Grenze International Journal of Engineering and Technology, January Issue

Intrusion Detection in Higher Educational Institution using Industrial Internet of Things through Software Defined Network

Laboni Sarkar[1], Somsubhra Gupta[2] and Ranjan Kumar Mondal[3]
[1-3]Swami Vivekananda University, Barrackpore -700121, WB
Email: Slaboni1995@gmail.com, gsomsubhra@gmail.com, ranjankm@svu.ac.in

***Abstract*— The focus of the presented work is to identify and prevent intrusion using Industrial Internet of Things. The motivation behind this work is a huge University data especially the dissertation and Thesis which are of immeasurable intellectual property significance if commercialized properly. The idea here is to protect this IP potential documents from getting espionage besides other important documents. "Industrial Internet of Things (IIOT)" is application of Internet of Things (IoT) to industrial management, where many machines and equipment are connected and synchronized to increase overall productivity through third-party platforms and software. Benefits of industrial IoT acquisition include automation, optimization, removal of manual operations, and increased overall efficiency; nevertheless, security still has to be considered. Improving IIoT security is hampered by the size of security features and the lack of trustworthy security solutions. Alarming attacks using IIoT network device vulnerabilities have been observed within the past several years. Furthermore, the attackers can delve further into the network by taking advantage of the connections inside the vulnerabilities. These kinds of network security risks cost industries and companies' money, harm their reputations, and result in the theft of critical data. This study suggests an SDN-based intrusion detection system for industrial IoT environments that uses machine learning performances. The potential cost savings of implementing this system are significant, as it can identify attacks on IIoT networks and devices with 99.7% accuracy, thereby reducing the financial impact of these security risks. SDN is a methodology that allows software applications to govern a network intelligently and centrally. The SDN controller in our system analyzes traffic flow data and then applies a machine-learning algorithm to watch industrial IoT devices and network behavior before developing SDN switch flow rules.**

***Keywords*— IoT, IIoT, SDN. intrusion detection.**

I. INTRODUCTION

Precarious infrastructures, like the Internet, have long operated independently from extrinsic networks, for example, communication networks, energy systems, and manufacturing systems. But in these inflexible environments, cutting-edge technologies like software-defined networking and artificial intelligence are gradually being integrated to offer additional advantages like better quality and flexibility. The Software Defined Network is defined as follows: "The underlying network infrastructure is abstracted from the applications, network intelligence, and state are logically centralized, and the control plane and data plane are decoupled" [1].

Grenze ID: 01.GIJET.12.1.14_1

An SDN controller is created by centralizing switch control functions. After that, the switches execute orders from the SDN controller and act as packet-processing devices [2].
The SDN controllers can enhance network security and monitoring using deep learning and machine learning [3]. Another one of these technologies is the IIoT. Simple sensors, wearable technology, and smartphones are all part of the standard Internet of Things. Integrating automated systems with networked devices facilitates the collection, analysis, and creation of actions aimed at helping individuals accomplish specific tasks or gain insights from the process. It includes beacons in businesses, smart mirrors, and more. Using the advantages of the IoT in industrial process management, the IIoT is a creative attempt to create an intelligent manufacturing environment. To help businesses and industries operate more reliably and efficiently, industrial IoT focuses on big data, machine learning, and machine-to-machine (M2M) interactions. By showcasing its excellence, industrial IoT use redefines manufacturing and industrial segmentation. As seen in Figure 1, the IIoT is rapidly developing and encompasses a variety of services and sectors. Using intelligence and integrated sensors, the IoT may assist the hotel sector by anticipating customers' demands and comprehending their surroundings. The IoT offers countless opportunities for the healthcare industry. The IoT is the foundation of the telemedicine system. It is the practice of delivering healthcare using interactive audiovisuals and data communications. Academic institutions are also utilizing a variety of IoT applications. For instance, e-learning uses the IoT.

Fig. 1. IoT in altered sectors.

It appears that the financial services industry is embracing IoT as well. Insurance firms use telematics apps to predict and evaluate potential hazards that might lead to a customer claim. Energy firms usage of smart grids to gather analytics, enhance security, and facilitate quick restoration during a power outage. IoT is altering the way the retail market operates. The front of the stores is equipped with automated checkouts. This solution agrees employees to concentrate on company prospects and demands in place of spending time as cashiers. Manufacturing is one of the best instances of a sector embracing IoT applications. The manufacturers use the IoT to monitor production flow throughout the production process. Manufacturers can gauge the quality of their products with the support of data collected by IoT devices.
The Industrial Control System (ICS) is essential to the automated industry. The ICS comprises many controllers that monitor and regulate industrial facilities to ensure proper operations [4, 5]. ICSs come in various forms, including supervisory control, programmable logic controllers. Open architectural settings have replaced closed systems in industrial systems since the emergence of the Internet of Things. And industrial control systems are now susceptible to security flaws and assaults. According to a UK Government report, the average cost of a cyber-security breach for small and medium-sized businesses is projected to be between £75,000 and £311,000. For more prominent organizations, the price varies from £1.46m to £3.14m. A notable example of a cyberattack is the Stuxnet strike 2010 on a nuclear power plant in Iran. And in 2010, a SQL injection assault was carried out against oil corporations worldwide using a Trojan known as the Night Dragon. North American energy corporations were the target of Havex in 2014 and the Trojan dubbed Dragonfly in 2013 [6].

The most well-known attacks that block authorized consumers from using services they have paid for are "Distributed Denial of Service (DDoS) and Denial of Service (DoS)" assaults. Because they consume resources and deactivate services, these attacks have become significant security hazards for computer networks [7]. IIoT networks and devices are also impacted by DoS/DDoS attacks [8, 9, 10]. Attacks using jamming techniques are also used against IIoT networks and devices. During unsuccessful communication attempts, this attack uses fictitious signals to disrupt the IoT devices' ongoing radio broadcasts while draining their energy, bandwidth, CPUs, sensors, and memory [11, 12, 13]. Therefore, one of the most critical issues facing researchers today is the security of IIoT devices and networks. The deployment of security in IIoT networks and devices faces some difficulties. IIoT systems are heterogeneous systems with various device kinds, data types being exchanged and transmitted, communication channels, device resource levels, and system configurations. The difficulties with IoT security are a result of all these factors together. Second, when it comes to security, nominal function, and resilience, there is an enormous amount of study to be done since billions of devices are linked.

ICSs were previously closed from the outside world and operated as autonomous systems. They were, hence, impervious to assaults. However, due to the increased integration of 'ICSs with the Internet for industrial management and communication', these systems are now more susceptible to anomalies and cyberattacks. Due to the sensitive nature of industrial IoT systems, security has become a significant concern. The absence of security criteria in the communication protocols jeopardizes industrial Internet of Things systems' dependability, security, and availability.

II. Problem Statement

Industrial control systems, or ICSs, leverage IoT technology, which the IIoT utilizes. Because they operate constantly, ICSs generate a lot of data as well. Because of internet access, these systems are now susceptible to malicious assaults and network attacks. As a result, it is impossible to guarantee the data's integrity. Protecting IIoT devices besides the IIoT network is a severe issue that requires attention.

III. Limitations of Existing Work

The literature has examined several artificial intelligence-based intrusion detection and categorization systems. Most security frameworks created for industrial Internet of Things networks had a significant false alert rate. Moreover, they were unable to identify any unidentified network assaults. As a result, they were ineffective at preventing network assaults on industrial IoT networks, which led to expensive network damage, data loss, and revenue loss. Therefore, our framework applied SDN technology and machine learning algorithms to identify malicious assaults, network incursion, and aberrant behavior in industrial IoT devices and networks.

IV. Contributions of This Paper

Our article makes several substantial contributions.

- This article covers cyberattacks and security risks to the industrial Internet of Things ecosystem.
- We examine traffic flow data to provide an SDN-based security architecture to identify industrial IoT network infiltration.
- The primary goal of our work is to prevent evil attacks and security risks on IIoT networks and devices. To do this, we consider several assaults on industrial IoT setups, including man-in-the-middle, jamming, and DoS/DDoS attacks.
- We employ machine learning methods, such as SVM and Decision Tree, on a Software-Defined Network controller to identify early intrusions in a network or industrial IoT device. Based on the data analysis, we designed the SDN switches' flow rules.
- We use the NSL-KDD intrusion detection dataset to assess the suggested SDN-based security system.
- The evaluation's findings establish that the suggested framework offers excellent security efficiency and can identify malevolent intrusions and assaults in industrial IoT networks.

The foundation of IoT systems is made up of the leading IoT layers. Effective Internet of Things multilayered architecture may be developed using these layers as a foundation. We talk about these levels below.

- Perception Layer: It is the actual layer comprising machines, actuators, sensors, and other physical components. Gauges, meters, and probes are sensors that perceive and collect data about the industrial Internet of Things environment. Actuators convert electrical data from IoT systems into motion, as seen in robotic arms, motor controls, and lasers.

- Transport Layer: This layer uses WiFi, LPWAN, Ethernet, and ZigBee to transfer sensor data between the perception and processing layers.
- Processing Layer: Another name for this layer is middleware. The processing layer gathers and processes data from the transport layer [14].
- Application Layer: The application layer handles direct communication with end users. It is made up of a variety of programs, including corporate information services, mobile apps, and software for tracking devices. Every application has a protocol at the application layer. And IoT systems have a few more layers that meet the business requirements of Internet of Things systems. The following is a description of these layers:
- Edge Layer: This handles data preprocessing near the edge. It happens on network edge nodes such as gateways, local servers, etc.
- Business Layer: Decisions made by enterprises are made at this layer using data that has been gathered.
- Security Layer: A security layer covers all the Internet of Things above levels, including cloud security, device security, and connection security.

V. IIoT

The term "industrial IoT" describes the application of IoT in commercial and industrial contexts. The IIOt is the nexus of information and operational technology. A machine generates a preemptive alert on an impending malfunction; cloud-based intelligent factory floors get real-time updates on the state of raw material progress or assembly line output. These are prototypes of the factories and industries of the future. Control System for Industry: Industrial control systems are called industrial control systems: Hardware components and software integration that support and keep an eye on vital infrastructures [29].

VI. Mechanisms of IIoT

The IIoT might have different components depending on the need. Generally speaking, they fall into three categories, depicted in Figure 2 and covered below.

Fig. 2: Components of industrial IoT.

- Connectivity Technology: Data must be sent to the cloud after gathering data. The IIoT system receives directives from the cloud in a similar manner. Bluetooth, WiFi, LPWAN, mesh networks, and other wireless technologies are the backbone of industrial Internet of Things systems.

Data Analysis for IIoT Platforms: The industrial IoT system has software for examining received and sent data. Additionally, the program can decide and relay directives back to the edge controllers.

Industry 4.0

The term ‘industrial 4. 0’ means the ‘fourth industrial revolution. Industrial 4. 0’ is a term used interchangeably for the ‘fourth industrial revolution’. Undefined To enhance the learning experience and improve connections between the related disciplines focusing on supply chain and manufacturing industries, ‘Industry 4. 0’ combines material production and business processes Management, including the IIoT and intelligent manufacturing. It is well-defined as the current state and direction of manufacturing technology. Intelligent machines, or cyber-physical systems, are the foundation of Industry 4.0. These systems take advantage of contemporary control systems incorporated with software and have Internet addresses to connect to the Internet of Things. This approach creates new production methods, real-time optimization, and value creation possible by connecting production and goods to the network and allowing them to interact. The aim is to provide real-time asset and process monitoring, empowering processes to act independently and satisfy client demands.

VII. Proposed Methodology

This part provides a methodology for industrial IoT threat detection based on SDN. As seen in Figure 3, the proposed architecture consists of three parts: IIoT devices, a 'centralized SDN controller', with SDN-enabled switches.

- Any IoT-enabled equipment used in the industry is considered an IIoT device. Some examples include smart meters, intelligent irrigation devices, innovative frost systems, bright assembly lines, various sensors, etc. All these gadgets are connected to a defined switch with SDN capability.
- Every industry gets a Software Defined Network switch to connect equipment in that industry. It is a switch with security rules installed and supports the SDN technology. The Software Defined Network controller integrates traffic information from the SDN-enabled switches and oversees traffic distribution in IIoT devices.
- The 'SDN controller' is connected to the SDN switches connected to the IIot devices. The SDN controller uses machine learning to identify unusual traffic patterns and flow abnormalities. Consequently, the switches' flow rules are established.

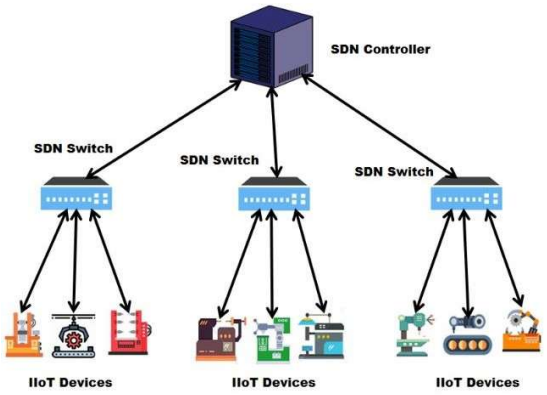

Figure 3. IIoT Anomaly Detection SDN-Based Model

The 'Software Defined Network'-enabled switch is connected to the IIoT devices operating in the same sector. The Software Defined Network-enabled switches send traffic flow data to the Software Defined Network controller, identifying abnormal or regular traffic flow. A Software Defined Network controller is equipped with a machine-learning algorithm for anomaly detection. By precisely forecasting potentially vulnerable hosts, machine-learning approaches can help create security rules for Software Defined Network controllers.

VIII. Data Analysis

The proposed framework's performance is evaluated using the NSL-KDD dataset employed in network intrusion detection. Instead of choosing a small piece of the dataset at random, this dataset allows tests to be conducted on the entire set at a fair cost due to the acceptable quantity of test and train set records. Each record has 41 properties, categorized as usual or assault type, explaining different flow components. Information on the five types of network connection vectors—those are separated into four attack classes and one regular class—is contained in the 42nd attribute. The following are some benefits of the NSL-KDD dataset:

- The test set has no duplicate records, which leads to better reduction rates;
- The train set has no duplicate records; hence, the classifier won't afford biased results.

This dataset contains 22 distinct assault types, categorized into four main categories. The four categories of attacks are DoS, R2L, Probe, and U2R.

IX. Data Preprocessing

Feature selection process takes place during data preprocessing to select the number of characteristics relevant for the model. We have also used what is appropriately known as 'Correlation based feature selection'. So, Correlation is the process of determining the extent of linear association between two or more variables. Correlation-based feature selection is used because desirable variables have a significant link with the aim. Additionally, there should be no correlation between the variables and a correlation between them and the goal.

If two variables are associated, we can predict one based on the other because the second feature doesn't add any new information, so the model needs one of two correlated features. Twenty-three uncorrelated characteristics were chosen for prediction using the correlation-based feature selection algorithm.
'Support Vector Machine': It is a supervised learning method for issue regression and classification. Regression and classification data analysis uses SVM kernels and algorithms. The objective of the SVM method is to draw a decision boundary, also known as the best line that can divide the n-dimensional space into classes such that fresh data points may be classified into the wrong category in the future. The hyperlink is the most significant line. Support Vector Machine selects the extreme points to create a hyperlink. The technique is termed a Support Vector Machine because the extreme points are referred to as support.
Decision Tree: Using a predetermined parameter to divide the data, the Decision Tree be a supervised machine-learning approach. The Decision Tree has two different kinds of entities: leaves and decision nodes. The leaves represent the results while the data is split on the decision nodes. Depending on the sort of target variable, decision trees can be of two types:

- Categorical Variable Decision Trees: Decision trees with categorical target variables fall under this category.
- 'Continuous Variable Decision Trees': Decision trees with continuous target variables fall under this category. The suggested Software Defined Network -based system successfully solves the IIoT network anomaly detection issue. The Software Defined Network switches provide monitoring data to the Software Defined Network controller with a global perspective. The Software Defined Network switches monitor the traffic flow of the IIoT devices, which forward each packet of flow to the Software Defined Network controller. The Software Defined Network controller uses the switches' data to identify unusual activity. The 'Software Defined Network Controller' uses the machine learning technique to identify potentially hazardous network traffic. This architecture is useful for detecting network anomalies since the 'Software Defined Network' controller establishes the traffic flow rules for the switches based on the categorized data.

X. Classification using SVM

Both the quadratic and linear Support Vector Machine classification models are used for the NSL-KDD dataset. Despite being a linear model, SVM has the advantage that its kernels may be used to represent data that is not linearly separable. Additionally, SVM is more effective in big dimensional spaces and requires a significant reduction in memory use. The linear and quadratic Support Vector Machine models use one hundred twenty-five thousand nine hundred seventy-three observations to classify the dataset. The quadratic Support Vector Machine classifier model is more correct than the linear SVM model. The linear SVM model predicts more quickly than the quadratic SVM model. The NSL-KDD dataset takes 699.22 seconds to classify using the linear SVM model, whereas the quadratic SVM requires 465.28 seconds.

XI. Classification using Decision Tree

A 'Decision Tree classifier model', namely the Fine Tree and Medium Tree models, is used to classify the NSL-KDD dataset. Finding the most significant factors and the connections between two or more variables is quick and easy with the help of a decision tree. They are swift and effective when compared to other classification methods. Furthermore, the decision tree requires less data and is free from outside influence and missing data. Classification of the dataset is based on 125,973 observations. The Satisfactory Tree classifier model has substantially greater accuracy than the Medium Tree classifier model. A Fine Tree classifier has a far faster prediction speed than a Medium Tree classifier. The Medium Tree classifier model requires 35.687 seconds for training, whereas the Fine Tree classifier model requires 11.029 seconds.

Table I: Fine Tree and Medium Tree Classification Results

Model Name	Accurateness	Expectation Speed	Training Time
Fine Tree	99.4%	570,000 obs/s	11.029 s
Medium Tree	95.9%	190,000 obs/s	35.687 s

XII. Performance an analysis

We categorized the data using the Decision Trees and SVM models. We employed the linear and Quadratic Support Vector Machine (QSVP) models in the SVM model and the fine tree and medium tree models in the Decision Trees. The QSVM model has the best accuracy of the three models, 99.7%, as the bar chart illustrates.

Our experiments' most accurate data categorization model is the quadratic SVM model. The Fine Tree classifier model take less time in predicting the new observation which is 570,000 obs/s more efficient than the other three models. Therefore, the Fine Tree Model represents the highest PREDICT-ONLY Speed that has been employedin our experimentation.

XIII. CONCLUSION

Deploying IoT in the industrial sector offers numerous advantages, including enhanced efficiency, automation, optimization, and removing human procedures. Security is still a problem for IIoT networks and devices, though. Cyberattacks and security risks to industrial IoT networks and devices result in financial losses, harm to a company's reputation, and the theft of critical data for industries and enterprises. Numerous methods and structures have been utilized to detect intrusions in IIoT devices and networks. These strategies heavily rely on machine learning techniques. In this study, we suggested an Software Defined Network -based framework to identify vulnerabilities and cyberattacks in IIoT devices and networks by utilizing machine learning techniques. In our experiment, we employed the NSL-KDD dataset for classification. We assess our system using SVM and 'Decision Tree classification models'. When the 'Support Vector Machine and Decision Tree' performances were compared, the Quadratic Support Vector Machine produced results with an accuracy of 99.7%. We want to utilize more recent data sources to improve our research's flexibility and effectiveness.

REFERENCES

[1] Xie, J., Yu, F. R., Huang, T., Xie, R., Liu, J., Wang, C., & Liu, Y. (2018). A survey of machine learning techniques applied to software-defined networking (SDN): Research issues and challenges. IEEE Communications Surveys & Tutorials, 21(1), 393-430.

[2] Yang, G., Shin, C., Yoo, Y., & Yoo, C. (2021, November). A case for SDN-based network virtualization. In 2021 29th International Symposium on Modeling, Analysis, and Simulation of Computer and Telecommunication Systems (MASCOTS) (pp. 1-8). IEEE.

[3] Sultana, N., Chilamkurti, N., Peng, W., & Alhadad, R. (2019). Survey on SDN based network intrusion detection system using machine learning approaches. Peer-to-Peer Networking and Applications, 12(2), 493-501.

[4] Asghar, M. R., Hu, Q., & Zeadally, S. (2019). Cybersecurity in industrial control systems: Issues, technologies, and challenges. Computer Networks, 165, 106946.

[5] Azzam, M., Pasquale, L., Provan, G., & Nuseibeh, B. (2023). Forensic readiness of industrial control systems under stealthy attacks. Computers & Security, 125, 103010.

[6] Venkatachary, S. K., Prasad, J., & Samikannu, R. (2018). Cybersecurity and cyber terrorism-in energy sector–a review. Journal of Cyber Security Technology, 2(3-4), 111-130.

[7] Ali, T. E., Chong, Y. W., & Manickam, S. (2023). Machine learning techniques to detect a DDoS attack in SDN: A systematic review. Applied Sciences, 13(5), 3183.

[8] Verma, A., & Ranga, V. (2020). Machine learning-based intrusion detection systems for IoT applications. Wireless Personal Communications, 111(4), 2287-2310.

[9] Marinov, M. B., Nikolov, N., Dimitrov, S., Todorov, T., Stoyanova, Y., & Nikolov, G. T. (2022). Linear interval approximation for smart sensors and IoT devices. Sensors, 22(3), 949.

[10] Debauche, O., Mahmoudi, S., & Guttadauria, A. (2022). A new edge computing architecture for IoT and multimedia data management. Information, 13(2), 89.

[11] Xiao, L., Wan, X., Lu, X., Zhang, Y., & Wu, D. (2018). IoT security techniques based on machine learning: How do IoT devices use AI to enhance security? IEEE Signal Processing Magazine, 35(5), 41-49.

[12] Uyanık, H., & Ovatman, T. (2022). An investigation of the transmission success in Lorawan enabled IoT-HAPS communication. Internet of Things, 20, 100611.

[13] Morais, R., Mendes, J., Silva, R., Silva, N., Sousa, J. J., & Peres, E. (2021). A versatile, low-power and low-cost IoT device for field data gathering in precision agriculture practices. Agriculture, 11(7), 619.

[14] Burhan, M., Rehman, R. A., Khan, B., & Kim, B. S. (2018). IoT elements, layered architectures and security issues: A comprehensive survey. sensors, 18(9), 2796.

[15] Xin, Y., Kong, L., Liu, Z., Chen, Y., Li, Y., Zhu, H., ... & Wang, C. (2018). Machine learning and deep learning methods for cybersecurity. Ieee access, 6, 35365-35381.