Department of Industrial Engineering & Maintenance

Monitoring and Securing SCADA Systems Using Machine Learning : A Review of Current Methods and Future Directions

OUAR Narimane & LEBKARA Haithem

Master's thesis in GI

OUAR Narimane
LEBKARA Haithem

Advisor:
BELAYADI Djahida

Co-advisors:
DJAGHLOUF Asma

Academic year:
2024-2025

Abstract: SCADA systems are used to effectively monitor and control critical industrial infrastructure . Due to Industry 4.0 , SCADA systems have evolved towards linked architectures, which has enhanced operational efficiency but also made them more vulnerable to cyberattacks. SCADA systems, which were once intended to be dependable, are now at risk from malware, DoS attacks, illegal access,and various types of threats endangering both safety and service continuity. In this context, artificial intelligence enables real-time detection of anomalies and cyberattacks especially by ML and deep DL based IDS. This paper offers a thorough analysis of current AI strategies for SCADA security, emphasising important techniques, difficulties, and results .

Key-Words: Artificial intelligence, attack detection, cybersecurity, Industrial Internet of Things (IIoT), Supervisory Control and Data Acquisition (SCADA).

Contents

1 Introduction 2
2 SCADA Systems and Cybersecurity 2
3 Related Works 5
4 Experimental Framework 7
5 Conclusions 11
A Appendix 14

1. Introduction

Control and data acquisition systems (SCADA) are essential components of industrial infrastructures, enabling centralized supervision, real-time data collection and remote control in sectors such as energy, water, transport and manufacturing[1]. A standard SCADA architecture consists of Programmable Logic Controllers (PLC), Remote Terminal Units (RTU), Master Terminal Units (MTU) and Human-Machine Interfaces (HMI), These systems rely on both wired and wireless communication networks to exchange information across geographically distributed areas, together they ensure seamless monitoring and control of distributed processes assets.[2].

The integration of SCADA into larger digital infrastructures, particularly under the dominance of Industry 4.0, has allowed systems to move from isolated and proprietary installations to highly connected and interoperable architectures. This transformation is mainly driven by the convergence of Information Technology (IT) and Operational Technology (OT), as well as the adoption of Industrial Internet of Things (IIoT) concepts that improve data visibility, predictive maintenance and remote diagnostics [3].

However, this increased connectivity has created significant cybersecurity challenges. SCADA systems, initially designed for availability and reliability,[4] are now facing a wider variety of cyber threats, such as denial-of-service (DoS) attacks, malware, SQL injection, phishing and unauthorized access [5]. These threats are likely to disrupt essential services, damage critical assets and compromise the safety of industrial operations. [6]Key events such as Stuxnet and power grid attacks have illustrated the devastating effect of cyber-attacks on ICS environments [7].

To address these evolving risks, researchers are increasingly turning to Artificial Intelligence (AI) to enhance the security of SCADA. AI-based intrusion detection systems (IDS) offer promising opportunities to detect and classify cyber threats in real time, including in complex and dynamic environments [8]. These methods examine network traffic patterns and system behavior to identify anomalies that signal malicious activity.[9]

To provide a comprehensive overview of current developments in the field, we conducted a systematic literature review based on recent research aimed at securing SCADA systems using AI approaches .We also developed and evaluated an AI-based IDS model using nine algorithms : : Adaptive Boosting (AdaBoost), Extreme Gradient Boosting (XGBoost), Gradient Boosting (GBoost), Long Short-Term Memory (LSTM), Convolutional Neural Networks (CNN), Recurrent Neural Networks (RNN), Random Forest (RF), Decision Tree (DT), and k-Nearest Neighbor (KNN). This experimental study offers useful information on how different methods work in comparison when used for SCADA cybersecurity.

The paper is structured as follows: Section 2 discusses SCADA systems and cybersecurity. Section 3 reviews related research in the field. Section 4 describes the experimental study and results . Finally, the conclusion summarizes key findings.

2. SCADA Systems and Cybersecurity

This section contains an overview of SCADA systems where detailing SCADA components , their evolution with time , and the potential possible threats .

2.1. SCADA architecture

A typical architecture of a modern SCADA system (see Figure 1) is generally consists of three main functional segments: the centralized control segment , the field equipment segment and the communication network segment [10].

At the heart of the architecture is the Master Terminal Unit (MTU), .This unit acts as the core of the system, coordinating all functions of control, processing, data visualization and sending instructions to monitored areas. The MTU exchanges data with Remote Terminal Units (RTUs) and Programmable Logic Controllers (PLCs), which are responsible for collecting data, to interact with the actuators and to ensure the execution of the commands locally.

RTUs receive real-time information from various field equipment, such as sensors, switches, intelligent electronic devices (IEDs), or actuators, which they rearrange before transmitting to the MTU for processing and archiving.Conversely, the MTU generates control commands that are relayed by the RTUs to the relevant devices for execution [4]. The human-machine interface (HMI) allows operators to interact with the SCADA system through intuitive graphical representations, thus facilitating the supervision of operations and the management of alarms. resilience.

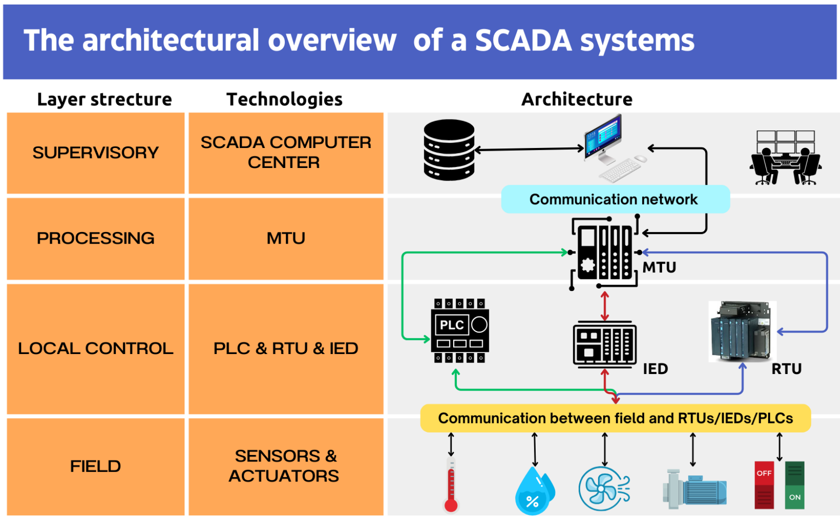

Figure 1: The architectural overview of a SCADA system

2.2. SCADA evolution through generations

Over the last few decades, SCADA systems have undergone a significant architectural change, moving from isolated and centralized to integrated, interconnected platforms . This progression can be defined in four distinct generations:

The first generation, launched in the 1960s and 1970s, consisted of monolithic SCADA systems that were completely independent and based on proprietary hardware and software. [11].

The second generation, enabled by the advancement of microprocessors and Local Area Networks (LANs). It was now possible for parts like RTUs, PLCs, and HMIs to be dispersed throughout locations while still maintaining connectivity. [12].

Using Wide Area Networks (WANs) and IP-based protocols like Modbus TCP and DNP3, the third generation adopted networked architectures . These systems improved interoperability and allowed for remote monitoring from several locations. However, the increased connectivity also introduced significant cybersecurity risks.[13].

IoT-enabled SCADA systems are represented by the fourth generation, which began in the 2010s and continues to this day. These platforms enable real-time analytics and wise decision-making by combining cloud computing, edge processing, smart sensors, and AI algorithms. [13]They provide scalability and integration with ERP and MES systems, but because of their increased interconnectedness, they also present difficult cybersecurity issues [12].

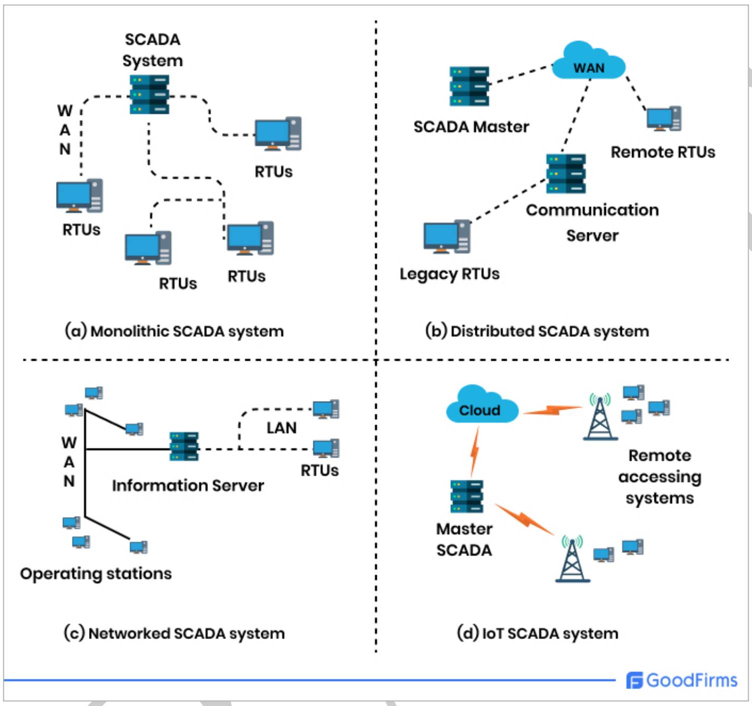

Figure 2: SCADA system evolution

Table 1: Summary of SCADA System Generations

SCADA Generation	**Architecture & Communication**	**Scalable**	**Reliable**	**Security Model**	**Key Technologies / Features**
Monolithic (1st Gen) 1960s–1970s	Standalone, proprietary, no networking	Not scalable	Low	Air-gapped, physical isolation	Mainframes, proprietary I/O
Distributed (2nd Gen) 1970s–1980s	LAN-connected nodes (PLCs, RTUs)	Moderate	Moderate	Security through obscurity	LANs, microprocessors, modular design
Networked (3rd Gen) 1990s–2000s	WAN-based, IP communication, centralized control	High	High (with backups)	Basic cybersecurity (firewalls, open protocols)	Modbus TCP, DNP3, OPC, centralized data systems
IoT-enabled (4th Gen) 2010s–Present	Cloud-integrated, edge computing, IoT protocols	Very high	Very high	TLS/SSL, access control, anomaly detection	Cloud/edge computing, AI, mobile access, ERP/MES integration

2.3. Cybersecurity and Threats in SCADA Systems

SCADA systems are vulnerable to different cyber attacks, depending on the targeted segments. MTU and RTU are the main targets of internal attacks, which exploit organizational flaws such as unsecured physical access, the use of weak passwords or the uncontrolled distribution of access privileges[8].These attacks include , SQL injection, , password attacks and malware such as viruses and ransomware.

As for communication segments, they are more often the target of external attacks using open protocols. Passive attacks such as reconnaissance, phishing , traffic analysis , denial of service (DOS) [6] attacks that compromise availability, as well as attacks to modify or falsify such as replay and man in the middle, threatening the integrity and authenticity of the system . Thus, for effective protection, it is necessary to adopt a separate and tailored strategy for each segment of the SCADA architecture.[14]

Type of Attack	**Description**
Denial of Service (DoS)	Disrupts the availability of SCADA by overwhelming them with traffic.
Phishing	Social engineering attacks to access to sensitive information.
SQL Injection	Inserting malicious SQL queries to manipulate SCADA database .
Man-in-the-Middle (MiTM)	Intercepting communication between SCADA components to gain access.
Reconnaissance	Collecting data about SCADA before launching an attack.
Password Attacks	Attempting to crack passwords to gain unauthorized access to SCADA.
Privilege Escalation	Gaining high access levels in SCADA systems to execute commands.

Table 2: Some Types of Attacks Involved in SCADA Systems

3. Related Works

We began our research with an extensive literature review using eleconic libraries, such as Google Scholar, ScienceDirect, and IEEE Xplore where 30 scientific papers and 10 blog sites were selected.

In the following stage, we evaluated these sources to determine whether they aligned with our research goals by looking at their abstracts, keywords, and introductions. 15 of the most current and pertinent publications were chosen based on predetermined inclusion and exclusion criteria. The following table provides a summary of the main contributions and limitations of these works.

Ref	Year	Contribution	Limitation
[15]	2023	• Creation of an annotated SCADA dataset integrating various types of attacks. • Intended for the evaluation of anomaly detection techniques.	• Article non peer-reviewed. • Dataset still not widely used.
[16]	2022	• DNN hybrid model to classify DDoS attacks in IIoT networks with SDN.	• Highly DDoS/SDN oriented. • Little generalizable to classic SCADA
[17]	2023	• Comparison of ML models to classify DDoS attacks in IIoS.	• Validation on simulated data. • Absence of actual experimentation.
[18]	2023	• Study of the impact of adversarial attacks on AI models applied to ICS.	• exploratory approach. • Absence of real application.
[19]	2023	• Application of CNN and BiLSTM to improve detection in SCADA.	• High data requirement. • Vulnerable to adversarial attacks.
[20]	2023	• Review of DL approaches: CNN, GAN, Autoencoders, etc. to secure SCADA.	• No experimental validation. • Limited scope
[21]	2022	• ICS detection by classical AI methods (SVM, RF) + statistical analysis.	• Simulated validation only.
[22]	2023	• FNN-LSTM to detect correlated and uncorrelated attacks in SCADA.	• Lack of robustness to noise. • Risk of overfitting.
[23]	2020	• DL-based multiclass method (Omni-SCADA-ID) for SCADA networks.	• Complex architecture difficult to implement.
[24]	2024	• Presentation of AI/ML techniques to strengthen cybersecurity. • Best practice recommendations (IDS, SIEM, encryption, etc.).	• No experimental validation. • Little detailed practical implementation.

[25]	2023	of SCADA-cloud vulnerabilities.Identification of 4 major sources of risk. Security solutions adapted to the cloud.	• Limited to the cloud context. • No empirical validation.
[26]	2024	• Design of an HIDS for SCADA. • Detection via USB tagging and process memory. • Tests on three typical scenarios.	• Need for field tests. • Effectiveness on complex threats not proven.
[27]	2025	• Proposal for a verified DRL framework to counter cyber-physical attacks on smart grids. • Integration of scope analysis to ensure DRL security.	• Validation limited to simulations; no tests under real conditions. • Complexity of implementation in existing industrial environments.
[28]	2024	• Identification of protocol weaknesses and IT integration challenges. • Recommendations to enhance the security of critical systems.	• Mainly theoretical study; lack of empirical validation. • Applicability of proposed solutions to specific environments not demonstrated.
[29]	2025	• Importance of corporate visibility and resilience. • Strategies to balance digital transformation and security.	• General approach without in-depth technical details. • No experimental validation of the proposed strategies.

4. Experimental Framework

4.1. Methodology

The experiment conducted in this study is based on the use of public data sets and the evaluation of several models of artificial intelligence for the detection of cyberattacks in SCADA systems. It is structured around the following elements:

- **Datasets used** : Two databases were exploited: **WUSTL-IIOT-2018** [30] and **WUSTL-IIOT-2021** [31]. The first contains about 1.2 million records, including DoS attacks, command injection, recognition, etc. The second includes more than 7 million instances, mainly related to recognition attacks

- **Data Preprocessing**: The data was cleaned, normalized with MinMaxScaler and then split into two sets: 70% for training and 30% for testing.

- **Methodology applied** : Three groups of algorithms were tested for detection of SCADA attacks. Classic models (**DT**, **kNN**, **RF**) provide quick and interpretable results. Deep Learning models (**CNN**, **RNN**, **LSTM**) capture complex patterns in time data. Finally, Boosting models (**AdaBoost**, **GBoost**, **XG-Boost**) improve accuracy and robustness especially on unbalanced data

- **Hyperparameter optimization**: The search for the best parameters was performed via **RandomizedSearchCV** with cross-validation (3-fold), in order to optimize performance , balancing training efficiency, convergence speed, and generalization while reducing overfitting.

- **Performance Evaluation**: In addition to the *accuracy* , metrics such as *precision*, *recall*, *score F1*, ROC curve and PR curve were used to better interpret performance, especially in the presence of unbalanced classes.

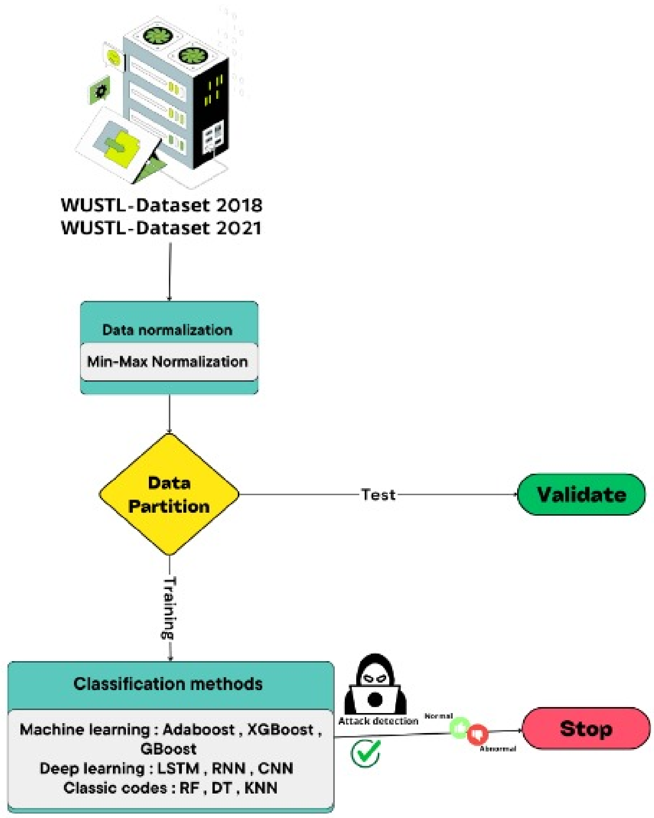

Figure 3: Our Methodology's Flowchart

4.2. Results and Discussion

Our tests on datasets WUSTL-SCADA-2018 and WUSTL-SCADA-2021 have demonstrated excellent performance on all evaluated models. Boosting algorithms, notably XGBoost, achieved flawless accuracy , while CNN and LSTM also achieved near-perfect scores with minimal false positives and false negatives in the confusion metrics. Traditional models such as the Random Forest and the Decision Tree have also retained a high degree of precision.

The results for the 2021 dataset closely mirror those of 2018, as shown in Table 4, which confirms the models' robustness and strong generalization ability for anomaly detection in SCADA systems. The ROC And PRC evaluation revealed highly good results, for example in the Deep learning analyses CNN and LSTM models achieved a perfect AUC of 1.00, while RNN attained a close 0.99, indicating very low misclassification rates. The Precision-Recall curves further highlighted LSTM's ability to maintain perfect precision across all recall levels, and CNN's balanced performance with consistently high recall.

Dataset	**Method**	**Train Acc (%)**	**Test Acc (%)**	**Precision**	**R**	**F**	**FPR**
	AdaBoost	99.98	99.98	0.9991	0.9965	0.9964	0.0864
	XGBoost	100	100	1.0000	0.9996	0.9985	0.0252
	GBoost	99.99	99.99	1.0000	0.9997	0.9998	0.0678
	RF	100	100	0.9999	1.0000	0.9999	0.066
WUSTL-IIOT-2018	**DT**	100	99.99	0.9999	0.9999	0.9999	0.3333
	KNN	100	99.99	0.9989	0.9994	0.9991	0.1430
	LSTM	99.95	99.96	0.9942	0.9984	0.9963	0.5833
	RNN	99.91	99.92	0.9915	0.9953	0.9934	0.4612
	CNN	99.95	99.97	0.9953	0.9989	0.9971	0.5370
	AdaBoost	99.95	99.95	0.9953	0.9968	0.9961	0.0342
	XGBoost	100	99.99	0.9999	0.9999	0.9998	0.0279
	GBoost	99.99	99.99	0.9981	1.0000	0.9990	0.0240
	RF	99.99	99.99	0.9999	0.9995	0.9997	0.0192
WUSTL-IIOT-2021	**DT**	100	99.99	0.9997	0.9996	0.9997	0.3333
	KNN	99.99	99.99	0.9997	0.9991	0.9994	0.1429
	LSTM	99.99	99.95	0.9992	0.9939	0.9966	0.2303
	RNN	99.91	99.91	0.9987	0.9893	0.9940	0.3491
	CNN	99.99	99.99	0.9888	0.9987	0.9966	0.3416

Table 4: Performance Results

Tables 5 and 6 present a comparison of our study's performance metrics with those found in recent literature on SCADA anomaly detection. Previous research, such as the ANN model in [32], reported an accuracy of 98.40%, while boosting methods and traditional classifiers mentioned in [35] and [37] typically achieved accuracies ranging from 79% to 98%. In contrast, our findings show nearly flawless performance across all models evaluated. For example, our boosting models—XGBoost and GBoost—reached accuracies of 100% and 99.99% respectively, with precision, recall, and F1-scores close to 100%.

Table 5: Comparison of Model Performance with recent studies for Wustl-IIOT-2021

Reference	**Model**	**Acc (%)**	**P (%)**	**R (%)**	**F1 (%)**
[33]	Modified DT	99.99	99.99	00.88	99.93
	RF	99.99	99.93	99.88	99.93
	AdaBoost	99.98	99.97	99.80	99.88
	XGB	99.99	99.99	99.82	99.91
	GB	99.99	99.99	99.91	99.95
[34]	RF	99.57	99.67	99.57	99.59
	CNN	92.74	89.25	99.89	98.71
	LSTM	95.76	95.07	95.76	95.64
[35]	RF	95.80	95.40	99.70	95.60
	kNN	94	94.60	99.50	94.20
	MLP	79.20	88.20	97.20	83.20
[36]	GRU	99.75	99.76	99.43	99.50
	CNN-GRU	98.18	99.10	98.95	98.85
This study	**AdaBoost**	99.95	99.53	99.68	99.61
	XGBoost	100	99.99	99.99	99.98
	GBoost	99.99	99.81	100	99.90
	LSTM	99.99	99.92	99.39	99.66
	RNN	99.91	99.87	98.93	99.40
	CNN	99.99	98.88	99.87	99.66
	RF	99.99	99.99	99.95	99.97
	DT	100	99.97	99.96	99.97
	KNN	99.99	99.97	99.91	99.94

Table 6: Comparison of Model Performance with recent studies for Wustl-IIOT-2018

Reference	Model	Acc (%)	P (%)	R (%)	F1 (%)
[32]	ANN	98.40	99.57	98.02	98.97
	Modified DT	89.00	87.31	86.47	86.47
	RF	87.31	87.31	87.31	87.31
[33]	AdaBoost	86.47	86.47	86.47	86.47
	XGB	86.47	86.47	86.47	86.47
	GB	87.31	87.31	87.31	87.31
	GSFTNN	98.54	98.70	98.42	98.61
[37]	ResNet	97.70	98.10	97.54	97.89
	RNN	94.22	93.64	93.73	94.38
	LSTM	95.98	96.30	95.78	96.17
	GRU	99.93	99.95	99.94	99.95
[36]	CNN-GRU	99.98	99.98	99.98	99.98
	Naive Bayes	94.20	94.60	94.20	93.00
[38]	SVM	94.20	94.50	94.20	92.60
	J48	99.20	99.20	99.20	99.10
	AdaBoost	99.98	99.91	99.65	99.64
	XGBoost	100	100	99.96	99.85
	GBoost	99.99	100	99.97	99.88
	LSTM	99.95	99.15	99.53	99.34
This study	**RNN**	99.91	99.15	98.53	99.34
	CNN	99.95	98.53	99.89	99.71
	RF	100	100	99.99	99.97
	DT	100	99.99	99.99	99.99
	KNN	99.99	99.89	99.94	99.91

5. Conclusions

Through this study the changing landscape of ICS was examined , with a highlight on SCADA systems. We started with determining the vulnerabilities impacting new SCADA architecture and assessed the effectiveness of AI-based intrusion detection techniques in mitigating these threats by a structured literature research . Our results demonstrate the increasing importance of anomaly detection and machine learning in improving real-time protection systems against sophisticated cyberattacks.

The resilience of industrial networks may be increased by combining security measures with technology developments. But challenges remain, particularly in terms of scalability,AI model interpretability, and practical implementation. Future research should focus on hybrid approaches combining signature-based and anomaly-based detection, as well as the integration of secure-by-design principles in SCADA system development.

References

[1] K. Stouffer, J. Falco, and K. Scarfone. *Guide to Industrial Control Systems (ICS) Security*. Special Publication 800-82 Revision 2. National Institute of Standards and Technology (NIST), Gaithersburg, MD, 2015.

[2] J. Smith and T. Brown. Vulnerabilities in scada systems: A survey. *Journal of Industrial Security*, 5(2):123–135, 2018.

[3] A. Williams and L. Zhang. Detection of reconnaissance attacks in scada systems using network traffic analysis. *IEEE Transactions on Industrial Informatics*, 10(4):1827–1836, 2020.

[4] Ahmad Zainudin, Love Allen Chijioke Ahakonye, Rubina Akter, Dong-Seong Kim, and Jae-Min Lee. An efficient hybrid-dnn for ddos detection and classification in software-defined iiot networks. *IEEE Internet of Things Journal*, 10(10):8491–8504, 2022.

[5] G. Qaiser, S. Chandrasekaran, R. Chai, and J. Zheng. Classifying ddos attack in industrial internet of services using machine learning. In *Proceedings of the 15th International Conference on Computer and Automation Engineering (ICCAE)*, pages 546–550, 2023.

[6] Z. Xu, Y. Li, and H. Zhang. Artificial intelligence for cybersecurity in critical infrastructure protection: A review. *Future Generation Computer Systems*, 106:719–734, 2020.

[7] S. Trivedi, T.A. Tran, N. Faruqui, and M.M. Hassan. An exploratory analysis of effect of adversarial machine learning attack on iot-enabled industrial control systems. In *Proceedings of the International Conference on Smart Computing and Application (SCA)*, pages 1–8, 2023.

[8] M.A. Teixeira, T. Salman, M. Zolanvari, R. Jain, N. Meskin, and M. Samaka. Scada system testbed for cybersecurity research using machine learning approach. *Future Internet*, 10(8):76, 2018.

[9] David E Rumelhart, Geoffrey E Hinton, and Ronald J Williams. Learning representations by backpropagating errors. *Nature*, 323(6088):533–536, 1986.

[10] A. Tesfahun and D.L. Bhaskari. A scada testbed for investigating cyber security vulnerabilities in critical infrastructures. *Automatic Control and Computer Sciences*, 50:54–62, 2016.

[11] V. M. Igure, S. A. Laughter, and R. D. Williams. Security issues in scada networks. *Computers & Security*, 25(7):498–506, 2006.

[12] J. D. McDonald. Scada and automation systems. In *Electric Power Substations Engineering*, pages 453–476. CRC Press, 2012.

[13] M.F.E.G.I.M. Génie industriel et management des systèmes : Architecture scada. Proceedings of M.F.E.G.I.M. (2024/2025), 2024. Mémoire académique non publié.

[14] M. Karami and S. Shamsi. A survey of cyber-attacks on scada systems and their countermeasures. *Journal of Computer Networks and Communications*, 2019:1–17, 2019.

[15] A. Dehlaghi-Ghadim et al. A comprehensive scada dataset for anomaly detection in industrial control systems. *arXiv preprint arXiv:2301.00000*, 2023.

[16] A. Zainudin, L.A.C. Ahakonye, R. Akter, D.S. Kim, and J.M. Lee. An efficient hybrid-dnn for ddos detection and classification in software-defined iiot networks. *IEEE Internet of Things Journal*, 10(10):8491–8504, 2022.

[17] G. Qaiser et al. Comparative evaluation of machine learning models for ddos attack detection in iiot. In *2023 International Conference on Computer Applications and Engineering (ICCAE)*, pages 1–6, 2023.

[18] S. Trivedi, T.A. Tran, N. Faruqui, and M.M. Hassan. An exploratory analysis of effect of adversarial machine learning attack on iot-enabled industrial control systems. In *2023 International Conference on Smart Computing and Application (ICSCA)*, pages 1–6, 2023.

[19] X. Gao et al. Deep learning models for intrusion detection in scada systems: A comparative study. *Journal of Industrial Cybersecurity*, 2(1):45–60, 2023.

[20] Y. Wu et al. A review of deep learning approaches for scada system security. *Journal of Cybersecurity and Automation*, 5(2):123–135, 2023.

[21] W. Wang et al. An ai-based framework for intrusion detection in industrial control systems. *International Journal of Critical Infrastructure Protection*, 36:100456, 2022.

[22] J. Gao et al. Fnn-lstm based detection of correlated and uncorrelated attacks in scada systems. *Journal of Industrial Cybersecurity*, 2(2):75–88, 2023.

[23] J. Gao et al. Omni-scada-id: A deep learning-based multiclass intrusion detection system for scada networks. *IEEE Internet of Things Journal*, 7(5):4371–4381, 2020.

[24] Emmanouil Skrodelis, Iosif Kalamaras, and Dimitrios Zissis. Cybersecurity in scada systems with advanced ai and ml techniques. *ResearchGate*, 2024.

[25] Abdulrahman Al-Ali, Saeed Khan, and Anam Jamal. Cybersecurity in supervisory control and data acquisition systems. *Sustainability*, 15(10):8076, 2023.

[26] Biplab Sen, Sagar Yasasvi, Sachin Pandey, Harshit Bedi, Pankaj Bedi, and Neeru Saini. Enhancing scada security: Developing a host-based intrusion detection system to safeguard against cyberattacks. *Computers*, 13(4):97, 2024.

[27] Suman Maiti and Soumyajit Dey. Smart grid security: A verified deep reinforcement learning framework to counter cyber-physical attacks. *arXiv preprint arXiv:2409.15757*, 2025.

[28] Helmy Hanyff Hairudin Ruzaili and Mohamad Fadli Zolkipli. Security challenges in scada systems. *Borneo International Journal*, 7(2):12–26, 2024.

[29] GE Vernova. Navigating scada cyber security challenges, 2025.

[30] Washington University in St. Louis. Wustl-iiot-2018: Industrial internet of things dataset. Dataset, 2018. Available at: https://www.wustl.edu.

[31] Washington University in St. Louis. Wustl-iiot-2021: Industrial internet of things dataset. Dataset, 2021. Available at: https://www.wustl.edu.

[32] T. Chen, H. Zhang, and W. Li. Security challenges and solutions in scada systems: A survey. *Journal of Computer Security*, 25(1):1–30, 2017.

[33] Nesibe Yalçın, Semih Çakır, and Sibel Ünaldı. Attack detection using artificial intelligence methods for scada security. *IEEE Internet of Things Journal*, 2024.

[34] Zil E. Huma, Shahid Latif, Jawad Ahmad, Zeba Idrees, Anas Ibrar, Zhuo Zou, Fehaid Alqahtani, and Fatmah Baothman. A hybrid deep random neural network for cyberattack detection in the industrial internet of things. *IEEE Access*, 9:55595–55605, 2021.

[35] Abdulrahman Al-Abassi, Hadis Karimipour, Ali Dehghantanha, and Reza M. Parizi. An ensemble deep learning-based cyberattack detection in industrial control system. In *Proceedings of the IEEE*, 2020.

[36] Ali Alzahrani and Theyazn H. H. Aldhyani. Design of efficient based artificial intelligence approaches for sustainable of cyber security in smart industrial control system. *Sustainability*, 15(10):8076, 2023.

[37] Sayawu Yakubu Diaba, Theophilus Anafo, Lord Anertei Tetteh, Michael Alewo Oyibo, Andrew Adewale Alola, Miadreza Shafie-Khah, and Mohammed Elmusrati. Scada securing system using deep learning to prevent cyber infiltration. *Neural Networks*, 165:321–332, 2023.

[38] et al. Sara Tamy, Hicham Belhadoui. An evaluation of machine learning algorithms to detect attacks in scada network. In *Proceedings of the IEEE Conference on*, 2019.

A. Appendix

- AI : Artificial Intelligence.
- ML: Machine learning.
- DL: Deep Learning.
- PdM: Predictive Maintenance.
- GPU: Graphics Processing Unit
- IT: Information Technologies.
- 4IR: Industry 4.0
- CPS: Cyber-Physical Systems.
- kNN: k-Nearest Number
- DT: Decision Tree
- CNN: Convolutional Neural Network.
- GB : Gradient Boosting .
- RNN: Recurrent Neural Network.
- LSTM: Long Short-Term Memory.
- XGB : Extreme Gradient Boosting.
- IoT: Internet of Things.
- HMI: Human-Machine Interface.
- RUL: Remaining Useful Life.
- MTU : Master Terminal Unit
- PLC : Programmable Logic Controller