**LITERATURE REVIEW**

**“Multilayer Data-Driven Cyber-Attack Detection System for Industrial Control Systems Based on Network, System, and Process Data” F. Zhang, H. A. D. E. Kodituwakku:**

The growing number of attacks against cyber-physical systems in recent years elevates the concern for cybersecurity of industrial control systems (ICSs). The current efforts of ICS cybersecurity are mainly based on firewalls, data diodes, and other methods of intrusion prevention, which may not be sufficient for growing cyber threats from motivated attackers. To enhance the cybersecurity of ICS, a cyber-attack detection system built on the concept of defense-in-depth is developed utilizing network traffic data, host system data, and measured process parameters. This attack detection system provides multiple-layer defense in order to gain the defenders precious time before unrecoverable consequences occur in the physical system. The data used for demonstrating the proposed detection system are from a real-time ICS testbed. Five attacks, including man in the middle (MITM), denial of service (DoS), data ex-filtration, data tampering, and false data injection, are carried out to simulate the consequences of cyber attack and generate data for building data-driven detection models. Four classical classification models based on network data and host system data are studied, including k-nearest neighbor (KNN), decision tree, bootstrap aggregating (bagging), and random forest (RF), to provide a secondary line of defense of cyber-attack detection in the event that the intrusion prevention layer fails. Intrusion detection results suggest that KNN, bagging, and RF have low missed alarm and false alarm rates for MITM and DoS attacks, providing accurate and reliable detection of these cyberattacks. Cyber-attacks that may not be detectable by monitoring network and host system data, such as command tampering and false data injection attacks by an insider, are monitored for by traditional process monitoring protocols. In the proposed detection system, an auto-associative kernel regression model is studied to strengthen early attack detection. The result shows that this approach detects physically impactful cyber attacks before significant consequences occur. The proposed multiple-layer data-driven cyber-attack detection system utilizing network, system, and process data is a promising solution for safeguarding an ICS.10

**“Machine Learning-Based Network Vulnerability Analysis of Industrial Internet of Things,”M. Zolanvari, M. A. Teixeira, L. Gupta:**

It is critical to secure the Industrial Internet of Things (IIoT) devices because of potentially devastating consequences in case of an attack. Machine learning (ML) and big data analytics are the two powerful leverages for analyzing and securing the Internet of Things(IoT) technology. By extension, these techniques can help improve the security of the IIoT systems as well. In this paper, we first present common IIoT protocols and their associated vulnerabilities. Then, we run a cyber-vulnerability assessment and discuss the utilization of ML in countering these susceptibilities. Following that, a literature review of the available intrusion detection solutions using ML models is presented. Finally, we discuss our case study, which includes details of a real-world testbed that we have built to conduct cyber-attacks and to design an intrusion detection system (IDS). We deploy backdoor, command injection, and Structured Query Language (SQL) injection attacks against the system and demonstrate how a ML-based anomaly detection system can perform well in detecting these attacks. We have evaluated the performance through representative metrics to have a fair point of view on the effectiveness of the methods.

**“HML-IDS: A hybrid-multilevel anomaly prediction approach for intrusion detection in SCADA systems”I. A. Khan, D. Pi, Z. U. Khan, Y. Hussain, and A. Nawaz :**

Critical infrastructures, e.g., electricity generation and dispersal networks, chemical processing plants, and gas distribution, are governed and monitored by supervisory control and data acquisition systems(SCADA). Detecting intrusion is a prevalent area of study for numerous years, and several intrusion detection systems have been suggested in the literature for11cyber-physical systems and industrial control system (ICS). In recent years, the viruses seismic net, duqu, and flame against ICS attacks have caused tremendous damage to nuclear facilities and critical infrastructure in some countries. These intensified attacks have sounded the alarm for the security of the ICS in many countries. The challenge in constructing an intrusion detection framework is to deal with unbalanced intrusion datasets.

**“Anomaly detection in industrial control systems usinglogical analysis of data”T. K. Das, S. Adepu, and J. Zhou:**

Critical infrastructures, e.g., electricity generation and dispersal networks, chemical processing plants, and gas distribution, are governed and monitored by supervisory control and data acquisition systems (SCADA). Detecting intrusion is a prevalent area of study for numerous years, and several intrusion detection systems have been suggested in the literature for cyber-physical systems and industrial control system (ICS). In recent years, the viruses seismic net, duqu, and flame against ICS attacks have caused tremendous damage to nuclear facilities and critical infrastructure in some countries. These intensified attacks have sounded the alarm for the security of the ICS in many countries. The challenge in constructing an intrusion detection framework is to deal with unbalanced intrusion datasets, i.e. when one class is signified by a lesser amount of instances (minority class). To this end, we outline an approach to deal with this issue and propose an anomaly detection method for the ICS. Our proposed approach uses a hybrid model that takes advantage of the anticipated and consistent nature of communication patterns that occur among ground devices in ICS setups. First, we applied some preprocessing techniques to standardize and scale the data. Second, the dimensionality reduction algorithms are applied to improve the process of anomaly detection. Third, we employed an edited nearest-neighbor rule algorithm to balance the dataset. Fourth, by using the Bloom filter, a12signature database is created by noting the system for a specific period lacking the occurrence of abnormalities. Finally, to detect new attacks, we combined our package contents-level detection with another instance-based learner to make a hybrid method for anomaly detection. The experimental results with areal large-scale dataset generated from a gas pipeline SCADA system show that the proposed approach HML-IDS outperforms the benchmark models with an accuracy rate of 97%.

**“Efficient cyber attack detection in industrial control systems using lightweight neural networks and pca”M. Kravchik and A. Shabtai:**

Industrial control systems (ICSs) are widely used and vital to industry and society. Their failure can have severe impact on both the economy and human life. Hence, these systems have become an attractive target for physical and cyber-attacks alike. In this paper, we examine an attack detection method based on simple and lightweight neural networks, namely,1D convolutional neural networks and auto encoders. We apply these networks to both the time and frequency domains of the data and discuss the pros and cons of each representation approach. The suggested method is evaluated on three popular public datasets, and detection rates matching or exceeding previously published detection results are achieved, while demonstrating a small footprint, short training and detection times.