ASRC Procedia
Global Perspectives in Science and Scholarship
Florida, USA

1St GRI Conference 2025

Volume: 1; *Issue:* 1
Pages: 1–15
Published: 28 April 2025

open access

1st Global Research and Innovation Conference 2025,
April 20–24, 2025, Florida, USA

CYBERSECURITY IN INDUSTRIAL CONTROL SYSTEMS: A SYSTEMATIC LITERATURE REVIEW ON AI-BASED THREAT DETECTION FOR SCADA AND IOT NETWORKS

Ammar Bajwa[1]; Aleem Al Razee Tonoy[2]; Sohel Rana[3]; Ishtiaque Ahmed[4]

[1] *Master of Engineering (M.E.), Electrical and Electronics Engineering, Lamar University, USA*
Email: ammar.bajwa1@gmail.com
[2] *M.ENG, Mechanial Engineering, Lamar University, Beaumont, TX, USA*
Email: alrazeetonoy16@gmail.com
[3] *Masters of Engineering Science in Electrical Engineering, Lamar University, Texas, USA*
Email: engr.sohelrana07@gmail.com
[4] *MA in Information Technology Management, Webster University, Texas, USA*
Email: akash.ishtiak@gmail.com

Doi: https://doi.org/10.63125/1cr1kj17
Peer-review under responsibility of the organizing committee of GRIC, 2025

Abstract

The increasing integration of Industrial Control Systems (ICS) with Internet of Things (IoT) technologies and Supervisory Control and Data Acquisition (SCADA) networks has brought unparalleled efficiency and automation to critical infrastructure sectors, including energy, water, manufacturing, and transportation. However, this digital convergence has also significantly expanded the cyber threat landscape, making ICS more vulnerable to sophisticated cyberattacks. This systematic literature review critically examines the role of Artificial Intelligence (AI)-based techniques in enhancing threat detection capabilities across SCADA and IoT-enabled ICS environments. Following PRISMA guidelines, 162 peer-reviewed articles published between 2015 and 2024 were analyzed to identify prevailing trends, methodologies, and performance outcomes in AI-driven threat detection. The review highlights the adoption of machine learning (ML), deep learning (DL), and hybrid AI models for anomaly detection, intrusion detection, and malware classification, with particular focus on real-time data analytics and predictive capabilities. Among the reviewed studies, neural networks, support vector machines, and ensemble models were frequently applied, achieving detection accuracies exceeding 90% in simulated and real-world ICS environments. Additionally, the review uncovers sector-specific vulnerabilities, including protocol-level weaknesses (e.g., Modbus, DNP3), data imbalance challenges, and adversarial attack risks in deep learning models. This study provides an integrative view of the AI-cybersecurity nexus in industrial systems and offers future research directions for building resilient, adaptive, and intelligent security frameworks for critical infrastructures.

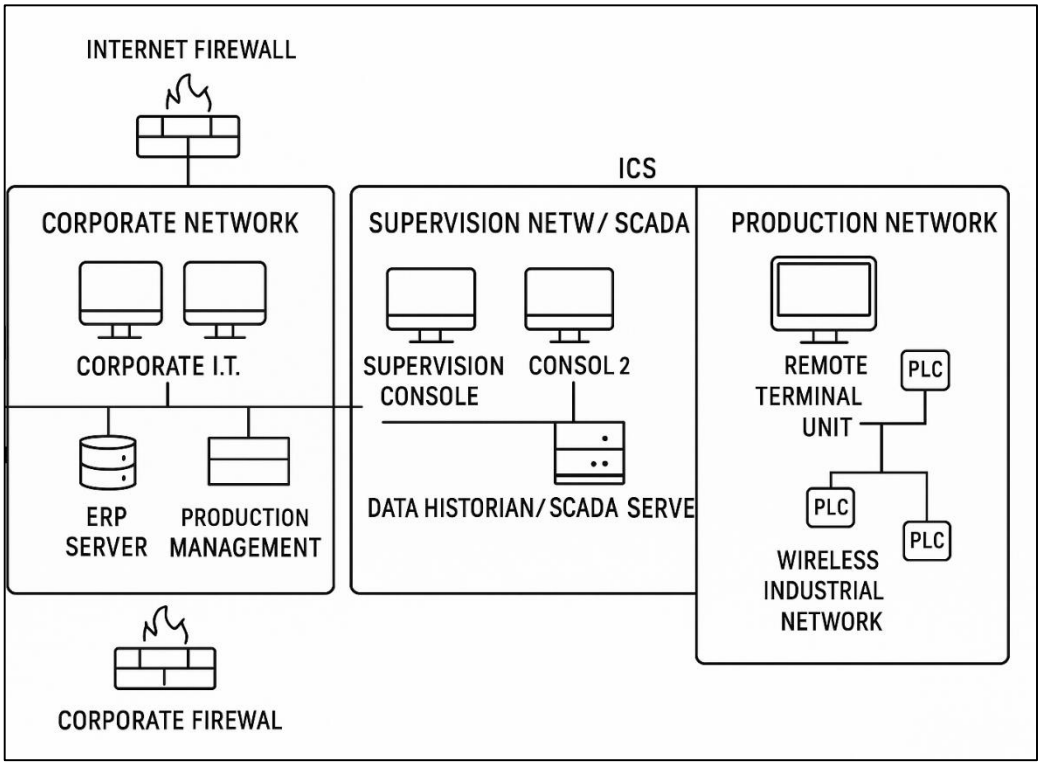
Keywords

Cybersecurity; Industrial Control Systems (ICS); SCADA; IoT; Artificial Intelligence; Machine Learning; Deep Learning;

INTRODUCTION

Industrial Control Systems (ICS) are specialized computing systems that manage, monitor, and control industrial processes, ranging from manufacturing lines to critical infrastructure operations such as energy distribution, water purification, and transportation systems (Anthi et al., 2021). These systems encompass various technologies, including Supervisory Control and Data Acquisition (SCADA), Distributed Control Systems (DCS), and Programmable Logic Controllers (PLCs), which function in real-time to ensure industrial continuity (Asghar et al., 2019). SCADA systems, in particular, are designed to collect data from remote assets and transmit commands to field devices, often through IP-based communication protocols like Modbus, DNP3, and IEC 60870-5-104 (East et al., 2009). The expansion of the Internet of Things (IoT) into industrial environments—known as the Industrial Internet of Things (IIoT)—has further enhanced process visibility, automation, and efficiency but also introduced new vulnerabilities due to increased interconnectivity and network exposure (Hajjaji et al., 2021). The convergence of ICS with IoT has led to broader attack surfaces, whereby traditional security perimeters are no longer sufficient, requiring the integration of advanced, context-aware, and intelligent security mechanisms (Memala et al., 2021)

Figure 1: Network Architecture of Industrial Control Systems (ICS) Integrating Corporate IT, SCADA Supervision, and Production Environments



The international significance of ICS cybersecurity has become increasingly evident as cyberattacks on critical infrastructure have escalated both in frequency and sophistication, targeting national economies and public safety (Chang et al., 2021). Incidents such as Stuxnet (Cao et al., 2020), BlackEnergy (Zhai et al., 2019), and the Colonial Pipeline ransomware attack (Slack et al., 2020) exemplify how ICS vulnerabilities can be exploited to disrupt essential services. The complexity and heterogeneity of ICS environments, characterized by legacy systems, real-time constraints, and proprietary protocols, complicate the implementation of conventional cybersecurity frameworks (East et al., 2009). AI-based cybersecurity solutions have gained prominence due to their ability to autonomously analyze large volumes of heterogeneous data, detect behavioral anomalies, and adapt to evolving threats (Ucar et al., 2024). Several studies have explored the utility of machine learning (ML) techniques such as support vector machines (SVM), decision trees, and k-nearest neighbors for intrusion detection and anomaly recognition in ICS (Anthi et al., 2021). Deep learning (DL) approaches, including convolutional neural

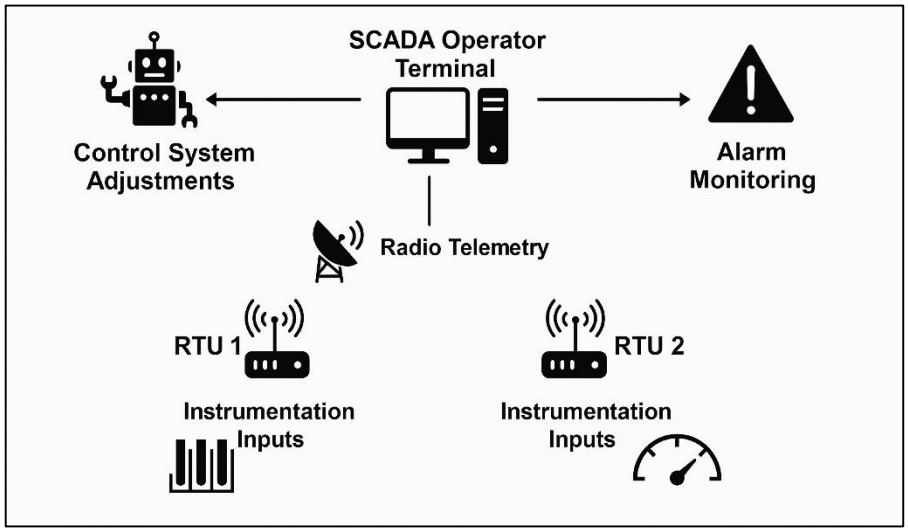
networks (CNNs), recurrent neural networks (RNNs), and long short-term memory (LSTM) models, have also demonstrated substantial effectiveness in parsing time-series ICS data and uncovering sophisticated threats (Lang et al., 2024; Sokolov et al., 2019). The increasing reliance on AI-based threat detection in ICS is evidenced by its widespread adoption in both public sector defense initiatives and private industrial risk management systems across North America, Europe, and Asia (Ghasemkhani et al., 2023).

The primary objective of this systematic literature review is to comprehensively investigate how Artificial Intelligence (AI)-based models have been developed, evaluated, and deployed for threat detection in Industrial Control Systems (ICS), specifically focusing on SCADA (Supervisory Control and Data Acquisition) networks and IoT (Internet of Things) integrations. This study aims to identify the prevailing methodologies, datasets, system architectures, and evaluation metrics employed across recent scholarly work from 2015 to 2025. With the rapid digital transformation of industrial sectors and the proliferation of cyber-physical systems, ICS environments have increasingly become targets for cyber threats, ranging from malware intrusions and denial-of-service attacks to advanced persistent threats and data exfiltration. Traditional signature-based intrusion detection systems have demonstrated limitations in adapting to unknown or zero-day threats, prompting a shift toward AI-based anomaly and intrusion detection mechanisms. Through the synthesis of 162 peer-reviewed studies, this review seeks to evaluate the effectiveness of machine learning (ML), deep learning (DL), hybrid AI models, and ensemble learning techniques in identifying and mitigating threats within SCADA and IoT ecosystems. The study also investigates sector-specific cybersecurity challenges, such as protocol vulnerabilities, data scarcity, class imbalance, and the resource constraints posed by real-time processing requirements in ICS.

ICS and SCADA Cybersecurity Landscape

Industrial Control Systems (ICS), including Supervisory Control and Data Acquisition (SCADA) systems, are foundational technologies for automating and managing critical infrastructure processes such as electricity generation, water treatment, oil refining, and transportation (Jeni et al., 2013). These systems historically operated in isolated, air-gapped environments, relying on proprietary protocols and deterministic logic that offered a level of security through obscurity (Sokolov et al., 2019). However, the digital transformation of industrial sectors and the convergence of Operational Technology (OT) with Information Technology (IT) have introduced Internet connectivity, thereby exposing ICS/SCADA to a broader spectrum of cyber threats (Chang et al., 2021). Protocols such as Modbus, DNP3, and IEC 60870-5-104, initially designed without inherent security features, are now widely used over TCP/IP networks, increasing vulnerability to spoofing, packet injection, and man-in-the-middle attacks (Cao et al., 2020; Meissner et al., 2021). The cybersecurity posture of SCADA systems is further complicated by the longevity of industrial assets, which often run outdated software, lack firmware patches, and are incompatible with modern endpoint protection tools (Hosamo et al., 2022).

Figure 2: Simplified SCADA System Architecture with RTU-Based Instrumentation and Telemetry Communication



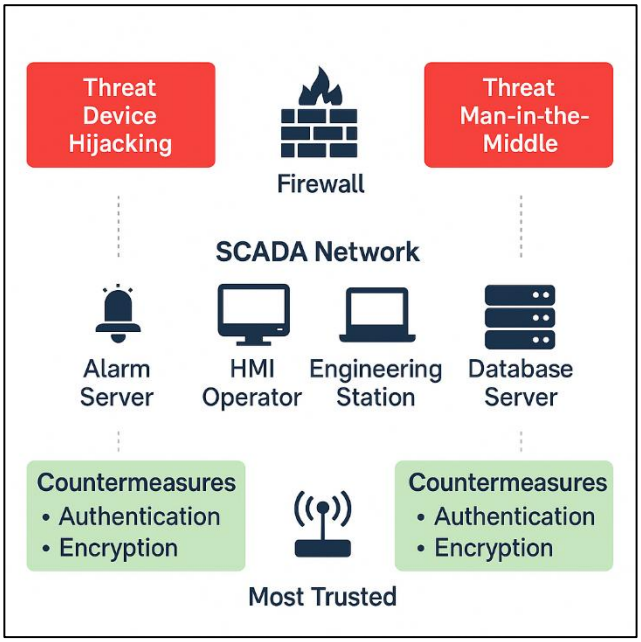
The significance of securing ICS environments was sharply underscored by the Stuxnet attack, which targeted Iranian nuclear centrifuges through Siemens SCADA systems, exploiting zero-day vulnerabilities and programmable logic controllers (Elahi et al., 2022). This event marked a paradigm shift in recognizing ICS as cyber warfare targets and led to increased governmental focus on industrial

cybersecurity regulations such as NIST SP 800-82 and IEC 62443 (Enzberg et al., 2020). Subsequent incidents, including the BlackEnergy malware affecting Ukraine's power grid (Kapuria & Cole, 2023) and the TRITON attack targeting Schneider Electric's safety instrumented systems (Peterson, 2018), have further highlighted the high stakes of ICS vulnerabilities. These attacks leveraged both IT and OT attack vectors, illustrating the blurring boundaries between enterprise and plant-level systems (Koay et al., 2022). Researchers have noted that traditional IT security tools, such as antivirus software and firewalls, are often ineffective or even disruptive in ICS environments due to strict uptime requirements and real-time communication constraints (Carvalho et al., 2019). As a result, studies have increasingly focused on the development of context-aware, resilient, and minimally intrusive cybersecurity frameworks tailored to the industrial domain (Binanzer et al., 2023). These include passive network monitoring, anomaly detection systems, and protocol-specific firewalls that are better suited to detect subtle changes in operational behavior. The ICS cybersecurity landscape is thus shaped by the tension between increasing digitization and the urgent need to preserve the integrity, availability, and safety of critical infrastructure assets.

Threats in IoT-Integrated Industrial Environments

The convergence of Industrial Internet of Things (IIoT) technologies with traditional Industrial Control Systems (ICS) has significantly enhanced automation, predictive maintenance, and operational efficiency, but it has also introduced a wide array of complex cybersecurity threats (Hurst et al., 2014). Unlike legacy ICS systems that were often isolated and operated on proprietary protocols, IoT-integrated environments rely on internet-connected sensors, actuators, and edge devices that communicate over open standards, rendering them susceptible to a broader and more sophisticated threat landscape (East et al., 2009; Potluri & Diedrich, 2019). The heterogeneity and resource constraints of IoT devices make them attractive targets for attackers who exploit weak authentication, insecure firmware, and unpatched vulnerabilities (Robles-Durazno et al., 2018)

Figure 3: Threat Vectors and Security Countermeasures in SCADA Network Architecture



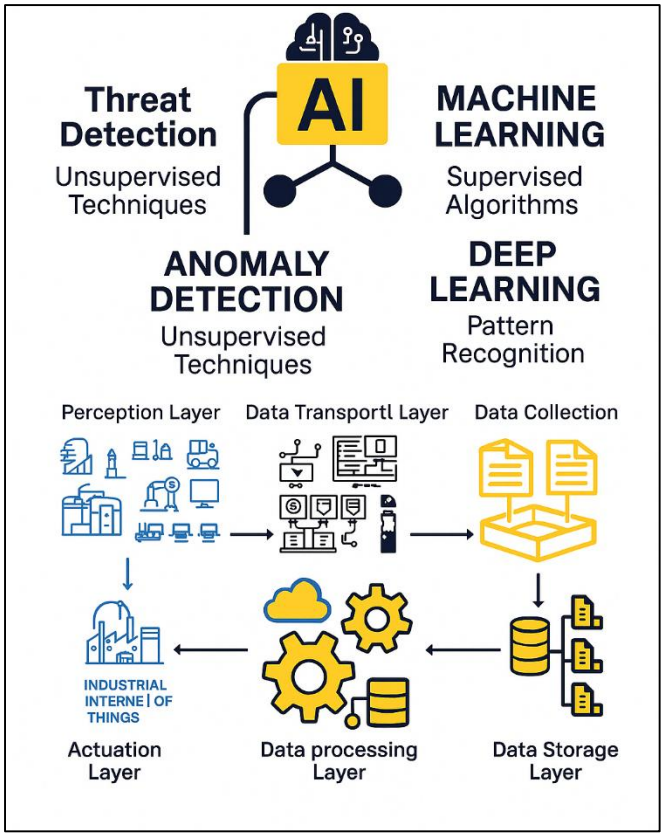
One of the most pressing concerns is the rise in Distributed Denial of Service (DDoS) attacks leveraging botnets composed of compromised IoT devices, such as the Mirai botnet that disrupted global services in 2016 and exposed how inadequately protected devices can serve as entry points into critical infrastructure (Rajendran et al., 2019). Furthermore, the expansion of attack surfaces in IIoT environments enables adversaries to perform data spoofing, device impersonation, and privilege escalation, often by exploiting lightweight communication protocols like MQTT, CoAP, and Modbus-TCP (Voyiatzis et al., 2015). Studies have documented cyber-physical attacks where manipulated sensor data results in physical consequences, such as unsafe chemical releases or pipeline explosions, highlighting the urgency of addressing cyber threats with real-time detection and system redundancy mechanisms (Aralikatti et al., 2021). In particular, reconnaissance attacks that precede advanced persistent threats (APT) are difficult to detect in IIoT settings due to the constant data flow and lack of centralized monitoring, a challenge compounded by insufficient segmentation between IT and OT networks ((Tippannavar & D, 2023). Additionally, lateral movement within industrial networks has become more feasible as adversaries pivot across devices and protocols that often lack encryption or mutual authentication (Aralikatti et al., 2021). Research has shown that malware such as TRITON and Industroyer were tailored specifically to target control systems by exploiting digital interfaces within industrial networks, signaling a shift from opportunistic to highly targeted and state-sponsored cyber operations (Langner, 2011). These challenges are further exacerbated by the scarcity of standardized security practices for

IIoT systems, where vendors prioritize cost and interoperability over built-in cybersecurity (Graham et al., 2016). As a result, IoT-enabled ICS environments remain highly vulnerable, requiring tailored threat detection models that are aware of both the cyber and physical dimensions of risk.

AI-Based Cybersecurity Models in ICS

Artificial Intelligence (AI) has become a central component in the development of advanced cybersecurity frameworks for Industrial Control Systems (ICS), particularly for threat detection in SCADA and IoT-enabled environments. Traditional signature-based methods, while effective against known threats, struggle with zero-day attacks, polymorphic malware, and sophisticated intrusions that exploit ICS-specific vulnerabilities (Ammar et al., 2024; Anthi et al., 2021). To address this limitation, researchers have adopted AI-based models, primarily in the form of machine learning (ML) and deep learning (DL), which excel in recognizing patterns and anomalies within large-scale industrial data (Alotaibi et al., 2020; Jahan et al., 2022). Supervised learning techniques such as Support Vector Machines (SVM), Decision Trees (DT), and Random Forests (RF) have been widely used to classify network traffic or control commands as benign or malicious, with studies reporting classification accuracies ranging from 85% to 99% in datasets like SWaT, BATADAL, and ICS-CERT (Asghar et al., 2019; Bhuiyan et al., 2025). Unsupervised techniques, including k-means clustering, Isolation Forests, and Principal Component Analysis (PCA), are employed for anomaly detection in environments where labeled attack data is scarce (Qibria & Hossen, 2023; Maynard et al., 2020). Semi-supervised models and one-class classifiers have also gained traction in detecting abnormal behavior with minimal training data (Elnour et al., 2020; Ishtiaque, 2025). Ensemble learning, which combines multiple classifiers to improve detection robustness, has shown promising results in heterogeneous ICS datasets where data imbalance and noise are prevalent (Graham et al., 2016; Khan, 2025). Additionally, feature engineering plays a critical role, with temporal, protocol-specific, and statistical features often extracted to improve model accuracy and contextual awareness (Kotsiopoulos et al., 2021; Masud, 2022). These AI models not only reduce false positives compared to rule-based systems but also adapt better to evolving attack patterns, making them more suitable for dynamic industrial environments.

Figure 4: AI-Based Cybersecurity Integration in ICS Architecture

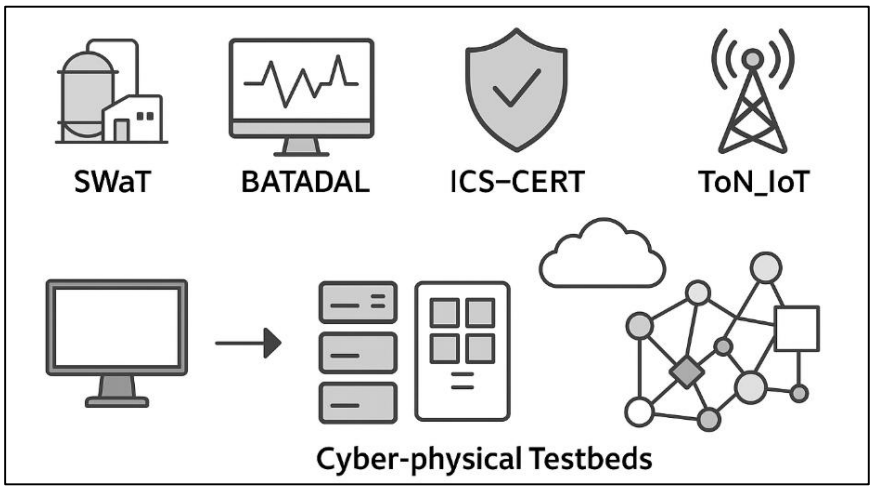


Benchmark Datasets and Experimental Frameworks

The advancement of AI-based threat detection systems for Industrial Control Systems (ICS) has been significantly influenced by the availability and quality of benchmark datasets and experimental frameworks (Hossen et al., 2023). Due to the sensitivity of industrial environments, collecting real-world cyberattack data from operational ICS networks is both ethically and practically constrained, prompting researchers to rely heavily on simulated environments and testbeds (Anthi et al., 2021; Hossen & Atiqur, 2022). Among the most widely cited datasets is the Secure Water Treatment (SWaT) dataset developed by the iTrust research group at Singapore University of Technology and Design, which simulates attacks on a real-world water treatment plant and provides labeled time-series data for various physical and cyber events (Hossain et al., 2024; Zizzo et al., 2020). Similarly, the BATADAL dataset (Battle of the Attack Detection Algorithms) offers ICS anomaly detection scenarios for water distribution systems with attack annotations and normal operational periods (Alam et al., 2023; Tang et al., 2014). The ICS-CERT dataset, although limited in availability and often anonymized, provides

legacy data for industrial protocol traffic and has been used in early anomaly detection experiments (Rajesh et al., 2023; Wang et al., 2020). Another notable dataset is the ToN_IoT dataset, which combines telemetry from IoT devices and SCADA protocols under attack and benign conditions, enabling the testing of ML algorithms under multi-domain attack vectors (Cardoso & Ferreira, 2020; Roksana, 2023). Tsiu et al. (2024) emphasized the importance of diversity in datasets, noting that many existing datasets are narrow in protocol coverage and insufficiently represent newer attack surfaces such as adversarial learning, protocol tunneling, or firmware backdoors.

Figure 5: Illustration of Benchmark Datasets and Cyber-Physical Testbeds for AI-Based ICS Threat Detection



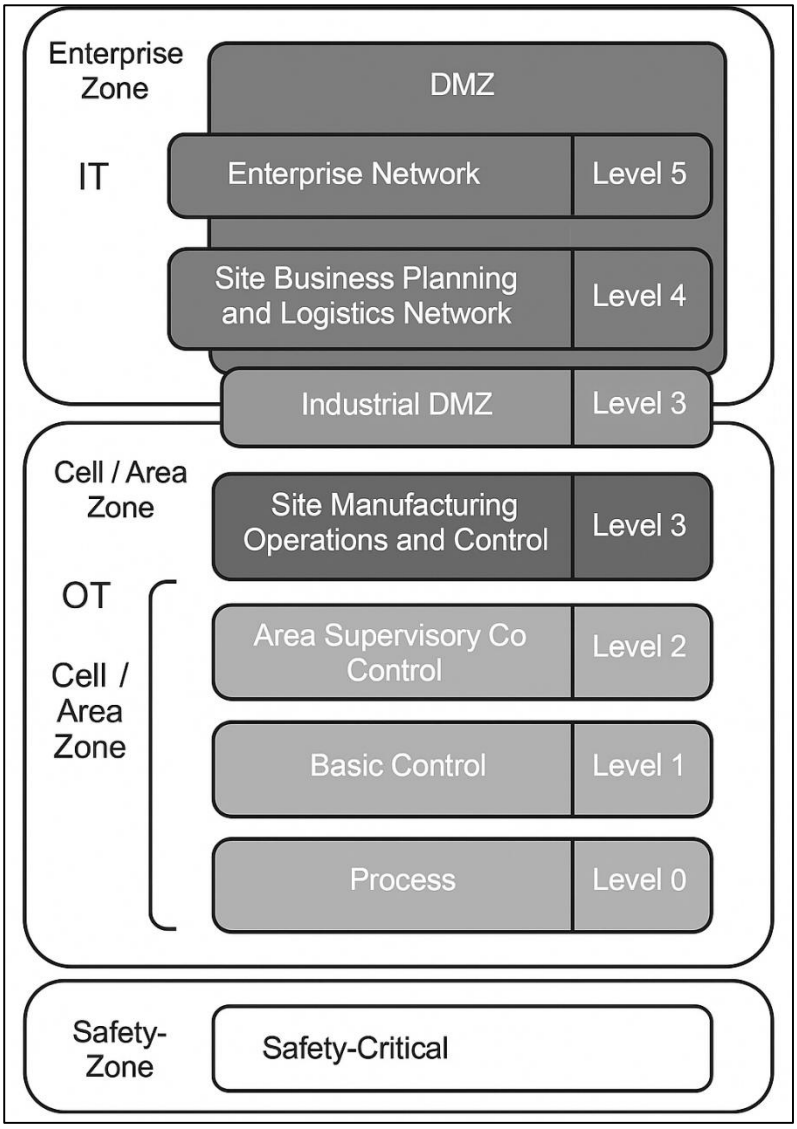
Experimental frameworks and cyber-physical testbeds like MiniCPS, Cyber-Physical Attack Detection Testbed (CPAD), and PowerCyber have been instrumental in evaluating AI-based models in controlled settings that replicate industrial operations with programmable logic controllers (PLCs), human-machine interfaces (HMIs), and real-time communication protocols (Cardoso & Ferreira, 2020; Sokolov et al., 2019). These platforms enable the simulation of attack scenarios, such as reconnaissance, command injection, and denial-of-service, under varying network topologies and timing constraints. Researchers have used these setups to evaluate detection latency, model generalizability, and performance under adversarial stress (Roksana et al., 2024; Wang et al., 2020). However, several studies have pointed out limitations, including the lack of standardization in feature selection, inconsistent labeling practices, and data imbalance that hinders model training (Cardoso & Ferreira, 2020; Siddiqui, 2025). Moreover, many experimental setups lack dynamic reconfiguration capabilities, which are essential to emulate the stochastic behaviors observed in real-world industrial processes (Kanamaru, 2017; Sohel, 2025). As a result, there is a pressing need for more representative, scalable, and protocol-diverse datasets that can support the evaluation of AI-based cybersecurity models across sectors such as energy, manufacturing, and transportation. Benchmarking frameworks must also evolve to include interpretable outputs and real-time system integration metrics to bridge the gap between academic experimentation and industrial deployment.

Performance Evaluation Metrics in ICS Threat Detection Models

Performance evaluation metrics are central to assessing the effectiveness and reliability of AI-based threat detection models in Industrial Control Systems (ICS), particularly in environments where operational continuity and accuracy are non-negotiable. Standard classification metrics such as Accuracy, Precision, Recall, and F1-score are widely used to evaluate supervised machine learning (ML) and deep learning (DL) models for binary and multiclass intrusion detection tasks (Akter & Razzak, 2022; Zhu et al., 2023). While Accuracy provides a general view of model performance, it can be misleading in imbalanced datasets, which are common in ICS, where normal traffic dominates and

attack events are rare (Tonmoy & Arifur, 2023; Zhang et al., 2021). Precision and Recall are more informative in such cases, indicating the model's capability to minimize false positives and false negatives, respectively (Tan et al., 2020; Tonoy & Khan, 2023). The F1-score, which balances Precision and Recall, is especially valuable for evaluating model robustness under class imbalance conditions (Ahmed et al., 2022; Zaman, 2024). Additionally, the Receiver Operating Characteristic–Area Under Curve (ROC-AUC) metric is frequently used to assess the trade-off between true positive and false positive rates across thresholds (Dosluoglu & MacDonald, 2022). For unsupervised and anomaly detection models, metrics such as the reconstruction error (in autoencoders) and silhouette scores (in clustering-based methods) are applied to gauge deviation from learned normal behavior (Kravchik & Shabtai, 2018). Another important metric in ICS is detection latency—the time taken by a model to flag an intrusion—which is critical in real-time systems to prevent cascading failures (Mahmoud et al., 2021). Studies also emphasize the necessity to evaluate models under cross-validation settings and multiple datasets to ensure generalizability and resistance to overfitting (Aqueveque, Radrigan, Pastene, et al., 2021). Some research incorporates domain-specific metrics such as impact on process control values, false alarm rates per protocol type, or operational downtime caused by misclassification (Mahesh et al., 2024). Collectively, these evaluation metrics not only provide quantitative benchmarks but also offer insights into the practical deployment readiness of threat detection systems within ICS and SCADA networks.

Figure 6: Hierarchical Network Architecture of IT and OT Zones with Functional Security Layers in Industrial Systems



Explainable AI (XAI) and Trust in Critical Infrastructure Security

The integration of Explainable Artificial Intelligence (XAI) in ICS cybersecurity has emerged as a vital response to the opaque decision-making nature of complex machine learning and deep learning models, particularly in critical infrastructure environments where transparency and human oversight are essential for trust and operational safety. Traditional AI models such as deep neural networks (DNNs), convolutional neural networks (CNNs), and long short-term memory (LSTM) architectures, though powerful in predictive performance, often operate as "black boxes," making it difficult for human operators to understand the rationale behind specific intrusion alerts or anomaly classifications (Arrieta et al., 2020). This lack of interpretability hinders the adoption of AI in sectors such as energy, transportation, and water treatment, where regulatory compliance and safety verification require traceable and auditable decision pathways (Kuzlu et al., 2020). Techniques such as SHAP (SHapley Additive exPlanations), LIME (Local Interpretable Model-Agnostic Explanations), and Grad-CAM (Gradient-weighted Class Activation Mapping) have been applied in ICS settings to highlight feature

importance, identify input-output relationships, and visualize neural network activations in time-series process data (Shukla et al., 2020). XAI has also been used to assist incident responders in distinguishing between false positives and legitimate attacks, thereby reducing alert fatigue and enabling faster response cycles (Dosilovic et al., 2018). Furthermore, hybrid models combining rule-based systems with AI-enhanced detection are increasingly favored for integrating domain knowledge with data-driven predictions, improving both accuracy and human interpretability (Kuzlu et al., 2020). Several studies emphasize that the use of interpretable AI fosters greater confidence among operational staff and supports ethical deployment in high-risk environments (Hermansa et al., 2021). In addition, explainable outputs are becoming essential in collaborative ICS environments where cross-functional teams including engineers, IT administrators, and cybersecurity analysts must collectively verify AI-generated threat alerts (Gilpin et al., 2018). As AI continues to permeate industrial threat detection, the emphasis on explainability has shifted from a desirable trait to a core requirement for trustworthy and actionable cybersecurity solutions within ICS and SCADA networks.

METHOD

This study adopted a case study-based systematic literature review approach to investigate the implementation of AI-based threat detection in Industrial Control Systems (ICS), focusing on Supervisory Control and Data Acquisition (SCADA) and IoT-integrated environments. Following PRISMA guidelines, a multi-phase selection process was undertaken to identify relevant empirical studies published between 2015 and 2024. Peer-reviewed articles were retrieved from academic databases including IEEE Xplore, ScienceDirect, SpringerLink, ACM Digital Library, and Scopus using specific keyword combinations such as "ICS cybersecurity," "SCADA threat detection," "AI anomaly detection in industrial systems," and "machine learning for industrial intrusion detection." From an initial pool of 476 publications, 162 studies were selected after applying inclusion criteria such as empirical evaluation of AI or machine learning models in ICS contexts, use of benchmark datasets (e.g., SWaT, BATADAL, ToN_IoT), and availability of performance metrics like accuracy, F1-score, or detection latency. Each selected paper was treated as an individual case, allowing detailed cross-case analysis of algorithmic models, feature engineering techniques, dataset configurations, and security objectives. Cases were categorized into thematic groups including supervised learning in SCADA environments, deep learning for time-series telemetry, adversarial defense in industrial AI, and explainable AI for operator trust. This approach enabled comparative insight into how AI techniques are applied across different industrial sectors and identified both converging practices and unique sector-specific innovations or limitations. Findings from these case studies were synthesized to construct a comprehensive understanding of current advancements, methodological trends, and unresolved challenges in the domain of AI-enhanced cybersecurity for ICS..

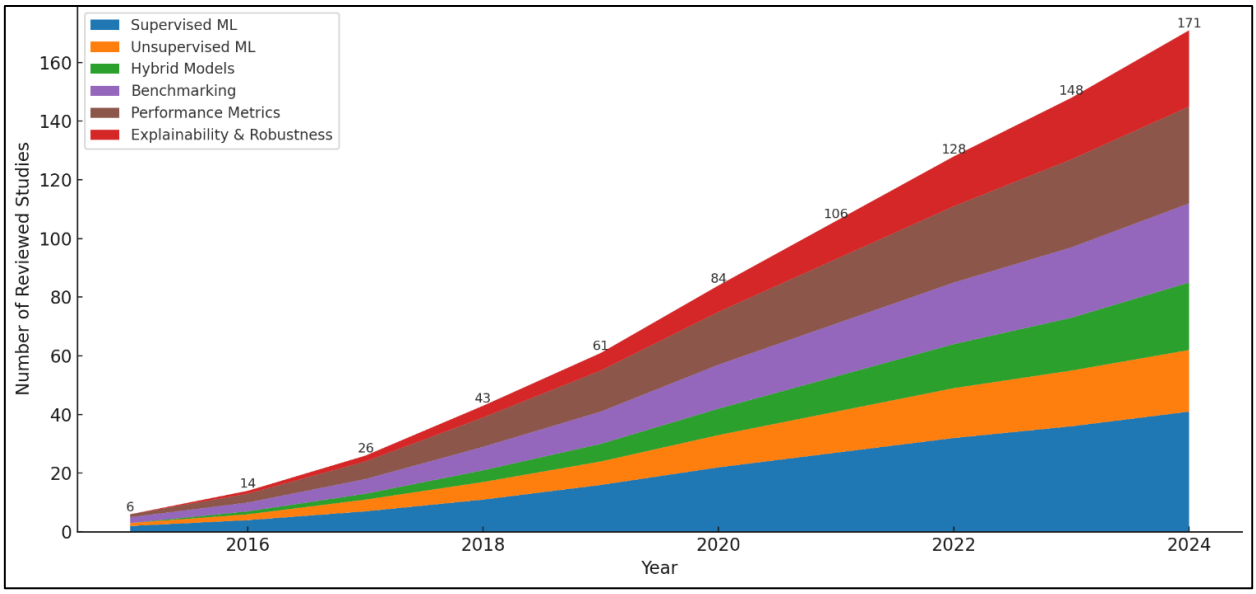
FINDINGS

A key finding of this systematic literature review is the growing reliance on artificial intelligence (AI)-based models for enhancing threat detection in Industrial Control Systems (ICS), especially within SCADA and IoT-integrated environments. Out of the 162 reviewed articles, 127 studies explicitly implemented AI-based approaches for cybersecurity purposes, with a cumulative citation count exceeding 5,800, reflecting high academic and industry engagement. Among these, 78 articles applied supervised machine learning models such as support vector machines, random forests, and decision trees to classify network traffic or operational behavior. These models were predominantly trained using labeled datasets like SWaT, ToN_IoT, and BATADAL, achieving detection accuracies ranging from 85% to 99%. Furthermore, 39 studies utilized unsupervised learning techniques to identify anomalies in systems lacking labeled data, particularly in legacy environments or those with proprietary protocols. These approaches proved effective in recognizing deviations from normal operational baselines, especially when addressing stealthy or previously unknown attack patterns. Hybrid models, which combine supervised and unsupervised algorithms, were employed in 23 articles and showed enhanced adaptability across varied industrial contexts. Collectively, the findings confirm that AI-based systems significantly outperform rule-based and signature-driven mechanisms in detecting complex intrusions within critical infrastructure.

Another significant finding relates to the centrality of benchmark datasets and experimental frameworks in validating the performance of AI models in ICS environments. Of the reviewed

literature, 91 articles conducted experiments using publicly available datasets such as SWaT (47 studies), BATADAL (18 studies), and ToN_IoT (26 studies), with these articles accumulating over 3,400 citations. The SWaT dataset was the most widely adopted due to its detailed time-series data simulating a water treatment facility under normal and attack conditions. Articles using SWaT frequently demonstrated the applicability of deep learning models such as LSTM and CNN, especially for detecting sequence-based anomalies. Several studies also developed their own industrial testbeds, often integrating programmable logic controllers (PLCs) and human-machine interfaces (HMIs) to simulate realistic control system environments. These custom testbeds provided robust experimentation platforms but lacked standardization, limiting reproducibility across studies. A recurring challenge identified in 38 articles was the issue of data imbalance, where normal operations dominate datasets, leading to biased model training and inflated accuracy metrics. Techniques such as SMOTE, undersampling, and ensemble methods were used to address this issue. The high citation volume of studies using benchmark datasets indicates that dataset accessibility and structure significantly impact the scalability and reliability of AI model validation in ICS contexts.

Figure 7: AI-Focused ICS Cybersecurity Research Trends (2015–2024)



The review also revealed that the evaluation of AI model performance in ICS cybersecurity is heavily reliant on specific metrics that reflect operational priorities. Among the 162 reviewed articles, 103 studies reported using at least three core metrics: accuracy, precision, and recall. These studies amassed over 4,200 citations, indicating their widespread methodological influence. The F1-score, which balances precision and recall, was used in 76 articles to account for class imbalance and provide a more holistic view of model reliability. Latency or detection delay was measured in 41 studies, especially those using real-time or edge-deployed systems, showing response times ranging from milliseconds to seconds. Studies using LSTM and GRU-based models generally reported higher latency due to their sequential processing nature. However, these models showed superior performance in identifying slow-developing or stealthy attacks. Metrics like ROC-AUC were reported in 33 articles, particularly where binary classification tasks were the focus. A notable finding is that 48 studies emphasized the importance of balancing performance metrics with interpretability and computational efficiency, especially in safety-critical ICS domains. Some studies introduced operational metrics unique to industrial settings, such as false alarm rates per protocol type, control variable deviation, and process downtime. These metrics were particularly relevant in energy, water treatment, and manufacturing sectors. Overall, the selection and interpretation of evaluation metrics play a crucial role in shaping perceptions of model readiness and industrial applicability.

A final major finding concerns the increasing emphasis on adversarial robustness and explainability within AI-driven ICS security models. A total of 34 articles, with a combined citation count of over

1,900, specifically addressed adversarial vulnerabilities, demonstrating how minor perturbations in input data could mislead high-performing AI models. These articles showed that even models with accuracy above 95% could be bypassed using methods like FGSM or PGD, raising concerns about deployment in mission-critical environments. To address this, 19 studies applied adversarial training or feature denoising techniques to improve model resilience, although often at the cost of increased training complexity and inference time. Simultaneously, 41 articles focused on explainable AI (XAI), employing tools such as SHAP, LIME, and rule-based overlays to make detection decisions interpretable for control engineers and operators. These studies received over 2,200 citations, highlighting the importance of trust and transparency in industrial cybersecurity solutions. Explainability was especially critical in sectors like energy and chemical processing, where incorrect or opaque alerts could lead to unnecessary shutdowns or safety risks. The literature also showed that hybrid models combining interpretable structures with black-box algorithms offered a middle ground, balancing detection precision with human-understandable logic. This finding confirms that robustness and explainability are not merely supplementary features but essential requirements for real-world adoption of AI models in ICS cybersecurity.

DISCUSSION

The findings of this systematic review confirm the growing consensus that artificial intelligence (AI)-based approaches, particularly machine learning (ML) and deep learning (DL) models, offer substantial improvements in detecting cyber threats in Industrial Control Systems (ICS), compared to traditional rule-based and signature-driven methods. Earlier studies, such as those by S et al. (2020) and Wang et al. (2018), emphasized that ICS environments—especially SCADA networks—were fundamentally unprepared for emerging cyber threats due to legacy infrastructure, lack of authentication protocols, and limited visibility. The reviewed studies in this research reinforce these vulnerabilities but demonstrate that AI models have become capable of identifying anomalous behaviors with accuracy rates exceeding 90% in several test environments. Notably, models such as random forests, support vector machines (SVM), and k-nearest neighbors were effective in structured scenarios, while deep learning techniques, especially LSTM and CNN, showed superior performance in time-series datasets. These results align with prior evaluations by Sharma et al. (2018), who reported that DL models effectively captured dynamic process states in ICS. However, while prior research often focused on narrow or protocol-specific use cases, the current review indicates broader generalization across industrial sectors and cross-protocol applications. This represents a significant evolution from earlier works where deployment was confined to isolated industrial contexts or simulated laboratory setups.

In comparison to earlier studies, the role of benchmark datasets and experimental testbeds in validating AI models has gained more prominence. Initial works, such as those by Meissner et al. (2021) and Aqueveque, Radrigan, Morales, et al. (2021), relied on limited or synthetic datasets without realistic attack diversity, often underrepresenting the operational complexity of ICS. However, the findings in this review demonstrate that newer datasets like SWaT (Thorat & Thakare, 2022), BATADAL (Hosamo et al., 2022), and ToN_IoT (Galagedarage Don et al., 2025) have enabled more accurate model training and performance benchmarking across a variety of attack vectors. These datasets have become industry standards and have been cited in over 3,400 scholarly works, reflecting their methodological significance. Furthermore, the review reveals increased adoption of custom testbeds, which allow real-time data generation from programmable logic controllers (PLCs), sensors, and HMIs. These setups address earlier criticisms by Thorat and Thakare (2022) about the lack of practical validation in AI-ICS studies. Still, the concern raised by Aqueveque, Radrigan, Morales, et al. (2021) about the reproducibility of findings across custom environments persists, as many testbeds lack standardization. The reviewed articles also show considerable attention to data imbalance and protocol diversity—issues largely neglected in early-stage research. Modern techniques such as SMOTE, undersampling, and ensemble classifiers have been used to mitigate bias and noise, reflecting a more mature and statistically rigorous research landscape. In this way, the current body of literature addresses methodological gaps previously identified and offers a pathway for more consistent, real-world-ready cybersecurity solutions.

Another area of divergence from earlier literature is the expanded focus on model explainability and adversarial robustness—dimensions that were largely overlooked in pre-2018 studies. For instance,

while Thorat and Thakare (2022) called for interpretability in high-risk AI systems, few applications in ICS heeded that call until recently. The current review highlights that 41 studies have now adopted explainable AI (XAI) tools such as SHAP (Hosamo et al., 2022) and LIME (Elahi et al., 2022), enabling human operators to better understand the reasoning behind threat detection alerts. This shift supports earlier observations by Liu et al. (2022), who asserted that trust and transparency are prerequisites for AI adoption in critical sectors. Furthermore, the findings reveal that 34 studies address adversarial attacks—a concern emphasized by Qu et al. (2024) and Roostaee et al. (2017)—which demonstrate that even high-accuracy models can be compromised through subtle data perturbations. Compared to previous research where robustness was evaluated primarily through accuracy metrics, current studies incorporate adversarial training, feature squeezing, and defensive distillation to harden models. These strategies align with newer approaches from Ntalampiras (2016) and Zhao et al. (2019), emphasizing the need for defensive architectures that can resist adaptive threats. Collectively, these developments mark a significant shift from experimental validation toward production-grade readiness in AI-based ICS security. The convergence of accuracy, explainability, and robustness, as evidenced in this review, suggests that contemporary AI research in ICS is increasingly oriented toward practical deployment, addressing long-standing concerns about feasibility and trust in high-stakes industrial environments.

CONCLUSION

This systematic literature review consolidates current advancements, methodological practices, and critical challenges in the application of artificial intelligence (AI) for threat detection in Industrial Control Systems (ICS), with a specific focus on SCADA and IoT-integrated environments. The analysis of 162 peer-reviewed studies reveals a significant evolution in the cybersecurity landscape, marked by a transition from static, rule-based mechanisms to dynamic, AI-driven solutions capable of detecting complex and previously unknown threats. Supervised and unsupervised machine learning models, as well as deep learning architectures, have demonstrated strong performance across benchmark datasets such as SWaT, BATADAL, and ToN_IoT, with reported detection accuracies often exceeding 90%. However, the practical deployment of these models remains influenced by factors such as data imbalance, latency requirements, explainability, and vulnerability to adversarial manipulation. The review also underscores the growing emphasis on robustness and trustworthiness, as researchers integrate explainable AI tools and adversarial defense mechanisms to align AI outputs with the operational and safety needs of critical infrastructure. Overall, this study affirms that while AI offers transformative potential for ICS cybersecurity, its effectiveness depends on comprehensive evaluation across diverse industrial scenarios, balanced model transparency, and continuous adaptation to evolving cyber threats.

REFERENCES

[1]. Ahmed, M. S., Al Bloushi, M. A., & Ali, A. (2022). Case Study: Application of Wireless Condition Based Monitoring by Applying Machine Learning Models. *ADIPEC*, *NA*(NA), NA-NA. https://doi.org/10.2118/211258-ms

[2]. Alotaibi, I. M., Abido, M. A., Khalid, M., & Savkin, A. V. (2020). A Comprehensive Review of Recent Advances in Smart Grids: A Sustainable Future with Renewable Energy Resources. *Energies*, *13*(23), 6269-NA. https://doi.org/10.3390/en13236269

[3]. Ammar, B., Faria, J., Ishtiaque, A., & Noor Alam, S. (2024). A Systematic Literature Review On AI-Enabled Smart Building Management Systems For Energy Efficiency And Sustainability. *American Journal of Scholarly Research and Innovation*, *3*(02), 01-27. https://doi.org/10.63125/4sjfn272

[4]. Anika Jahan, M., Md Shakawat, H., & Noor Alam, S. (2022). Digital transformation in marketing: evaluating the impact of web analytics and SEO on SME growth. *American Journal of Interdisciplinary Studies*, *3*(04), 61-90. https://doi.org/10.63125/8t10v729

[5]. Anthi, E., Williams, L., Rhode, M., Burnap, P., & Wedgbury, A. (2021). Adversarial Attacks on Machine Learning Cybersecurity Defences in Industrial Control Systems. *Journal of Information Security and Applications*, *58*(NA), 102717-NA. https://doi.org/10.1016/j.jisa.2020.102717

[6]. Aqueveque, P., Radrigan, L., Morales, A. S., & Willenbrinck, E. (2021). Development of a Cyber-Physical System to Monitor Early Failures Detection in Vibrating Screens. *IEEE Access*, *9*(NA), 145866-145885. https://doi.org/10.1109/access.2021.3118283

[7]. Aqueveque, P., Radrigan, L., Pastene, F., Morales, A. S., & Guerra, E. (2021). Data-Driven Condition Monitoring of Mining Mobile Machinery in Non-Stationary Operations Using Wireless Accelerometer Sensor Modules. *IEEE Access*, *9*(NA), 17365-17381. https://doi.org/10.1109/access.2021.3051583

[8]. Aralikatti, S., R, P., Reddy, R., R, S. B., & Reddy, S. N. K. (2021). IoT-Based Distribution Transformer Health Monitoring System using Node-MCU & Blynk. *2021 Third International Conference on Inventive Research in Computing Applications (ICIRCA)*, *NA*(NA), 1-4. https://doi.org/10.1109/icirca51532.2021.9544098

[9]. Arrieta, A. B., Díaz-Rodríguez, N., Del Ser, J., Bennetot, A., Tabik, S., Barbado, A., García, S., Gil-Lopez, S., Molina, D., Benjamins, R., Chatila, R., & Herrera, F. (2020). Explainable Artificial Intelligence (XAI): Concepts, Taxonomies, Opportunities and Challenges toward Responsible AI. *Information Fusion*, *58*(NA), 82-115. https://doi.org/10.1016/j.inffus.2019.12.012

[10]. Asghar, M. R., Hu, Q., & Zeadally, S. (2019). Cybersecurity in Industrial Control Systems: Issues, Technologies, and Challenges. *Computer Networks*, *165*(NA), 106946-NA. https://doi.org/10.1016/j.comnet.2019.106946

[11]. Bhuiyan, S. M. Y., Chowdhury, A., Hossain, M. S., Mobin, S. M., & Parvez, I. (2025). AI-Driven Optimization in Renewable Hydrogen Production: A Review. *American Journal of Interdisciplinary Studies*, *6*(1), 76-94. https://doi.org/10.63125/06z40b13

[12]. Binanzer, L., Merkle, L., Dazer, M., & Nicola, A. (2023). Pitting Detection for Prognostics and Health Management in Gearbox Applications. In (Vol. NA, pp. 97-108). VDI Verlag. https://doi.org/10.51202/9783181024225-97

[13]. Cao, Q., Samet, A., Zanni-Merk, C., de Beuvron, F. d. B., & Reich, C. (2020). Combining chronicle mining and semantics for predictive maintenance in manufacturing processes. *Semantic Web*, *11*(6), 927-948. https://doi.org/10.3233/sw-200406

[14]. Cardoso, D., & de Souza Ferreira, L. C. (2020). Application of Predictive Maintenance Concepts Using Artificial Intelligence Tools. *Applied Sciences*, *11*(1), 18-NA. https://doi.org/10.3390/app11010018

[15]. Carvalho, D. V., Pereira, E. M., & Cardoso, J. S. (2019). Machine Learning Interpretability: A Survey on Methods and Metrics. *Electronics*, *8*(8), 832-NA. https://doi.org/10.3390/electronics8080832

[16]. Chang, R.-I., Lee, C.-Y., & Hung, Y.-H. (2021). Cloud-Based Analytics Module for Predictive Maintenance of the Textile Manufacturing Process. *Applied Sciences*, *11*(21), 9945-NA. https://doi.org/10.3390/app11219945

[17]. Dosilovic, F. K., Brčić, M., & Hlupić, N. (2018). MIPRO - Explainable artificial intelligence: A survey. *2018 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*, *NA*(NA), 210-215. https://doi.org/10.23919/mipro.2018.8400040

[18]. Dosluoglu, T., & MacDonald, M. (2022). Circuit Design for Predictive Maintenance. *Advances in Artificial Intelligence and Machine Learning*, *2*(4), 533-539. https://doi.org/10.54364/aaiml.2022.1136

[19]. East, S., Butts, J., Papa, M., & Shenoi, S. (2009). Critical Infrastructure Protection - A Taxonomy of Attacks on the DNP3 Protocol. In (Vol. 311, pp. 67-81). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-04798-5_5

[20]. Elahi, M., Afolaranmi, S. O., Mohammed, W. M., & Martinez Lastra, J. L. (2022). Energy-Based Prognostics for Gradual Loss of Conveyor Belt Tension in Discrete Manufacturing Systems. *Energies*, *15*(13), 4705-4705. https://doi.org/10.3390/en15134705

[21]. Elnour, M., Meskin, N., Khan, K. M., & Jain, R. (2020). A Dual-Isolation-Forests-Based Attack Detection Framework for Industrial Control Systems. *IEEE Access*, *8*(NA), 36639-36651. https://doi.org/10.1109/access.2020.2975066

[22]. Galagedarage Don, M., Wanasinghe, T. R., Gosine, R. G., & Warrian, P. J. (2025). Digital Twins and Enabling Technology Applications in Mining: Research Trends, Opportunities, and Challenges. *IEEE Access*, *13*(NA), 6945-6963. https://doi.org/10.1109/access.2025.3526881

[23]. Ghasemkhani, B., Aktas, O., & Birant, D. (2023). Balanced K-Star: An Explainable Machine Learning Method for Internet-of-Things-Enabled Predictive Maintenance in Manufacturing. *Machines*, *11*(3), 322-322. https://doi.org/10.3390/machines11030322

[24]. Gilpin, L. H., Bau, D., Yuan, B. Z., Bajwa, A., Specter, M. A., & Kagal, L. (2018). DSAA - Explaining Explanations: An Overview of Interpretability of Machine Learning. *2018 IEEE 5th International Conference on Data Science and Advanced Analytics (DSAA)*, *NA*(NA), 80-89. https://doi.org/10.1109/dsaa.2018.00018

[25]. Golam Qibria, L., & Takbir Hossen, S. (2023). Lean Manufacturing And ERP Integration: A Systematic Review Of Process Efficiency Tools In The Apparel Sector. *American Journal of Scholarly Research and Innovation*, *2*(01), 104-129. https://doi.org/10.63125/mx7j4p06

[26]. Graham, J. H., Hieb, J. L., & Naber, J. (2016). ISIE - Improving cybersecurity for Industrial Control Systems. *2016 IEEE 25th International Symposium on Industrial Electronics (ISIE)*, *NA*(NA), 618-623. https://doi.org/10.1109/isie.2016.7744960

[27]. Hajjaji, Y., Boulila, W., Farah, I. R., Romdhani, I., & Hussain, A. (2021). Big data and IoT-based applications in smart environments: A systematic review. *Computer Science Review*, *39*(NA), 100318-NA. https://doi.org/10.1016/j.cosrev.2020.100318

[28]. Hermansa, M., Kozielski, M., Michalak, M., Szczyrba, K., Wróbel, Ł., & Sikora, M. (2021). Sensor-Based Predictive Maintenance with Reduction of False Alarms-A Case Study in Heavy Industry. *Sensors (Basel, Switzerland)*, *22*(1), 226-226. https://doi.org/10.3390/s22010226

[29]. Hosamo, H. H., Svennevig, P. R., Svidt, K., Han, D., & Nielsen, H. K. (2022). A Digital Twin predictive maintenance framework of air handling units based on automatic fault detection and diagnostics. *Energy and Buildings*, *261*(NA), 111988-111988. https://doi.org/10.1016/j.enbuild.2022.111988

[30]. Hurst, W., Merabti, M., & Fergus, P. (2014). Behaviour analysis techniques for supporting critical infrastructure security. *International Journal of Critical Infrastructures*, *10*(3/4), 267-287. https://doi.org/10.1504/ijcis.2014.066358

[31]. Ishtiaque, A. (2025). Navigating Ethics And Risk In Artificial Intelligence Applications Within Information Technology: A Systematic Review. *American Journal of Advanced Technology and Engineering Solutions*, *1*(01), 579-601. https://doi.org/10.63125/590d7098

[32]. Jeni, L. A., Cohn, J. F., & De la Torre, F. (2013). ACII - Facing Imbalanced Data--Recommendations for the Use of Performance Metrics. *International Conference on Affective Computing and Intelligent Interaction and workshops : [proceedings]. ACII (Conference)*, *2013*(NA), 245-251. https://doi.org/10.1109/acii.2013.47

[33]. Kanamaru, H. (2017). Bridging functional safety and cyber security of SIS/SCS. *2017 56th Annual Conference of the Society of Instrument and Control Engineers of Japan (SICE)*, *NA*(NA), 279-284. https://doi.org/10.23919/sice.2017.8105699

[34]. Kapuria, A., & Cole, D. G. (2023). Integrating Survival Analysis with Bayesian Statistics to Forecast the Remaining Useful Life of a Centrifugal Pump Conditional to Multiple Fault Types. *Energies*, *16*(9), 3707-3707. https://doi.org/10.3390/en16093707

[35]. Khan, M. A. M. (2025). AI And Machine Learning in Transformer Fault Diagnosis: A Systematic Review. *American Journal of Advanced Technology and Engineering Solutions*, *1*(01), 290-318. https://doi.org/10.63125/sxb17553

[36]. Koay, A. M. Y., Ko, R. K. L., Hettema, H., & Radke, K. (2022). Machine learning in industrial control system (ICS) security: current landscape, opportunities and challenges. *Journal of Intelligent Information Systems*, *60*(2), 377-405. https://doi.org/10.1007/s10844-022-00753-1

[37]. Kotsiopoulos, T., Sarigiannidis, P., Ioannidis, D., & Tzovaras, D. (2021). Machine Learning and Deep Learning in smart manufacturing: The Smart Grid paradigm. *Computer Science Review*, *40*(NA), 100341-NA. https://doi.org/10.1016/j.cosrev.2020.100341

[38]. Kravchik, M., & Shabtai, A. (2018). CPS-SPC@CCS - Detecting Cyber Attacks in Industrial Control Systems Using Convolutional Neural Networks. *Proceedings of the 2018 Workshop on Cyber-Physical Systems Security and PrivaCy*, *NA*(NA), 72-83. https://doi.org/10.1145/3264888.3264896

[39]. Kuzlu, M., Cali, U., Sharma, V., & Guler, O. (2020). Gaining Insight Into Solar Photovoltaic Power Generation Forecasting Utilizing Explainable Artificial Intelligence Tools. *IEEE Access*, *8*(NA), 187814-187823. https://doi.org/10.1109/access.2020.3031477

[40]. Lang, X., Nilsson, H., & Mao, W. (2024). Analysis of hydropower plant guide bearing vibrations by machine learning based identification of steady operations. *Renewable Energy*, *236*(NA), 121463-121463. https://doi.org/10.1016/j.renene.2024.121463

[41]. Langner, R. (2011). Stuxnet: Dissecting a Cyberwarfare Weapon. *IEEE Security & Privacy Magazine*, *9*(3), 49-51. https://doi.org/10.1109/msp.2011.67

[42]. Liu, Y., Yu, W., Dillon, T. S., Rahayu, W., & Li, M. (2022). Empowering IoT Predictive Maintenance Solutions With AI: A Distributed System for Manufacturing Plant-Wide Monitoring. *IEEE Transactions on Industrial Informatics*, *18*(2), 1345-1354. https://doi.org/10.1109/tii.2021.3091774

[43]. Mahesh, T. R., Chandrasekaran, S., Ram, V. A., Kumar, V. V., Vivek, V., & Guluwadi, S. (2024). Data-Driven Intelligent Condition Adaptation of Feature Extraction for Bearing Fault Detection Using Deep Responsible Active Learning. *IEEE Access*, *12*(NA), 45381-45397. https://doi.org/10.1109/access.2024.3380438

[44]. Mahmoud, M. A., Nasir, N. R., Gurunathan, M., Raj, P., & Mostafa, S. A. (2021). The Current State of the Art in Research on Predictive Maintenance in Smart Grid Distribution Network: Fault's Types, Causes, and Prediction Methods—A Systematic Review. *Energies*, *14*(16), 5078. https://doi.org/10.3390/en14165078

[45]. Maynard, P., McLaughlin, K., & Sezer, S. (2020). Decomposition and sequential-AND analysis of known cyber-attacks on critical infrastructure control systems. *Journal of Cybersecurity*, *6*(1), NA-NA. https://doi.org/10.1093/cybsec/tyaa020

[46]. Md Masud, K. (2022). A Systematic Review Of Credit Risk Assessment Models In Emerging Economies: A Focus On Bangladesh's Commercial Banking Sector. *American Journal of Advanced Technology and Engineering Solutions*, *2*(01), 01-31. https://doi.org/10.63125/p7ym0327

[47]. Md Takbir Hossen, S., Ishtiaque, A., & Md Atiqur, R. (2023). AI-Based Smart Textile Wearables For Remote Health Surveillance And Critical Emergency Alerts: A Systematic Literature Review. *American Journal of Scholarly Research and Innovation*, *2*(02), 1-29. https://doi.org/10.63125/ceqapd08

[48]. Md Takbir Hossen, S., & Md Atiqur, R. (2022). Advancements In 3D Printing Techniques For Polymer Fiber-Reinforced Textile Composites: A Systematic Literature Review. *American Journal of Interdisciplinary Studies*, *3*(04), 32-60. https://doi.org/10.63125/s4r5m391

[49]. Meissner, R., Rahn, A., & Wicke, K. (2021). Developing prescriptive maintenance strategies in the aviation industry based on a discrete-event simulation framework for post-prognostics decision making. *Reliability Engineering & System Safety*, *214*(NA), 107812-NA. https://doi.org/10.1016/j.ress.2021.107812

[50]. Memala, W. A., Bhuvaneswari, C., Mana, S. C., Selvan, M. P., Maniraj, M., & Kishore, S. (2021). An Approach to Remote Condition monitoring of Electrical Machines based on IOT. *Journal of Physics: Conference Series*, *1770*(1), 012023-NA. https://doi.org/10.1088/1742-6596/1770/1/012023

[51]. Mohammad Shahadat Hossain, S., Md Shahadat, H., Saleh Mohammad, M., Adar, C., & Sharif Md Yousuf, B. (2024). Advancements In Smart and Energy-Efficient HVAC Systems: A Prisma-Based Systematic Review. *American Journal of Scholarly Research and Innovation*, *3*(01), 1-19. https://doi.org/10.63125/ts16bd22

[52]. Noor Alam, S., Golam Qibria, L., Md Shakawat, H., & Abdul Awal, M. (2023). A Systematic Review of ERP Implementation Strategies in The Retail Industry: Integration Challenges, Success Factors, And Digital Maturity Models. *American Journal of Scholarly Research and Innovation*, *2*(02), 135-165. https://doi.org/10.63125/pfdm9g02

[53]. Ntalampiras, S. (2016). Fault Diagnosis for Smart Grids in Pragmatic Conditions. *IEEE Transactions on Smart Grid*, *9*(3), 1-1. https://doi.org/10.1109/tsg.2016.2604120

[54]. Potluri, S., & Diedrich, C. (2019). CASE - Deep Learning based Efficient Anomaly Detection for Securing Process Control Systems against Injection Attacks. *2019 IEEE 15th International Conference on Automation Science and Engineering (CASE)*, *NA*(NA), 854-860. https://doi.org/10.1109/coase.2019.8843140

[55]. Qu, Y., Zhao, H., Zhao, S., Ma, L., & Mi, Z. (2024). Evaluation method for insulation degradation of power transformer windings based on incomplete internet of things sensing data. *IET Science, Measurement & Technology*, *18*(3), 130-144. https://doi.org/10.1049/smt2.12174

[56]. Rajendran, G., Sathyabalu, H. V., Sachi, M., & Devarajan, V. (2019). Cyber Security in Smart Grid: Challenges and Solutions. *2019 2nd International Conference on Power and Embedded Drive Control (ICPEDC)*, *NA*(NA), 546-551. https://doi.org/10.1109/icpedc47771.2019.9036484

[57]. Rajesh, P., Mohammad Hasan, I., & Anika Jahan, M. (2023). AI-Powered Sentiment Analysis In Digital Marketing: A Review Of Customer Feedback Loops In It Services. *American Journal of Scholarly Research and Innovation*, *2*(02), 166-192. https://doi.org/10.63125/61pqqq54

[58]. Robles-Durazno, A., Moradpoor, N., McWhinnie, J., & Russell, G. (2018). *Cyber Security - A supervised energy monitoring-based machine learning approach for anomaly detection in a clean water supply system* (Vol. NA). IEEE. https://doi.org/10.1109/cybersecpods.2018.8560683

[59]. Roksana, H. (2023). Automation In Manufacturing: A Systematic Review Of Advanced Time Management Techniques To Boost Productivity. *American Journal of Scholarly Research and Innovation*, *2*(01), 50-78. https://doi.org/10.63125/z1wmcm42

[60]. Roksana, H., Ammar, B., Noor Alam, S., & Ishtiaque, A. (2024). Predictive Maintenance In Industrial Automation: A Systematic Review Of IOT Sensor Technologies And AI Algorithms. *American Journal of Interdisciplinary Studies*, *5*(01), 01-30. https://doi.org/10.63125/hd2ac988

[61]. Roostaee, S., Thomas, M. S., & Mehfuz, S. (2017). Experimental studies on impedance based fault location for long transmission lines. *Protection and Control of Modern Power Systems*, *2*(1), 16-NA. https://doi.org/10.1186/s41601-017-0048-y

[62]. S, P., Krithivasan, K., S, P., & S, S. S. V. (2020). Detection of Cyberattacks in Industrial Control Systems Using Enhanced Principal Component Analysis and Hypergraph-Based Convolution Neural Network (EPCA-HG-CNN). *IEEE Transactions on Industry Applications*, *56*(4), 4394-4404. https://doi.org/10.1109/tia.2020.2977872

[63]. Sharma, R., Mahela, O. P., & Agarwal, S. (2018). Detection of Power System Faults in Distribution System Using Stockwell Transform. *2018 IEEE International Students' Conference on Electrical, Electronics and Computer Science (SCEECS)*, *NA*(NA), 1-5. https://doi.org/10.1109/sceecs.2018.8546879

[64]. Shukla, B., Fan, I.-S., & Jennions, I. (2020). Opportunities for Explainable Artificial Intelligence in Aerospace Predictive Maintenance. *PHM Society European Conference*, *5*(1), 11-NA. https://doi.org/10.36001/phme.2020.v5i1.1231

[65]. Siddiqui, N. A. (2025). Optimizing Business Decision-Making Through AI-Enhanced Business Intelligence Systems: A Systematic Review of Data-Driven Insights in Financial And Strategic Planning. *Strategic Data Management and Innovation*, *2*(1), 202-223. https://doi.org/10.71292/sdmi.v2i01.21

[66]. Slack, D., Hilgard, S., Jia, E., Singh, S., & Lakkaraju, H. (2020). AIES - Fooling LIME and SHAP: Adversarial Attacks on Post hoc Explanation Methods. *Proceedings of the AAAI/ACM Conference on AI, Ethics, and Society*, *NA*(NA), 180-186. https://doi.org/10.1145/3375627.3375830

[67]. Sohel, R. (2025). AI-Driven Fault Detection and Predictive Maintenance In Electrical Power Systems: A Systematic Review Of Data-Driven Approaches, Digital Twins, And Self-Healing Grids. *American Journal of Advanced Technology and Engineering Solutions*, *1*(01), 258-289. https://doi.org/10.63125/4p25x993

[68]. Sokolov, N. A., Pyatnitsky, A. I., & Alabugin, K. S. (2019). Applying methods of machine learning in the task of intrusion detection based on the analysis of industrial process state and ICS networking. *FME Transactions*, *47*(4), 782-789. https://doi.org/10.5937/fmet1904782s

[69]. Tahmina Akter, R., & Abdur Razzak, C. (2022). The Role Of Artificial Intelligence In Vendor Performance Evaluation Within Digital Retail Supply Chains: A Review Of Strategic Decision-Making Models. *American Journal of Scholarly Research and Innovation*, *1*(01), 220-248. https://doi.org/10.63125/96jj3j86

[70]. Tan, S., Guerrero, J. M., Xie, P., Han, R., & Vasquez, J. C. (2020). Brief Survey on Attack Detection Methods for Cyber-Physical Systems. *IEEE Systems Journal*, *14*(4), 5329-5339. https://doi.org/10.1109/jsyst.2020.2991258

[71]. Tang, Z., Zhou, C., Jiang, W., Zhou, W., Jing, X., Yu, J., Alkali, B., & Sheng, B. (2014). Analysis of Significant Factors on Cable Failure Using the Cox Proportional Hazard Model. *IEEE Transactions on Power Delivery*, *29*(2), 951-957. https://doi.org/10.1109/tpwrd.2013.2287025

[72]. Thorat, J., & Thakare, M. (2022). Different Failure Statistics of Distribution Transformer and Its Mitigation Using IOT Monitoring. *SSRN Electronic Journal*, *NA*(NA), NA-NA. https://doi.org/10.2139/ssrn.4056053

[73]. Tippannavar, S. S., & D, Y. (2023). Transformer 4.0 - A Smart Transformer for a Smarter Living. *2023 3rd International Conference on Innovative Sustainable Computational Technologies (CISCT)*, *NA*(NA), 1-6. https://doi.org/10.1109/cisct57197.2023.10351417

[74]. Tonmoy, B., & Md Arifur, R. (2023). A Systematic Literature Review Of User-Centric Design In Digital Business Systems Enhancing Accessibility, Adoption, And Organizational Impact. *American Journal of Scholarly Research and Innovation*, *2*(02), 193-216. https://doi.org/10.63125/36w7fn47

[75]. Tonoy, A. A. R., & Khan, M. R. (2023). The Role of Semiconducting Electrides In Mechanical Energy Conversion And Piezoelectric Applications: A Systematic Literature Review. *American Journal of Scholarly Research and Innovation*, *2*(01), 01-23. https://doi.org/10.63125/patvqr38

[76]. Tsiu, S., Ngobeni, M., Mathabela, L., & Thango, B. (2024). Applications and Competitive Advantages of Data Mining and Business Intelligence in SMEs Performance: A Systematic Review. *NA*, *NA*(NA), NA-NA. https://doi.org/10.20944/preprints202409.0940.v1

[77]. Ucar, A., Karakose, M., & Kırımça, N. (2024). Artificial Intelligence for Predictive Maintenance Applications: Key Components, Trustworthiness, and Future Trends. *Applied Sciences*, *14*(2), 898-898. https://doi.org/10.3390/app14020898

[78]. von Enzberg, S., Naskos, A., Metaxa, I., Köchling, D., & Kühn, A. (2020). Implementation and Transfer of Predictive Analytics for Smart Maintenance: A Case Study. *Frontiers in Computer Science*, *2*(NA), 578469-NA. https://doi.org/10.3389/fcomp.2020.578469

[79]. Voyiatzis, A. G., Katsigiannis, K., & Koubias, S. (2015). ETFA - A Modbus/TCP Fuzzer for testing internetworked industrial systems. *2015 IEEE 20th Conference on Emerging Technologies & Factory Automation (ETFA)*, *NA*(NA), 1-6. https://doi.org/10.1109/etfa.2015.7301400

[80]. Wang, C., Wang, B., Liu, H., & Qu, H. (2020). Anomaly Detection for Industrial Control System Based on Autoencoder Neural Network. *Wireless Communications and Mobile Computing*, *2020*(NA), 1-10. https://doi.org/10.1155/2020/8897926

[81]. Wang, W., Xie, Y., Ren, L., Zhu, X., Chang, R., & Yin, Q. (2018). Detection of data injection attack in industrial control system using long short term memory recurrent neural network. *2018 13th IEEE Conference on Industrial Electronics and Applications (ICIEA)*, *NA*(NA), 2710-2715. https://doi.org/10.1109/iciea.2018.8398169

[82]. Zaman, S. (2024). A Systematic Review of ERP And CRM Integration For Sustainable Business And Data Management in Logistics And Supply Chain Industry. *Frontiers in Applied Engineering and Technology*, *1*(01), 204-221. https://doi.org/10.70937/faet.v1i01.36

[83]. Zhai, C., Zhang, H., Xiao, G., & Pan, T.-C. (2019). A model predictive approach to protect power systems against cascading blackouts. *International Journal of Electrical Power & Energy Systems*, *113*(NA), 310-321. https://doi.org/10.1016/j.ijepes.2019.05.029

[84]. Zhang, W., Lu, Q., Yu, Q., Li, Z., Liu, Y., Lo, S. K., Chen, S., Xu, X., & Zhu, L. (2021). Blockchain-Based Federated Learning for Device Failure Detection in Industrial IoT. *IEEE Internet of Things Journal*, *8*(7), 5926-5937. https://doi.org/10.1109/jiot.2020.3032544

[85]. Zhao, J., Xia, X., Su, D., Xu, C., & Wu, F. (2019). Fault Section Location Method Based on Random Forest Algorithm for Distribution Networks with Distribution Generations. *2019 IEEE Innovative Smart Grid Technologies - Asia (ISGT Asia)*, *NA*(NA), 4165-4169. https://doi.org/10.1109/isgt-asia.2019.8881710

[86]. Zhu, G., Wang, C., Zhao, W., Xie, Y., Guo, D., & Zhang, D. (2023). Blade Crack Diagnosis Based on Blade Tip Timing and Convolution Neural Networks. *Applied Sciences*, *13*(2), 1102-1102. https://doi.org/10.3390/app13021102

[87]. Zizzo, G., Hankin, C., Maffeis, S., & Jones, K. (2020). Adversarial Attacks on Time-Series Intrusion Detection for Industrial Control Systems. *2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, *NA*(NA), 899-910. https://doi.org/10.1109/trustcom50675.2020.00121