Journal of Data Acquisition and Processing
ISSN: 1004-9037
https://sjcjycl.cn/
DOI: 10.5281/zenodo.777948

IOT - ENABLED CYBER PHYSICAL SYSTEMS TOWARDS CYBER-ATTACK DETECTION AND ATTRIBUTION

E.Padmavathi[1]*, Dr.G.Rajesh Chandra[2], Dr.Venkata Kishore Kumar Rejeti[3], R.Ramesh[4]

[1]*M.Tech Student, Department of CSE, KKR & KSR Institute of Technology and Sciences, Guntur, AP, India.

[2,3,4]Professor, Department of CSE, KKR & KSR Institute of Technology and Sciences, Guntur, AP, India.

Abstract:

It can be challenging to secure the cyber-physical systems (CPS) that power the Internet of Things (IoT), as security measures established for general information and technology operations (IT/OT) may not be effective in a CPS environment. In order to find attacks and techniques created specifically for CPS and more specifically for the control system, this article proposes a two-level common search. This initial phase involves designing a decision tree classifier and new deep learning model for attack detection in a variety of ICS environments. A deep neural network is created for the attack in the second layer. Real data from water pipelines and treatment facilities was used to test the projected model. The outcomes demonstrate that the suggested model performs better than other competing techniques facing comparable challenges.

INTRODUCTION

IoT devices are being integrated into cyber-physical systems (CPS), which include hazardous locations like dams and power plants. IoT devices, also known as Industrial IoT or IIoT, are frequently a component of the Industrial Control System, which is in charge of ensuring the process runs reliably. ICS can be widely defined to include Modbus-based systems, Programmable Logic Controllers (PLC), Control Systems (DCS), Supervisory Control and Data Acquisition (SCADA), and Programmable Logic Controllers (PLC). However, because they are connected to public networks, ICS or IIoT-based systems are susceptible to attack by hackers. An excellent illustration is the Stuxnet drive from 2010, which seriously damaged Iran's centrifuges for nuclear enrichment.

Another illustration is the 2011 pump malfunction that led to the failure of an Illinois water company. Another nuclear power plant in Ukraine, BlackEnergy3, caused pandemonium in 2015 that affected over 230,000 people [4]. ICS security solutions may not immediately apply to the mature security solutions envisaged for information technology (IT) and operational technology (OT) systems. This may be the result of a close integration between the linked systems and the physical control centre, for instance. To assess the behaviour of the body and manage its functional potential, a steady level approach is therefore necessary [1].

Contrary to most IT/OT systems (which are frequently crucial in defining sharing, integrity, and availability), the security goals of ICS are primarily in terms of availability, integrity, and privacy [5]. A (successful) cyberattack on the ICS might have major repercussions and possibly have an adverse impact on people and the environment because of the close

relationship between the response control loop and the physical system. This highlights the necessity of creating strong security mechanisms to identify and restrict access to ICS [1]. Although hybrid-based techniques are good at spotting malicious activity, they are unstable since networks change often, leading to various kinds of detection systems (IDS) [7]. Additionally, standard attack detection and prevention methods only analyse network metadata (such as IP address, forwarding port, traffic volume, and packet duration). As a result, leveraging machine learning (ML) or deep neural networks (DNN) as a strategy for attack and issue resolution has lately attracted considerable interest. Additionally, interruption detection techniques can be divided into network-based and host-based categories. Attack methods for network connection include cluster monitoring, single- or multi-unit Support Vector Machines (SVM), fuzzy logic, Artificial Neural Networks (ANN), and DNNs.

This expertise does real-time traffic data analysis to quickly identify malicious attempts. Attack detection, which merely takes into account network and host data, can, however, miss an attack or insider knowledge. Unsupervised models that use systems and physical data can do surveillance since they don't rely on precise knowledge of online risks. Intelligent attackers, such as nation-state actors, may frequently get around security measures if they have the necessary expertise and time. Additionally, the majority of current methodologies just simulate bodily behaviour and consistently highlight distinctions in the behaviour of the bad, ignoring the inconsistent nature of ICS data.This could be as a result of the small sample size in recent studies and actual life circumstances. Class models are frequently a smart way to prevent issues brought on by inconsistent data, however training models might not be able to recognise patterns in output patterns. In other words, this approach has a negative outcome and is unable to identify the unseen attack [8]. In order to model large concepts from elementary concepts without being reliant on craft, for instance, he sought to employ the DL approach to enable automated (representational) learning [9].

The two prerequisites for network security set out by Ensuring the Security of Intelligent Manufacturing Systems, Job 4.0 are "security by design" and security architecture in the future's intelligent systems [22]. The system will have to automatically find viruses, threats, and attacks with no formation in order to do this. Artificial intelligence will play a major part in cyber intelligence, which monitors, identifies, and analyses digital security risks to battle viruses, hackers, and criminals that are active online for a variety of reasons, in addition to the cyberthreats already stated to Internet commerce. Blackmail, blackmail, stock market manipulation, sophisticated corporate espionage, and preparing for or carrying out terrorist attacks are just a few examples. engineering, finance, medicine, and computational biology. It has been used successfully in several sectors. Another crucial area where we may apply EC&CI's strength is cybersecurity.

For cybersecurity issues, unlike other issues, solutions must be strong enough to withstand determined, knowledgeable attackers who could aim for a changed cyber-physical system. In our networked environment, cyber intelligence promises to be advantageous to everyone. Our future will be safe, secure, and affluent if we combine EC&CI with cybersecurity.

PROBLEM STATEMENT

"The scientific community is drawing attention to an increasing number of cybersecurity issues today. Particular solutions for investigating cyberattacks on IoT substructures are expanding. Definitely, the most inspired IoT cyber-attack finds its way through Machine learning Algorithms. To solve the Network attack detection problem, the authors of [14] propose a method to analyse IoT malware traffic. It is developed using multilevel intellect comprising of neural networks and binary visualization.

The three crucial layers of recording network connections are included in the technique for increasing performance by learning the error distribution, which conducts binary visualisation to save traffic links in ASCII, transforms it to a 2D picture, and renders/analyses the binary image. Tensor Flow tools, an end-to-end open-source platform created to employ machine learning to address various challenges, were used to analyse binary pictures. able to recognise and classify patterns. This tool's capacity to organise the reinstruction process and its visual recognition capabilities are its key benefits. An algorithm is used in the idea to display the collection as a picture that is tiled with the Binvis tool.

Tensor Flow Machine Device can make predictions. The use of charts allows the grouping of blocks followed by the charts to be determined. It can identify the need without mentioning its position in the received image. The offered system can act as gateway-level IoT device protection, bypassing IoT environment restrictions. Table 1 shows the performance analysis of machine learning algorithms for detecting cyber-attacks in IoT substructure.

Analysis of the impact study can regulate that most studies have a good measure; but the lack of research projects is that they don't include many of the features that might indicate a challenge. The investigation demonstrates that tried-and-true techniques for identifying IoT assaults are effective. However, there are limitations as well, including the inability to recognise and respond to unknown assaults (zero-day attacks), the inadequate detection of numerous attacks, the refusal to accept high fake good prices, lengthy real-time response times, and the enormous demand. computation tools. A minimal and adequate number of information network signatures must be chosen in order to be able to detect the existence or absence of cyber attacks on the IoT infrastructure.

LITERATURE REVIEW

"Detection and Reporting of Cyber Attacks in the Cyber Environment Hades Karimipour; Ali Dehghantanha; Kim-Kwang Raymond Choo

Digital and physical security because security solutions made for standard information/operational technology (IT/OT) may not function well in CPS environments, the Internet of Things (PSI) might be difficult to implement. In order to uncover the attack and develop a unique design for CPS, and more especially for the business management system (ICS), this article describes a multi-level collaborative effort. For attack detection in a heterogeneous ICS environment, a decision tree and a novel deep representation learning model are created in the first stage. A deep neural network is created to support the attack in the second layer. Real data collected from water pipelines and treatment facilities was used to evaluate the suggested model. The results demonstrate that the suggested model outperforms other competing techniques that face comparable challenges.

iAdf-CPS: Creative Anomaly Meaning Ghanammed S.Hammed S.Hammed S.Hammom MSE). Security is an important aspect of CPS. However, with increasing pressure and despicable attacks in CPS, the detection process always faces problems and the data volume becomes difficult to grow, requiring specific knowledge that can be used to directly identify these problems. To come out this problem, many deep learning-based error detection methods have been developed. In this study, we propose a vulnerability detection method by combining a deep learning technique called convolutional neural network (CNN) with a Gaussian mixture model (GMM) based on Kalman filter (KF). The proposed model was used to identify and analyse the abnormal behaviour in CPS. This proposed framework includes two main tasks. The first is to advance data by transforming and filtering raw data into a new format to complete data protection. Second, we propose a GMM-KF ensemble deep CNN model for error detection and measurement accuracy after error and formality in CPS.

Internet Security Challenges of Cyber Physical Systems and Opportunities for Evolutionary Business and Other Intelligence

Yoon Mei Ning, Karsten Feng, Tim Watson, Aşutuş Tiwari, Bogdan4 Gab 44, Yoon Mei Ning, Jin Yaochu, and The Fourth Industrial Revolution, or "Industrie 4.0," was ignited by the Internet of Things (IoT). By linking people, processes, and information, this revolution offers several advantages. For IoT-enabled cyber-physical systems, including linked devices used for business management and big data produced by goods employing huge IoT, cybersecurity is developing as a significant concern. Along with other intelligent tools like antivirus software for IoT security designs, data mining and fusion in IoT-enabled cyber-physical systems, and data-driven cybersecurity, evolutionary computing will play a significant role in cybersecurity. This article offers a general overview of the security issues that IoT-enabled cyber-physical systems face, as well as how evolutionary computing and other forms of artificial intelligence may help.

Intelligent Brain Computing Based Intrusion Detection for Industrial CPS

Author Links Open Scope Panel Maha M. Altobaitia K. Pradeep Mohan Kumarb Deepak Guptac Sachin Kumard Romany F. Mansour

Progress in Industrial Networking (PS) Transportation, smart cities, healthcare, energy distribution, agriculture, and many more industries can benefit from Io research. In addition, there are several dangers to user interests brought on by the growing usage of CPS enterprises. Artificial intelligence and artificial intelligence have recently opened up new possibilities for the CPS industry's evolution. Therefore, by employing AI-based Intrusion Detection Systems (IDS), it is possible to identify warranty and avoid its impact in order to protect the security of SUE operations. This article offers expertise on the application of modern IDSs for the safety of commercial CPS, using it as a starting point. A number of processing processes, including data collection, sequencing, feature selection, classification, and optimisation, may be included in the suggested model. Prior to analysing the data, sample preparation is necessary to eliminate any influence.

SECURECPS: A Cognitive Framework for Detecting Cyber Attacks in Cyber-Physical Systems

Aaisha Makkar and Jong HyukPark

In the era of standalone systems, security is an important module in environment flexible computing. New types of computing will emerge, such as cognitive heuristics, due to improvements in computing power and connection speed. This approach provides easy and fun human-centered service anytime, anywhere, on any device. Recently, cyber-physical computing as cyber-physical systems for smart cities, human-computer interaction, smart services and connected devices has been studied worldwide. However, the strategy carefully defines the basis of CPS security.

PageRank changes the way you rank and changes the cognitive power of search engines. The proposed system, called Secure CPS, is trained to use real-time data to record interactions on facial recognition websites. The eye area is marked using an illumination algorithm. The framework was validated using a machine learning model and achieved an accuracy of 98.
51%, outperforming existing systems.

New Intrusion Detection Methods for Cyber-Physical Systems in the Emerging Industrial Internet of Things

Himanshu Mittala Ashish Kumar Tripathib Avinash ChandraPandeyc Mohammad Dahman Alshehrid Mukesh Saraswata RajuPala

In addition, protecting anonymous data is a dangerous business. To this end, this article presents a new integration management approach. The program uses the latest version of the Gravity Search algorithm to find stars accurately. In channel, Kbest has changed to a reduced level with behaviours that conflict with the emotion map. To analyse the change, the IEEE CEC2013 benchmark function was compared with five algorithms. Experimental results were analysed with characteristic error, Wilcoxon rank sum test, convergence plot, box plot, and time complexity. The tuning strategy provides good results and longest duration in all dimensions, namely 10, 30, 50 and 90 in dimensions 10, 13, 15 and 10.

Additionally, the effectiveness of the integration process was tested on five IoT business cases. Evaluation is based on F-tests and time calculations.

Internet of Things CPS Security Research: Problems, Challenges, Threats, Solutions Kim, Nam Yong; One of the key technologies of the Internet of Things (IoT).

CPS is a new concept that aims to unify the physical and cyber worlds we live in.

However, some CPS issues in CPS can directly affect our security, and the CPS environment has local threats, including its various systems, so CPS security training is necessary. Therefore, research-based in-depth understanding of vulnerabilities, threats, and attacks on IoT CPS security and privacy is required. In this article, we identify security issues, threats, and solutions for IoT-CPS and evaluate current research. CPS presents many problems stemming from the current security industry and security issues.

This study also addresses the weaknesses and challenges of CPS and presents the challenges.

PROPOSED SYSTEM

The representation phase and the detection phase make up the search technique. On an imbalanced dataset, enhanced supervised machine learning techniques frequently produce machine learning models that learn the most class models while omitting native class features. The majority of academics attempt to address this problem by developing new models or eliminating certain existing models in order to stabilise the data before integrating it into a machine learning model. However, in ICS/IIoT security applications, adding or eliminating patterns is not a required answer. Due to the sensitivity of ICS/IIoT systems, it is hard to test the design in a real network since it might damage the network and have a significant negative impact on the environment or human life. Additionally, the examination of the output pattern takes time. The amount of attack patterns in ICS/IIoT datasets is often less than 10% of the dataset, and deleting 80% of the dataset discards the majority of the known information, therefore removing normal data from the dataset is not a solution. This study provides a novel machine learning technique that enables models to resolve data-consistent text problems without modifying, generating, or removing patterns, hence avoiding the aforementioned issues with inconsistent data. Two unsupervised autoencoder groups, each charged with discovering examples from a certain class, make up the model. As each model aims to extract the abstract structure of one class without taking into account the others, the output of the model is a good representation of its input. Three decoders and encoders with inputs and outputs make up stacked autoencoders. The ML model will then be better performing while doing binary classification and multi-label classification.

Advantages of Reporting Processes

- The proposed process improves the accuracy of results.
- Although our experiments showed that the performance of the technique was very good, the accuracy of the measurement indicates that it is a difficult task and deserves further investigation.
- We believe this test can further inform a new set of methods used in different treatments to predict depression and other variables.

SYSTEM ARCHITECTURE

The design concept, Detection and Connection of Cyber Attacks in IoT, uses three increased machine learning models, multiclass classifier and binary classifier to detect cybersecurity irregularities. Figure 1 illustrates the concept of binary classification, while Figure 2 shows different types of classification. It relies on supervised learning, which uses domain names to gain intelligence to predict cyber-attacks. The framework uses the UNSW_NB15 dataset as input. The data is then pre-processed for regularization.

First, apply the logarithmic scaling method to the data to constrain the minimum and maximum of the measured range.

where the maximum value and minimum value are represented by max and min respectively. After preprocessing, the data is divided into training and test sets in a ratio of 70:30. Since the proposed ML model must predict the class list, the training set contains characters while the

test does not contain the class list. The development model will be designed for learning and getting the necessary skills throughout the education process.

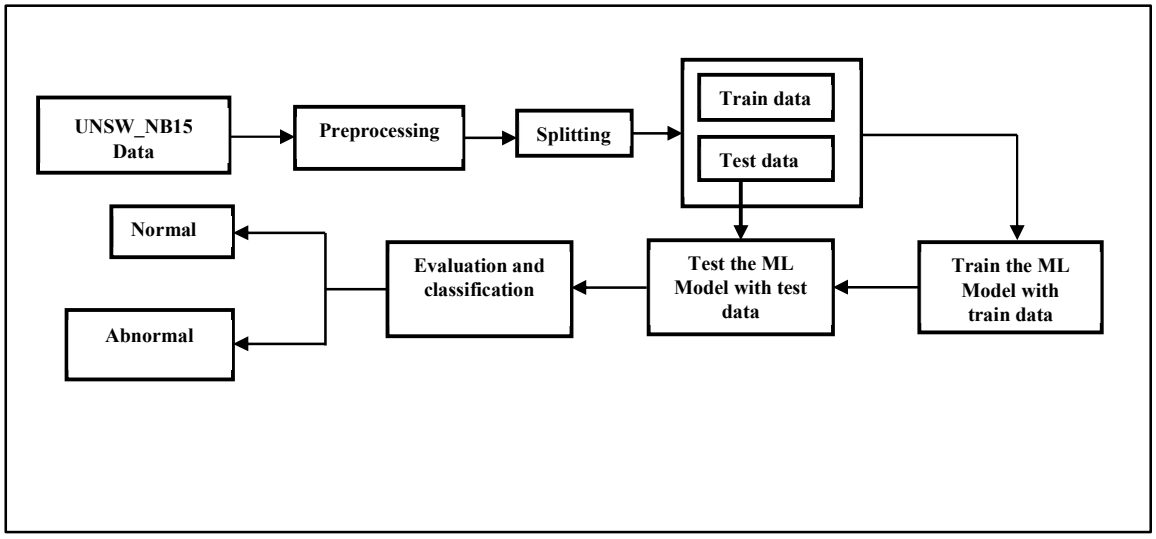

Fig 1 Architecture for binary classification

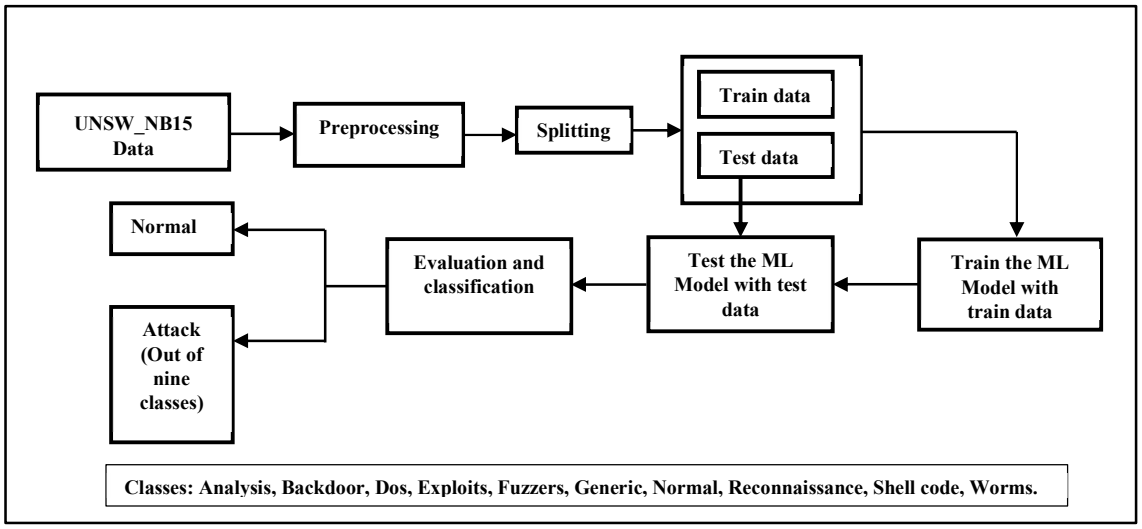

Fig 2 Architecture for Multi Class classification

The knowledge gained in the training phase is used further to predict class labels for each test instance. We designed enhanced ML model to be a multi-class classifier and binary classifier that detects all nine kinds of attack classes and it also detects in binary as normal and Abnormal.

A. UNSW_NB15 DATA

The UNSW-NB15 dataset used in this study is collected from [33]. It was created by UNSW Cyber Range Lab. It has a mix of attack behaviours and normal flows. Tcp dump tool was used

to have this dataset from 100 GB Pcap files with raw network traffic content. It has 47 features along with class label. The dataset has behaviours of nine kinds of attacks as shown in Table 1

Sl. No.	Attack Class	Number of Instances
1	Analysis	677
2	Backdoor	583
3	DoS	4089
4	Exploits	11132
5	Fuzzers	6062
6	Generic	18871
7	Normal	37000
8	Reconnaissance	3496
9	Shellcode	378
10	Worms	44

Table 1: Nine kinds of attack behaviours reflect in UNSW-NB15 dataset

B. Pre-processing

Pre-processing of data for initial processing or further analysis. The term can be used for all pre-orders or pre-orders when multiple steps are required to prepare the data for the user.

C. Splitting

Data splitting means splitting data into two or more groups. Generally, there are two parts, one for evaluation or test data and another for training the model.

Classifying data, especially building data-driven models, is an important part of data science.

D. Training data and test data

"Algorithms are used in machine learning to draw knowledge from datasets. They create and assess judgements as well as identify patterns and gain insight. Data is separated into two divisions for machine learning. The first subset, referred known as the training data, is made up of the actual data that was used to develop the machine learning model. He produced three models this way. Test data is a further subset.

You need unobserved data to test your machine learning model on once you develop it (using training data). You may utilise this data, which is referred to as test data, to assess the effectiveness and development of the training algorithm and to modify or enhance the outcomes. Two important things are in the test file.

• should depict actual data

• Sufficient in size to allow for effective prediction

E. EVALUATION AND CLASSIFICATION

Model measurement is the process of measuring different parameters to understand the effectiveness and power of a machine learning model and Model evaluation is to assess the validity of the model during initial research important and also plays a role in maintaining the model. Classification in machine learning is a prediction problem that is modelled in a catalog for specific instances of input data. For example, identifying typed characters, detecting spam, etc. For classification, it should have training data with large input and output data.

Algorithm

Algorithm: (IOT-DACA)
Input: UNSW-NB15 data as (D), ML Models as (M)
Output: attack type or normal response (R)
1. Begin
2. Read data (D)
3. P← pre-process data(D)
4. t_1, t_2← splitting data(P)
5. Apply Normalization (t_1, t_2)
6. For model m in M
7. train the model (t_1)
8. end For
9. For model m in M
10. test the model (t_2)
11.end For
12. Evaluation of models (M)
13. results
14. return R

Algorithm: Proposed algorithm
As presented in Algorithm, it takes training data and test data as inputs. It produces prediction results Machine Learning approach. It used training data to train proposed Model. This will help the algorithm to gain knowledge from the data. This knowledge is used while performing prediction using test data. The test data is classified into Attack type and Normal Samples. The algorithm also generates confusion matrix from which the performance metrics are derived.

RESULTS
"The subtraction and custom categorization using machine learning algorithms are carried out by a learning machine dubbed DACA-IOT, which also generates the findings. It is a multi-vector kind of security that may operate within a network. The DACA-IOT framework offers tools to construct the appropriate security conditions for the network to be established as an exit mode against the network by the kind of attack in addition to tools to detect assaults. This programme offers a number of modules that concentrate on addition, packing, and subtraction, as well as on creating unique classifications using machine learning methods and producing results. The scikit-learn library serves as the foundation for the feature taxonomy of the framework. For Python programmers, it is a free machine learning library.

BINARY CLASSIFICATION			
Models	**precision**	**recall**	**f1-score**
Linear Regression	98	96	97
LR	98	96	97

LSVM	98	96	97
KNN	98	97	98
RF	98	98	98
DT	98	98	98
Multi-Layer Perceptron	98	98	98

Table 2 performance of models in binary classification

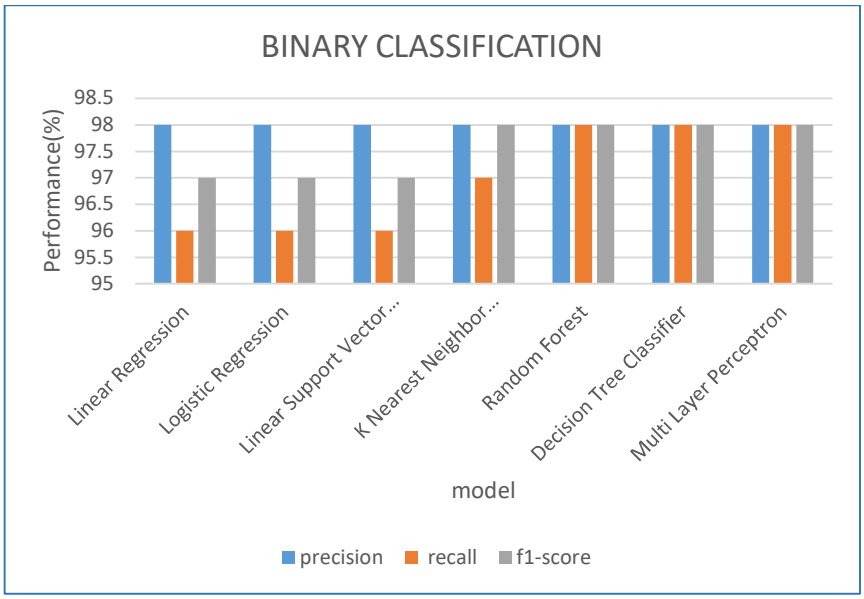

Fig 3 Performance graph of models in binary classification

MULTI CLASS CLASSIFICATION			
Model	**precision**	**recall**	**f1-score**
Linear Regression	0.01	0.01	0.01
Logistic Regression	97	98	97
LSVM	97	98	98
KNN	97	97	97
RF	97	97	97
DT	97	97	97
Multi-Layer Perceptron	97	98	97

Table 3 performance of models in Multi Class classification

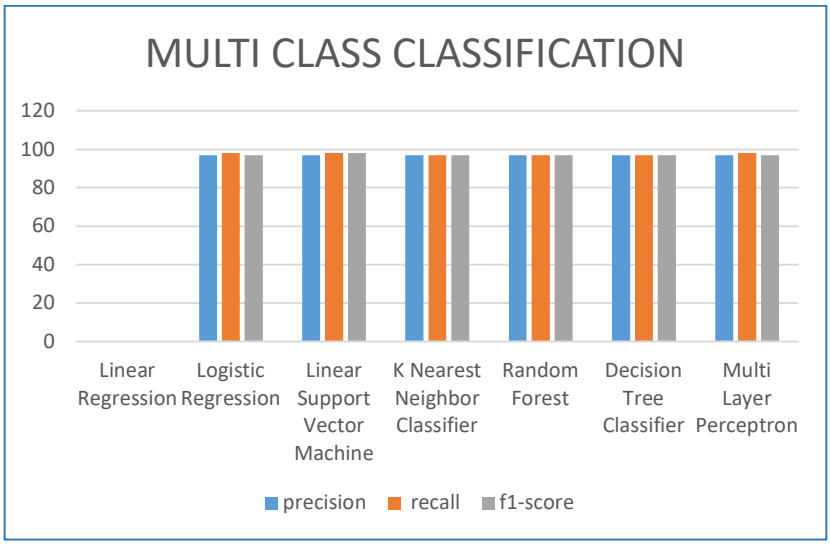

Fig 4 Performance graph of models in Multi Class classification

Accuracy Comparison		
Model	**Binary Classification**	**Multi-Class Classification**
Linear Regression	97.8	81.3
Logistic Regression	97.8	97.58
LSVM	97.85	97.59
KNN	98.3	97.37
RF	98.64	97.32
DT	98.09	97.2
Multi-Layer Perceptron	98.36	97.54

Table 4 Accuracy comparison table of models

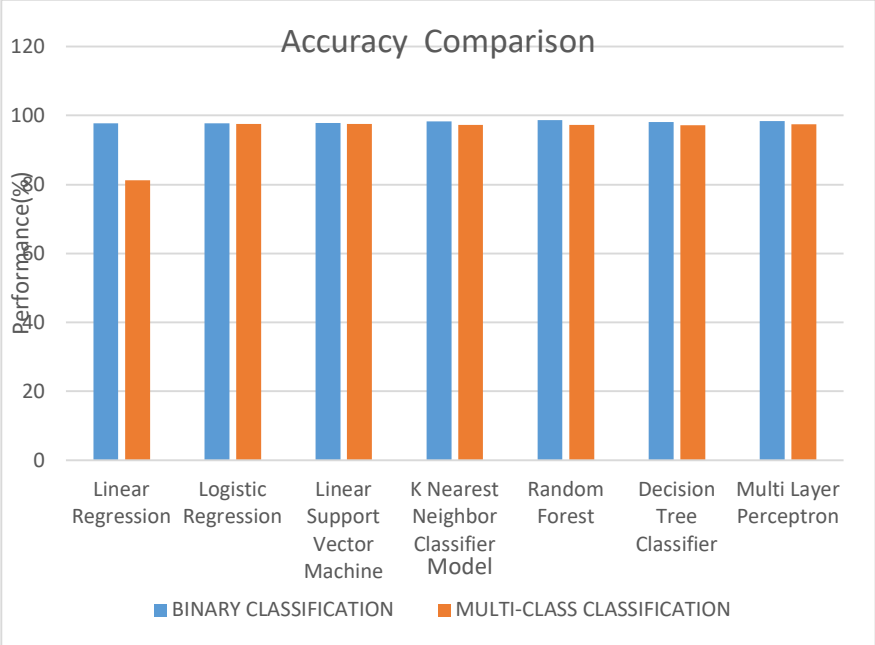

Fig 5 Accuracy Comparison graph of models

CONCLUSION

For sparse ICS data, we provide a novel approach to intrusion detection and intrusion detection based on two-stage hybrid machine learning. The intrusion detection system combines a framework to recognise attack patterns and machine learning to bring patterns to higher level settings. This level can recognise previously unnoticed threats and is robust to data variabilities. A different collection of one-to-many distributions, each trained on a distinct behaviour, is the target of the assault. The complexity of the training and testing phases is O (n 4) and O (n 2), respectively (n is the number of training samples), which is comparable to other machine learning-based machine learning, despite the fact that it is a standard set of algorithms. There are techniques listed in the literature. Additionally, the suggested framework has greater recovery and f-measurement than earlier research, and it can discover and quantify trends in real time. The primary findings of attribution in MLA demonstrate that whereas MLP algorithms produced the greatest results in multi-species classification, level regression produced the lowest results. Additionally, the detection of TCP, UDP, HTTP GET, and DNS tunnelling attacks is frequently on par with that of other IoT multi-vector network attack signatures based on flow-monitoring and signatures based on IoT applications. In this study, we investigate insinuations of established machine learning-based algorithms for detecting attacks on IoT infrastructure.

We are looking at the potential for traffic analysis and widely used IoT protocols including HTTP, MQTT, and DNS to identify attacks against IoT infrastructure. By using well-known data indicating assaults against IoT infrastructure including TCP, UDP, HTTP GET, and DNS tunnelling, well-known actors like Mirai, Dark Nexus, and Gafgyt were able to intercept traffic from these actors. Additionally, smart IoT traffic from devices like routers, thermometers, and

webcams is gathered while countermeasures are created utilising smart devices. The features provided at work are divided into several classes of machine learning and removed from traffic. The essential training components, as well as testing and customising the machine learning algorithm, determine the degree of detection of multi-vector assaults on IoT infrastructure.

FUTURE WORK

Future extensions include the creation of cyber threat hunting products to make it easier to identify liabilities that are not visible to the search engine; For example,
by creating standard layers during the body and assets, which is an important part of research. Therefore, future studies will focus on the following:

1. Different IoT techniques [64] remove traffic signals, which in the absence of traffic analysis will increase accuracy against searches;
2. Reduction is sufficient to control.
3. Develop a machine learning-based approach to trust of IoT systems by combining techniques of attack and penetration, replication and recovery.

REFERENCES

1. F. Zhang, H. A. D. E. Kodituwakku, J. W. Hines, and J. Coble, "Multilayer Data-Driven Cyber-Attack Detection System for Industrial Control Systems Based on Network, System, and Process Data," IEEE Transactions on Industrial Informatics, vol. 15, no. 7, pp. 4362–4369, 2019.
2. R. Ma, P. Cheng, Z. Zhang, W. Liu, Q. Wang, and Q. Wei, "Stealthy Attack Against Redundant Controller Architecture of Industrial CyberPhysical System," IEEE Internet of Things Journal, vol. 6, no. 6, pp. 9783–9793, 2019.
3. E. Nakashima, "Foreign hacker's targeted U.S. water plant in apparent malicious cyber-attack, expert says." [Online]. Available: https://www.washingtonpost.com/blogs/checkpointwashington/post/foreign-hackers-broke-into-illinois-water-plant-controlsystem-industry-expert-says/2011/11/18/gIQAgmTZYN blog.html
4. G. Falco, C. Caldera, and H. Shrobe, "IIoT Cybersecurity Risk Modeling for SCADA Systems," IEEE Internet of Things Journal, vol. 5, no. 6, pp. 4486–4495, 2018.
5. J. Yang, C. Zhou, S. Yang, H. Xu, and B. Hu, "Anomaly Detection Based on Zone Partition for Security Protection of Industrial Cyber-Physical Systems," IEEE Transactions on Industrial Electronics, vol. 65, no. 5, pp. 4257–4267, 2018.
6. S. Ponomarev and T. Atkison, "Industrial control system network intrusion detection by telemetry analysis," IEEE Transactions on Dependable and Secure Computing, vol. 13, no. 2, pp. 252–260, 2016.
7. J. F. Clemente, "No cyber security for critical energy infrastructure," Ph.D. dissertation, Naval Postgraduate School, 2018.
8. C. Bellinger, S. Sharma, and N. Japkowicz, "One-class versus binary classification: Which and when?" in 2012 11th International Conference on Machine Learning and Applications, vol. 2, 2012, pp. 102–106.

9. Goodfellow, Y. Bengio, and A. Courville, Deep learning. MIT Press, 2016. [Online]. Available: http://www.deeplearningbook.org
10. Y. Bengio, A. Courville, and P. Vincent, "Representation learning: A review and new perspectives," IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 35, no. 8, pp. 1798–1828, 2013.
11. M. Zolanvari, M. A. Teixeira, L. Gupta, K. M. Khan, and R. Jain, "Machine Learning-Based Network Vulnerability Analysis of Industrial Internet of Things," IEEE Internet of Things Journal, vol. 6, no. 4, pp. 6822–6834, 2019.
12. A. Khan, D. Pi, Z. U. Khan, Y. Hussain, and A. Nawaz, "HML-IDS: A hybrid-multilevel anomaly prediction approach for intrusion detection in SCADA systems," IEEE Access, vol. 7, pp. 89 507–89 521, 2019.
13. T. K. Das, S. Adepu, and J. Zhou, "Anomaly detection in industrial control systems using logical analysis of data," Computers & Security, vol. 96, p. 101935, 2020.
14. J. J. Q. Yu, Y. Hou, and V. O. K. Li, "Online False Data Injection Attack Detection With Wavelet Transform and Deep Neural Networks," IEEE Transactions on Industrial Informatics, vol. 14, no. 7, pp. 3271–3280, 2018.
15. M. M. N. Aboelwafa, K. G. Seddik, M. H. Eldefrawy, Y. Gadallah, and M. Gidlund, "A machine-learning-based technique for false data injection attacks detection in industrial iot," IEEE Internet of Things Journal, vol. 7, no. 9, pp. 8462–8471, 2020.
16. W. Yan, L. K. Mestha, and M. Abbaszadeh, "Attack detection for securing cyber physical systems," IEEE Internet of Things Journal, vol. 6, no. 5, pp. 8471–8481, 2019.
17. Cook, A. Nicholson, H. Janicke, L. Maglaras, and R. Smith, "Attribution of Cyber Attacks on Industrial Control Systems," EAI Endorsed Transactions on Industrial Networks and Intelligent Systems, vol. 3, no. 7, p. 151158, 2016.
18. L. Maglaras, M. Ferrag, A. Derhab, M. Mukherjee, H. Janicke, and S. Rallis, "Threats, Countermeasures and Attribution of Cyber Attacks on Critical Infrastructures," ICST Transactions on Security and Safety, vol. 5, no. 16, p. 155856, 2018.
19. M. Alaeiyan, A. Dehghantanha, T. Dargahi, M. Conti, and S. Parsa, "A Multilabel Fuzzy Relevance Clustering System for Malware Attack Attribution in the Edge Layer of Cyber-Physical Networks," ACM Transactions on Cyber-Physical Systems, vol. 4, no. 3, pp. 1–22, 2020.
20. U. Noor, Z. Anwar, T. Amjad, and K.-K. R. Choo, "A machine learning-based FinTech cyber threat attribution framework using high-level indicators of compromise," Future Generation Computer Systems, vol. 96, pp. 227–242, 2019.
21. S. Wold, K. Esbensen, and P. Geladi, "Principal component analysis," Chemometrics and Intelligent Laboratory Systems, vol. 2, no. 1, pp. 37 – 52, 1987, proceedings of the Multivariate Statistical Workshop for Geologists and Geochemists.
22. N. Jahromi, J. Sakhnini, H. Karimpour, and A. Dehghantanha, "A deep unsupervised representation learning approach for effective cyber-physical attack detection and identification on highly imbalanced data," in Proceedings of the 29th Annual International Conference on Computer Science and Software Engineering, ser. CASCON '19. USA: IBM Corp., 2019, p. 14–23.

23. T. Morris, Z. Thornton, and I. Tunipseed, “Industrial control system simulation and data logging for intrusion detection system research,” in 7th Annual Southeastern Cyber Security Summit, 2015.
24. J. Goh, S. Adepu, K. N. Junejo, and A. Mathur, “A dataset to support research in the design of secure water treatment systems,” in Critical Information Infrastructures Security, G. Havarneanu, R. Setola, H. Nassopoulos, and S. Wolthusen, Eds. Cham: Springer International Publishing, 2017, pp. 88–99.
25. S. N. Shirazi, A. Gouglidis, K. N. Syeda, S. Simpson, A. Mauthe, I. M. Stephanakis, and D. Hutchison, “Evaluation of anomaly detection techniques for scada communication resilience,” in 2016 Resilience Week (RWS), 2016, pp. 140–145.