JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Improve Security of Industrial IoT Intrusion Detection System using Machine Learning : A Comparative Study

[1]Trashank Chouhan, [2]Devendra Kumar Meda
[1,2] Department of Electronics and Communication
[1,2] Jabalpur Enguneering College,Jabalpur,India

Abstract: Machine learning is a branch of artificial intelligence that focuses on developing algorithms. An interconnection between electronic devices through the Internet is known as the Internet of Things. Internet of Things is a connection between devices and it exchanges information between devices. But the main concern lies in the IoT devices which are more prone to cyber attacks like malware attacks, phishing etc. We try to improve the security of industrial intrusion detection system with the help of several methods of machine learning. The accuracy of the system tries to reach 94.27% to 99.97%.

Keywords: Machine learning, Internet of Things, Intrusion Detection System, Security.

I. INTRODUCTION

The Internet of Things (IoT) has a wide range of applications, from smart home appliances to large critical appliances. Such networks of devices equipped with sensing, communication and unique identifiable characteristics. The widespread adoption of connected services using IoT devices and networks has helped IoT applications grow [1]. Despite its strong presence in our daily lives. IoT remains a difficult concept to understand. The main purpose of IoT devices is to protect against cyber attack. IoT devices easily become targets or middlemen for attack.

Machine learning is a systematic process of deriving knowledge patterns from well defined inputs. Many researchers use DL and ML techniques to develop industrial IoT based intrusion detection systems capable of detecting attacks in IoT environments. Industrial IoT is a subset of IoT, which is the application of IoT applied to industrial process by facilitating internet connection of entities such as switches, automation systems, sensors, controllers, etc. Industrial IoT systems have a huge database about plants such as nuclear power plant. Which are vulnerable to various types of cyber attacks due to both IoT and Industrial IoT systems. These cyber attacks can damage industrial IoT systems and steal databases and change the behavior of automation systems that the industry is working on [2].

In the case of industrial control systems, security is as important as the concept of security. Security addresses such concerns as ensuring the protection of humans, the environment, and equipment against the consequences of system failures. To understand the importance of some critical industrial infrastructure, think about a nuclear plant using Industrial IoT systems and the consequences of a cyber attack on this infrastructure [3].

In November 2020 the Kundakulam Nuclear Power Plant which is the largest nuclear power plant in India was targeted through a cyber attack. We develop Intrusion Detection System (IDS) to protect industrial IoT systems but the main challenge of the system is to deal with the accuracy of the system. Cyber Attacks on Industrial IoT System In order to counter cyber attack increased day by day, we have to increase the accuracy of Industrial IoT System.

There are many types of cyber attacks: 1. Phishing; 2. Denial-of-Service Attack; 3. Malware; 4. SQL Injection; 5. DNS Tunneling; 6. Colonial Pipeline - Ransom ware Attack; 7. Install malware or additional harmful software; 8. Supply Chain Attack.

The development of machine learning technology has brought new solutions. Because it can adapt to changes in the environment through continuous learning. Industrial IoT is targeted by cyber criminals because content accessible in those networks can include valuable and confidential manufacturing and production data. Through machine learning technology, we can combat the problem of cyber attacks and improve the accuracy of industrial IoT systems [4].

II. LITERATURE SURVEY

The rapid growth of Internet of Things (IoT) devices has introduced various security challenges, including the need for effective intrusion detection systems (IDS). Machine learning techniques have shown promising results in detecting and mitigating IoT-related security threats. This literature survey aims to provide an overview of the existing research on machine learning-based IoT intrusion detection systems. This comprehensive survey highlights the challenges and opportunities in designing intrusion detection systems for IoT environments. It covers different types of attacks, existing IDS architectures, and discusses machine learning-based solutions. Although not specifically focused on IoT, this survey provides an excellent overview of machine learning approaches used in traditional intrusion detection systems. It covers various machine learning algorithms, feature selection techniques, and evaluation metrics. Industrial IoT systems have immense potential to transform industries by enabling connectivity, data collection, and intelligent decision-making. This literature review has provided an overview of the existing research on industrial IoT systems, covering topics such as architecture, applications, challenges, and future directions. Researchers and practitioners can refer to these papers to gain insights into the current state-of-the-art in industrial IoT and identify key areas for further exploration and innovation.

III. INTRUSION DETECTION APPROACHES IN IOT

Signature-based Approach: Signature-based detection system separates malicious from standard traffic patterns and application data. Signature-based detection system is a style of detection, unique identifiers are generated about a known attack so that any attack of that kind is rapidly dealt with it [6].

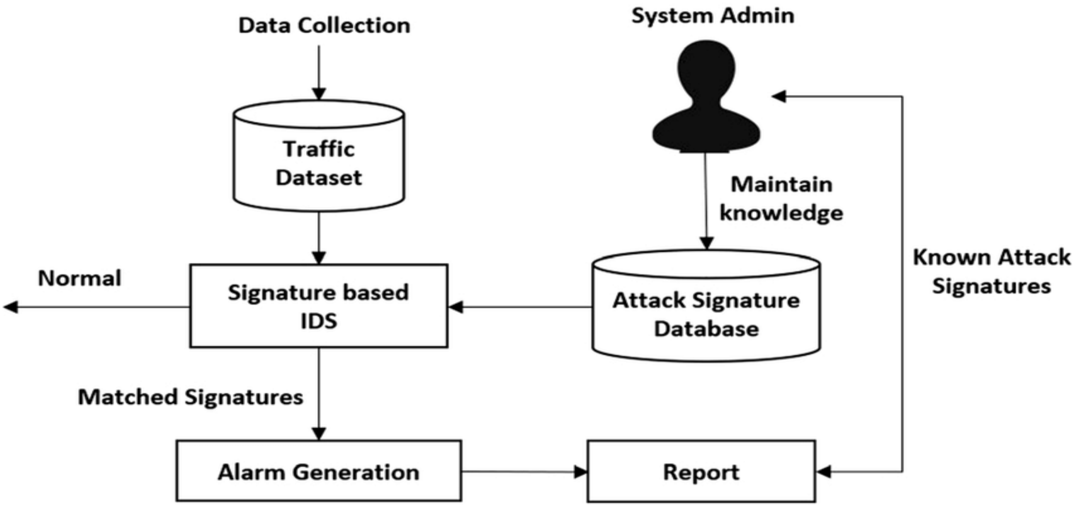

Fig. 1. Signature based Approach

Anomaly-based Methods: Anomaly-based methods, also known as anomaly detection or outlier detection, are techniques used in machine learning and data analysis to identify patterns that deviate significantly from the norm or expected behavior. The goal is to detect unusual or anomalous instances that may indicate potential security threats, system failures, or fraudulent activities. Anomaly-based methods find applications in various domains, such as cyber security, fraud detection, network monitoring, system health monitoring, and predictive maintenance. For example, in cyber security, anomaly detection can help identify unusual network traffic patterns that may indicate a potential intrusion or malicious activity. In industrial systems, it can detect abnormal sensor readings that may indicate equipment failures or anomalies in the manufacturing process [7].

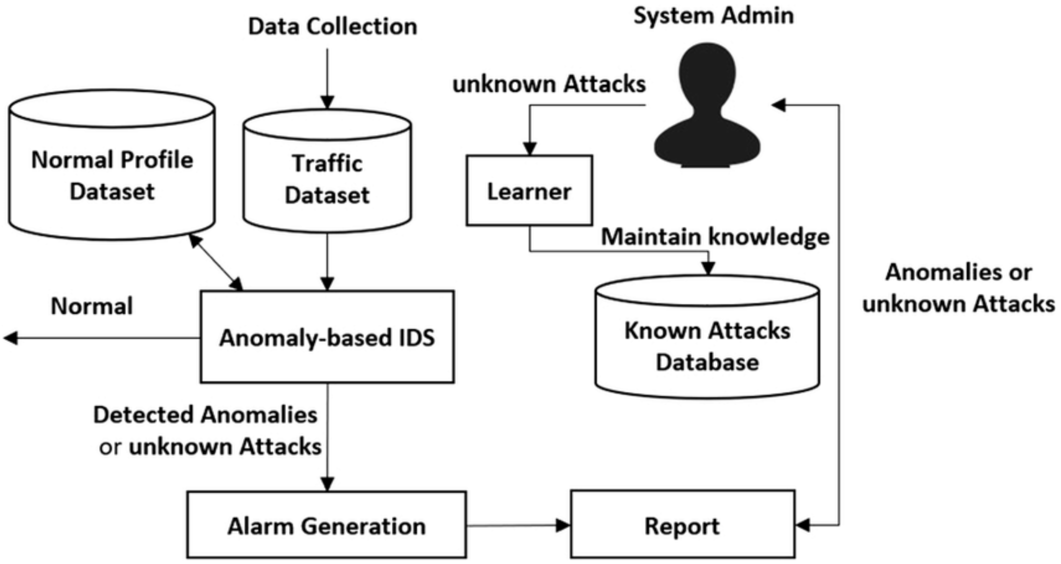

Fig. 2. Anomaly based Approach

Hybrid Methods: A hybrid intrusion detection system (IDS) combines multiple detection techniques or approaches to enhance the accuracy and effectiveness of intrusion detection in computer networks or systems. It aims to leverage the strengths of different detection methods while compensating for their individual limitations. The hybrid approach combines two or more types of IDS, typically signature-based and anomaly-based detection, to achieve comprehensive threat detection. By combining signature-based and anomaly-based detection, a hybrid IDS can mitigate the limitations of individual methods and provide more robust intrusion detection. The signature-based component can quickly identify known attacks, while the anomaly-based component can capture novel or evolving threats. The hybrid system can leverage the strengths of both approaches to achieve higher accuracy, reduce false positives, and provide a comprehensive defense against a wide range of attacks [8].

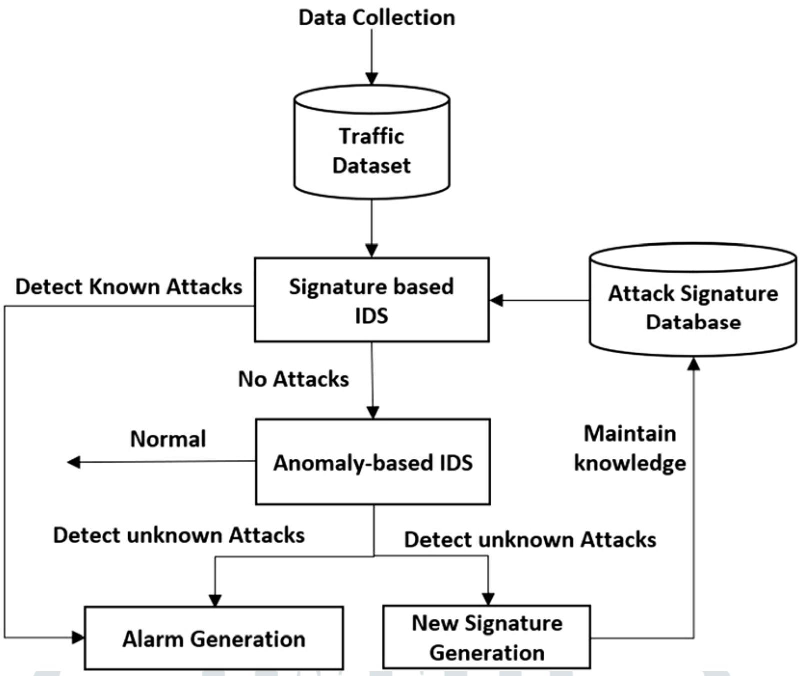

Fig. 3. Hybrid Approach

IV. MACHINE LEARNING ALGORITHM FOR IOT INTRUSION DETECTION SYSTEM

Support Vector Machines (SVM): SVM is a popular algorithm for intrusion detection because it can handle both linear and non-linear data. It is effective in classifying data into different categories based on their features**.**

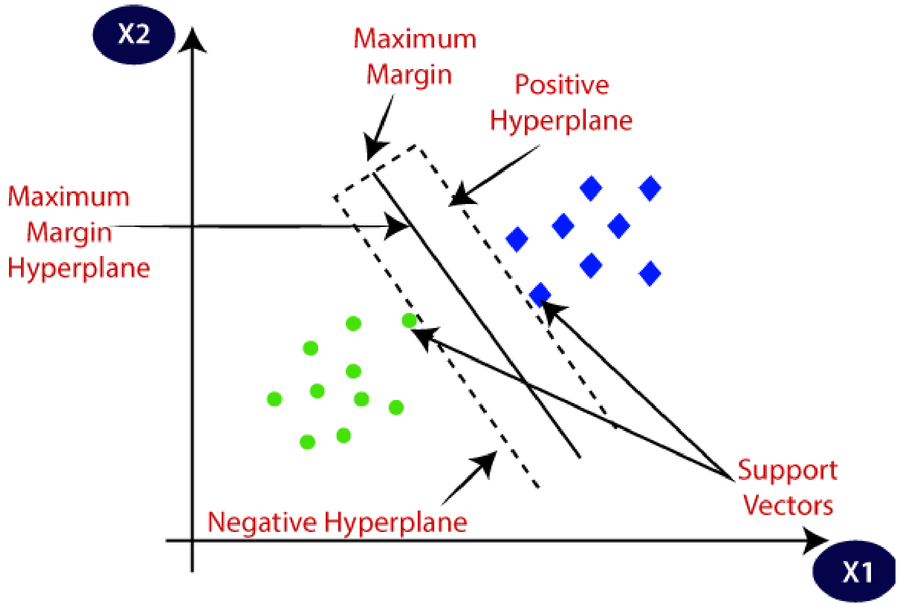

Fig. 4. Graph of Support Vector Machines Algorithm

Random Forest: Random Forest is an ensemble learning algorithm that uses multiple decision trees to classify data. It can handle large datasets and is known for its accuracy and ability to detect complex patterns in data.

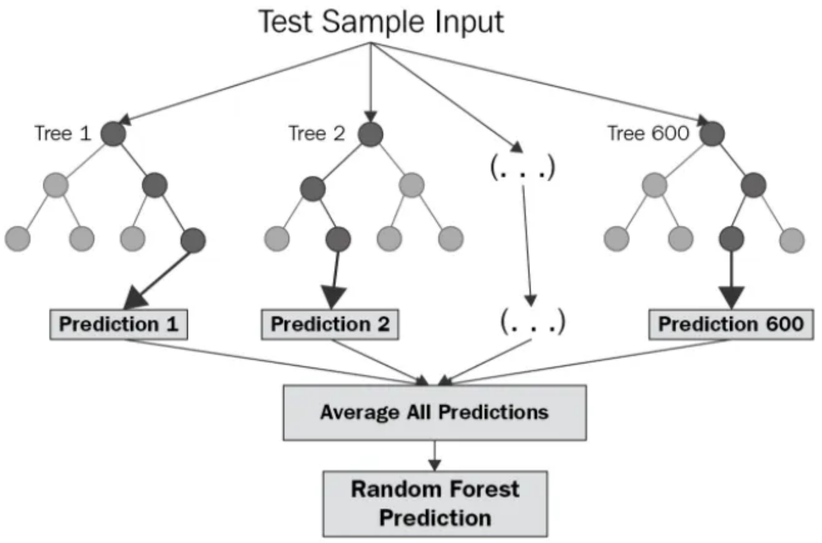

Fig. 5. Random Forest Prediction

K-Nearest Neighbor (KNN): KNN is a simple and effective algorithm for intrusion detection. It classifies data based on the proximity of the data points to each other in the feature space. KNN is effective in detecting outliers and can adapt to changes in the data over time.

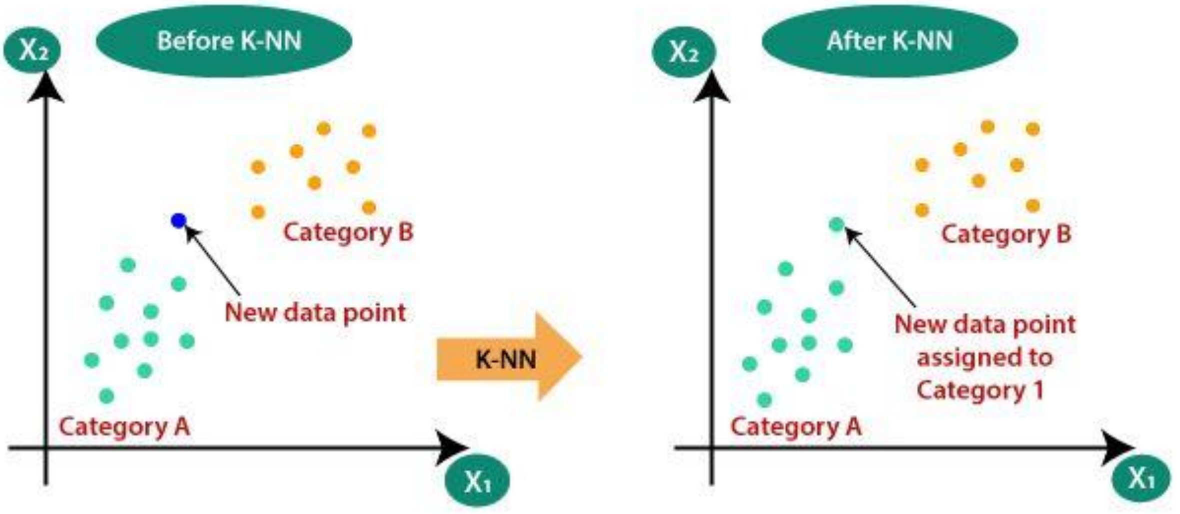

Fig. 6. Graph of K- Nearest Neighbor Algorithm

Deep Learning: Deep Learning algorithms, such as Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs), are becoming increasingly popular for intrusion detection. They are effective in detecting complex patterns in data and can adapt to changes in the data over time [10].

Naive Bayes: Naive Bayes is a simple and fast algorithm that is effective in classifying data into different categories based on their features. It is particularly useful for detecting spam and phishing attacks in IoT environments.

V. CONCLUSION

In this paper we have discussed various machine learning approaches for intrusion detection systems for IoT networks and machine learning algorithms for IoT intrusion detection systems. After a general introduction to IoT and Industrial IoT (IIoT), security in IIoT, specifically industrial control systems, is described. Applications cannot be limited on machine learning, which acts as a universal process for a wide variety of industrial and technological flows with IoT systems. In the digital world, IoT interconnects all the devices or gadgets into a single system. In response to different attack types, network intrusion detection methods are summarized as three categories, signature-based, anomaly-based, and hybrid approaches.

References

[1] Amar Amouri, Vishwa T Alaparthy, and Salvatore D Morgera. 2020. A machine learning based intrusion detection system for mobile Internet of Things. Sensors 20, 2 (2020), 461.

[2] Hansong Xu, Wei Yu, David Griffith, and Nada Golmie. 2018. A survey on industrial Internet of Things: A cyber physical systems perspective. IEEE Access 6 (2018), 78238–78259.

[3] Bijoy Babu, Thafa salIjyas, MuneerP., and Justin Varghese 2017. Security issues in SCAD A based industrial control systems. In 2017 2nd International Conference on Anti Cyber Crimes (ICACC). IEEE, Abha, SaudiArabia.

[4] Abhishek Verma and Virender Ranga. [n.d.]. Machine Learning Based Intrusion Detection Systems for IoT Applications. 111,4([n.d.]), 2287–2310.

[5] Nagaraj Balakrishnan, Arunkumar Rajendran, Danilo Pelusi, and Vijayakumar Ponnusamy. 2021. Deep Belief Network enhanced intrusion detection system to prevent security breach in the Internet of Things. Internet of things 14 (2021), 100112

[6] Philokypros Ioulianou, Vasileios Vasilakis, Ioannis Moscholios, and Michael Logothetis. 2018. A signature-based intrusion detection system for the Internet of Things. Information and Communication Technology Form (2018).

[7] Xiali Wangand Xiang Lu. 2020. A host-based anomaly detection frame work using XG Boost and LSTM for IoT devices. Wireless Communications and Mobile Computing 2020 (2020).

[8] Pradeep Singh and M Venkatesan. 2018. Hybrid approach for intrusion detection system. In 2018 International Conference on Current Trends towards Converging Technologies (ICCTCT). IEEE, 1–5.

[9] 2021. A new distributed architecture for evaluating AI-based security systems at the edge: Network TON_IoT datasets. Sustainable Cities and Society 72 (2021), 102994.

[10] Mohammed Ali Al-Garadi, Amr Mohamed, Abdulla Khalid Al-Ali, Xiaojiang Du, Ihsan Ali, and Mohsen Guizani. 2020. A survey of machine and deep learning methods for internet of things (IoT) security.IEEE Communications Surveys &Tutorials22, 3(2020), 1646–1685.