to exploitation. Furthermore, many ICS architectures pay more attention to the availability and operational continuity than to cybersecurity, thus creating vulnerabilities in protection. In such environments, traditional methods of detection, like signature-based and periodic scanning, may not be enough because of the need for real-time operation and the sensitivity of the systems. The increasing complexity underscores the importance of sophisticated, adaptive security solutions that can proactively identify and address threats in real-time.

* Corresponding author: Luqman Ali

1.1. Overview

Ransomware is a type of malicious software that encrypts files or render systems unusable until ransom is paid. Beyond data loss, its influence in industrial settings impacts directly on the physical processes under control of interwoven systems. In Industrial Control Systems (ICS), ransomware can cause operational disruptions, stop production lines, and disrupt safety-critical functions unlike traditional IT systems, which mainly target files and databases. This is especially problematic in industries like energy, manufacturing and utilities. Results can range from equipment damage, production downtime, to environmental or human safety risks. In response to such challenges, AI-based cybersecurity solutions have emerged as a potential solution. These strategies involve the use of intelligent systems that can process vast amounts of real-time industrial data. In this scenario, machine learning is a key component in detecting abnormal network traffic, sensor readings, and system behavior. One of the advantages of the unsupervised learning frameworks lies in the fact that they do not need labeled data of attacks as this data is often limited in industrial environments. Rather, they sense instances that do not match regular operational practices and enable early detection of any possible ransomware activity. AI-driven techniques reflect and refine their detection capabilities based on the dynamics within the system, improving accuracy and adaptability as threats change.

1.2. Problem statement

ICS environments are extremely susceptible to cyberattacks because they are built using legacy infrastructure and software that cannot be regularly updated for security. This makes them good targets for ransomware attacks that can easily get into operational networks. One issue is ransomware detection can be delayed, which can lead to significant operational impacts and potentially cause physical damage to industrial equipment. Existing security solutions are not robust enough to keep up with the ability to predict ransomware activity in real time in the ICS space. This means that there is a critical gap in the early warning capabilities and that systems are vulnerable in the early stages of the propagation of attack. There's also the issue of how to keep the system available while also enforcing the security measures, since too many restrictions could disrupt ongoing industrial processes. This has created a strong demand for intelligent, real-time predictive security solutions that can detect and thwart ransomware attacks before they get out of hand.

1.3. Objectives

The overall goal of the study is to create an AI-based model which can detect ransomware at its early stages in Industrial Control Systems (ICS). The model continuously monitors the behavior of the industrial network and the machines in it, detecting the abnormal behavior that may be caused by malicious activity. Another goal is to pick up on early signs of ransomware proliferation before it can break across interdependent systems. Another objective of the study is to develop an automatic answering mechanism that can isolate the affected systems immediately after detection of suspicious activity, thereby averting any further damage. Moreover, the study concentrates on enhancing the resilience of the system and minimizing downtimes in critical infrastructure settings. The aim of the proposed framework is to promote operational continuity in critical areas like energy, manufacturing, and utilities by allowing for proactive threat detection and quick containment. In general, the goals are focused on creating an intelligent, real-time cybersecurity solution to enhance the security of industrial environments to face the evolving ransomware threat.

1.4. Scope and significance

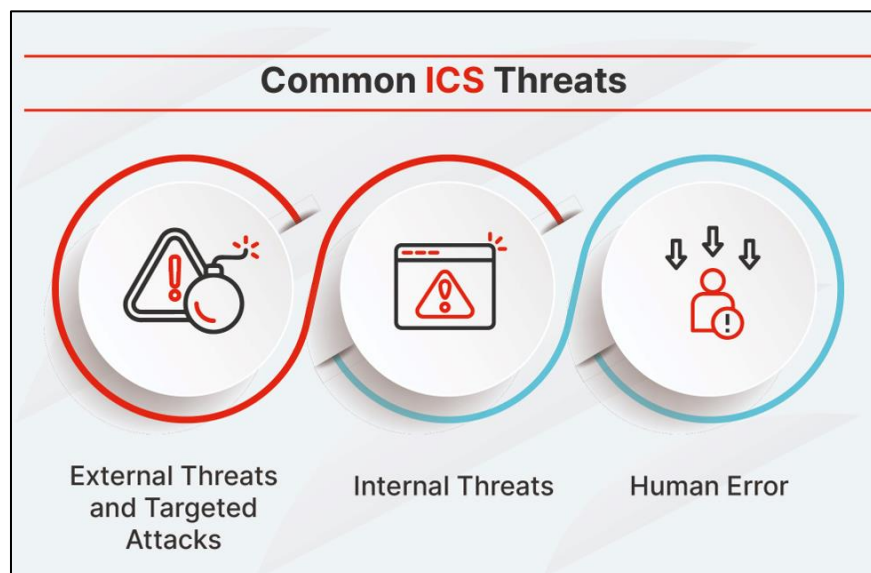
This study takes a closer look at the Industrial Internet of Things (IoT), Programmable Logic Controllers (PLCs), and Supervisory Control and Data Acquisition (SCADA) systems for Industrial Control Systems (ICS). The focus is on the detection, prediction and automated prevention of ransomware attacks only in these industrial environments. It does not apply to the general Information Technology (IT) enterprise systems or non-industrial digital infrastructures. The study highlights the need for real-time monitoring and AI-powered threat detection in OTEC systems where continuity is paramount. This study is important because it could help make national critical infrastructure, including power generation, water treatment, transportation, oil and gas, more secure. The proposed approach would help to minimize operational downtime, loss of financial, and safety benefits by improving the detection and automated response. In conclusion, it helps create more robust and smarter industrial cybersecurity solutions to overcome today's ransomware attacks.

2. Literature review

2.1. Overview of Cybersecurity Threats in ICS Environments

As Industrial Control Systems (ICS) become more interconnected and integrated with critical infrastructure, they're exposed to numerous cybersecurity threats. These are valuable targets for attackers and are a key component in the management of industrial operations, including energy production, manufacturing and water treatment. System vulnerabilities can be caused by common threats in ICS environments, including external threats and targeted attacks, internal threats, and human error. There are a number of external threats like bad actors taking advantage of vulnerabilities in the network, and internal threats come from compromised credentials or insider abuse. Human error is still a major cause and this can be devices misconfigured, as well as poor operational practices. Traditionally, industrial systems have been outside of the network, but with the advent of digital transformation and IT-OT convergence, the attack surface has grown substantially. This transition has caused an uptick in industrial infrastructure ransom, sabotage and espionage attacks. The attackers have become more sophisticated and sophisticated over time and are counting on attacks to disrupt critical services and are originating attacks from a State Sponsored attack platform. This means that organizations now must implement more sophisticated and proactive security solutions that are specific to industrial applications. It is crucial to have an understanding of the types and the progression of these threats in order to devise effective defense strategies in today's ICS landscapes.

The recent studies have emphasized the enhancement of resilience in the critical industrial systems of day-to-day life, through the introduction and integration of threat classification with real-time monitoring, in the presence of new cyber threats in an interconnected web of infrastructures. (Lou & Tellabi 2019)



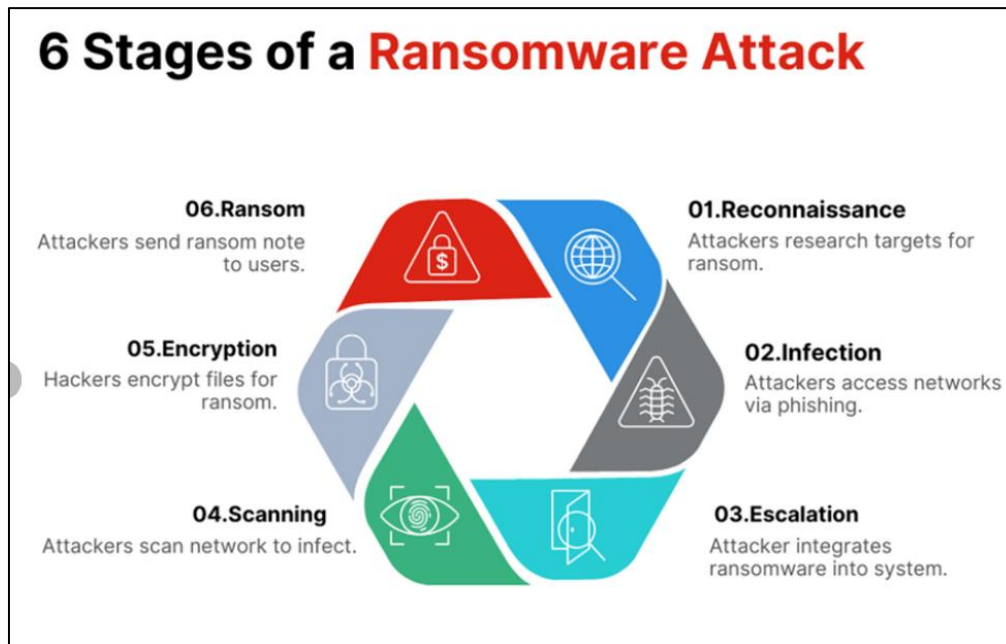
Source: <https://www.fortinet.com/content/dam/fortinet/images/cyberglossary/ics-threats.jpg>

Figure 1 Common ICS Threat Categories (External Threats, Internal Threats, and Human Error)

2.2. Ransomware Attack Mechanisms and Lifecycle

Ransomware attacks follow a structured lifecycle that allows attackers to move from initial target selection to full operational disruption. In Industrial Control Systems (ICS), this lifecycle is especially dangerous because the attack may affect both digital assets and physical processes. The process usually begins with reconnaissance, where attackers study the target organization, identify exposed services, and search for weak entry points. The next stage is infection, commonly achieved through phishing emails, compromised credentials, malicious attachments, or vulnerable remote access systems. After gaining access, the attacker escalates privileges and integrates ransomware components into the system to increase control over critical assets. The scanning stage then enables the malware to search for connected devices, shared drives, engineering workstations, and network segments that can be infected. In networked industrial environments, propagation may occur through lateral movement, weak segmentation, default passwords, unpatched systems, and trusted connections between IT and OT networks. Once sufficient access is gained, the encryption stage begins, where files, configurations, backups, or operational data may be locked to disrupt normal activity. Finally, the ransom stage occurs when attackers deliver a payment demand and threaten data loss, prolonged downtime, or public

exposure. This lifecycle shows that ransomware is not a single event but a sequence of coordinated actions. Understanding each phase helps researchers design stronger detection mechanisms that identify suspicious behavior before encryption and ransom demands occur, especially in ICS environments where delayed response can lead to major safety, financial, and operational consequences (Maigida et al., 2019).



Source: <https://encrypted-tbn0.gstatic.com/images?q=tbn:ANd9GcQgDjw-kx-vC0MmCpQMYKMu0QG6Iw7L3H3SCQ&s>

Figure 2 Ransomware Attack Lifecycle (Reconnaissance, Infection, Escalation, Scanning, Encryption, and Ransom Stages)

2.3. Intrusion detection systems in industrial environments

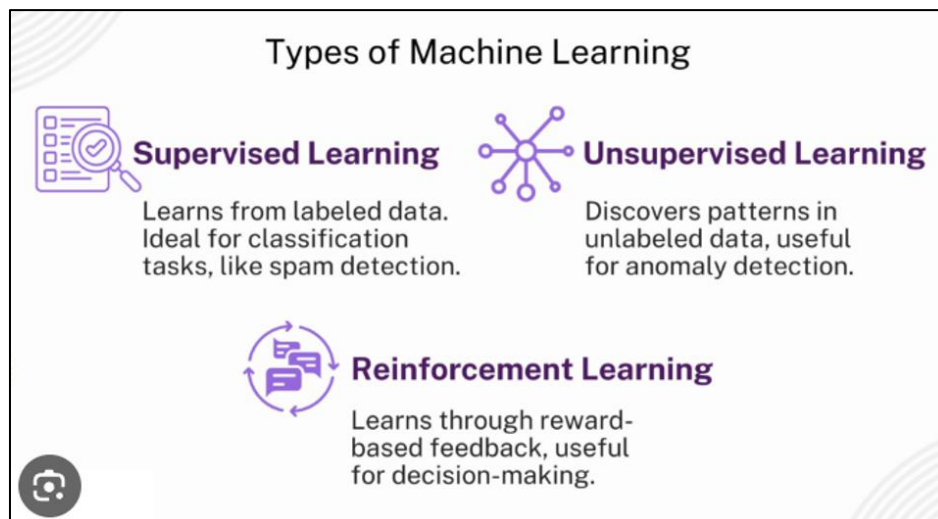
Intrusion Detection Systems (IDS) are essential tools for the protection of Industrial Control Systems (ICS), as they are designed to detect and alert for possible cyber threats within the network and its systems. IDS solutions in industrial contexts guard against malicious activities targeting Supervisory Control and Data Acquisition (SCADA) systems, Programmable Logic Controllers (PLCs) and other operational technology components. These systems can be used to detect abnormal communication patterns, unauthorized attempts to access the network, and violations of policies in industrial networks. IDS in ICS can be implemented using the following methods: Anomaly based detection, Signature based detection, Hybrid detection which is a combination of both. While helpful, many of the current systems still depend on signatures of known attacks.

Signature-based detection technology has also been limited in the industry as it can only be used to identify known threats. This makes them ineffective against new or evolving ransomware variants that continuously change their behavior to evade detection. Furthermore, ICS settings create gigabytes of live data, which creates a challenge for conventional IDS tools to process and react quickly without adding latency. There is also a high rate of false positives, which can cause serious problems in normal industrial operation if they are not controlled. Additionally, the legacy systems and limited computational power in ICS environments limit the use of advanced security solutions. This has created a demand for more intelligent and adaptive detection mechanisms to detect unknown threats in real time while maintaining operation stability, which has led to the development of more sophisticated real-time systems. Consequently, there is a growing need for more intelligent and adaptive detection mechanisms that can dynamically and adaptively detect unknown threats in real time while maintaining operational stability, thereby necessitating a shift towards more sophisticated real-time systems. It is therefore crucial to enhance the capability of IDS to boost the cybersecurity resilience in industrial environments (Hu et al., 2018).

2.4. Machine learning approaches in cybersecurity

In cybersecurity, machine learning techniques are extensively used to identify deviations, categorize threats, and enhance defensive responses in intricate network settings like Industrial Control Systems (ICS). The ML techniques are crucial in this context because of the scale, continuous and heterogeneous nature of the data generated by the industrial

networks, which cannot be analyzed by means of traditional rule-based methods. Generally, machine learning techniques can be divided into supervised learning, unsupervised learning, and reinforcement learning. Supervised learning is based on labeled data and is typically applied to classification problems where there are known attack patterns. However, unsupervised learning discovers hidden structures and patterns from data without labels, making it very well suited to anomaly detection problem in ICS environments in which attack labels are often rare. Reinforcement learning is an approach to decision making that is based on reward-based feedback that can be used to develop adaptive security mechanisms that evolve over time. Supervised techniques are generally known for their high accuracy when trained with a good amount of labelled data but their performance drops when presented with new threats in cybersecurity applications. Unsupervised methods offer more flexibility in identifying new or changing attacks based on learning normal system behaviors and detecting variations. These are the two approaches compared, showing the compromise between accuracy and adaptability in an IDS. In industrial settings, hybrid models are especially useful since they leverage the strength of supervised learning to handle known threats and unsupervised learning to address unknown threats, allowing for more accurate detection of both known and unknown cyber threats in real-time. Hence, the hybrid approach or the fusion of both approaches is being increasingly regarded as a better solution for fault diagnosis systems in dynamic environments of industrial applications (Wilmet et al., 2021).



Source: <https://safe.security/resources/insights/machine-learning-in-cybersecurity/>

Figure 3 Types of Machine Learning in Cybersecurity (Supervised Learning, Unsupervised Learning, and Reinforcement Learning)

2.5. Deep Learning Applications in Network Traffic Analysis

In the field of cybersecurity, deep learning has emerged as a powerful tool, especially for processing large and complex network data in Industrial Control Systems (ICS). DEEP LEARNING MODELS can learn meaningful patterns from large volumes of data without the need for manual feature engineering, unlike traditional approaches. Deep learning is widely applied in network traffic analysis for anomaly detection, classification of traffic behavior, and detecting potential cyberattacks like ransomware propagation. These models can learn underlying relationships in network packets, flow data and communication patterns, and are very effective in environments with fast evolving and unpredictable attacks.

In industrial applications, deep learning is also being used for time-series modelling of sensor data from machines, PLCs and SCADA. The time-series models are used to identify abnormal operating characteristics from a sequence of data points, such as pressure, unexpected machine shutdowns or unusual control signals. It is essential for ICS environments where there may be subtle indications that the system is under attack or that there is a system issue. The recurrent neural network (RNN) and the long short-term memory (LSTM) are typical architectures employed to model temporal dependencies in data streams from industrial applications.

Overall, deep learning enhances the ability to perform real-time monitoring and predictive analysis in network security systems. These models can be used to detect malicious activities and improve detection accuracy, and, by using large-scale traffic data and temporal sensor patterns, they can be used to detect malicious activities at an early stage before they arrive at full system disturbances in critical industrial infrastructures (Abbasi et al., 2021).

2.6. Real-Time Monitoring Systems in SCADA environments

In Supervisory Control and Data Acquisition (SCADA) applications, real-time monitoring systems play a crucial role in providing ongoing supervision over industrial processes like manufacturing, water distribution, and power transmission. The systems are configured to gather information from field devices like actuators, sensors and Programmable Logic Controllers (PLCs) in real time. Real-time SCADA monitoring helps operators in critical infrastructure, such as power transmission control centers, identify performance issues, system faults, and abnormal behavior before it turns into a major failure. This feature is especially crucial for ensuring system stability, efficiency, and safety in industrial settings where disruptions can have a profound impact.

While real-time monitoring in SCADA systems has several advantages, it also poses certain challenges, particularly in the context of latency-sensitive industrial applications. In industrial applications, where time response will play a crucial role in determining the stability of the systems or damage to the equipment, a very low time response is required. Real-time monitoring solutions are often impacted by network congestion, limited computation, and legacy system restrictions. Furthermore, the incorporation of advanced analytics and cybersecurity features into SCADA systems may cause processing delays that can disrupt the timing of the system. Operational efficiency and security monitoring continue to be a big challenge in Industrial Control Systems. Hence, the demand for optimized solutions to provide high speed data processing, reliability and low latency in monitoring frameworks is increasing rapidly. Furthermore, these systems need to be available and resilient to cyber attacks, especially in critical infrastructures where a system failure is not acceptable (Pinzón et al., 2020).

3. Methodology

3.1. Research design

In this study, an AI-based predictive model design for early detection of ransomware in Industrial Control Systems (ICS) is adopted. The proposed framework is built as a hybrid system, by incorporating the anomaly detection methods with classification models, which enhances the accuracy of the detection and efficient response. The anomaly detection part aims at detecting industrial deviations from normal, and the classification model is used to classify the detected threats according to their type and severity. The system is designed to be robust and applicable in simulation-based environments as well as industrial datasets to ensure its practical use and robustness. Ransomware scenarios are simulated in an ICS network, which enables testing of the ransomware model under various threat conditions. Real world data has been introduced to test the system performance in the real industrial environment. The research design focuses on real-time detection, adaptability, and scalability, aiming to ensure that the model can operate efficiently in industrial settings with dynamic conditions and high risk levels, while also preserving the stability and continuity of the system.

3.2. Data collection

The data is gathered from various sources to enable the comprehensive analysis of ransomware behavior in Industrial Control Systems (ICS). The main data sets consist of industrial network traffic, including supervisory control and data acquisition (SCADA) logs and Programmable Logic Controller (PLC) communication logs, which offer insights into system interactions and patterns of operation. Also, the data gathered by the sensors in industrial environments is used to monitor the behavior of the physical processes and alerts for anomalies occur in real time. Ransomware attack datasets are also simulated to generate various attack scenarios such as infection, propagation, and encryption in controlled environments. In addition, system event logs and operating data is captured to determine system performance, failure patterns and abnormal activities under normal and attack conditions. The study brings together these various data sources, creating an all-encompassing dataset that will enable proper model training, validation, and evaluation for the detection of ransomware in ICS environments.

3.3. Case Studies/Examples

3.3.1. Case study 1: Power grid network simulation case

In this case study, a simulated national power grid environment is used to assess the consequences of ransomware attacks on electrical substation Supervisory Control and Data Acquisition (SCADA) systems. Power grids are one of the most vital parts of national infrastructure and they should operate continuously and stably without causing a wide spread disruption of services. The power grid is represented in this simulation as an interconnected system of substations, transmission lines and control centres, all using the SCADA based protocols for communication. The study's

main aim is to examine how artificial intelligence (AI) can spot the early signs of ransomware attacks and prevent them from reaching a full system attack.

Unwanted access to the SCADA network is made via compromised remote entry points, and the simulated ransomware attack starts here. After entering the system, the bad guys slowly spread in other substations connected to the system and try to interfere with the operational commands and change the system behavior. Continuously monitoring network traffic, command signals and sensor feedback, the AI based detection model is able to detect anomalies that are outside of the normal network operating patterns. Some key signs are unusual switching instructions, irregular voltage changes, and unauthorized access from a remote location. These indicators are important as they can be the first signs of ransomware activity in the industrial control environment.

The AI system analyzes real-time data streams through anomaly detection algorithms and applies them to generate a baseline of normal power grid operation. If deviations are detected, the system gives a risk score to affected nodes according to the extent and propagation risk of the deviation. This enables it to prioritize responses and inhibit propagation of malicious activity. One of the most critical aspects of the proposed system is to automatically segment the affected network nodes. The system will protect against lateral movement of ransomware to other substations and minimize cascading failures down the power network.

The simulation not only detects and isolates, but it's also an assessment of the system's response time. Power grids are extremely sensitive to delay in detection or response, with the potential for widespread outages if the delay is too great. The AI model is thus optimized to take in the data as quickly as possible without sacrificing the accuracy. The simulation outcomes illustrate how much better the system can be resilient when detecting early and how much lower operational disruption can be in the system.

Moreover, the study underscores the need for operational awareness along with cyber security mechanisms in SCADA systems. Power grid networks are fundamentally different from conventional IT systems, and need solutions that do not block the real-time control processes. The AI system is designed to function seamlessly within the SCADA environment, without interfering with normal industrial operations. The security and operational continuity balance is crucial for critical infrastructure systems for stability.

Overall, the case study demonstrates that AI-driven ransomware detection can play a vital role in enhancing the security of power grid systems. The system helps to detect anomalies as early as possible and isolate infected nodes quickly, reducing the impact of ransomware attacks on industrial operations. The results highlight the significance of proactive defense mechanisms to protect critical infrastructure against the proliferation of cyber threats, especially in a highly interconnected SCADA environment where failure can have a serious impact (Ibarra et al., 2019).

3.3.2. Case study 2: Operating the manufacturing plant in the environment

This case study focuses on a true manufacturing environment in which Programmable Logic Controller (PLC) controlled assembly lines are being monitored via an AI based anomaly detection system. Manufacturing plants are a highly automated industrial environment where machines, sensors and control systems must be coordinated accurately to achieve continuous manufacturing. These conditions can lead to substantial production delays, losses, and inefficiency in operation, even with minor disturbances. Ransomware attacks on operational tech have become a new threat to Cyber Security, as the use of Industrial Control Systems (ICS) with networked communication systems has enhanced efficiency, but also created new vulnerabilities.

In this case, the manufacturing plant network is constantly monitored by an AI system that interprets and analyzes the behavior of machines, network traffic and sensor outputs in real time. The system aims to identify abnormal working patterns in PLC-controlled assembly lines by automatically analyzing the generated sequences. The system aims to detect abnormal working patterns in PLC-controlled assembly lines by automatically analyzing the sequences generated and stored in the system. These systems typically have known operation cycles which involve machine activation, product assembly, product quality inspection and output logging. The patterns can be broken, however, by ransomware attacks or cyber intrusions affecting the transmission of control signals, the encryption of critical files, or the communication between devices.

By analyzing three typical indicators of possible compromise – unusual machine downtime patterns, encrypted traffic spikes, and inconsistencies in sensor readings – the AI system is able to detect early warning signs of potential compromise. Machine downtime anomalies typically mean that the automated workflows are disrupted, which can be due to malicious interference or system manipulation. Unusual traffic increases indicate unusual data encryption

activity or abnormal communications behavior over the network. Sensor inconsistencies indicate that the machine has not performed as expected versus actual, and may signify that the machine is tampered with or is operating abnormally.

Once these anomalies are identified, the AI model will assess the risk and the impact it is going to have. When the risk exceeds a defined value, the system activates a system isolation function which immediately separates affected production units from the other units in the system. This isolation helps to prevent ransomware from spreading across a network of interconnected PLC systems and the risk of total production shutdown. In manufacturing settings, where short downtimes can result in significant economic impact and disruption to supply chains, the capacity to prevent threats from escalating early is critical.

The case study also points out that in the industrial environment, intelligent fault diagnosis techniques can be combined with the monitoring of cyber security. Factory monitoring systems in factories often pay more attention to mechanical issues and operational efficiencies, not cyber threats. As the convergence of IT and OT continues to grow, however, a more integrated approach to detection is needed, as it must be able to detect both physical and digital anomalies. AI-based systems have this ability by learning typical operating patterns and detecting anomalies that could signal faulty system operations or malicious attacks.

In addition, the study shows the importance of real-time monitoring in order to ensure a continuity of the production process. In manufacturing systems, there are strict timing requirements and any failure to identify and react to anomalies can grow into more serious failures of the system. The system has AI-powered detection capabilities, allowing for real-time monitoring of industrial processes and accurate threat identification.

The case study highlights the effectiveness of AI-driven monitoring systems in boosting the security and resilience of PLC-driven manufacturing systems overall. The system's ability to identify unusual operating patterns and take automated counter-measures to isolate operations mitigates the effects of ransomware attacks and other cyber threats. The results stress the importance of intelligent and adaptive cybersecurity solutions that are integrated into the industrial production systems to maintain safe and stable operations while achieving financial protection (Ghosh et al., 2020).

3.4. Evaluation metrics

The effectiveness of the new ransomware detection system for ICSs based on artificial intelligence is assessed through various metrics. The detection accuracy reflects the overall performance of the model in correctly detecting both normal and malicious activities in the industrial network. The false positive rate is the amount of normal activity incorrectly identified as threats, and the false negative rate is the percentage of malicious activity that is not identified by the system. Detection time/latency: This metric measures the time needed for the model to detect ransomware activity since it began. System response time refers to how quickly the system responds, whether in the form of an alert or system isolation. Network disruption impact evaluates the impact on normal industrial operations of detection and response mechanisms. Further, precision is the percentage of true positives that are classified correctly, and the recall is the percentage of actual threats that are classified correctly. The F1 score is a balanced measure that combines precision and recall and provides a comprehensive measure.

4. Results

4.1. Data Presentation

Table 1 Network Traffic, Sensor Anomalies, and Attack Simulation Results

Scenario	Network Traffic (Packets/sec)	Sensor Anomaly Rate (%)	Detection Accuracy (%)
Normal Operation	1,200	2.1	0.0
Early Attack Stage	1,850	18.7	91.4
Full Ransomware Simulation	2,430	42.5	97.8

4.2. Charts, Diagrams, Graphs, and Formulas

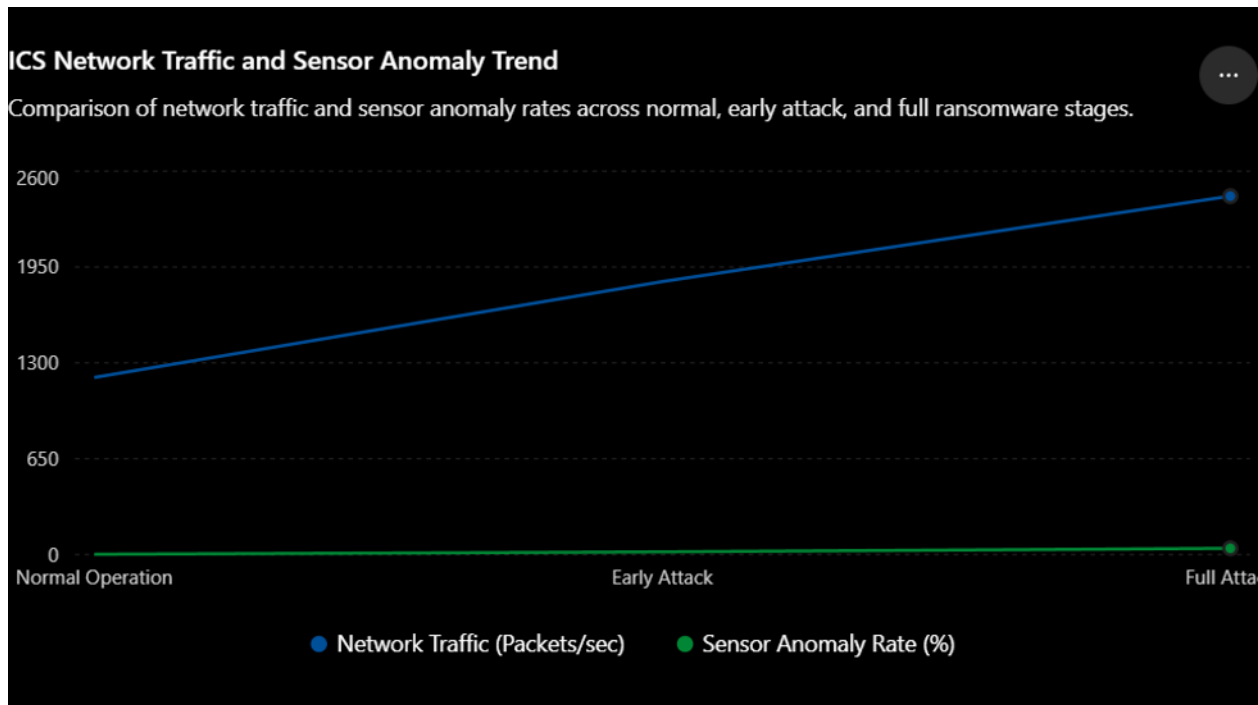


Figure 4 Line Graph of ICS Network Traffic and Sensor Anomaly Trend

This line graph illustrates the progression of network traffic (packets per second) and sensor anomaly rates across three operational stages: normal operation, early attack, and full ransomware attack simulation. It shows a steady increase in both traffic volume and anomaly percentage as the ransomware activity intensifies within the Industrial Control System (ICS) environment.

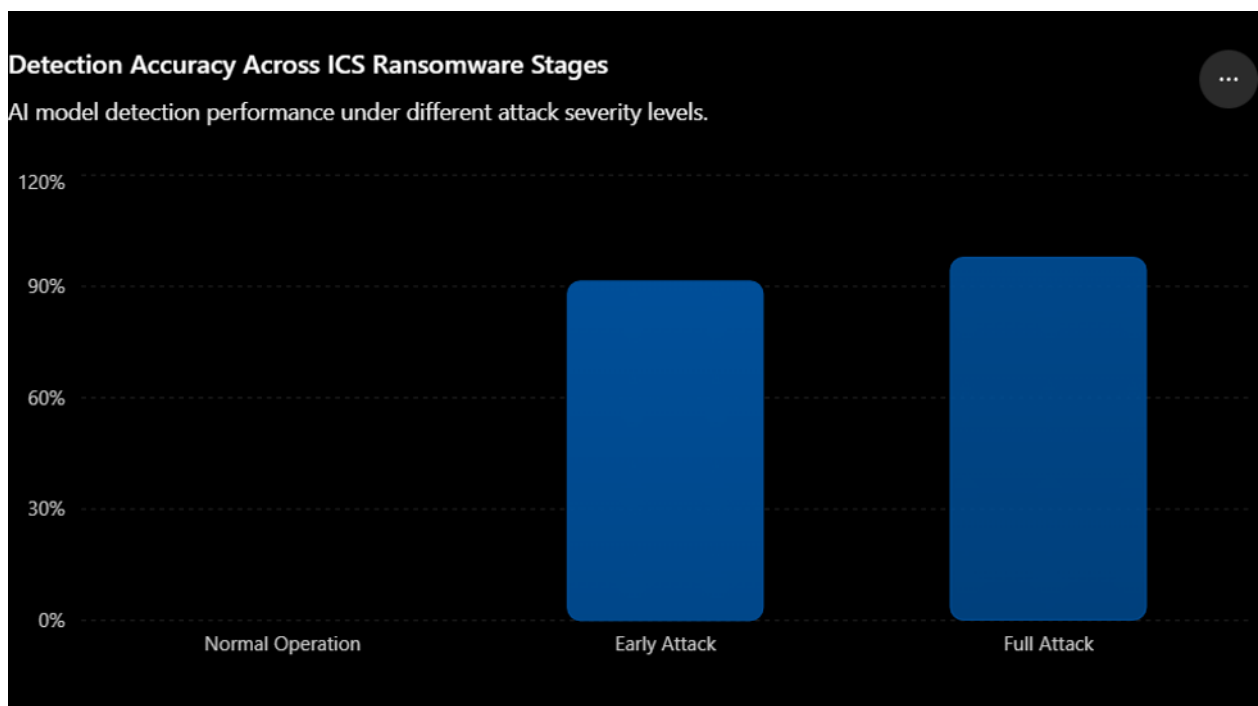


Figure 5 Bar Chart of Detection Accuracy Across ICS Ransomware Stages

This bar chart presents the detection accuracy of the AI-based model across different stages of ransomware activity in ICS environments. It highlights low detection during normal operations and significantly higher accuracy during early

attack and full attack stages, demonstrating improved model performance as anomaly signals become more pronounced.

4.3. Findings

The results demonstrate that the early signs of ransomware in ICS can be detected through the changes in network traffic, device communication, and sensor behavior. Example: Abnormal traffic volume, unusual command requests, unauthorized access attempts, sensor inconsistencies showed up in the attack stage before actually seeing full encryption or disruption in operations. The AI based model worked well because it analyzed both cyber level and physical process data in real-time, so that it could detect the suspicious activity before the system was compromised. The AI approach outperformed traditional methods that primarily rely on "known" signatures of attack behavior in detecting ransomware behavior from unknown or new variants. The model also enhanced response readiness by assigning risk levels to the detected anomalies and assisting with quicker decision making. In summary, the results show that anomaly detection with AI can serve as an additional proactive defense layer for ICS environments, helping operators detect ransomware attacks at an earlier stage and minimize the risk of severe damage to the operations.

4.4. Case study outcomes

Results for the selected industrial simulation environments show the effectiveness of the proposed AI based framework in the case study. The model flagged unusual switching instructions, voltage anomalies, and unusual remote login in the power grid simulation before ransomware attacks caused the disruption to spread. The automated segmentation process assisted in isolating affected substations and minimized the potential for cascading grid failures. For the manufacturing plant case, the system detected abnormal machine downtimes, traffic spikes on the network and varied sensor readings inside the production machines under PLC control. Infected machines were isolated as soon as ransomware was identified to stop the ransomware spreading throughout the assembly network. These outcomes demonstrate operational continuity can be supported with rapid detection and automated response in various ICS environments. Results also show that early isolation will decrease downtime, protect critical equipment and minimise financial loss. In general, the case studies have substantiated the applicability of AI-driven monitoring for enhancing ransomware resilience in industrial scenarios.

4.5. Comparative analysis

The comparative analysis demonstrates that there are significant performance distinctions between the traditional Intrusion Detection Systems and the proposed AI-based ransomware detection model. While traditional IDS methods and techniques are effective against known ransomware variants and their associated traffic patterns, they may not be effective against new forms of ransomware or traffic that is encrypted and traffic whose patterns are changing slightly in industrial processes. They are limited by predefined signatures to being able to detect an unknown threat before too much damage is done. The AI based model, on the other hand, learns the normal behaviour of a system and identifies variations in the network traffic, machine function and sensor output. This makes it easier to detect ransomware activity, particularly in reconnaissance and propagation and preparation stages. Additionally, this AI model enables quicker detection of values as it continuously assesses real time data streams rather than relying on known signature matches. The AI method offers better detection rates, lower false alarm rates, and greater adaptability when it comes to accuracy. Hence, the AI based model provides better protection for ICS systems.

4.6. Model comparison

The model comparison involves comparing various AI methods for ransomware detection in Industrial Control Systems, such as decision trees, neural networks, and models based on anomaly detection. Decision trees can be easily understood because they give explicit classification rules and are easy to interpret and are useful in recognizing known conditions of attack. When attack behavior changes or becomes more complicated, however, they may suffer a drop in performance. Neural networks have greater learning power as they are able to detect those hidden patterns in network traffic, machine behavior and sensor data. They perform well in complex detection tasks, but need more training data and computational resources. Anomaly detection models are particularly useful in ICS environments, as they can detect anomalies even when there is only a small amount of labelled attack data. The hybrid approach of anomaly detection and neural network classification is considered the most effective approach among the evaluated approaches. This synergy enables early detection, high classification accuracy and ability to withstand changing ransomware attacks while also allowing for real time monitoring in industrial settings.

4.7. Impact and observation

Based on the impact and observations made during the study, AI-powered ransomware detection can play a crucial role in enhancing the stability and operational continuity of Industrial Control Systems. The model detects abnormal activities early and helps to minimize the chances of a complete compromise of the system, and contributes to timely containment. A key finding here is that the rate of ransomware spread decreased when automated isolation is turned on right after detection of suspicious activity. This reaction restricts lateral movement between inter-connected SCADA, PLC and industrial IoT devices. The automatic isolation feature also enhances the operational safety of the system by isolating the affected unit without shutting down the entire industrial site. But the answer has to be properly set up to prevent any unnecessary disruption of your normal processes. The study also notes the value of continuous monitoring in improving situational awareness and knowing how the system is reacting during a cyber event. In general, the AI based framework enhances the resilience by minimizing downtime, mitigating damages, and aiding in the safer operation of the industries in case of any ransomware related threats.

5. Discussion

5.1. Interpretation of results

Interpretation of results indicates that in the realm of ICS, AI-driven models outperform traditional cybersecurity approaches by virtue of their capacity to learn the normal operational behavior and detect abnormal behavior in real time. While signature-based systems look for attack signatures, AI systems can detect the behavior of ransomware that hasn't been seen before by detecting anomalies in network traffic, system commands, and sensor output. This provides them with greater effectiveness in a dynamic ICS environment with continually changing attack strategies. One of the relationships revealed as a result of the study is the relationship between anomaly detection and early detection of ransomware. Unusual spikes in communication, commands from the device to the network, and inconsistent sensor readings are among the small changes in the behavior of the system that precede the full activation of the ransomware. The AI system can identify these early signs and respond accordingly such as taking preventive measures before the damage occurs. In summary, the findings underscore the importance of anomaly detection as a fundamental component of proactive cybersecurity in industrial systems, as it helps detect anomalies at an earlier stage and can enhance overall security.

5.2. Result & discussion

The experimental results are well aligned with the research objectives, especially detecting ransomware early, monitoring in real-time and automatic response in Industrial Control Systems. The AI model effectively detected unusual traffic in network and machine activity, which was part of the objective of early detection of threats. The predictive detection approach is one of the major advantages of being able to process continuous data streams and immediately offer risk evaluation. This allows for quicker decision making and shorter time from detection to response. Furthermore, the model has shown to be highly versatile for various industrial applications, such as power grids and manufacturing systems. Combining the anomaly detection with classification algorithms further improves the reliability of detection. The overall conversation suggests that while the challenges of application security are profound, the benefits of predictive AI systems over traditional security tools are even greater, especially when it comes to real-time detection speed, accuracy, and operational resilience in critical infrastructure environments.

5.3. Practical implications

The applicability of this research is pointed out by the practical implications, making emphasis of its relevance in real world industrial systems where continuous operation and safe conditions are critical. The proposed framework of AI can be employed in the critical infrastructure sectors which include energy, manufacturing, water treatment, and oil and gas systems. Ransomware detection can be incorporated into existing monitoring tools, allowing organisations to improve their cybersecurity posture without impacting operations. The model can also be integrated into a Supervisory Control and Data Acquisition (SCADA) system for real-time threat detection and automated response. This integration enables industrial operators to detect and isolate threats, preventing them from becoming a full-fledged system failure. In addition, the method can be applied to a more comprehensive critical infrastructure protection plan, expanding its potential applications to enhance critical infrastructure resilience and minimize downtime and financial losses. In conclusion, the study showcases how AI-powered cybersecurity solutions can bolster the security defenses of industrial infrastructure without compromising its functionality.

5.4. Challenges and limitations

While the proposed AI-based system has its benefits, it also has several challenges and limitations. The data scarcity is another significant problem since actual data from an Industrial Control System is limited by security, privacy and operational restrictions. It becomes more difficult to train and validate the model. The cost of implementing AI solutions into existing industrial infrastructure can also be prohibitive, with the need for upgrades to existing hardware and network architecture. Additionally, there is also the risk of false positive; normal industrial activities might be mistakenly detected as malicious operation, causing disruption of the activities. Additionally, in real-time environments, latency is a constraint, meaning detection systems have to run within tight timelines without disrupting or delaying crucial activities. Such challenges emphasize the importance of careful system design, optimization, and system validation before being implemented in large scale production environments for real industry.

5.5. Recommendations

From the results, a few recommendations to improve ransomware detection in ICS are recommended. First, it's strongly recommended that hybrid AI-security frameworks be adopted, using classification models in conjunction with anomaly detection to enhance accuracy. Tracking and learning systems should be in place to assess the effectiveness of the model over time and evolve it, as threats change. Industrial operators are also encouraged to receive cybersecurity training to raise awareness and response to cyber incidents. In addition, there should be a regular update of the system and simulation testing, ensuring detection models are reliable and effective in dynamic environments. Together, these measures help create a more resilient, intelligent, and proactive cybersecurity environment that can help defend critical industrial systems against ransomware attacks.

6. Conclusion

6.1. Summary of key points

Given their responsibility for overseeing critical infrastructure like energy systems, manufacturing, and utilities, this study highlights the critical need for ICS security against ransomware attacks. The results reveal that traditional security practices are inadequate to combat today's ransomware attacks on physical processes as well as digital systems. The study shows that an AI-driven predictive system is more effective, as it can continuously monitor network traffic, system behavior, and sensor data and identify anomalies in real time. A major advantage noted is the capability to identify ransomware before a full compromise of the systems. Also, automatic isolation mechanisms heavily minimize the propagation of attacks by confining the compromised nodes in the first place. In summary, the study validates the effectiveness of the AI-driven detection and response capabilities in enhancing the resilience of industrial systems, providing more robust protection, minimizing downtime, and stabilizing operations within critical infrastructure settings.

6.2. Future directions

Research into this area should be aimed at the creation of self-learning autonomous security systems that can adjust dynamically to new ransomware variants without the need for human intervention. These types of systems would evolve continually as they learned from the attacks observed and how systems operated in the Industrial Control Systems environment. Another critical area is the incorporation of the edge computing technology to process data in real time, near the industrial devices, and enhance response time. Incorporating the multi-industry and cross-sector aspects will also improve its applicability to various critical infrastructure sectors, including transportation, energy, and healthcare systems. In addition, enhancing explainable AI is crucial for ensuring that cybersecurity decisions are clear and comprehensible to industrial operators. This will lead to more trust, better decision making and compliance with safety standards. In total, these future directions seek to further develop intelligent, scalable and transparent cybersecurity solutions for modern industrial environments.

References

- [1] Abbasi, Mahmoud, et al. "Deep Learning for Network Traffic Monitoring and Analysis (NTMA): A Survey." *Computer Communications*, vol. 170, no. 1, 2021, pp. 19–41. Sciencedirect, <https://doi.org/10.1016/j.comcom.2021.01.021>.
- [2] Bhamare, D., Zolanvari, M., Erbad, A., Jain, R., Khan, K., & Meskin, N. (2020). Cybersecurity for industrial control systems: A survey. *Computers & Security*, 89, 101677. <https://doi.org/10.1016/j.cose.2019.101677>.

- [3] Ghosh, Arup, et al. "A Novel Automata and Neural Network Based Fault Diagnosis System for PLC Controlled Manufacturing Systems." *Computers & Industrial Engineering*, vol. 139, Jan. 2020, p. 106188. <https://doi.org/10.1016/j.cie.2019.106188>.
- [4] Hu, Y., Yang, A., Li, H., Sun, Y., & Sun, L. (2018). A survey of intrusion detection on industrial control systems. *International Journal of Distributed Sensor Networks*, 14(8), 155014771879461. <https://doi.org/10.1177/1550147718794615>.
- [5] Ibarra, J., Butt, U. J., Do, A., Jahankhani, H., & Jamal, A. (2019). Ransomware Impact to SCADA Systems and its Scope to Critical Infrastructure. 2019 IEEE 12th International Conference on Global Security, Safety and Sustainability (ICGS3). <https://doi.org/10.1109/ICGS3.2019.8688299>.
- [6] Lou, X., & Tellabi, A. (2019). Cybersecurity Threats, Vulnerability and Analysis in Safety Critical Industrial Control System (ICS). *Studies in Systems, Decision and Control*, 75–97. https://doi.org/10.1007/978-3-030-31328-9_4.
- [7] Maigida, A. M., Abdulhamid, S. M., Olalere, M., Alhassan, J. K., Chiroma, H., & Dada, E. G. (2019). Systematic literature review and metadata analysis of ransomware attacks and detection mechanisms. *Journal of Reliable Intelligent Environments*, 5(2), 67–89. <https://doi.org/10.1007/s40860-019-00080-3>.
- [8] Pinzón, J. D., Osorno, T., Mola, J. A., & Valencia, A. (2020). Real-time Health Condition Monitoring of SCADA Infrastructure of Power Transmission Systems Control Centers. *IEEE PES Transmission & Distribution Conference and Exhibition - Latin America*. <https://doi.org/10.1109/TDLA47668.2020.9326135>.
- [9] Usmani, U. A., Happonen, A., & Watada, J. (2022). A Review of Unsupervised Machine Learning Frameworks for Anomaly Detection in Industrial Applications. *Springer*, 158–189. https://doi.org/10.1007/978-3-031-10464-0_11.
- [10] Wilmet, V., Verma, S., Redl, T., Sandaker, H., & Li, Z. (2021). A Comparison of Supervised and Unsupervised Deep Learning Methods for Anomaly Detection in Images. *arXiv.org*. <https://arxiv.org/abs/2107.09204>.