e-ISSN:2582-7219

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH IN SCIENCE, ENGINEERING AND TECHNOLOGY

Volume 6, Issue 1, January 2023

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.54

6381 907 438 6381 907 438 ijmrset@gmail.com www.ijmrset.com

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.54|

| Volume 5, Issue 12, December 2022 |

| DOI:10.15680/IJMRSET.2022.0601004 |

Toward Identification and Attribution of Digital Assaults in IOT-Empowered Digital Actual Frameworks

[1]J Priyanka , [2]Dr. Jaideep Gera

[1]PG Scholar, Dept of AIML, St Mary's group of Institutions Guntur, AP, India

[2]Associate Professor, Dept of CSE, St Mary's group of Institutions Guntur, AP, India

ABSTRAT: Securing Internet of Things (IoT)-enabled cyber- physical systems (CPS) can be challenging, as security solutions developed for general information / operational technology (IT / OT) systems may not be as effective in a CPS setting. Thus, this paper presents a two-level ensemble attack detection and attribution framework designed for CPS, and more specifically in an industrial control system (ICS). At the first level, a deci- sion tree combined with a novel ensemble deep representation- learning model is developed for detecting attacks imbalanced ICS environments. At the second level, an ensemble deep neural network is designed for attack attribution. The proposed model is evaluated using real-world datasets in gas pipeline and water treatment system. Findings demonstrate that the proposed model outperforms other competing approaches with similar computational complexity.

KEYWORDS: IoT, Cyber, ICS, Attacks

I. INTRODUCTION

Getting Internet of Things(IoT)- empowered digital actual frameworks (CPS) can challenge, as security arrangements created for general data/functional innovation (IT/OT) frameworks may not be as compelling in a CPS setting. Subsequently, this paper presents a two-level group assault discovery and attribution structure intended for CPS, and all the more explicitly in a modern control framework (ICS). At the main level, a deci-sion tree joined with an original gathering profound portrayal learning model is produced for recognizing assaults imbalanced ICS conditions. At the subsequent level, an outfit profound brain network is intended for assault attribution. The proposed model is assessed utilizing genuine world datasets in gas pipeline and water treatment framework. Discoveries exhibit that the proposed model beats other contending approaches with comparable computational intricacy.

Internet of Things(IoT) gadgets are progressively coordinated in digital actual frameworks (CPS), remembering for basic foundation areas like dams and utility plants. In these settings, IoT gadgets (likewise alluded to as Modern IoT or IIoT) are in many cases part of a Modern Control Framework (ICS), entrusted with the dependable activity of the foundation. ICS can be extensively characterized to incorporate administrative control and information procurement (SCADA) frameworks, circulated control frameworks (DCS), and frameworks that include programmable rationale regulators (PLC) and Modbus conventions. The association between ICS or IIoT-based frameworks with public organizations, notwithstanding, expands their assault surfaces and dangers of being focused on by digital lawbreakers. One high-profile model is the Stuxnet lobby, which supposedly designated Iranian axes for atomic enhancement in 2010, making extreme harm the gear. Another model is that of the occurrence focusing on a siphon that brought about the disappointment of an Illinois water plant in 2011.
BlackEnergy3 was another mission that designated Ukraine power lattices in 2015, bringing about blackout that impacted roughly 230,000 individuals [4]. In spite of the fact that security arrangements produced for data innovation (IT) and functional innovation (OT) frameworks are generally adult, they may not be straightforwardly relevant to ICSs. For instance, this could be the situation because of the tight coordination between the controlled actual climate and the digital frameworks. In this manner, framework level security strategies are important to break down actual way of behaving and keep up with framework activity accessibility [1].

ICS security objectives are focused on in the request for accessibility, trustworthiness, and secrecy, in contrast to most IT/OT frameworks (by and large focused on in the request for classification, respectability, and accessibility) [5]. Because of close coupling between factors of the criticism control circle and actual cycles, (effective) digital assaults on ICS can bring about serious and possibly lethal ramifications for the general public and our current

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.54|

| Volume 5, Issue 12, December 2022 |

| DOI:10.15680/IJMRSET.2022.0601004 |

circumstance. This builds up the significance of planning very powerful wellbeing and security estimations to distinguish and forestall interruptions focusing on ICS [1]. Albeit half breed-based approaches are viable at distinguishing strange actuates, they are not solid because of successive organization overhauls, bringing about various Interruption Location Framework (IDS) typologies [7]. Past this, customary assault location and attribution methods mostly depend on network metadata examination (for example IP addresses, transmission ports, traffic length, and bundle spans). In this way, there has been recharged interest in using assault discovery and attribution arrangements in light of AI (ML) or Profound Brain Organizations (DNN) lately. Furthermore, assault recognition approaches can be arranged into network-based or have based approaches. Directed grouping, single-class or multi-class Backing Vector Machine (SVM), fluffy rationale, Fake Brain Organization (ANN), and DNN are regularly involved methods for assault identification in network traffic. These methods examine continuous traffic information to distinguish malignant assaults on time. In any case, assault identification that considers just organization and host information might neglect to recognize refined assaults or insider assaults.

Solo models that integrate interaction/actual information can supplement a framework's observing since they don't depend on point-by-point information on the digital dangers. By and large, a complex aggressor with adequate information and time, for example, a country state progressed relentless danger entertainer, might possibly dodge vigorous security arrangements. Besides, the greater part of the current methodologies disregards the imbalanced property of ICS information by displaying just a framework's typical way of behaving and revealing deviations from ordinary way of behaving as oddities. This is, maybe, because of restricted assault tests in existing datasets and true situations. Despite the fact that utilizing larger part class tests is a decent answer for stay away from issues due to imbalanced datasets, the prepared model will have no perspective on the assault tests' examples. All in all, such a methodology neglects to recognize concealed assaults and experiences a high bogus positive rate [8]. Consequently, there have been endeavors to use DL draws near, for instance, to work with robotized include (portrayal) figuring out how to show complex ideas from more straightforward ones [9] without relying upon human-created highlights [10].

To get brilliant assembling frameworks, Industry 4.0 raised two requests for digital protection: "Security Engineering" and "Security by Plan" in future shrewd frameworks [22]. This will expect frameworks to have programmed recognition of malware, dangers and assaults with zero-establishment. Computational insight will assume significant parts for digital knowledge - following, investigating, distinguishing advanced security dangers to battle infections, programmers and psychological militants that exist on the Web for various purposes, aside from the digital dangers to Modern IoT referenced above, including digital following and badgering, coercion, shakedown, financial exchange control, complex corporate reconnaissance, and arranging or completing fear monger exercises. Transformative Calculation and other Computational Knowledge strategies (EC&CI) have been effectively applied in different regions, like computational science, clinical science, finance, designing, and so forth. Digital protection is another key region where we can take advantage of the force of EC&CI. Not at all like other issue spaces, the plan of keen answers for Digital protection must be still up in the air, complex assailants who might focus on any versatile digital actual frameworks. Digital Knowledge is supposed to have the option to tie down the advantages to all from our digital associated world. Joining EC&CI with Network protection will assist with supporting our protected, secure and prosperous associated future.

II. LITERATURE REVIEW

Amir Namavar Jahromiet.al Getting Web of-Things (IoT)- empowered digital actual frameworks (CPS) can challenge, as security arrangements created for general data/functional innovation (IT/OT) frameworks may not be as compelling in a CPS setting. Subsequently, this article presents a two-level group assault discovery and attribution structure intended for CPS, and all the more explicitly in a modern control framework (ICS). At the main level, a choice tree joined with a clever troupe profound portrayal learning model is created for distinguishing assaults imbalanced ICS conditions. At the subsequent level, a gathering profound brain network is intended to work with assault attribution. The proposed model is assessed utilizing genuine informational indexes in gas pipeline and water treatment framework.

Discoveries exhibit that the proposed model beats other contending approaches with comparative computational intricacy. MuruganNagarajan et.al Digital Actual Frameworks (CPSs) becoming one of the most perplexing, astute, and complex frameworks. Guaranteeing security is a significant viewpoint towards CPSs. In any case, expansion in refined and intricacy assaults in CPSs, the customary oddity location techniques are dealing with issues and furthermore development in volume of information becomes testing which requires space explicit information that could be applied straightforwardly to dissect these difficulties. To conquer this issue, different profound learning-based irregularity discovery framework is created. In this examination, we propose an oddity discovery approach by coordination of astute profound learning strategy named Convolutional Brain Organization

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.54|

| Volume 5, Issue 12, December 2022 |

| DOI:10.15680/IJMRSET.2022.0601004 |

(CNN) with Kalman Channel (KF) based Gaussian-Blend Model (GMM). The proposed model is utilized for recognizing and distinguishing atypical way of behaving in CPSs.

This proposed system comprises of two significant cycles. First is to pre-process the information by changing and separating unique information into new configuration and accomplished protection conservation of the information. Furthermore, we proposed GMM-KF coordinated profound CNN model for abnormality identification and precisely assessed the back probabilities of atypical and real occasions in CPSs. Hongmei He et.al Web of Things (IoT) has led to the fourth modern transformation (Industrie 4.0), and it brings incredible advantages by interfacing individuals, cycles and information. In any case, network safety has turned into a basic test in the IoT empowered digital actual frameworks, from associated production network, Enormous Information delivered by tremendous measure of IoT gadgets, to industry control frameworks. Developmental calculation joining with other computational knowledge will assume a significant part for network safety, for example, counterfeit resistant component for IoT security design, information mining/combination in IoT empowered digital actual frameworks, and information driven online protection.

This paper gives an outline of safety challenges in IoT empowered digital actual frameworks and what developmental calculation and other computational knowledge innovation could contribute for the difficulties. The outline could give hints and direction to explore in IoT security with computational knowledge. MahaM.Althobaiti et.al Progressed advancements of Modern Digital Actual Frameworks (CPSs), containing Web of Things (IoT) finds valuable in a few application regions like transportation, savvy urban communities, medical care, energy conveyance, farming, and so on. Simultaneously, the expanded use of modern CPS offers numerous dangers which could have significant meanings for clients. As of late, mental registering and man-made reasoning strategies offer new open doors for the upheaval of modern CPSs. Consequently, to accomplish security in modern CPS, man-made intelligence-based interruption identification framework (IDS) can be created to identify irregularities and forestall their unsafe impacts. With this inspiration, this paper presents a clever mental figuring-based IDS method to accomplish security in modern CPS.

The proposed model includes various phases of activities like information securing, pre-processing, highlight determination, order, and boundary enhancement. The proposed model includes pre-processing to dispose of the commotion that exists in the information. Then, the introduced model purposes paired bacterial rummaging advancement (BBFO) based include choice strategy to choose an ideal subset of highlights. Other than the gated repetitive unit (GRU) model is applied to recognize the presence of interruptions in the modern CPS climate. At long last, Nesterov-sped up Versatile Second Assessment (NADAM) enhancer is applied for the hyperparameter improvement of the GRU model so that the location rate can be upgraded. To approve the exhibition of the BBFO-GRU model, a progression of tests was done utilizing the information from modern CPS and the resultant qualities featured the promising execution of the proposed model with a precision of 98.45%. AaishaMakkar et.al In the period of independent frameworks, the security is crucial module for adaptable figuring climate. Because of expanded PC power and organization speed, another figuring worldview, for example, mental roused processing, will arise. Such a worldview offers human-focused types of assistance that are helpful and pleasant at whenever, anyplace, and on any gadget.

On the underpinning of shrewd city climate, human PC cooperation, savvy administrations, and widespread gadget availability, Digital Actual Processing for Digital Actual frameworks has as of late been examined. Be that as it may, in this proposition, a mental motivated system for getting CPS is examined. The mental capacity is surrendered to the web indexes by refreshing the PageRank positioning procedure. The proposed structure, named SecureCPS is prepared with ongoing aggregate dataset for denoting the significance of website page with the help the looks. The eye locales are checked utilizing Point of convergence Identifier calculation. The system is approved with AI models and brought about accomplishing 98.51% precision and it's beating the current structures. Himanshu Mittal et.al In Modern Web of-Things, information streams across heterogeneous organizations which brings about a few digital actual assaults. Besides, the security of unlabelled information is a difficult undertaking. For the equivalent, this paper presents another bunching technique for interruption identification. The proposed strategy utilizes an original variation of gravitational hunt calculation to get ideal bunches. In the proposed variation, Kbest is changed as a dramatically diminishing capability with calculated planning based tumultuous way of behaving.

To approve the proposed variation, a near investigation on IEEE CEC2013 benchmark capabilities is directed against five existing calculations. Exploratory outcomes are examined as far as mean mistake esteem, Wilcoxon rank-aggregate test, combination diagram, box-plot, and time intricacy. It has been seen that proposed variation achieved best qualities for most extreme number of times on each aspect, for example 10, 13, 15, and 10 on 10, 30, 50, and 90 aspects, individually. Further, the adequacy of the proposed grouping technique is tried on five Modern Web of-Things datasets. The assessment is acted as far as F-measure and calculation time. Tests certify that the proposed strategy beats considered techniques on 80% of the datasets as far as F-measure and calculation time for guaranteeing security in a

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.54|

| Volume 5, Issue 12, December 2022 |

| DOI:10.15680/IJMRSET.2022.0601004 |

constant Modern Web of-Things climate. Kim, Nam Yong et.al As of late, Digital Actual Framework (CPS) is one of the center advances for acknowledging Web of Things (IoT). The CPS is another worldview that looks to combine the physical and digital universes in which we live.

Nonetheless, the CPS experiences specific CPS gives that could straightforwardly undermine our lives, while the CPS climate, including its different layers, is connected with on-the-spot dangers, making it important to concentrate on CPS security. Thusly, a review situated top to bottom comprehension of the weaknesses, dangers, and assaults is expected of CPS security and protection for IoT. In this paper, we dissect security issues, dangers, and answers for IoT-CPS, and assess the current explores. The CPS raises a number difficulties through current security markets and security issues. The concentrate likewise addresses the CPS weaknesses and assaults and infers difficulties. At long last, we suggest answers for every arrangement of CPS security dangers, and examine approaches to settling likely future issues.**3.3**

III. PROPOSED SYSTEM

The proposed assault identification comprises of two stages, specifically portrayal learning and discovery stage. Utilizing an Upgraded Directed AI techniques on an imbalanced dataset yielded a ML model that basically educated larger part class designs and missed minority class qualities. Most scientists have attempted to address this test by creating new examples or eliminating specific examples to make the dataset adjusted and afterward passing the information to a ML Model. Nonetheless, in ICS/IIoT security applications, creating or eliminating tests are not sensible arrangements. Because of the ICS/IIoT frameworks' responsiveness, produced tests ought to be approved in a genuine organization, which is unimaginable since the created assault tests might be destructive to the organization and cause extreme effects on the climate or human existence. What's more, approval of the produced tests is tedious. Besides, eliminating the typical information from a dataset isn't the right arrangement since the quantity of assault tests in ICS/IIoT datasets is generally under 10% of the dataset, and the majority of the dataset information is disposed of by eliminating 80% of the dataset.

To keep away from the previously mentioned issues in taking care of imbalanced datasets, this study proposed another directed AI technique to make the Models ready to deal with imbalanced datasets without evolving, creating, or eliminating tests. This model comprised of two solo stacked auto encoders, each liable for tracking down designs from one class. Since each model attempts to extricate unique examples of one class disregarding another, the result of that model addressed its bits of feedbacks well. The stacked auto encoders had three decoders and encoders with information and last portrayal layers. Then the ML models will actually want to perform twofold characterization and multi-name Arrangement with better precision execution.

3.3.1 Benefits OF PROPOSED Framework

- The proposed framework had further developed the precision results.
- Despite the fact that our examination shows that the exhibitions of applied philosophies are sensibly great, the outright upsides of the measurements demonstrate that this is a difficult undertaking and deserving of additional investigation.
- We accept this examination could additionally underline the foundation for new components applied in various areas of medical care to assess sadness and related factors.

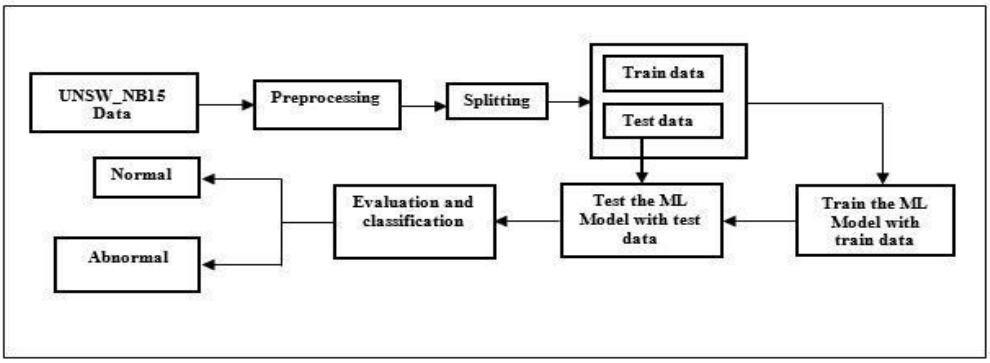


Fig 5.1.1 Architecture for binary classification

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.54|

| Volume 5, Issue 12, December 2022 |

| DOI:10.15680/IJMRSET.2022.0601004 |

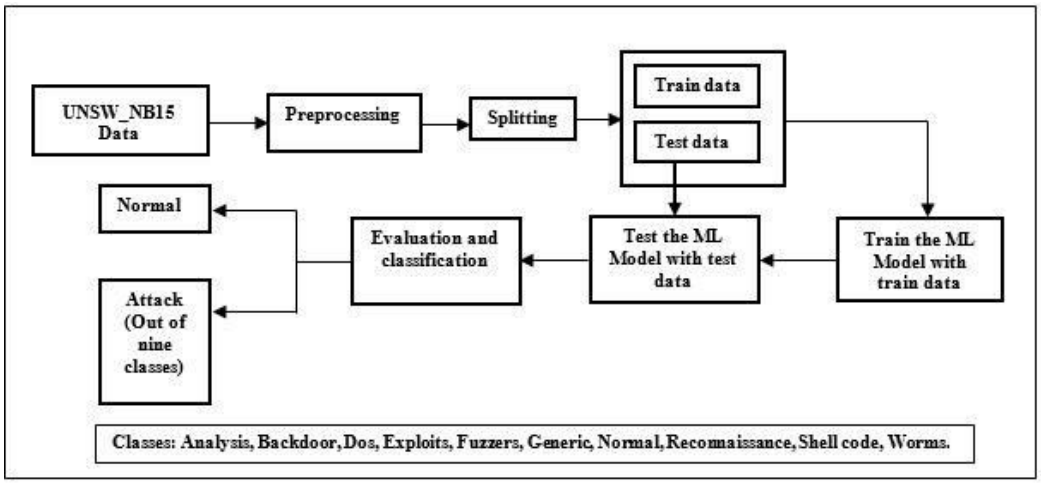
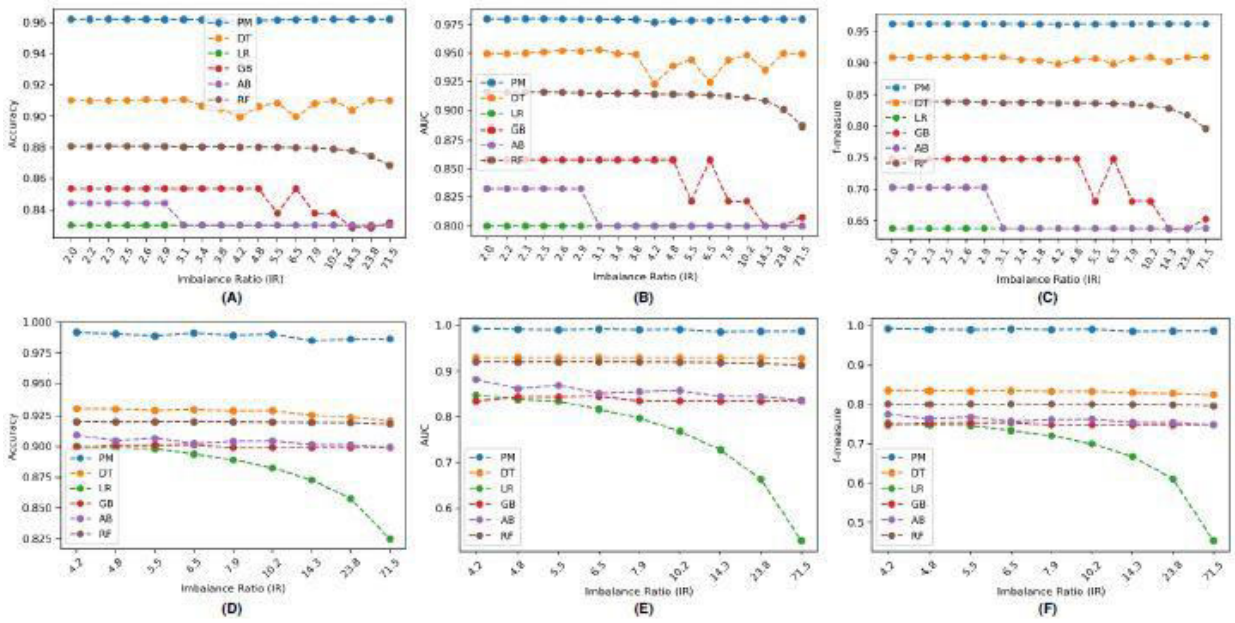


Fig 5.1.2 Architecture for Multi Class classification

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.

Results



Comparison of accuracy, AUC, and f-measure of the proposed attack detection method and other basic classifiers on original representation for different attack IR (A), (B), and (C) on the gas pipeline dataset and (D), (E), and (F) on the SWaT dataset. In the figures, PM is the proposed attack detection method, DT is the Decision Tree, LR is the Logistic Regression, GB is the Gradient Boosting, AB is the AdaBoost M1, and RF is the Random Forest.

IV. CONCLUSION

This paper proposed an original two-stage group AI based assault location and assault attribution system for imbalanced ICS information. The assault identification stage utilizes AI to plan the examples to the new higher layered space and applies a structure to recognize the assault tests. This stage is powerful to imbalanced datasets and fit for distinguishing already concealed assaults. The assault attribution stage is a troupe of a few one-versus all classifiers, each prepared on a particular assault quality. Regardless of the mind boggling design of the proposed structure, the computational intricacy of the preparation and testing stages are separately O(n 4) and O(n 2), (n is the quantity of

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.54|

| Volume 5, Issue 12, December 2022 |

| DOI:10.15680/IJMRSET.2022.0601004 |

preparing tests), which are like those of other ML-based methods in the writing. Besides, the proposed structure can identify and credit the examples opportune with a preferred review and f-measure over past works.

The primary analysis results concerning MLA contribution showed that direct Relapse in multi class grouping exhibited the most obviously awful outcomes, while the MLP calculation showed the best outcomes. Furthermore, the association of various IoT multi-vector digital assault highlights in view of stream examination and elements in light of the most regularly utilized IoT conventions caused the discovery of TCP, UDP, HTTP GET, and DNS burrowing assaults around at a similar level. In this Venture, we checked on the known ways to deal with identify assaults on the Web of Things foundation in light of AI and examined their adequacy. We explored the chance of identifying traffic assaults on the Web of Things framework in light of stream examination and the most usually utilized IoT conventions, like HTTP, MQTT, and DNS. Traffic from notable botnets, like Mirai, Dull Nexus, and Gafgyt was taken from notable information bases that address normal assaults on the Web of Things frameworks, for example, TCP, UDP, HTTP GET, and DNS burrowing, utilized as pernicious traffic. Likewise, assault traffic was produced utilizing known utilities, and harmless IoT traffic was gathered from gadgets like a switch, an indoor regulator, and a camcorder. The elements introduced in the work were grouped utilizing different techniques for AI and were taken out from the got traffic. The degrees of recognition of the multi-vector assaults on the Web of Things framework to a great extent rely upon the elaborate objects of preparing and test samplings/settings of AI calculations.

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] I. 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] I. 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.

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.54|

| Volume 5, Issue 12, December 2022 |

| DOI:10.15680/IJMRSET.2022.0601004 |

[17] A. 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] A. 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.

Impact Factor
7.54

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH IN SCIENCE, ENGINEERING AND TECHNOLOGY

| Mobile No: +91-6381907438 | Whatsapp: +91-6381907438 | ijmrset@gmail.com |

www.ijmrset.com