Intrusion Detection in SCADA Networks: From Traditional Approaches to Graph Convolutional Networks

Farisha K.R.
Department of Computer Science
Pondicherry University Puducherry, India

M. Nandhini, PhD
Department of Computer Science
Pondicherry University Puducherry, India

Sreeveni P.A.
Department of Computer Science
Pondicherry University Puducherry, India

ABSTRACT
Supervisory Control and Data Acquisition (SCADA) systems are widely used to control and monitor critical infrastructure such as power plants and water treatment facilities. These systems are part of Industrial Control Systems (ICS) and are increasingly integrated with IT and cloud infrastructures, which has significantly increased their exposure to cyber-attacks. To address these security challenges, several protective mechanisms have been developed for SCADA networks, among which intrusion detection systems (IDS) play a crucial role. This survey presents a comparative study of existing IDS approaches applied in SCADA systems, ranging from traditional rule-based, signature-based, and anomaly-based models to advanced machine learning and deep learning techniques. Furthermore, the strengths and limitations of these IDS approaches are analyzed to identify existing research gaps in SCADA-specific intrusion detection. Finally, a methodological direction aimed at improving IDS performance for effective detection and prevention of cyber-attacks on SCADA systems is discussed, providing valuable guidance for future research on SCADA-specific IDS.

General Terms
SCADA Security, Industrial Control Systems, Modbus

Keywords
SCADA Security, Intrusion Detection System, Graph Convolutional Networks, Critical Infrastructure

1. INTRODUCTION
In the early years, the design of the SCADA system was that of an isolated network, which was not connected to the corporate net- works. But with the growing need for technology development in the critical sector, the SCADA system was connected to the corporate networks and Internet of Things (IoT) systems, and thus the security environment for the SCADA system underwent a radical metamorphosis [1]. This has resulted in several instances of SCADA system attacks through the internet in the real world. The explosion in the Siberian pipeline and the attack at the Maroochy

Shire wastewater plant have identified the extreme vulnerabilities present in the early design of the SCADA system [2]. In the mean- while, the Stuxnet attack, which was targeted at the programmable logic controllers (PLCs), has identified the potential for the physical destruction of critical infrastructures through internet attacks [2].In order to secure SCADA in real-time, security measures need to be enforced without affecting the availability and reliability of industrial operations. Among these security measures, the role of intrusion detection systems (IDS) is highly significant. The technology of IDS has developed from traditional rule-based approaches towards more sophisticated approaches; however, some drawbacks still exist. Signature-based IDS, for example, are helpless against zero-day attacks, whereas anomaly-based IDS typically experience high rates of false alarms [3]. Additionally, in SCADA-based IDSs, often the lack of real-time coordination between multiple IDSs is highly detrimental regarding effectiveness. In more recent works within the literature for SCADA-based IDSs, machine learning (ML)-based approaches and deep learning (DL)-based approaches have been highly prevalent. This is primarily because SCADA communication naturally forms graphs, for which graph convolution networks (GCNs) have been shown highly capable of capturing structural information and anomalies suggesting malicious operations [4].

In the context of these advancements, the survey offers an in-depth discussion of intrusion detection mechanisms for SCADA networks and explores the benefit of combining IDS and automated firewalls for the real-time protection of unknown attacks. This paper begins by summarizing the basic concept of SCADA system architecture, the industrial threat environment, and the architecture of IDS and AFW. Following that, the article continues by covering multiple SCADA-based IDS schemes, including traditional schemes, ma- chine learning-based schemes, and deep learning-based schemes. Based on this discussion, the benefit of developing GCN-based IDS models in combination with AFW is considered for overcoming the aforementioned deficiencies. Lastly, the paper mentions the open issues in the SCADA-based IDS domain and proposes potential approaches for further advancements in the context of adaptive GCN-based IDS in conjunction with AFW and graph models for SCADA networks.

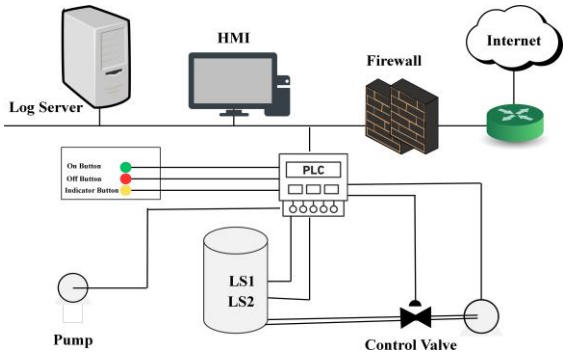

Fig. 1. Water Treatment SCADA System Architecture

2. BACKGROUND AND FUNDAMENTALS
2.1 SCADA Architecture
Supervisory Control and Data Acquisition (SCADA) systems con- sist of multiple layers, including the field layer, control

layer, and supervisory layer. The detailed components and operational work- flow of a water treatment SCADA system are illustrated in Fig. 1. SCADA systems use different protocols for the exchange of information between the different components of the system. Modbus protocol follows the server-client methodology, while the DNP3 protocol, which is more reliable, is used for the exchange of information between the master stations, remote terminal units (RTUs), and or intelligent electronic devices (IEDs). Although the protocols are adopted on a large scale, they are vulnerable to cyber attacks be- cause they do not possess any mechanism to ensure SCADA system security against cyber attacks [5]. The next section highlights the vulnerability associated with the SCADA network.

2.2 SCADA Network Threat Landscape

The threat landscape of the SCADA system defines the set of potential attackers and attack mechanisms, which clearly states who can launch attacks, in which manner these attacks can be per- formed, and which vulnerabilities can be exploited in SCADA. SCADA system architectures have matured from simple standalone systems to integrated IT and Cloud architectures, thereby significantly increasing the vulnerabilities of these SCADA systems for threats from cyber-crooks, hacktivists, and nation-states, giving rise to increasing instances of cyber-attacks. IT-based generic attacks that target SCADA systems include DNS poisoning attacks, net- work scanning, and phishing. Specific protocol-based attacks for SCADA include Modbus or DNP3 related attacks for protocol manipulation and session hijacking. SCADA system compromises can also be achieved through config-based manipulations like rogue master stations and improper modifications of PLC system config. Advanced SCADA system disruption attacks involve control pro- cess attacks like manipulation of the control process of SCADA and remote code execution for engineer workstations or PLCs [6, 7]. The typical threats to SCADA systems come in the form of attacks via virus infections, command injection, and replay attacks, which can lead to process interruption, tampering with the data, as well as physical damages to the SCADA infrastructure [8]. Owing to the threat exposure, it has become imperative to have effective security measures put in place. The next section highlights one of the most fundamental SCADA security measures, which is the intrusion de- tection system (IDS).

2.3 Intrusion Detection Systems in SCADA

The communication protocols being widely utilized in the exist- ing SCADA system, like Modbus, are lacking some basic security aspects, including authentication and encryption processes. The role of the Intrusion Detection System (IDS) is, therefore, imperative in shielding the SCADA system against these threats and has also developed from earlier detection methods to more modern approaches, as shown in Fig. 2.

Signature-based IDS identify threats by scanning traffic patterns against predefined signatures [9]. Anomaly-based IDS alert when there are differences from the expected normal behavior [10]. Specification-based IDS are guided by predefined rules and specifications, and yet the design and execution of these rules call for great domain knowhow and expertise [11]. Following these conventional methods, research and development work in the area of SCADA intrusion detection systems has advanced to more sophisticated techniques. Traditional machine learning-based IDS systems showed strong detection accuracy results but encountered scalability and adaptability issues to work in the industrial setting [10].

Nevertheless, each type of intrusion detection has some obvious limitations. For this purpose, the following section discusses the various intrusion detection systems already implemented in the context of SCADA systems.

3. EXISTING INTRUSION DETECTION TECHNIQUES

The SCADA systems that use legacy communication protocols face many security risks, especially considering that such systems control critical infrastructure. This section explores the development of Intrusion Detection Systems (IDS) and their contributions to SCADA security.

Initially, intrusion detection in SCADA focused on anomaly-based IDS, which identify deviations from normal operational patterns. Yang, Usynin, and Hines [12] proposed an anomaly detection method using the Auto associative Kernel Regression (AAKR) technique to model system patterns, coupled with the Sequential Probability Ratio Test (SPRT) to monitor deviations. This approach analyzed system input-output patterns, hardware performance, and low-level kernel parameters. It successfully detected Denial of Ser- vice (DoS) attacks but had limited performance for unseen attacks and was highly sensitive to normal process variations, leading to high false positives [12].

Signature-based IDS emerged as another traditional approach, us- ing known attack signatures or predefined rules. These systems are effective for known attacks with low false positives but perform poorly against zero-day attacks, requiring constant updates to the signatures. Common SCADA protocols like Modbus follow fixed request patterns, making subtle protocol attacks difficult to detect. To overcome the limitations of anomaly- and signature-based IDS, Specification-Based IDS (SIDS) was introduced. SIDS leverage pre-defined protocol rules based on official specifications. Nay et al. [11] describe SIDS as systems that analyze adherence to functional rules rather than relying solely on patterns or statistical anomalies. For Modbus-SCADA, SIDS can check function codes, command sequences, and data value ranges. These systems are effective for detecting insider misuse and protocol deviations, but re- quire domain expertise and frequent updates, limiting adaptability [11].

Recognizing these limitations, IDS research shifted toward Ma- chine Learning (ML)-based IDS, which can learn network patterns and adapt to changing conditions. Nay et al. [13] and Ahmed and

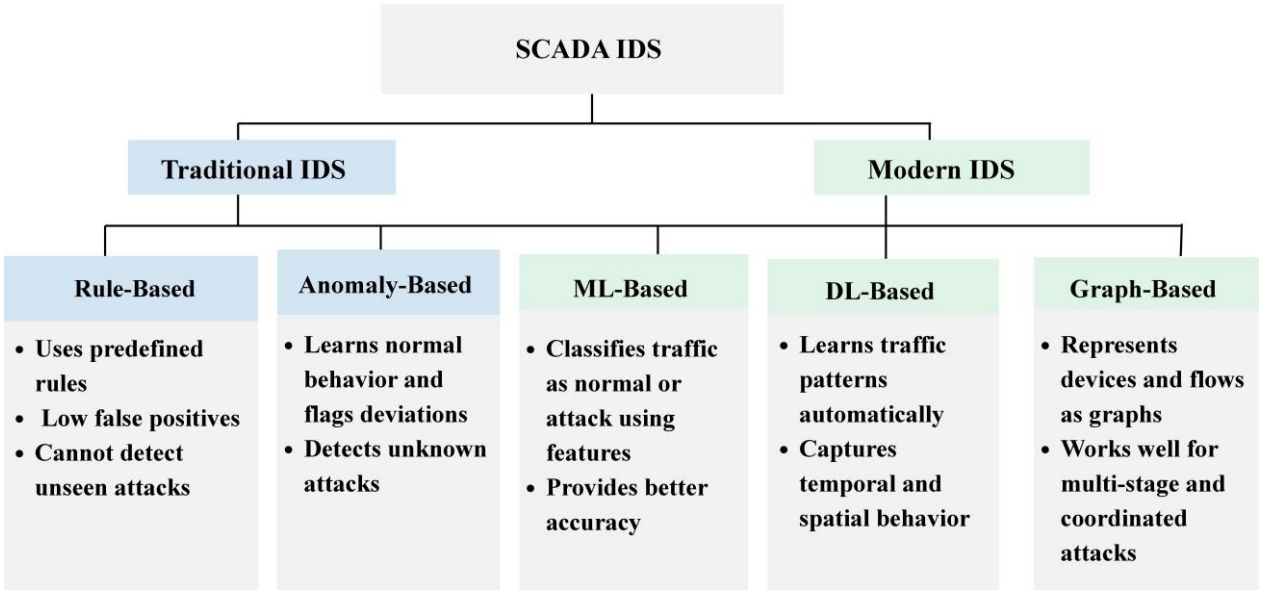

Fig. 2. Classification of intrusion detection systems

Tonoy [14] confirmed that ML-based IDS improve accuracy and adaptability compared to rule-based IDS. However, challenges include real-time scalability, interpretability of decisions, and performance in resource-constrained settings.

Although ML and deep learning (DL) approaches improve detection accuracy, most methods treat packets independently, ignoring structural relationships in SCADA networks. Graph-based IDS (Graph-IDS) address this by modeling SCADA devices as nodes and communication links as edges, capturing relational patterns. Balaba et al. [15] proposed a graph-based anomaly detection model that effectively detects flow-based attacks in industrial environments. Similarly, Alrumaih and Alenazi [16] introduced CGAAD, a Centrality- and Graph-Aware Deep Learning approach that lever- ages graph centrality to improve detection efficacy.

Table 1 summarizes different IDS approaches for SCADA systems, including datasets, detection focus, strengths, and limitations. The following section reviews these approaches comparatively, emphasizing their effectiveness against SCADA-specific operational, architectural, and security challenges.

4. COMPARATIVE ANALYSIS OF EXISTING INTRUSION DETECTION APPROACHES

A comparison of IDS approaches is necessary to achieve a view of the behavior that different IDS approaches will have within the SCADA environments. Table 2 provides a summary of the existing IDS techniques employed on SCADA systems and points out, by comparison, some relevant differences in the capabilities of their detection, adaptability, and computational requirements.

The comparison carried out in Table 2 shows that machine learning- and deep learning-based methods realize significant improvements concerning detection accuracy. However, most fail to model the relations and topological dependencies native in the patterns of SCADA communication. Contrariwise, graph-based IDSs are more context-aware and adaptable, thus making the detection of multi- stage and coordinated attacks feasible.

Yet, all IDS approaches have their own practical challenges while offering benefits: the limited availability of topology-rich industrial datasets, high computational overhead, and difficulties in real-time deployment. It is also evident that there is great motivation toward research in GCN-based adaptive IDS solutions by the need for an adaptive topology-aware intrusion detection framework in SCADA systems.

5. CHALLENGES AND OPEN RESEARCH PROBLEMS

Despite the promising results that current IDS solutions have shown, they also experience challenges that arise from the nature inherent in the SCADA environment. For example, rule-based and anomaly-based IDS would face difficulties in detecting new attack patterns because they utilize predefined rules and baselines. Ma- chine learning approaches in IDS offer improved accuracy, but they usually consider the network traffic independently, thereby ignoring the connections and dependencies between SCADA devices. A final challenge arises due to the dynamic nature of SCADA systems. A common occurrence here is the variety of continuous changes that happen to configurations, communications, and behaviors of SCADA devices. Most of the previous work done regarding IDS does not incorporate adaptability to adjust to dynamic changes without human intervention to affect real-time operations. This area shows there is a significant research gap to address.

Table 1. Summary of Existing Intrusion Detection Techniques for SCADA Systems

Model Type	Key References	Dataset / Testbed	Detection Focus	Strengths	Limitations
Rule-Based	Mohan et al. [17] (2020)	Simulated smart grid network	Node compromise, false data injection, replay attacks	Protocol-aware and deterministic detection	High rule complexity, limited scalability
Anomaly-Based	Yang et al. [12] (2013)	SCADA operational data	DoS and operational anomalies	Effective for unknown attacks	High false positives due to process variations
	Khan et al. [18] (2019)	SCADA testbed	Zero-day anomalies, protocol misuse	Multi-level anomaly coverage	Requires extensive tuning and data dependency
	Kreimel et al. [19] (2020)	Siemens substation testbed	MITM and DoS attacks	Capable of detecting unseen attacks	Needs domain expertise and labeled data
ML-Based	Nay et al. [13] (2024)	NSL-KDD, DS2OS, IoT botnet datasets	Normal vs abnormal traffic classification	High accuracy and adaptability	Interpretability and labeling requirements
	Idima et al. [20] (2025)	Wind turbine SCADA dataset	DoS and power output anomalies	High detection accuracy	Limited real-time adaptability
	Rajesh et al. [21] (2022)	Real-time SCADA testbed	Simulated SCADA attack scenarios	Realistic evaluation environment	Preprocessing overhead
DL-Based	Gao et al. [9] (2019)	Simulated SCADA, 10% KDD99	Packet-level attack detection	Simple architecture and high accuracy	Weak temporal dependency modeling
	Balla et al. [22] (2022)	Public SCADA/ICS datasets	DoS and multi-type attacks	Automated feature learning	High computational cost
Graph-Based IDS	Balaba et al. [15] (2025)	ICS communication datasets	Relational and flow-based attacks	Captures inter-device communication patterns	Scalability and computational overhead
	Alrumaih et al. [16] (2024)	ICS datasets	DoS, probing, insider threats	Graph-aware and interpretable detection	Limited real-time deployment

Table 2. Comparative Summary of Existing IDS Approaches for SCADA Systems

Criteria	Rule-Based IDS	Anomaly-Based IDS	Machine Learning IDS	Deep Learning IDS	Graph-Based IDS
Detection Performance	Effective for known attacks	Detects abnormal behavior	Improved generalization	High detection accuracy	Context-aware detection
Adaptability	Very poor	Moderate	Moderate	Moderate to high	High
Real-Time Feasibility	Excellent	Moderate	Moderate	Low to moderate	Low
Feature Requirements	Predefined rules required	Behavioral profiles needed	Manual feature engineering	Automatic feature learning	Graph-based feature extraction
Dataset Dependence	Very low	Requires clean normal data	Needs labeled datasets	Requires large labeled datasets	Requires topology-aware datasets
Advantages	Simple and fast	Detects unknown attacks	Balanced accuracy and efficiency	Strong pattern recognition	Rich contextual understanding
Limitations	Fails on unseen attacks	High false-positive rate	Feature design overhead	High computational cost	Graph construction overhead

This relates to incorporating an adaptive framework that focuses on modeling relational dependencies of SCADA devices.

The next section will present a proposed GCN-based adaptive intrusion detection system in SCADA networks that utilizes graph representations of SCADA traffic in order to address existing IDS scheme shortcomings that arise due to lack of understanding of SCADA network topology and behavior. This approach leverages the structural and communication patterns of SCADA components to improve anomaly detection accuracy. By capturing relationships that traditional IDS models often overlook, the proposed frame- work aims to provide a more adaptable and context-aware security solution for industrial control systems.

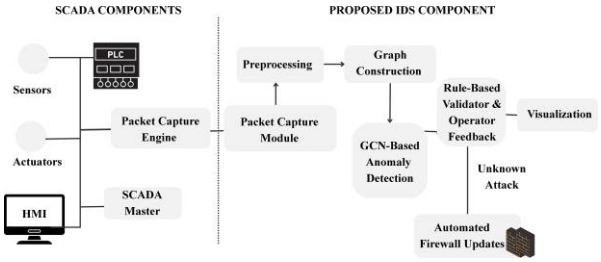

Fig. 3. Workflow of the proposed GCN-enabled intrusion detection system for SCADA

6. PROPOSED GCN-BASED ADAPTIVE IDS FOR SCADA SYSTEMS

To counter the rising issues associated with the current SCADA systems, this proposed work presents an adaptive intrusion prevention scheme through Graph Convolutional Networks (GCNs) for anomaly recognition in a SCADA environment. The basis of using GCNs for the scheme will be their efficiency in incorporating structural and communication relationships between the components of a SCADA system, which are usually not taken into consideration by the current intrusion prevention systems. The proposed framework is intended to improve adaptability and awareness of context based on the use of topology and communication patterns of the network, while still satisfying the severe constraint of industrial control systems. Fig. 3 illustrates the conceptual workflow of the proposed IDS, consisting of traffic acquisition, graph-based anomaly analysis, validation, and response mechanisms.

6.1 Traffic Acquisition and Packet Capture

The proposed IDS framework uses a non-intrusive traffic acquisition technique, which requires port mirroring of the SCADA traffic on the network. This technique ensures the acquired traffic does not interfere with the control process in the SCADA system.

The design conceptualized involves a packet capture module that will sniff or harvest plaintext network data and transmit it to the IDS module for analysis. The methodology prevents potential risks that can arise during inline implementation and can be effectively used in a safety-reliable SCADA environment because it performs passive monitoring operations.

6.2 Data Preprocessing and Extracting Features

In the proposed design, the process of preprocessing includes identification of the protocols, noise removal, aggregation of the flows, and normalization of the captured traffic. Unlike current IDS solutions that require extensive feature engineering, the proposed system concentrates on the identification of the required attributes for generating the graph.

This is expected to act as a conceptual means of lessening computational complexity while maintaining fundamental communication properties requisite for anomaly modeling within SCADA systems.

6.3 Graph Construction and GCN-Based Anomaly Detection

The central idea of proposed IDS is to abstract SCADA as a graph, where nodes represent SCADA elements, and communication links between elements are abstracted as edges. SCADA graph abstraction is capable of capturing structural as well as interaction aspects of SCADA.

In this regard, a Graph Convolutional Network is theoretically used for representation learning in a manner that aggregates information from neighboring nodes, and any deviation from communication patterns that are learnt is assumed to be an indicator of malicious activity. This model is very effective in detecting attacks that are a result of coordination and involve multiple stages and are, there- fore, very hard to detect with traditional methods of feature and sequence learning.

6.4 Automatic Response and Visualization

To enhance the concept in terms of resiliency as well as minimize the false positive ratio, the proposed framework for the IDS uses the hybrid verification process. This process makes use of the rule verification technique as well as the feedback process. This process is intended to make the adaptation process feasible.

After the confirmation of an intrusion, it involves automated actions in response to the intrusion, for instance, changing firewall rules and sending alerts. Furthermore, it encompasses the development of a visualization component that will support the operator in analyzing security events.

7. FUTURE RESEARCH DIRECTIONS

In future work on SCADA intrusion detection, there needs to be more focus on lightweight and explainable Graph Convolutional Networks, hybrid models for intrusion detection, topology-aware data set generation, and edge approaches for deployment. Such areas of focus are prominent for meeting the real-time needs and re- source constraints of industrial control settings.

In future, the implementation can also focus on incorporating the intrusion detection features of the GCNs in the reaction module, for example, the firewall and access control module, in order to efficiently counter the threats and improve the total security of the SCADA system.

In prospective studies, a SCADA system can be represented as a graph consisting of nodes and edges, where nodes symbolize important system components such as Programmable Logic Con- trollers (PLCs), Remote Terminal Units (RTUs), Human-Machine Interfaces (HMI), and sensors, and the edges represent their connectivity. By analyzing the network traffic and regular operations, it is hoped that graph representations will help in recognizing irregular interactions, which could not have been possibly accomplished through rule-based systems, machine learning techniques, or basic deep learning methods.

Future studies might therefore determine the capabilities of GCN- based approaches in order to analyze spatial and relational dependencies within dynamically changing SCADA traffic. Graph-based deep learning approaches are expected to capture insightful knowledge of complex attack behaviors and coordinated intrusion scenarios in highly interconnected SCADA environments by jointly taking into account node and edge features.

8. CONCLUSION

This work provides a systematic review of the developments in Intrusion Detection Systems from traditional rule-based methods to machine learning and deep learning solutions, and finally to graph models and the proposed use of Graph Convolutional Networks in SCADA security solutions. It is observed in the review that al- though traditional intrusions detection systems provide ease of use and implementation advantages, they have limitations in handling relationship data and high-level attacks.

Machine learning and deep learning methods show enhanced capabilities in detecting and adapting to different situations, though their efficiency remains dependent on the lesser aspects of structural connectivity and communication dependency, which always exist in the SCADA system. Based on these, graph representation can be considered for SCM to analyze topology and interaction.

In this context, graph models and GCN models of intrusion detection seem to have conceptual applicability regarding the complex communication patterns of SCADA systems. In graph models of intrusion detection, the communication patterns of the devices are represented by nodes and edges. This should improve the modeling of coordinated attacks that are difficult to model by simple learning methods.

Nevertheless, in view of the possible advantages presented and the areas in which they could be applicable and beneficial, there re- main some issues to be resolved in order for such solutions to be deployed in practice. These issues include the case of limited topology-aware SCADA datasets, the matter of scalability in the solution for the reality of real-time applications, the topology modification issues in operational topological structures, and the interpretability issues of the deep graph models.

Therefore, the focus of the upcoming study will be on the development of an optimal GCN-based intrusion detection system, as well as the development of a hybrid technique that uses traditional methods as well as graph-based learning in the SCADA environment.

9. REFERENCES

[1] D. Pliatsios et al., "A survey on SCADA systems: secure protocols, incidents, threats and tactics," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 3, pp. 1942–1976, 2020.

[2] M. Alanazi, A. Mahmood, and M. J. M. Chowdhury, "SCADA vulnerabilities and attacks: A review of the state- of-the-art and open issues," *Computers & Security*, vol. 125, p. 103028, 2023.

[3] B. Zhu and S. Sastry, "SCADA-specific intrusion detection/prevention systems: A survey and taxonomy," in *Proc. 1st Workshop on Secure Control Systems (SCS)*, 2010.

[4] R. Mohan and B. S. Narayana, "Distributed intrusion detection system using semantic-based rules for SCADA in smart grid," in *Proc. IEEE/PES Transmission and Distribution Conf. and Exposition (T&D)*, 2020.

[5] G. Yadav and K. Paul, "Architecture and security of SCADA systems: A review," *Int. J. Critical Infrastructure Protection*, vol. 34, p. 100433, 2021.

[6] N. R. Rodofile, K. Radke, and E. Foo, "Extending the cyber- attack landscape for SCADA-based critical infrastructure," *Int. J. Critical Infrastructure Protection*, vol. 25, pp. 14–35, 2019.

[7] A.B. Ajmal et al., "Last line of defense: Reliability through inducing cyber threat hunting with deception in SCADA net- works," *IEEE Access*, vol. 9, pp. 126789–126800, 2021.

[8] M. Robinson, "The SCADA threat landscape," in *Proc. 1st Int. Symp. for ICS & SCADA Cyber Security Research*, BCS Learning & Development, 2013.

[9] J. Gao et al., "Omni SCADA intrusion detection using deep learning algorithms," *arXiv preprint arXiv:1908.01974*, 2019.

[10] L. A. Maglaras and J. Jiang, "Intrusion detection in SCADA systems using machine learning techniques," in *Proc. Science and Information Conf.*, IEEE, pp. 626–631, 2014.

[11] H. S. Nay, M. O. Al-Kasassbeh, and M. A. Al-Akhras, "A sur- vey of specification-based intrusion detection systems," *Int. J. Computer Applications*, vol. 975, pp. 8887, 2015.

[12] D. Yang, A. Usynin, and J. W. Hines, "Anomaly-based intrusion detection for SCADA systems," in *Proc. NPIC&HMIT*, 2013.

[13] T. Nay, "Enhancing IoT security with AI-driven hybrid ma- chine learning and neural network-based intrusion detection system," *Babylonian J. Artificial Intelligence*, 2024.

[14] Ahmed and A. A. R. Tonoy, "Cybersecurity in industrial control systems: A systematic literature review on AI-based threat detection for SCADA and IoT networks," *ASRC Procedia*, 2025.

[15] S. Balaba et al., "Graph-based anomaly detection in industrial control systems," in *Proc. IEEE Ural-Siberian Conf. on Biomedical Engineering, Radioelectronics and Information Technology (USBEREIT)*, 2025.

[16] T. N. I. Alrumaih and M. J. F. Alenazi, "CGAAD: Centrality- and graph-aware deep-learning model for detecting cyberattacks targeting industrial control systems in critical infrastruc- ture," *IEEE Internet of Things Journal*, vol. 11, no. 13, pp. 24162–24182, 2024.

[17] S. N. Mohan, G. Ravikumar, and M. Govindarasu, "Distributed intrusion detection system using semantic-based rules for SCADA in smart grid," in *Proc. IEEE/PES Trans- mission and Distribution Conf. and Exposition (T&D)*, 2020.

[18] A. Khan et al., "HML-IDS: A hybrid-multilevel anomaly prediction approach for intrusion detection in SCADA systems," *IEEE Access*, vol. 7, pp. 89507–89521, 2019.

[19] P. Kreimel et al., "Anomaly detection in substation networks," *J. Information Security and Applications*, vol. 54, p. 102527, 2020.

[20] S. Idima, P. Nwaga, and P. Evah, "Comprehensive analysis of SCADA system data for intrusion detection using machine learning," *Global J. Engineering and Technology Advances*, vol. 22, no. 2, pp. 064–089, 2025.

[21] L. Rajesh and P. Satyanarayana, "Evaluation of machine learning algorithms for detection of malicious traffic in SCADA network," *J. Electrical Engineering & Technology*, vol. 17, no. 2, pp. 913–928, 2022.

[22] A. Balla et al., "Applications of deep learning algorithms for supervisory control and data acquisition intrusion detection system," *Cleaner Engineering and Technology*, vol. 9, p. 100532, 2022.