Explainable Artificial Intelligence Based Industrial Internet of Things Using Machine Learning and Fog Computing

***Abdulazeez Yusuf[1], Uba Yusuf Magaji[2], Salim Ahmad[3], Idris I. A. [4]**

[1]Department of Computer Science
Federal University Dutse

[2]Department of Software Engineering
Federal University Dutse

[3]Deparment of Information Technology
Federal University Dutse

[4]Sokoto Energy Research Center
Energy Commission of Nigeria

Corresponding Author: Ludbaw23@gmail.com

Abstract
The industrial internet of things (IIOT) is fast developing and gaining popularity among industries, this is attributed to its huge potentials in revolutionizing the production cycles. Thus resulting in profit maximization and reduced cost of production and services. These benefits are indeed enticing, but the lack of guaranteed security and copy right protections has created hesitance among many industries which resulted in scepticism to the wide adoption of IIOT by many other industries. Therefore, there is a need to elucidate the potentials of IIOT towards addressing their concerns, considering the pace at which cyber threats are emerging. This research aims at improving the acceptance of IIOT among industries by developing a robust and resilient IIOT network architecture that will reliable and trusted, which have the capabilities of early detection of threats, continuous normal operations even when known or unknown threats are encountered and during routine maintenance and when internet connectivity is interrupted using fog computing, machine learning (ML) and explainable artificial intelligence (AI) techniques. Fog computing and machine learning were used in network design and traffic monitoring while explainable AI was used to for interpretation of the rules used by the machine learning algorithm in detecting and responding to the threats. Thus eliminating the "black box" nature of artificial intelligence techniques and ensuring that the industries are more involved in the security and copy right protection management of their products.

Keywords: internet of things, fog computing, explainable artificial Intelligence, machine learning, industry 4.0

INTRODUCTION

The Internet of Things (IoT) is a system of interrelated devices that are connected to a network and to each other, exchanging data without necessarily requiring human-to-machine interaction (Park, 2019). It may also be considered as a network of physical objects or things empowered with limited computation, storage, and communication capabilities which are embedded with electronic elements such as sensors, actuators, microcontroller, software and network connectivity that enables them to collect, sometime process, and exchange data (Hussain *et. al.,* 2019). The sensors convert data and information received from IoT environment into signal which the actuators act upon to generate the required output. Application of IoT paradigms to various operational processes in the industry is referred to industrial internet of things (IIoT) or Industry 4.0 when IoT is applied to manufacturing industries. The IIoT is majorly concerned about how scarce resources could be used in achieving optimal performance in the areas of production, safety and security without necessarily incurring extra cost to the industries. Presently, we are experiencing a more comprehensive connectivity of different types of devices connected to the web; ranging from smart industries, smart medical devices, smart homes and smart cities. Indicating the rapidness in the growth and acceptance of IoT in different environments. Thus, it is undoubtedly a major research breakthrough in the field of computing and widely anticipated to continue to be the future of different technological advancements in businesses, industrialization and other socio-economic development, due to its promising potentials in improving and addressing numerous challenges in different sectors of our day to day activities.

This innovation needed to be constantly researched in order to continuously guarantee the safety, security and privacy of the IoT networks and in particular the IIoT networks due to its sensitivity. Because, any slight compromise in the IIoT network could have a devastating effect the network and the whole industrial setup may be affected.

A. The Need of Fog Computing in Improving IIOT Networks

Fog computing technique Koen *et al.,* (2020) can help in improving the IIoT networks in the following area:

I. It can serve as a storage source closer to base stations using fog nodes attached to devices where generated data could be temporarily stored and examine before onward transmission to the cloud or another station.

II. It could be used in providing intermediate connectivity due to attacks or when routine maintenance is being carried out on the network. Meaning only a section of the network will need to be disconnected. Therefore, operations of the industry will not have to be totally shutdown.

B. The Prospect of Machine Learning towards Improving IIOT Networks

Machine learning is an aspect of artificial intelligence (AI) that trains computer algorithms to learn the normal, regular behaviour and expected outcomes of systems after a series of trainings in order to perform certain actions on the system based on some already established rules Sadaf& Sultana, 2020; Dieber & Kirrane, 2022) such:

I. Machine learning algorithm can be adopted in monitoring the normal and regular behaviour of the various devices, networks and detection of any anomaly in the IIoT network.

II. Machine learning algorithms can be used to examine the patterns of the data generated by each device and network sub stations before and after transmission to ensure data protection and safety.

C. CAUSES OF HESITANCE TO IIoT ADOPTION

The numerous benefits of IIoT towards transforming industries cannot be over emphasized. Though, there are still some factors creating hesitance to the adaptation of IIoT technologies among industries which are major challenge that needs to be addressed if the potentials of this emerging technology is to be fully realized. Some of the factors causing hesitance among these industries include:

I. *Network security:* network security is a broad and sensitive component of the IIoT coincidentally, it is a major weakness that hinders the wide acceptability of IIoT by industries because it is highly targeted by malwares and other forms of threats. Therefore, there is need to constantly improve on network security to guarantee the security of IIOT and be steps ahead of any possibility of a cyber-attack. This will decrease hesitance and improve the confidence and trust among the industries. It will also encourage other industries to adopt the IIoT technology.

II. *Network Resilience:* threats and attacks are fast emerging and designed with the aim of causing maximum effect without been noticed or detected. It is therefore necessary to develop IIoT networks that are resilient and have the capability of early detection and reaction in order to minimize the impact of cyber-attacks on the IIoT network infrastructures and the industries as a whole.

III. *Network Maintenance*: routine network maintenance and device updating are expected to be regular occurrences in IIoT networks to guarantee maximum protection which in some cases might require total or partial shutdown the IIoT networks. During the periodic maintenance, productions will be temporarily suspended or unavailable thereby causing some inconvenience to the industries especially those that needed to always operate. This may create hesitance to regular network maintenance and device update especially when a threat is not envisaged. The continuous postponement of

network maintenance and device update may later render these networks vulnerable to emerging threats. There is need to design a network architecture which allows routine maintenance without necessarily halting the normal operations of the industries. This will encourage industries to regularly update their network and devices to ensure an up-to-date protection.

IV. *Data protection and Sharing:* data protection is of utmost importance in IIoT just like in any digital environment where internet connectivity is required. Data need to be protected and transferred from the source to the target destination in a safe and secured manner to ensure confidentiality which is a key security requirement of the industries. The fact that most data sharing based technologies do not indicate any evidence of intellectual property protection is a major concern to industries and further discourage some from adopting IIoT.

RELATED WORKS

The increasing demand for devices, products and services that have internet connectivity have rapidly transformed the market of "smart things" and encouraged many companies to engage in invention and manufacturing of devices, products and services that satisfy the market demand. According to the research of Andročec & Vrček, (2018) the main motivation of these companies is to release their products and services as fast as possible, to gain competitive advantage in the market. Therefore, many of these products and services are not designed with security in mind. This has made a lot of IoT devices, services and networks vulnerable to various security and privacy challenges. Especially, due to the possibility of having several access points in the network. IoT was defined by the institute of electrical and electronic engineering (IEEE) as a network of systems consisting of actuators, sensors, and smart objects whose purpose is to interconnect 'all' things, including day-to-day and industrial objects, in such a way as to make them intelligent, programmable, and more competent of interacting with humans and each other. In the work of Yusuf *et.al.*, (2019) IoT was defined as an open and comprehensive network of intelligent objects that have the capacity to auto organize, share information, data and resources, reacting and acting in the face of circumstance and transformation in the environment. The work also indicated that the most significant aspect of IoT is security.

According to Arafatur & Taufiq, (2019) the IoT paradigm is aimed at formulating a complex information system with the combination of sensor data acquisition, efficient data exchange through networking, machine learning, artificial intelligence, big data, and clouds. Conversely, collecting information and maintaining the confidentiality of an independent entity, and then running together with privacy and security

provision in IoT is the main concern. However, the massive amount of data being exchanged as well as the way it is being processed in the cloud and edge devices of IoT platforms may not always leverage upon secure and reliable protocols and mechanism. Therefore, with so many IoT devices, applications and services already in use, and many more are expected to continuously come online; IoT security and performance are of utmost importance. Poorly secured IoT devices and services will serve as entry points for cyber-attacks, which may compromise sensitive data and threaten the safety of individuals and organizations using IoT services.

The research work of Park, (2019) describes IoT as a network that creates linkages and connections between physical devices by incorporating software applications that can allow users to access information and control their devices from anywhere using a variety of internet-connected devices. It also categorised IoT into: Industrial Internet of things (IIoT), Internet of Medical Things (IoMT), Smart Cities and Smart Homes. This indicates that the challenges experienced in IoT are most likely going to be similar to what may be experienced in the IIoT, IoMT, smart cities and smart homes.

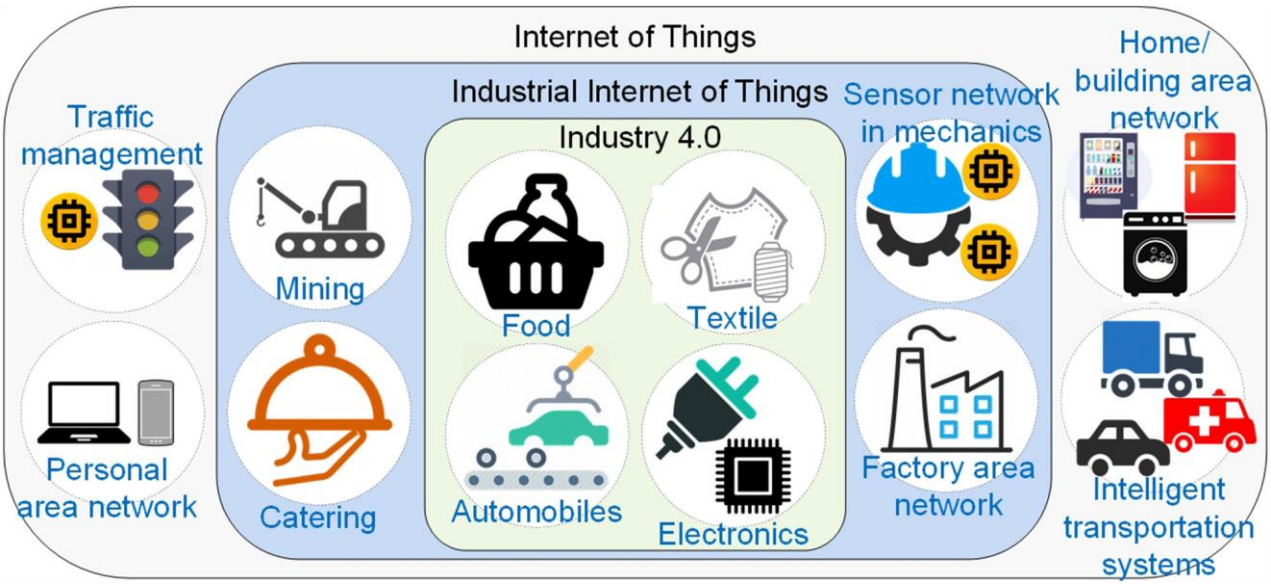

Figure 1:IoT, IIoT and Industry 4.0 (Mohammed *et al.*,(2018))

According to Mohammad *et al*., (2018) IIoT is made up of cyber physical systems (CPS), extreme automation, smart factory, industrial robots, actuators, etc. It is working toward making industrial systems robust, faster, and more importantly secured. The research also pointed out that the full potential of IIoT is yet to be realized because several research challenges needed to be addressed by the research community. These challenges include standardization, interoperability, scalability, usability, privacy, and security. With tele-robotics and semiautonomous machines that can be controlled remotely through virtual interfaces,

precision and timely responses are required.

Most of the aforementioned challenges by Mohammed *et al.,* (2018) were also corroborated in the research work of Sadaf& Sultana, (2020) which state that the proliferation of IoT devices for real-time applications; high latency, high energy consumption, intrusion detection and secure communication have become pertinent issues. A new technology called Fog computing has emerged as a solution to address some of these challenges like the high latency and high energy consumption problems of cloud computing the is currently been adopted by most IIoT.

Fog computing was also described by Ahmed *et al.,* (2020) as a powerful paradigm, where data are processed and filtered near the end of the IoT nodes and it is useful for improving the quality of service (QoS) of the IoT and by extension IIoT networks. This is because cloud technologies involve significant latency and they are not suitable for time sensitive applications. Furthermore, the cloud paradigm has been constrained by data privacy issues, such as for health monitoring and home devices. Consequently, the solutions that Cloud computing approach provides are becoming limited in the backdrop of growing needs of the present. In contrast to the centralized cloud, Fog computing follows a distributed approach. It also provides services of pre-processing, including data trimming by filtering the data to be consumed locally and managing resources. It complements the Cloud to the edge of the network. Fog computing is provided over heterogeneous physical resources and it supports the distributed deployment of applications. This characteristics of Fog computing that makes it suitable for IIoT because it has the following attributes: rapid response to time critical data, flexibility of task distribution among large number of nodes, and ability to analyze heterogeneous data in near real time.

Koen *et al.,* (2020) states that the emergence of IIoT will revolutionize production and manufacturing through the use of large numbers of networked embedded sensing devices, and the combination of emerging computing technologies, such as Fog/Cloud Computing and Artificial Intelligence. The IIoT is characterized by an increased degree of inter-connectivity, which not only creates opportunities for the industries that adopt it, but also for cyber-criminals. Indeed, security currently represents one of the major obstacles that is preventing the widespread adoption of IIoT technology because many companies are sceptical about the safety of the IIoT. This challenge is receiving some responses from the research community through the conduct of research work using different techniques that try to improve on the security of the IIoT with the aim of guarantying the safety and privacy of the IoT and IIoT technologies.

A deep learning intrusion detection method with a two stage anomalies detection was developed by Sadaf& Sultana, (2020) using auto-encoder and isolation forest to detect anomalies in the NSL-KDD dataset in a fog computing environment. The result of

their research show that their model has a better accuracy of 95.4% when compared with some other machine learning approaches. A fog computing IoT technique was used to determine air quality in urban centers by Ahmed *et al.,* (2020) the research made use of a three tier architecture comprising of the sensor layer, for data accusation using IoT nodes, distributed fog layer for the pre-processed, filtering and cleaning of the dataset to remove anomalies and cloud layer where the data is stored for advance analytics using machine learning algorithms. The result indicates that SVM has the best performance with an accuracy of 99% on the test set, whereas Multi-layer perceptron (MLP), K-nearest Neighbour (KNN) and Naïve Bayes (NB) gave satisfactory performance on the clustered dataset. The worst performance is shown by Decision Tree (DT) with an accuracy of 69%. The research work of Hosen *et al.*, (2022) proposed a framework for security and privacy preservation task management in edge computing using light weight encryption scheme based on public unclonable function (PUF) generated symmetric key and a modified ElGmal digital signature (mElGDSs) that verifies the data. A verified task is encrypted and stored in the application database (ADB) corresponding to a hashed index. In this manner, control over access to the data stored in the ADB is ensured. The framework has a better time complexity, better latency and less energy consumption when compared with other alternative models. This framework has shown a lot of promise in addressing the challenges of IIoT security and privacy but a major drawback is the use of signature based scheme to detect anomalies. This assertion was supported by the work of Sadaf& Sultana, (2020) In a world where new threats and attacks surface every other day, updating the database of signature-based intrusion detection systems (IDS) is not feasible. Therefore, anomaly-based detection of attacks works well for network security. In anomaly-based IDS, the normal behaviour of the system is considered as a model and if the current behaviour deviates from the normal, the system classifies it as an anomaly and takes corrective measures. This will ensure that the system is able to notice any emerging threat unlike where the database of the signature based intrusion detection system has to be regularly up dated to be aware of the emerging threats. The literature suggests that there is need to continuously research this technology in other to come up with a method that will work optimally regardless of the nature and architecture of the industry and network. In addition, the method should be trustworthy and reliable so as to motive more industry to key into the IIoT technology.

METHODOLOGY

The IIoTis largely considered to be made up of industrial automation, cloud computing and machine learning. While fog computing is considered as new paradigm serving as the point of intersection of these three IIoT components.

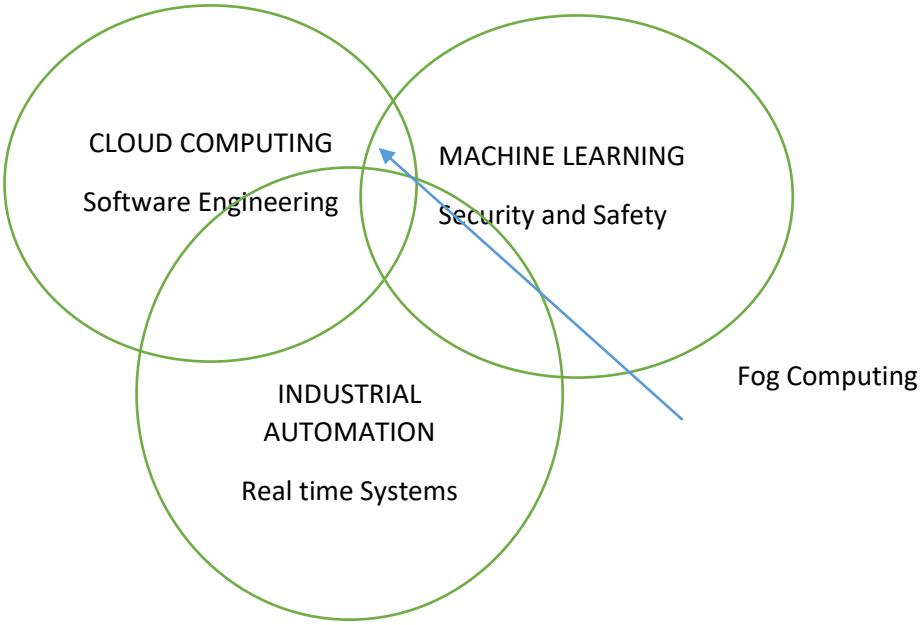

Figure 2: Industrial internet of things (source: IIoT by CISCO)

INDUSTRIAL AUTOMATION

Industrial automation is considered as the process of transforming manufacturing and other industrial processes into autonomous setups. This transformation can be carried out using artificial intelligence (AI), wireless sensor network (WSN) software defined network (SDN) and cloud computing technologies. Which have the ability to improve production capacities, efficiency and profitability among various industries. With the use of AI in industries, routine human activities can be complimented by expert systems using sensors and actuators which can emulate human decision making in a real time manner. Therefore, our industrial automation architecture is an incremental bottom–up design approach to the analysis and management of the IIoT network architecture by ensuring that the data generated by the IIoT devices are secured and safely transmitted through the WSN to the fog nodes and finally to the cloud and likewise data retrieval from the cloud follows the same steps before getting to the devices. Considering fog computing as the intersection of the various components which makes up the IIoT. The fog naturally was used as the bridge between the edge devices of the network and the cloud. It also serves as a temporary source of storage of data generated by the sensors and actuators and where the ML algorithm carries out analysis to detect anomalies. In addition, fog base station was used for storing vital and sensitive data relating to products or services of the industry which needs not to be shared to the cloud.

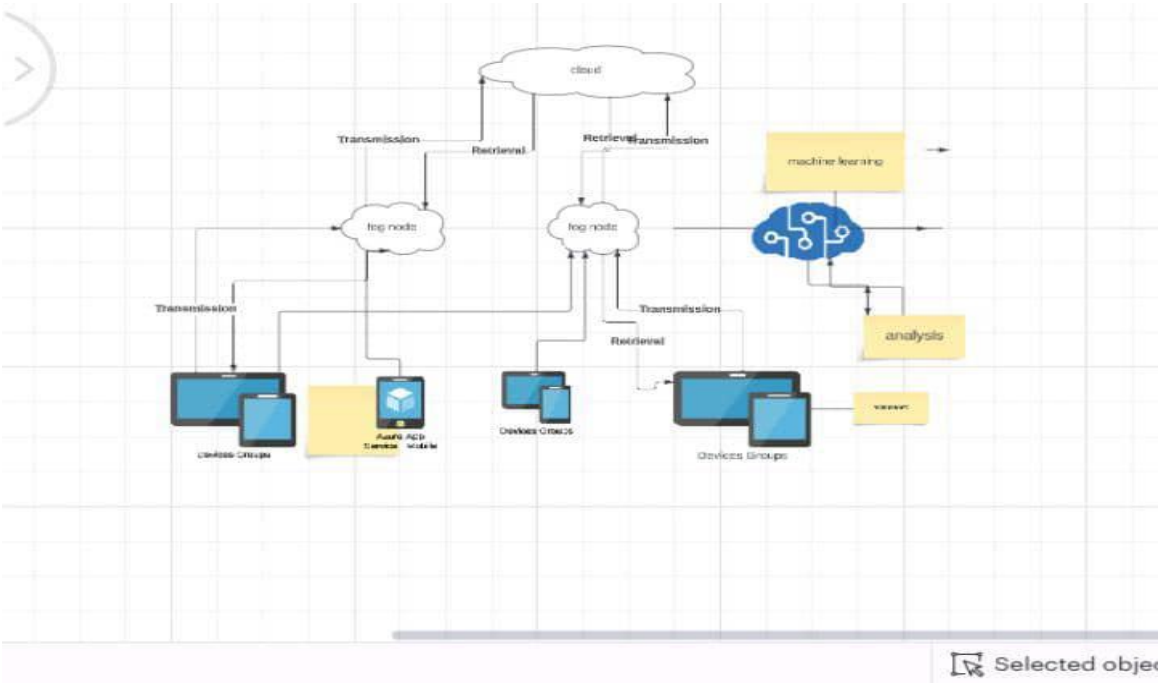

Figure 3: proposed distributed IIoT architecture

MACHINE LEARNING

It is clear that in any industrial set up ensuring real time security is of utmost importance therefore, our approach is concerned about regular monitoring and analysis to detection of anomalies in the fog computing environment of our proposed IIoT network architecture. Our research focused on the regular monitoring of network traffic and data generated by the network devices using ML algorithms to detect and report anomaly in the generated data and network traffic at the fog layer of the network before onward transmission to the cloud or any other device within the network. Our method proceeds as follow:

1. network traffic and data generated by IOT devices are analysed using ML at the fog layer of the network
2. classification of analysed data as either normal or abnormal
3. abnormal data get blocked then
4. XAI used to simplify the complex rules "black box" nature of ML to the decision making process
5. finally, all instances wrongly classified as either threat or normal during training will be noted and retrained to learn how correctly classify such instances.

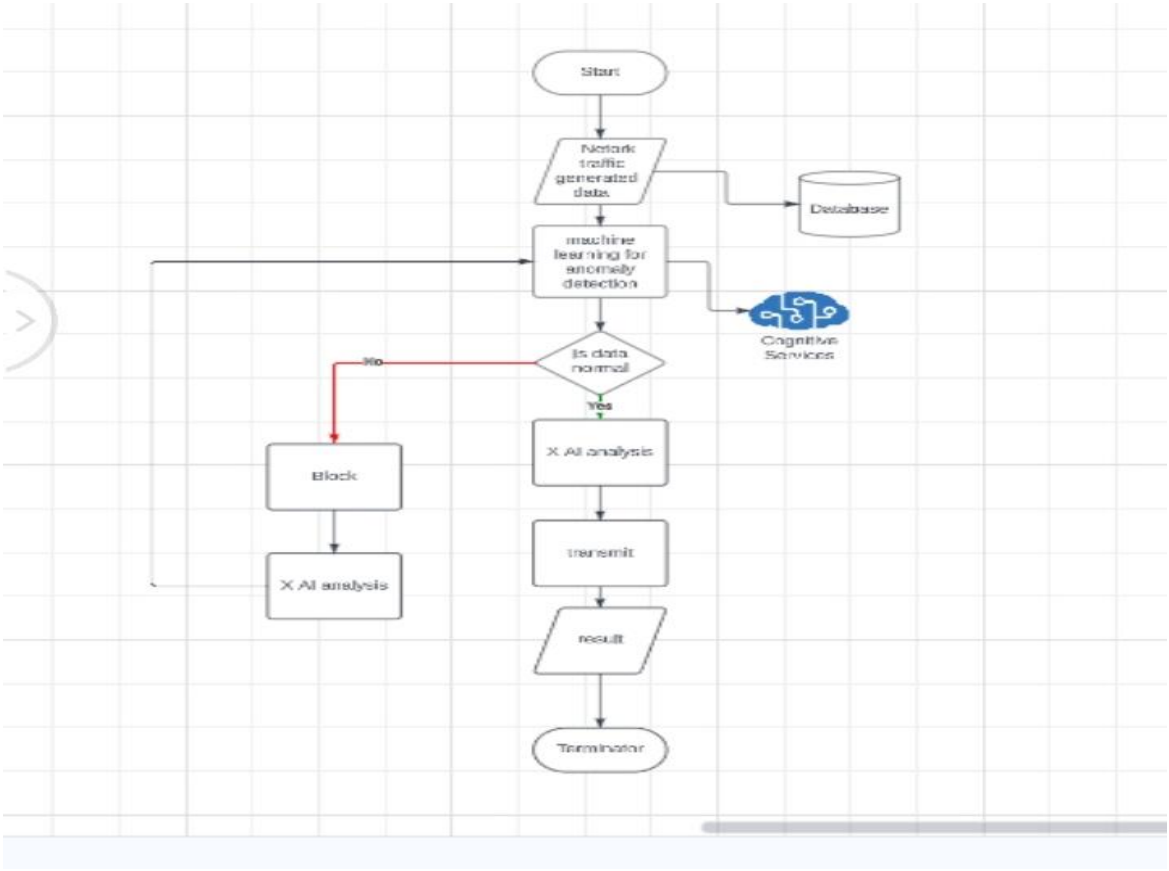

Figure 4: flow chart of the procedure for classification of dataset

Machine learning is regarded as a subset of artificial intelligence (AI), which trains computer algorithms to learn certain patterns in a systematic manner that will aid in knowledge discovery about those systems. These algorithms will later be able to apply this acquired knowledge to predict future out comes or occurrences based on the pre-established rules. Our approach basically used ML to monitor the regular behaviour and patterns of data generated by the various components of the IIoT network and detection of any anomaly in the regular or normal behaviour of the devices or transmitted data to prevent intrusion or information falsification. In addition to this the ML algorithm cross check the signature of the device the package was send from to also verify the authenticity of the network devices.

EXPLAINABLE ARTIFICIAL INTELLIGENCE

A major factor discouraging the adoption of IIoT by industries is the black box nature of ML algorithms and lack of technical knowledge ofML among industry players. The inability of industries to understand the decision making processes of ML algorithms has cause lack of trust among the industries. To overcome this challenge, our research decides to use XAI methods for simplification and interpretation of the approach adopted by ML in making decision about an event using Local Interpretable Model-Agnostic Explanation Method (LIME). LIME

was used to simplify the black box nature of ML decision making process to the industry operators understanding thus, making them to be part of the decision making process. With the use of LIME, specific observations made on the dataset that influence the decision making process are explained to the understanding of the user and the features that have direct impact on why certain decisions are taken by the model produced as the final result of the XAI model.

RESULT

The IIoT architecture developed in this research work when implemented will be evaluated using the NSL-KDD dataset to ascertain the accuracy, precision, f-score and root mean square error that are produced by the model in identifying threats and the response time to mitigation or isolation of those identified threats. In addition, the model performance will be compared to the performance of the model developed by Sadaf& Sultana (2020) using auto-encoder and isolation forest in a fog environment.

We wish to present the findings in the research in both qualitative and quantitative forms Therefore, the XAI model used for the simplification of the complex machine learning decision making process to the understanding of the industries will also be measured base on the findings in Dieber and kirrane, (2019) and compared to the work of Maede et al., (2021). Responses will be sought from the operators and non-experts working on the field about their user experiences and usability of the model

DISCUSSION

The proposed model improves the rate at which the IIoT networks are monitored to prevent intrusion and cyber-attack and without adding any extra computational cost to the system and also ensure real time detection of threat. The industries also have roles to play in the overall decision making processes because the model was able to simplify the method taken by ML algorithms in arriving at a decision. Thus all instances wrongly classified by the model can be easily detected and rectified. The network devices and packages transmitted between the devices are also regularly scrutinised strategically in the fog nodes in different base station to detect any inconsistency in the normal pattern of the generated data or alteration of the device signatures. The distributed nature of the network architecture gives it the capability to support routine maintenance without necessarily shutting down the entire network while threat can be quickly isolated within a section of the network thereby preventing other components of the network from been compromised.

The model in general can be summarised as having; the capability of real time detection of threats, continuous normal operations even when known or unknown threats are encountered and during routine maintenance or when internet connectivity is interrupted. It is believed that the new IIoT network architecture will improve the acceptance of IIOT among industries and enhance their productivity.

REFERENCE

1. Andro˘cec, D. and Vr˘cek, N. (2018) "Machine Learning for the Internet of Things Security: A Systematic Review" *In Proceedings of the 13th International Conference on Software Technologies* (ICSOFT 2018), pages 563-570 ISBN: 978-989-758-320-9 DOI: 10.5220/000684120563057
2. Fatima Hussain, Rasheed Hussain, Syed Ali Hassan, and Ekram Hossain, (2019) "Machine Learning in IoT Security: Current Solutions and Future Challenges" arXiv:1904.05735v1 [cs.CR] 14 Mar 2019 pp. 1-23
3. JurgenDieber and Sabrina kirrane, (2022) "A novel model usability evaluation framework (MUsE) for explainable artificial intelligence" *Elsevier Information Fusion*Volume 81, May 2022, Pages 143-153
4. KishwarSadaf and Jabeen Sultana, (2020) "Intrusion Detection Based on Autoencoder and Isolation Forest in Fog Computing" *IEEE ACCESS*, VOLUME 8, PAGE 167059-167068
5. Koen Tange, Michele De Donno, XenofonFafoutis and Nicola Dragoni, (2020) " A systematic Survey of Industrial Internet of Things Security: Requirements and Fog Computing Opportunities" *IEEE Communications Survey and Tutorials* Vol. 22 No. 4. Pp. 2489 – 2520.
6. MaedeZolanvari, Zebo Yang, Khaled Khan, Raj Jain, and Nader Meskin (2021) "TRUST XAI: Model-Agnostic Explanations for AI with a Case Study on IIoT Security" *IEEE Journal of Internet of Things (JIOT) doi 10.1109/JIOT/.2021.3122019 JIOT.*
7. MdArafatur Rahman and A. TaufiqAsyhari (2019) "The Emergence of Internet of Things (IoT): Connecting Anything, Anywhere" *Computers 2019, 8, 40; doi:10.3390/computers8020040 www.mdpi.com/journal/computers*
8. Mehreen Ahmed 1 ,RafiaMumtaz 1 , Syed Mohammad Hassan Zaidi, Maryam Hafeez, Syed Ali Raza Zaidi and Muneer Ahmad (2020) "Distributed Fog Computing for Internet of Things (IoT) Based Ambient Data Processing and Analysis"*Electronics 2020, 9, 1756; doi:10.3390/electronics 9111756*
9. Mohammad Aazam,SheraliZeadally , and Khaled A. Harras (2018) "Deploying Fog Computing in Industrial Internet of Things and Industry 4.0" *IEEE Transactions On Industrial Informatics,* VOL. 14, NO. 10, OCTOBER 2018 Page 4674 - 4682.
10. Sanwar Hosen A. S. M., Pradip Kumar Sharma, In-Ho Ra and Gi Hwan Cho (2022) "SPTM-EC: A Security and Privacy Preserving Task Management in Edge Computing for IIOT" IEEE *Transactions On Industrial*

Informatics, Vol. 18, No. 9, September 2022 Page 6330 -6339

11. Suzy E. Park, (2019) "Congressional Research Service" Journal*: Informing The Legislative Debate Since If11239* · Version 2 ·Https://Crsreports.Congress.Gov
12. Yusuf Perwej, Mahmoud Ahmed AbouGhaly, BedineKerim and Hani Ali Mahmoud Harb (2019) "An Extended Review on Internet of Things (IoT) and its Promising Applications"*Communications on Applied Electronics (CAE)* – ISSN: 2394-4714 Foundation of Computer Science FCS, New York, USA Volume 7– No. 26, February 2019 – www.caeaccess.org