International Journal of Technology Management & Humanities (IJTMH)
e-ISSN: 2454 – 566X, Volume 09, Issue 2, (June 2023), www.ijtmh.com

Machine Learning (ML) –Based Cyber Threat Modelling for Industrial Control Systems in critical Infrastructure

Agim Takon
Novation Ltd., Canada
Email ID: atakon2000@gmail.com

DOI: 10.21590/ijtmh.2023090208

Abstract

ICS are operational systems that jot up the backbone of critical infrastructure systems like energy, water, transportation, and manufacturing. The rising integration of the operational and information technology has greatly broadened the cyber-attack surface of these systems to advanced and persistent threats that cannot be easily stopped using conventional rule-based security measures. Cyber threat modelling with the use of machine learning (ML) has become a potential activity that can improve the performance of cyber threat detection, analysis, and prediction in ICS environments. This paper analyses the use of ML in the context of cyber threat modelling in critical infrastructure with respect to the capability of detecting abnormal behaviour, discovering never-before-seen attack patterns, and helping to motivate mitigation of risk earlier. The abstract covers the popular ML paradigms in the context of ICS security, such as supervised, unsupervised, and hybrid learning models, and their application in the industrial network structure, such as the SCADA systems and programmable logic controllers. The main issues associated with data quality, model explanation, real-time application, and safety of operations are also discussed. In general, ML-based cyber threat modelling offers a strategic channel of enhancing resilience, situational awareness, and adaptive defense capacity within ICS-driven critical infrastructure.

Keywords: Machine Learning; Cyber Threat Modelling; Industrial Control Systems; Critical Infrastructure; SCADA Security; Operational Technology; Anomaly Detection

Introduction

ICS is the backbone of the utilization of the most vital sectors of the infrastructure, such as energy production and distribution, water treatment, transport, manufacturing, and food security. These systems which include Supervisory Control and Data Acquisition (SCADA), Distributed Control Systems (DCS), and Programmable Logic Controllers (PLCs) were originally configured to be reliable, deterministic, and safe, and not to be cybersecure. Nevertheless, the gradual integration of operational technology (OT) with information technology (IT) and more communication with

enterprise networks and cloud services has greatly increased the attack surface of ICS environments (Bhamare et al., 2020). Consequently, critical infrastructure has emerged as a prime target by advanced cyber attackers who can inflict physical damage, economic damages and risk to the communities.

The legacy cybersecurity technologies, employed in ICS, like signature-based intrusion detection systems and set-in-stone rule-based threat modeling, are becoming no longer sufficient to deal with the various and camouflaged attacks. These methods have difficulties with the detection of zero-day exploits, advanced persistent threats, and process-level anomalies that are only slightly different than the usual operations of the system (MR et al., 2021). Moreover, industrial settings have a low applicability of traditional IT security measures due to the existence of legacy devices, proprietary protocols, and hard real-time requirements (Zolanvari et al., 2019).

Machine Learning (ML) has become an enabling disruptive capability in cyber threat modelling in ICS since it enables systems to learn multifaceted patterns out of data and respond to changing threat environments. Based on network traffic, system logs, and process level sensor data, ML-based techniques are used to detect anomalies, classify intrusions, and predict risks (Selim et al., 2021; Mokhtari et al., 2021). In particular, deep learning and ensemble models have proven to be very successful in detecting known and unrecognized attacks in industry (Al-Abassi et al., 2020; Alkahtani and Aldhyani, 2022). These abilities assist in a transition to responsive security postures to active and intelligence-led defense procedures.

Even with potential, there is a lot of difficulty in deploying ML-based cyber threat models in ICS. Problems with data insufficiency, imbalanced classes, and explainability of the model and adversarial influence of a learning system are all significant issues (Anthi et al., 2021; Olowononi et al., 2020). Opaque decision-making processes in safety-critical settings can become obstacles to trust and operational adoption, and interpretable and resilient ML frameworks are required. Moreover, it is necessary to incorporate security analytics based on ML with wider cyber risk management and governance models to guarantee that it is in tandem with organizational and regulatory needs (Kure et al., 2022).

New developments in scalable data architectures, cloud and hybrid data environments, and DevSecOps methods have an additional impact on the viability of ML-based threat modelling in key infrastructure.High-throughput data ingestion frameworks and data lakehouse architectures enable large-scale analysis of heterogeneous industrial data streams, supporting real-time and predictive security analytics (Azmi et al., 2022; Syed et al., 2023). Moreover, automated security controls and continuous monitoring approaches, as emphasized in DevSecOps models, provide a foundation for integrating ML-based threat intelligence across distributed and multi-cloud environments (Okafor et al., n.d.).

Within this context, ML-based cyber threat modelling represents a strategic approach to enhancing the resilience, situational awareness, and adaptive defense capabilities of ICS-driven critical infrastructure. By leveraging data-driven intelligence while addressing operational and security constraints, ML techniques offer a pathway toward more robust and future-ready cybersecurity frameworks for industrial environments.

ICS Cyber Threat Environment

Industrial Control Systems (ICS) operate at the core of critical infrastructure, enabling real-time monitoring and control of physical processes across sectors such as energy, water treatment, food production, transportation, and manufacturing. Unlike conventional IT systems, ICS environments are designed for availability, determinism, and safety, often relying on legacy hardware and proprietary protocols that were not originally developed with cybersecurity as a primary concern. The increasing integration of ICS with Industrial Internet of Things (IIoT), enterprise IT networks, and cloud-based analytics has substantially expanded the cyber threat surface, exposing critical infrastructure to sophisticated and persistent cyber attacks (Bhamare et al., 2020).

Threat Landscape and Attack Vectors

The ICS cyber threat environment is characterized by a diverse set of attack vectors targeting both cyber and physical layers. Common threats include malware injection, ransomware, command injection, denial-of-service attacks, insider threats, and supply-chain compromises. Adversaries frequently exploit weak authentication mechanisms, unpatched vulnerabilities, and insecure communication protocols to gain unauthorized access to supervisory control and data acquisition (SCADA) systems, programmable logic controllers (PLCs), and human–machine interfaces (HMIs) (Zolanvari et al., 2019; MR et al., 2021). Once access is established, attackers can manipulate sensor readings, alter control logic, or disrupt system availability, potentially leading to physical damage, service outages, or safety incidents.

Advanced persistent threats increasingly leverage stealthy techniques that blend into normal operational traffic, making detection difficult using signature-based or rule-driven security mechanisms. Anomaly-based approaches are therefore gaining prominence, as they aim to identify deviations from established operational baselines rather than relying on known attack signatures (Selim et al., 2021; Mokhtari et al., 2021).

Unique Characteristics of ICS Environments

Several structural and operational characteristics distinguish ICS cyber threat environments from traditional IT settings. ICS networks often have long system lifecycles, limited computational resources, strict real-time constraints, and low tolerance for latency or downtime. Security updates

and patch management are frequently constrained by safety certification requirements and continuous operation demands, resulting in prolonged exposure to known vulnerabilities (Alkahtani & Aldhyani, 2022). Additionally, the deterministic nature of industrial processes means that even minor disruptions or false alarms can have disproportionate operational consequences.

The convergence of IT, OT, and cloud infrastructures further complicates the threat environment. Hybrid architectures, data lakes, and multi-cloud deployments used for analytics and decision support introduce new dependency chains and attack surfaces, requiring coordinated cybersecurity governance across heterogeneous platforms (Azmi et al., 2022; Syed et al., 2023; OKAFOR et al.).

Implications for Machine Learning–Based Threat Modelling

Given the scale, complexity, and heterogeneity of modern ICS deployments, machine learning has emerged as a critical enabler for modeling cyber threats in these environments. ML techniques can analyze high-dimensional data streams from sensors, network traffic, and logs to uncover subtle attack patterns and predict emerging risks (Al-Abassi et al., 2020; Kure et al., 2022). However, the ICS threat environment also poses challenges for ML adoption, including limited labeled datasets, adversarial manipulation of learning models, and the need for explainable outputs to support operator trust and safety-critical decision-making (Anthi et al., 2021; Olowononi et al., 2020).

Major ICS Cyber Threat Categories

Table 1 summarizes key cyber threat categories in ICS environments, their typical targets, potential impacts, and relevance to ML-based detection approaches.

Table 1: Cyber threat categories in ICS environments, their typical targets, potential impacts, and relevance to ML-based detection approaches

Threat Category	Typical Targets	Potential Impact	Relevance to ML-Based Modelling
Malware & Ransomware	SCADA servers, HMIs, engineering workstations	System outages, loss of control, operational downtime	Behavioral analysis and anomaly detection for early identification (Al-Abassi et al., 2020)
Network Intrusion	ICS network traffic, fieldbus protocols	Unauthorized access, lateral movement	Traffic pattern learning and intrusion classification (MR et al., 2021)

Sensor/Data Manipulation	Sensors, PLC input/output signals	Incorrect control decisions, physical damage	Time-series anomaly detection and measurement validation (Mokhtari et al., 2021)
Insider Threats	Control logic, operator interfaces	Sabotage, safety incidents	User behavior modeling and deviation analysis (Selim et al., 2021)
Supply-Chain Attacks	Firmware, software updates, third-party components	Persistent compromise, hidden backdoors	Model-based risk prediction and integrity monitoring (Bhamare et al., 2020)
Adversarial ML Attacks	ML-based security systems	Evasion or poisoning of detection models	Robust and resilient ML model design (Anthi et al., 2021; Olowononi et al., 2020)

Overall, the ICS cyber threat environment is dynamic, high-impact, and fundamentally different from traditional IT security contexts. These characteristics underscore the necessity of adaptive, data-driven, and resilient ML-based cyber threat modelling frameworks capable of operating within the stringent safety and reliability constraints of critical infrastructure systems.

Machine Learning in Cyber Threat Modelling

Machine Learning (ML) has become a central enabler for advanced cyber threat modelling in Industrial Control Systems (ICS), particularly within critical infrastructure environments where conventional signature-based and rule-driven security mechanisms are insufficient. The dynamic nature of cyber threats, coupled with the heterogeneity and legacy constraints of ICS architectures, necessitates adaptive, data-driven approaches capable of learning complex system behaviors and detecting deviations indicative of malicious activity (Bhamare et al., 2020).

Role of Machine Learning in ICS Threat Modelling

ML-based cyber threat modelling focuses on learning normal operational patterns of industrial processes, network communications, and control commands, and subsequently identifying anomalies or attack signatures that diverge from these baselines. Unlike traditional IT systems, ICS environments emphasize availability and safety, making passive monitoring and high-precision detection essential (MR et al., 2021). ML models are therefore trained on diverse data

sources, including network traffic flows, sensor measurements, control logic states, and system logs, to construct comprehensive threat models (Mokhtari et al., 2021).

Supervised learning techniques are commonly employed when labeled attack datasets are available, enabling classification of known attack types such as denial-of-service, command injection, or data manipulation (Selim et al., 2021). In contrast, unsupervised and semi-supervised methods are particularly valuable in ICS settings due to the scarcity of labeled attack data, allowing detection of zero-day attacks through anomaly and behavior-based modelling (Alkahtani & Aldhyani, 2022).

ML Paradigms and Detection Strategies

Deep learning and ensemble-based approaches have demonstrated improved detection accuracy in complex ICS environments by capturing non-linear relationships and temporal dependencies in industrial data streams (Al-Abassi et al., 2020). Recurrent neural networks and autoencoders are frequently applied for time-series analysis of sensor and actuator data, while ensemble models improve robustness by combining multiple classifiers to mitigate false positives and single-model bias.

Additionally, ML-based threat modelling is increasingly integrated with cyber risk prediction frameworks to support proactive defense strategies. By correlating detected anomalies with asset criticality and system dependencies, ML models can contribute to dynamic risk scoring and impact-aware decision-making (Kure et al., 2022). Network-level vulnerability analysis using ML further enhances threat modelling by identifying weak points in industrial communication paths and IIoT components (Zolanvari et al., 2019).

Cross-Domain ML Integration and Supporting Technologies

Beyond traditional anomaly detection, ML-driven threat modelling in ICS benefits from cross-domain techniques such as behavioral analytics, natural language processing (NLP), and large-scale data engineering frameworks. Behavioral analytics strengthen insider threat detection and process-aware security monitoring (Uppuluri, 2020), while NLP techniques can be leveraged to analyze unstructured threat intelligence reports and security logs for contextual enrichment (Uppuluri, 2019). Scalable data architectures, including hybrid cloud data lakes and lakehouse frameworks, support the high-throughput ingestion and processing required for ML-driven ICS security analytics (Azmi et al., 2022; Syed et al., 2023).

However, ML-based cyber threat modelling must also account for adversarial machine learning risks. Attackers may attempt to poison training data or evade detection through carefully crafted inputs, necessitating resilient and explainable ML models tailored for cyber-physical systems (Anthi et al., 2021; Olowononi et al., 2020).

Major ML Techniques for Cyber Threat Modelling in ICS

Table 2 summarizes the primary machine learning approaches applied to cyber threat modelling in ICS environments, highlighting their typical use cases, strengths, and limitations.

Table 2: Machine Learning Techniques for Cyber Threat Modelling in Industrial Control Systems

ML Approach	Typical Algorithms	Application in ICS	Key Advantages	Key Limitations
Supervised Learning	SVM, Random Forest, k-NN, Neural Networks	Classification of known cyber-attacks and intrusion detection	High accuracy for known threats; interpretable results	Requires labeled datasets; limited zero-day detection
Unsupervised Learning	K-means, Autoencoders, Isolation Forest	Anomaly and zero-day attack detection	Effective with unlabeled data; adaptive to new threats	Higher false positives; interpretation challenges
Deep Learning	CNN, RNN, LSTM, DNN	Temporal and multivariate process anomaly detection	Captures complex patterns and dependencies	Computationally intensive; limited explainability
Ensemble Learning	Bagging, Boosting, Hybrid Models	Robust intrusion and attack detection	Improved detection stability and accuracy	Increased model complexity
Behavioral Analytics	Statistical ML, Sequence Models	Insider threat and process deviation detection	Context-aware security monitoring	Requires detailed process knowledge
ML-Based Risk Prediction	Hybrid ML + Risk Models	Impact-aware threat prioritization	Supports proactive defense strategies	Dependence on accurate asset modeling

Overall, machine learning provides a foundational capability for modern cyber threat modelling in ICS-driven critical infrastructure. By enabling adaptive detection, predictive risk assessment, and

system-aware security analytics, ML enhances both the resilience and situational awareness of industrial environments. Nevertheless, challenges related to data quality, operational safety, model interpretability, and adversarial robustness remain critical considerations for the effective deployment of ML-based cyber threat modelling solutions (MR et al., 2021; Anthi et al., 2021).

ML-Based Threat Modelling Architectures

Machine Learning (ML)–based threat modelling architectures for Industrial Control Systems (ICS) are designed to address the unique operational constraints, deterministic communication patterns, and safety-critical requirements of critical infrastructure environments. Unlike conventional IT systems, ICS architectures require security models that operate with minimal latency, high reliability, and strong contextual awareness of industrial processes. As a result, ML-based threat modelling architectures are typically layered, hybrid, and tightly integrated with operational technology components (Bhamare et al., 2020).

1. Layered ML Threat Modelling Architecture

A common architectural approach adopts a multi-layered design, where ML models are deployed across perception, network, and application layers of the ICS environment. At the field level, data is collected from sensors, actuators, and programmable logic controllers (PLCs). At the network level, traffic flows between SCADA servers, Human–Machine Interfaces (HMIs), and remote terminal units (RTUs) are monitored. ML models analyze this data to identify deviations from expected operational baselines (Selim et al., 2021; Mokhtari et al., 2021).

Supervised learning models are often placed at higher layers where labeled historical attack data is available, while unsupervised or semi-supervised models operate closer to the process layer to detect novel or zero-day attacks through anomaly detection (MR et al., 2021).

2. Anomaly-Based and Behavior-Based Architectures

ML-based threat modelling architectures generally fall into two complementary categories: anomaly-based and behavior-based systems.
Anomaly-based architectures rely on unsupervised learning techniques such as clustering, autoencoders, and statistical learning to model normal system behavior and flag deviations that may indicate cyber intrusions or process manipulation (Mokhtari et al., 2021). These architectures are particularly effective in ICS environments where attack signatures are scarce or constantly evolving.

Behavior-based architectures, on the other hand, focus on learning sequential and temporal patterns of user actions, control commands, and system state transitions. Deep learning models,

including recurrent neural networks and ensemble architectures, are used to capture complex dependencies between cyber events and physical processes (Al-Abassi et al., 2020; Alkahtani & Aldhyani, 2022).

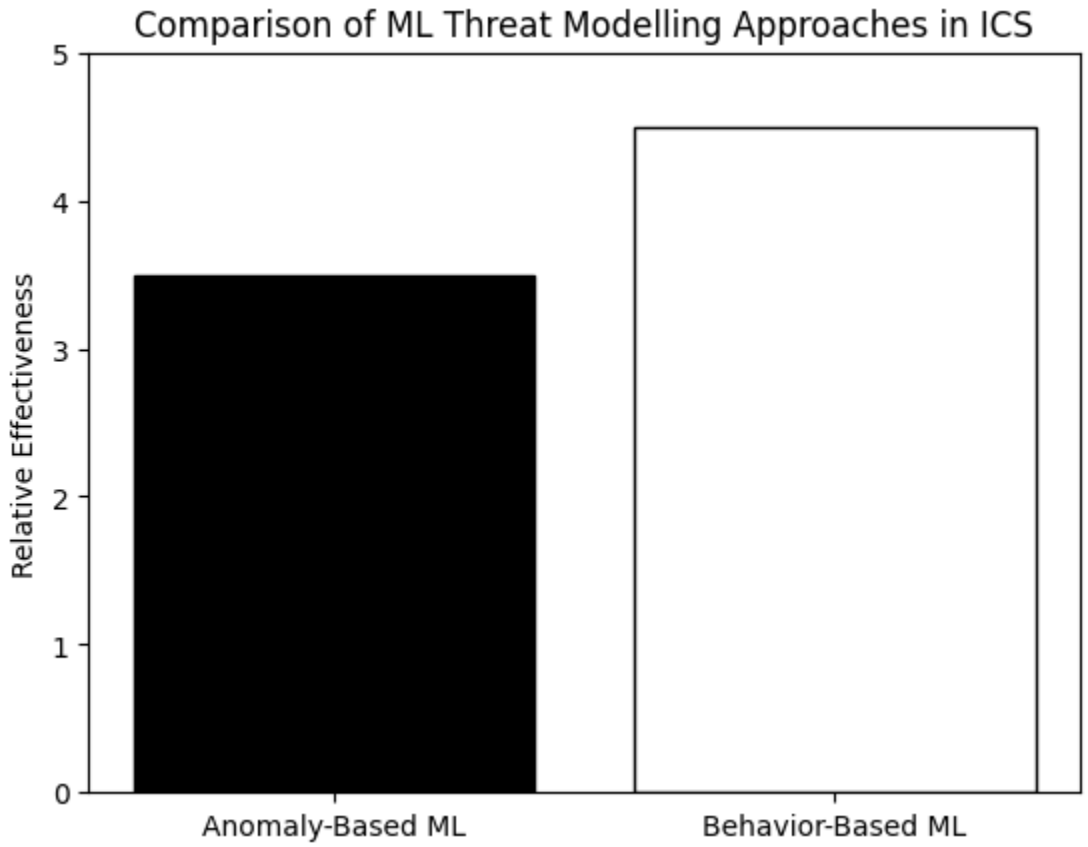

Fig 1: The bar chart compares Anomaly-Based ML and Behavior-Based ML threat modelling approaches in Industrial Control Systems (ICS).

3. Centralized and Edge-Based ML Architectures

To balance computational efficiency and real-time responsiveness, ML-based threat modelling architectures are often deployed using centralized, edge-based, or hybrid configurations. Centralized architectures aggregate ICS data into a security operations or analytics platform, where advanced ML models perform correlation, risk scoring, and threat prediction across multiple assets (Kure et al., 2022).

Edge-based architectures deploy lightweight ML models closer to ICS endpoints, enabling near real-time detection and localized response without disrupting industrial processes. Hybrid architectures combine both approaches, leveraging edge intelligence for immediate anomaly

detection and centralized systems for deeper analysis and long-term threat modelling (Zolanvari et al., 2019; Olowononi et al., 2020).

4. Integration with Risk Management and DevSecOps Frameworks

Modern ML-based threat modelling architectures increasingly integrate with cyber risk management and DevSecOps-oriented security frameworks. ML outputs are mapped to risk metrics, asset criticality scores, and threat likelihood models to support decision-making and incident prioritization (Kure et al., 2022). In cloud-connected or multi-cloud ICS environments, ML threat models are embedded within automated security pipelines to support continuous monitoring, policy enforcement, and data protection (OKAFOR et al.; Azmi et al., 2022; Syed et al., 2023).

Natural language processing and behavioral analytics techniques further enhance these architectures by enabling the analysis of unstructured logs, alerts, and operator reports, thereby improving contextual awareness and response accuracy (Uppuluri, 2019; Uppuluri, 2020).

5. Architectural Limitations and Security Considerations

Despite their advantages, ML-based threat modelling architectures face critical challenges related to model robustness, explainability, and adversarial manipulation. Attackers may exploit ML models through data poisoning or evasion techniques, undermining detection accuracy (Anthi et al., 2021). Consequently, resilient ML architectures incorporate ensemble learning, redundancy, and continuous model validation to maintain trustworthiness and operational safety (Al-Abassi et al., 2020; Olowononi et al., 2020).

Overall, ML-based threat modelling architectures provide a scalable and adaptive foundation for securing ICS-driven critical infrastructure. By combining layered deployment, behavioral intelligence, edge analytics, and risk-aware integration, these architectures significantly enhance the ability of industrial systems to detect, predict, and respond to sophisticated cyber threats while preserving operational continuity.

Threat Detection and Prediction Capabilities

Machine Learning (ML)–based cyber threat modelling significantly enhances the ability of Industrial Control Systems (ICS) in critical infrastructure to detect, classify, and predict cyber threats beyond the capacity of traditional signature- and rule-based mechanisms. By learning patterns from historical and real-time operational data, ML models enable adaptive, data-driven security monitoring that is well suited to the dynamic and heterogeneous nature of industrial environments (Bhamare et al., 2020).

Anomaly-Based Threat Detection

One of the most prominent capabilities of ML in ICS security is anomaly detection. Unsupervised and semi-supervised learning techniques, such as clustering, autoencoders, and statistical learning models, establish baselines of normal system behavior using process variables, sensor measurements, and network traffic. Deviations from these baselines can indicate stealthy attacks, zero-day exploits, or process manipulation attempts that do not match known signatures (Selim et al., 2021; Mokhtari et al., 2021). This capability is particularly valuable in ICS networks where attack datasets are scarce and system behavior is highly deterministic.

Intrusion and Attack Classification

Supervised ML and deep learning models are widely used to classify known attack types, including denial-of-service attacks, command injection, data integrity violations, and unauthorized control actions. Ensemble and deep neural network approaches have demonstrated improved detection accuracy and robustness when compared to single-model techniques, especially in complex ICS traffic patterns (Al-Abassi et al., 2020; Alkahtani & Aldhyani, 2022). These models support faster incident triage by associating detected anomalies with probable attack classes.

Behavioral and Context-Aware Detection

ML-based threat modelling extends beyond packet-level analysis by incorporating behavioral analytics. By correlating system logs, user actions, process states, and temporal patterns, ML models can detect lateral movement, privilege escalation, and insider threats that unfold gradually over time (MR et al., 2021; Zolanvari et al., 2019). Context-aware detection improves situational awareness and reduces false positives, which is critical for operational continuity in safety-sensitive environments.

Predictive Threat Modelling and Risk Forecasting

Beyond detection, ML enables predictive threat modelling by estimating the likelihood, impact, and propagation of cyber attacks. Predictive analytics and risk scoring models leverage historical incidents, vulnerability data, and system dependencies to forecast potential attack paths and high-risk assets (Kure et al., 2022). Such predictive capabilities support proactive defense strategies, including prioritized patching, dynamic access control, and preemptive isolation of vulnerable components.

Integration with Enterprise and Cloud-Based Analytics

Advanced ML-driven threat detection increasingly integrates with scalable data architectures, such as hybrid cloud data lakes and DevSecOps pipelines, enabling high-throughput ingestion and real-time analytics across distributed ICS environments (Okafor et al., n.d.; Azmi et al., 2022; Syed et

al., 2023). These integrations enhance cross-domain visibility while maintaining operational constraints.

Table 3. ML-Based Threat Detection and Prediction Capabilities in ICS

Capability Area	**ML Techniques Applied**	**Primary Data Sources**	**Security Outcome**	**Key References**
Anomaly Detection	Autoencoders, Clustering, Statistical ML	Sensor data, process variables	Detection of zero-day and stealth attacks	Selim et al. (2021); Mokhtari et al. (2021)
Intrusion Classification	SVM, Random Forest, Deep Neural Networks	Network traffic, control commands	Accurate identification of known attack types	Al-Abassi et al. (2020); Alkahtani & Aldhyani (2022)
Behavioral Analysis	Sequence models, Temporal ML	Logs, user actions, system states	Detection of insider threats and lateral movement	MR et al. (2021); Zolanvari et al. (2019)
Predictive Risk Modelling	Predictive analytics, Hybrid ML models	Historical incidents, vulnerability data	Forecasting attack likelihood and impact	Kure et al. (2022)
Scalable Threat Analytics	Distributed ML, Cloud-based pipelines	Multi-source ICS and OT data	Enterprise-wide situational awareness	Bhamare et al. (2020); Okafor et al. (n.d.)

Overall, ML-based threat detection and prediction capabilities transform ICS security from a reactive posture to a proactive and intelligence-driven approach. While these capabilities significantly improve resilience, their effectiveness depends on data quality, model robustness against adversarial manipulation, and alignment with operational safety requirements (Anthi et al., 2021; Olowononi et al., 2020).

Conclusion

Machine Learning (ML)-driven cyber threat modelling is a highly important innovation in the protection of Industrial Control Systems (ICS) that forms the basis of contemporary critical infrastructure. With the constantly evolving technology environment with more sophisticated, stealthy and persistent cyber threats, the old signature-based and rule-driven systems of security are no longer effective in providing reliability, safety and availability of the system. The analyzed methods show that ML tools, in particular, anomaly detection, ensemble learning, and deep learning, have a robust potential to detect abnormal behavior, recognize previously unseen attacks, and enhance situation awareness in ICS and Industrial Internet of Things (IIoT) settings (Alkahtani and Aldhyani, 2022; Selim et al., 2021; Al-Abassi et al., 2020).

The experience of other researchers indicates the efficiency and shortcomings of the ML-based intrusion detection in industrial environments. Although ML models demonstrated excellent detection precision under controlled settings, real-world applications are still limited by imbalance in data, the lack of labeled data, heterogeneity of systems and stringent real-time operation demands (MR et al., 2021; Bhamare et al., 2020). Besides, the fact that most deep learning models are opaque poses a challenge to explainability, trust, and compliance in safety-critical infrastructure, which supports the use of interpretable and resilient ML systems (Mokhtari et al., 2021; Olowononi et al., 2020).

The changing nature of threats also subjects ML-based defenses to adversarial manipulation, model poisoning, and evasion attacks, which negatively affect detection reliability in case they are not dealt with appropriately (Anthi et al., 2021). The incorporation of ML threat models into larger cybersecurity systems (e.g., risk prediction models, DevSecOps pipelines, scalable cloud or hybrid data platforms, etc.) has thus become critical to the long-term security and elasticity (Kure et al., 2022; Okafor et al., n.d.; Azmi et al., 2022). The scalability of monitoring critical infrastructure at large scale is also supported by the advances in data lakehouse architecture and high-throughput analytics (Syed et al., 2023).

In conclusion, ML-based cyber threat modelling offers a strategic and necessary pathway toward proactive, adaptive, and intelligence-driven security for ICS in critical infrastructure. However, its effectiveness depends on careful system integration, robust data governance, resilience against adversarial threats, and alignment with operational constraints. Future progress in this domain must emphasize explainable ML, secure model lifecycle management, and cross-domain collaboration to ensure that intelligent cyber defenses enhance—not compromise—the safety and reliability of critical infrastructure systems.

References

1. Alkahtani, H., & Aldhyani, T. H. (2022). Developing cybersecurity systems based on machine learning and deep learning algorithms for protecting food security systems: industrial control systems. *Electronics*, *11*(11), 1717.
2. Selim, G. E. I., Hemdan, E. E. D., Shehata, A. M., & El-Fishawy, N. A. (2021). Anomaly events classification and detection system in critical industrial internet of things infrastructure using machine learning algorithms. *Multimedia Tools and Applications*, *80*(8), 12619-12640.
3. MR, G. R., Ahmed, C. M., & Mathur, A. (2021). Machine learning for intrusion detection in industrial control systems: challenges and lessons from experimental evaluation. *Cybersecurity*, *4*(1), 27.
4. Al-Abassi, A., Karimipour, H., Dehghantanha, A., & Parizi, R. M. (2020). An ensemble deep learning-based cyber-attack detection in industrial control system. *Ieee Access*, *8*, 83965-83973.
5. Bhamare, D., Zolanvari, M., Erbad, A., Jain, R., Khan, K., & Meskin, N. (2020). Cybersecurity for industrial control systems: A survey. *computers & security*, *89*, 101677.
6. Kumar, S. (2007). *Patterns in the daily diary of the 41st president, George Bush* (Doctoral dissertation, Texas A&M University).
7. Uppuluri, V. (2019). The Role of Natural Language Processing (NLP) in Business Intelligence (BI) for Clinical Decision Support. *ISCSITR-INTERNATIONAL JOURNAL OF BUSINESS INTELLIGENCE (ISCSITR-IJBI)*, *1*(2), 1-21.
8. OKAFOR, C., VETHACHALAM, S., & AKINYEMI, A. A DevSecOps MODEL FOR SECURING MULTI-CLOUD ENVIRONMENTS WITH AUTOMATED DATA PROTECTION.OKAFOR, C., VETHACHALAM, S., & AKINYEMI, A. A DevSecOps MODEL FOR SECURING MULTI-CLOUD ENVIRONMENTS WITH AUTOMATED DATA PROTECTION.
9. Azmi, S. K., Vethachalam, S., & Karamchand, G. (2022). The Scalability Bottleneck in Legacy Public Financial Management Systems: A Case for Hybrid Cloud Data Lakes in Emerging Economies.
10. Syed, K. A., Vethachalam, S., Karamchand, G., & Gopi, A. (2023). *Implementing a Petabyte-Scale Data Lakehouse for India's Public Financial Management System: A High-Throughput Ingestion and Processing Framework*.
11. Barua, S. (2023). Hybrid Electro-membrane Reactors for Decentralized Removal of Forever Chemicals From Industrial Wastewater. *SAMRIDDHI: A Journal of Physical Sciences, Engineering and Technology*, *15*(04), 461-468.
12. Moetiara, E. (2022). From Compliance to Prediction: Integrating Real-Time Direct-Reading Instruments into Proactive Occupational Exposure Control Frameworks. *SRMS JOURNAL OF MEDICAL SCIENCE*, *7*(02), 110-117.
13. Gutpa, N. (2021). CROSS-SECTOR DATA INTEGRATION AND AI FOR PANDEMIC PREPAREDNESS AND CRISIS RESPONSE. *Google. Com*.

14. Nagraj, A. (2022). GitOps and Continuous Delivery in Financial Software: Best Practices for Efficient DevOps Pipelines. Frontiers in Computer Science and Artificial Intelligence, 1(1), 37-42.
15. KOTA, S. K. (2022). A Real-World Deployment of an Enterprise Conversational AI Platform for Demand Generation and Lead Generation Using Guided Workflows with a Rasa-Based Chatbot. Frontiers in Computer Science and Artificial Intelligence, 1(1), 24-30.
16. Singh, S. S. (2022). Accessibility and Universal Design in Transportation Infrastructure. *SAMRIDDHI: A Journal of Physical Sciences, Engineering and Technology*, *14*(04), 210-214.
17. Adepoju, S. (2021). Hybrid Retrieval Architectures: Integrating Vector Search into Production Systems.
18. Njenge, S. E. (2021). Mathematical Optimization of Fiscal Policy under Budget Constraints. *Multidisciplinary Innovations & Research Analysis*, *2*(4), 56-73.
19. Alampally, J. (2022). Designing High-Performance OLAP Cubes for Advanced Analytical Decision-Making. Frontiers in Computer Science and Artificial Intelligence, 1(1), 31-36.
20. Nagraj, A. Architectural Trade-offs: Microservices vs. Monoliths in Financial Systems. J Artif Intell Mach Learn & Data Sci 2019, 2(1), 3259-3265.
21. Vallemoni, R. K. (2021). Settlement, Fees, and Interchange: Data Models for Accurate Reconciliation and Exception Handling. AL-KINDI CENTER FOR RESEARCH AND DEVELOPMENT.
22. Vallemoni, R. K. (2022). Authorization-to-settlement at scale: A reference data architecture for ISO 8583/ISO 20022 coexistence. Journal of Computer Science and Technology Studies, 4(1), 88-98.
23. Vallemoni, R. K. (2022). Canonical payment data models for merchant acquiring: Merchants, terminals, transactions, fees, and chargebacks. International Journal of Computer Science and Engineering (ISCSITR-IJCSE), 3(1), 42-66.
24. ALAMPALLY, J. (2022). Prescriptive analytics on anonymized patient data using regression and distributed computing. Journal of Computer Science and Technology Studies, 4(1), 107-111.
25. Jagadeeswar, A. Optimizing Enterprise BI Platforms for High-Volume Healthcare Data Warehouses. J Artif Intell Mach Learn & Data Sci 2021, 4(2), 3270-3273.