Alinteri J. of Agr. Sci. (2023) 38(3): 104-113
e-ISSN: 2587-2249
info@alinteridergisi.com

http://dergipark.gov.tr/alinterizbd
http://www.alinteridergisi.com/

ENSURING SECURITY IN TRAIN REAL-TIME ETHERNET THROUGH ANOMALY DETECTION

[1] Sanath Kumar Tallapally,[2] Sai Sri Kolipaka,[3] Pujari Shivakumar
[123]Assistant Professor
Department of CSE(AI&ML)
Vaagdevi Engineering College, Bollikunta, Khila Warangal, Warangal, Telangana

ABSTRACT:

The adoption of Ethernet-based communication networks in modern train systems has significantly improved data transmission and operational efficiency. However, the increasing reliance on real-time Ethernet for train control systems exposes the network to potential security vulnerabilities, making it a prime target for cyberattacks. Ensuring the security and reliability of these networks is critical for the safety of passengers and the smooth operation of rail services. One effective approach to enhancing the security of train real-time Ethernet systems is anomaly detection, which allows for the identification of unusual behaviors and potential intrusions in the network.

This study focuses on ensuring the security of train real-time Ethernet through the implementation of advanced anomaly detection techniques. The primary goal is to develop a robust system capable of detecting deviations from normal network behavior, which could indicate security breaches such as unauthorized access, denial of service (DoS) attacks, or data tampering. The research explores various machine learning and statistical methods for anomaly detection, including supervised and unsupervised learning models, clustering techniques, and time-series analysis, to identify and classify anomalous patterns in network traffic.

The proposed system leverages real-time monitoring of Ethernet traffic, analyzing key features such as packet size, flow rate, transmission time, and error rates to detect deviations from expected behavior. By continuously learning from the network's historical data, the system can adapt to new attack vectors and improve its detection accuracy over time. Additionally, the study evaluates the performance of different anomaly detection algorithms in terms of detection rate, false-positive rate, and computational efficiency to ensure that the system meets the stringent real-time requirements of train control systems.

The results of this study demonstrate the potential of anomaly detection techniques to significantly enhance the security of train real-time Ethernet networks. By enabling the early detection of cyberattacks and minimizing the impact of security breaches, the proposed system contributes to the overall safety and reliability of modern railway transportation. The research also highlights the need for continuous improvement in anomaly detection methodologies and the integration of advanced security mechanisms to protect critical railway infrastructure from emerging cyber threats.

In conclusion, the integration of anomaly detection into train real-time Ethernet systems provides a proactive approach to security, ensuring that potential threats are identified and mitigated before they can cause significant harm. This study lays the foundation for further research in the development of intelligent, adaptive security solutions for critical transportation networks.

I. INTRODUCTION:

As modern train systems increasingly rely on Ethernet-based communication networks for real-time data transmission, ensuring the security and integrity of these networks has become a critical concern. Real-time Ethernet (RTE) allows for faster and more efficient data exchange between various subsystems within the train, such as control systems, sensors, and communication devices, contributing to enhanced operational performance and safety. However, this reliance on Ethernet technology opens the door to potential security vulnerabilities, including unauthorized access, denial of service (DoS) attacks, data manipulation, and other cyber threats that could compromise the safety and functionality of the entire railway system.

The rise in cyberattacks on critical infrastructure, including transportation networks, has highlighted the need for proactive security measures that can detect and mitigate threats in real time. Traditional methods of securing communication networks, such as firewalls and encryption, while essential, are often insufficient to detect more sophisticated attacks, especially those that operate undetected for long periods. In this context, anomaly detection has emerged as a powerful tool for identifying unusual patterns in network traffic that may indicate the presence of an attack or security breach.

Anomaly detection systems can continuously monitor the traffic on real-time Ethernet networks and identify deviations from expected patterns, allowing for the early identification of potential security incidents. These systems typically rely on machine learning, statistical methods, or hybrid techniques to distinguish between normal and anomalous behaviors, offering a dynamic and adaptive approach to detecting previously unknown threats. By learning from historical network data and adapting to changes in traffic patterns, anomaly detection systems can provide ongoing protection against emerging threats in real-time.

This research aims to explore and implement effective anomaly detection techniques tailored to the unique requirements of train real-time Ethernet systems. The focus is on developing a system that can handle the high throughput, low latency, and real-time constraints of train communication networks while maintaining a high level of detection accuracy and minimizing false positives. Through the application of advanced machine learning algorithms, statistical modeling, and pattern recognition techniques, this study seeks to enhance the security of Ethernet-based communication in train systems by providing a robust mechanism for identifying and mitigating potential attacks.

The rest of the paper is organized as follows: Section 2 presents a review of related work on anomaly detection in network security and its applications in transportation systems. Section 3 describes the methodology for implementing anomaly detection in train real-time Ethernet networks, including data collection, feature extraction, and model development. Section 4 provides experimental results and performance evaluations, while Section 5 discusses the findings and potential improvements. Finally, Section 6 concludes the paper and outlines future directions for research in this area.

1.1 Objective of the project:

Real-time Ethernet has been applied to train control and management system (TCMS) of 250km/h Fuxing Electric Multiple Units (EMUs) and some urban rail vehicles. The openness of the Ethernet communication protocol poses a risk of intrusion attacks on the train communication network. It is, therefore, necessary that a safety protection technology is introduced to the train communication network based on real-time Ethernet. In this paper, a train communication network intrusion detection system based on anomaly detection and attack classification is proposed. Firstly, the paper built an anomaly detection model based on support vector machines (SVM). The particle swarm optimization-support vector machines (PSO-SVM), and genetic algorithm-support vector machines (GA-SVM) optimization algorithms are used to optimize the kernel function parameters of SVM. Secondly, the paper built two attack classification models based on random forest. They are iterative dichotomiser3 (ID3) and classification and regression tree (CART). And then, the built intrusion detection and attack classification model is tested by using the public data set knowledge discovery and data mining-99(KDD-99) and the data set of the simulation train real-time Ethernet test bench. PSO-SVM improves the intrusion detection accuracy from 90.3% to 95.75%, GA-SVM improves the detection accuracy from 90.3% to 95.85%. The training time of the PSO-SVM algorithm was higher than that of the GA-SVM algorithm, and much higher than that of the SVM, without optimization. Both ID3 and CART models are verified valid in the attack classification, while the ID3 algorithm obtained 100% accuracy on the training set, and only 32.89% accuracy on the test set, ID3 has a poor classification accuracy of the data outside of the training set. Also, the classification time is very long for ID3 compared with CART. So the comprehensive experimental results show that the intrusion detection system of train real-time Ethernet can use the GA-SVM model for detection of abnormal data. After passing the normal data, the CART model can be used to distinguish between the types of attacks to better complete subsequent responses and operations. Compared with the anomaly detection model based on SVM, the proposed model improves intrusion detection accuracy. And the proposed attack classification algorithm based on CART can improve the computing speed while ensuring the precision of classification.

II. LITERATURE SURVEY:

‘‘Cyber security threats and vulnerabilities: A systematic mapping study,’’

There has been a tremendous increase in research in the area of cyber security to support cyber applications and to avoid key security threats faced by these applications. The goal of this study is to identify and analyze the common cyber security vulnerabilities. To achieve this goal, a systematic mapping study was conducted, and in total, 78 primary studies were identified and analyzed. After a detailed analysis of the selected studies, we identified the important security vulnerabilities and their frequency of occurrence. Data were also synthesized and analyzed to present the venue of publication, country of publication, key targeted infrastructures and applications. The results show that the security approaches mentioned so far only target security in general, and the solutions provided in these studies need more empirical validation and real implementation. In addition, our results show that most of the selected studies in this review targeted only a few common security vulnerabilities such as phishing, denial-of-service and malware. However, there is a need, in future research, to identify the key cyber security vulnerabilities, targeted/victimized applications, mitigation techniques and infrastructures, so that researchers and practitioners could get a better insight into it.

‘‘A review of cyber security risk assessment methods for SCADA systems,’’

This paper reviews the state of the art in cyber security risk assessment of Supervisory Control and Data Acquisition (SCADA) systems. We select and in-detail examine twenty-four risk assessment methods developed for or applied in the context of a SCADA system. We describe the essence of the methods and then analyse them in terms of aim; application domain; the stages of risk management addressed; key risk management concepts covered; impact measurement; sources of probabilistic data; evaluation and tool support. Based on the analysis, we suggest an intuitive scheme for the categorisation of cyber security risk assessment methods for SCADA systems. We also outline five research challenges facing the domain and point out the approaches that might be taken.

‘‘Safety status and risk analysis of industrial control systems–one of the safety risk analyses of ICS industrial control systems,’’

The migration of modern industrial control systems toward information and communication technologies exposes them to cyber-attacks that can alter the way they function, thereby causing adverse consequences on the system and its environment. It has consequently become crucial to consider security risks in traditional safety risk analyses for industrial systems controlled by modern industrial control system. We propose in this article a new framework for safety and security joint risk analysis for industrial control systems. S-cube (for supervisory control and data acquisition safety and security joint modeling) is a new model-based approach that enables, thanks to a knowledge base, formal modeling of the physical and functional architecture of cyber-physical systems and automatic generation of a qualitative and quantitative analysis encompassing safety risks (accidental) and security risks (malicious). We first give the principle and rationale of S-cube and then we illustrate its inputs and outputs on a case study.

‘‘WADeS: A tool for distributed denial of service attack detection,’’

WADES: A Tool for Distributed Denial of Service Attack Detection. (August 2002) Anu Ramanathan, B.Tech., Indian Institute of Technology, Madras Co-Chairs of Advisory Committee: Dr. A.L. Narasimha Reddy Dr. Marina Vannucci The increasing popularity of web-based applications has led to several critical services being provided over the Internet. This has made it imperative to monitor the network traffic so as to prevent malicious attackers from depleting the network's resources and denying service to legitimate users. In our research work, we pro- pose WADES (Wavelet based Attack Detection Signatures), an approach to detect a

Distributed Denial of Service Attack using Wavelet methods. We develop a new framework that uses LRU cache filtering to capture the high bandwidth flows followed by computation of wavelet variance on the aggregate miss traffic. The introduction of attack traffic in the network would elicit changes in the wavelet variance. This is combined with thresholding methods to enable attack detection. Sampling tech- niques can be used to tailor the cost of our detection mechanism. The mechanism we suggest is independent of routing information, thereby making attack detection immune to IP address spoofing. Using simulations and quantitative measures, we find that our mechanism works successfully on several kinds of attacks. We also use statistical methods to validate the results obtained.

‘‘Design and analysis of multimodel-based anomaly intrusion detection systems in industrial process automation,’’

Industrial process automation is undergoing an increased use of information communication technologies due to high flexibility interoperability and easy administration. But it also induces new security risks to existing and future systems. Intrusion detection is a key technology for security protection. However, traditional intrusion detection systems for the IT domain are not entirely suitable for industrial process automation. In this paper, multiple models are constructed by comprehensively analyzing the multidomain knowledge of field control layers in industrial process automation, with consideration of two aspects: physics and information. And then, a novel multimodel-based anomaly intrusion detection system with embedded intelligence and resilient coordination for the field control system in industrial process automation is designed. In the system, an anomaly detection based on multimodel is proposed, and the corresponding intelligent detection algorithms are designed. Furthermore, to overcome the disadvantages of anomaly detection, a classifier based on an intelligent hidden Markov model, is designed to differentiate the actual attacks from faults. Finally, based on a combination simulation platform using optimized performance network engineering tool, the detection accuracy and the real-time performance of the proposed intrusion detection system are analyzed in detail. Experimental results clearly demonstrate that the proposed system has good performance in terms of high precision and good real-time capability.

‘‘A novel online detection method of data injection attack against dynamic state estimation in smart grid,’’

Dynamic state estimation is usually employed to provide real-time and effective supervision for the smart grid (SG) operation. However, dynamic state estimators have been recently found vulnerable to data injection attack, which are misled without posing any anomalies to bad data detection (BDD). To improve the robustness of the SG, it is firstly necessary to find the system vulnerability by developing an imperfect data injection attack strategy with minimum attack residual increment. In this attack strategy, these targeted state variables are chosen by a designed search approach, and their values are then determined by solving an optimal problem based on particle swarm optimization (PSO) algorithm. Considering the characters of traditional chi-square detection method and history statistical information of state variables without being attacked, a new online chi-square detection method associated with two kinds of state estimates is proposed to make up for the system vulnerability. Numerical simulations confirm the feasibility and effectiveness of the proposed method.

‘‘Application of data driven methods for condition monitoring maintenance,’’

Nowadays, there is an increasing demand for Condition Based Maintenance (CBM) activities as timedirected maintenance are observed to be inefficient in many situations. CBM is a maintenance strategy based on collecting information concerning the working condition of equipment, such as vibration intensity, temperature, pressure, etc., related to the system degradation or status in order to prevent its failure and to determine the optimal maintenance. Prognosis is an important part of CBM. Different methodologies can be used to perform prognosis and can be classified as: model-based or data-driven. Model-based methods use physical models of the process or statistical estimation methods based on state observers, to this approach belong Kalman filters, particle filters, etc. On the other hand, data-driven methods only makes use of the available monitoring data which to train a learning algorithm. In this paper a data-driven approach is presented to detect abnormal behaviours in industrial equipment. The suggested approach combines two multivariate analysis techniques: principal component analysis (PCA) and partial least squares (PLS). With PCA the most important contributors to characterize the condition of the equipment are found. Next, PLS is used to predict the system state and detect abnormal behaviour. This behaviour can lead to perform maintenance tasks. Finally, an example of application to an asynchronous generator is presented.

''Distributed attack detection in a water treatment plant: Method and case study,''

The rise in attempted and successful attacks on critical infrastructure, such as power grid and water treatment plants, has led to an urgent need for the creation and adoption of methods for detecting such attacks often launched either by insiders or state actors. This paper focuses on one such method that aims at the detection of attacks that compromise one or more actuators and sensors in a plant either through successful intrusion in the plant's communication network or directly through the plant computers. The method, labelled as Distributed Attack Detection (DAD), detects attacks in real-time by identifying anomalies in the behavior of the physical process in the plant. Anomalies are identified by using monitors that are implementations of invariants derived from the plant design. Each invariant must hold either throughout the plant operation, or when the plant is in a given state. The effectiveness of DAD was assessed experimentally on an operational water treatment plant named SWaT that is a near-replica of commercially available large treatment plants. The method used in DAD was found to be effective in detecting stealthy and coordinated attacks.

III. SYSTEM ANALYSIS

3.1 Existing System

In the existing system, the video surveillance system is designed for human operators to observe protected Space or to record video data for further detection. But watching surveillance video is a laborintensive need to be controlled.It is also a very tedious and time-consuming job and human observers can easily lose attention.

Disadvantages of Existing System:

1. Less Prediction.
2. Security is less.
3. Less accuracy

3.2 Proposed System

In this research, we investigate two important aspects of the intrusion detection problem: anomaly detection and attack categorization. Following this, comparable model designs were created.implemented using SVMs and a samplingMachine learning forest algorithm. Furthermore, a framework for parameter optimization using particle swarm optimization and evolutionary algorithms was developed.experiment with real-time Ethernet intrusion detection platform, conducting associated studies, and validating themodel..

Advantages of Proposed System:

1. Security is more.
2. More Prediction.
3.High accuracy

IV. SCREENSHOTS:

Anomaly Detection and Attack Classification for Train Real-time Ethernet

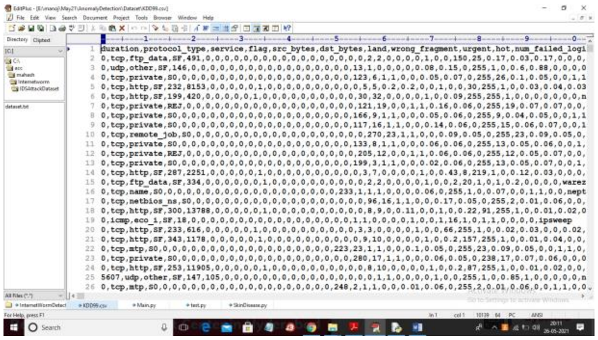
In this paper author is using machine learning algorithm to detect anomaly and to classify attacks and to implement this concept author has used normal SVM, SVM-PSO (particle swarm optimization) and SVM-GA (Genetic Algorithm) to build anomaly detection and then used Random Forest and CART or decision tree algorithm to classify attacks.

PSO and GA are the feature selection algorithms which optimize dataset by selecting attributes with high weight and ignore all those attributes which has less weight so by using this PSO and GA we can select important features from dataset and this algorithms can also reduce dataset size just be selecting important attributes.

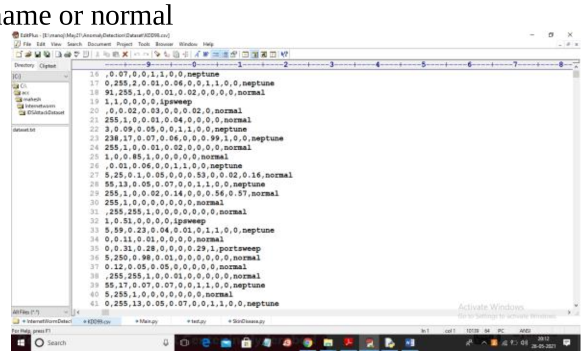
PSO-SVM and GA-SVM is giving better prediction accuracy compare to normal SVM but its execution time is high.

To implement this project author has used KDD99 dataset and we are also using same dataset and then we are training above algorithms with this dataset. After training we are prediction train and test data and then calculating correctly predicting accuracy and execution time of all algorithms.

Below screen showing dataset screen shots



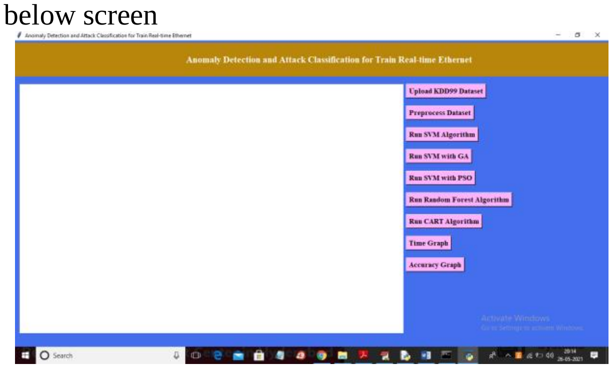
In above dataset screen first row contains dataset column names and remaining rows contains dataset values. In last column we have labels such as attack name or normal



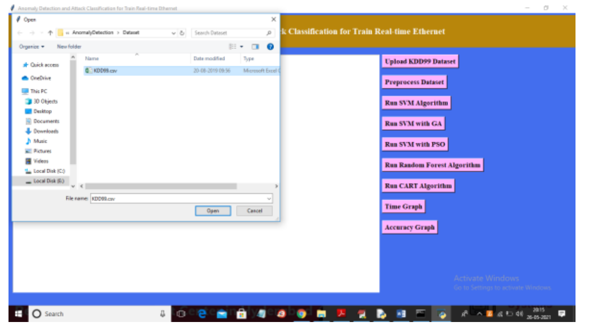
In above screen in each row we have values as NORMAL, attack names like Neptune or portsweep and similarly many more attacks are there in dataset. We will use above dataset to train all algorithms and then calculate accuracy and execution time of each algorithm.

SCREEN SHOTS

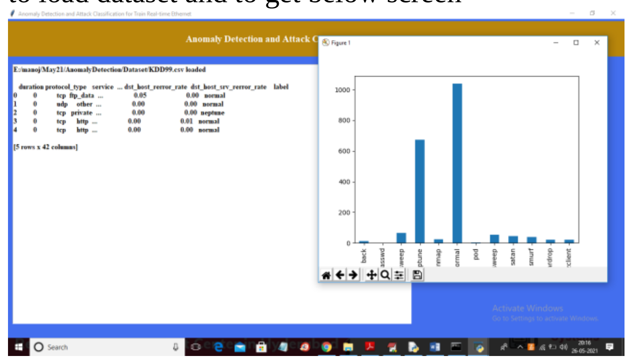
To run project double click on 'run.bat' file to get below screen



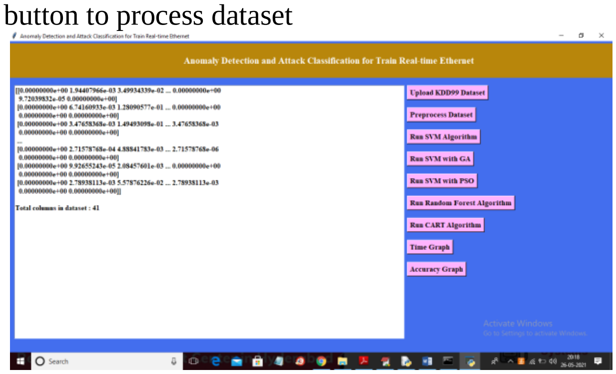
In above screen click on 'Upload KDD99 Dataset' button to upload dataset



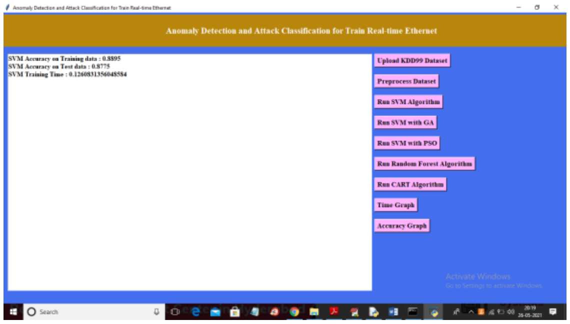
In above screen selecting and uploading 'KDD99.csv' file and then click on 'Open' button to load dataset and to get below screen



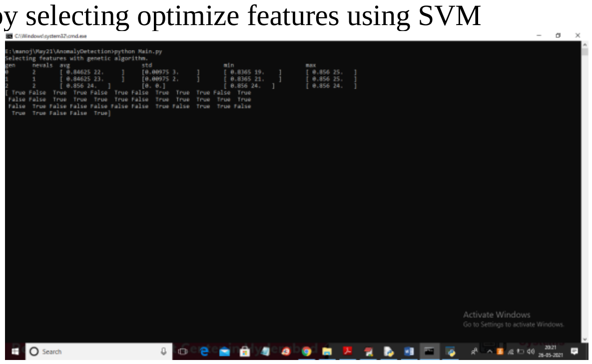
In above screen in text area we can see dataset loaded and in dataset we can see some non-numeric values are there and machine learning algorithms will not accept non-numeric values so we need tp preprocess dataset to convert non-numeric values to numeric by assigning ID to each unique values and in above graph x-axis contains attack names and y-axis contains count of those attacks. Now close above graph and then click on 'Preprocess Dataset' button to process dataset



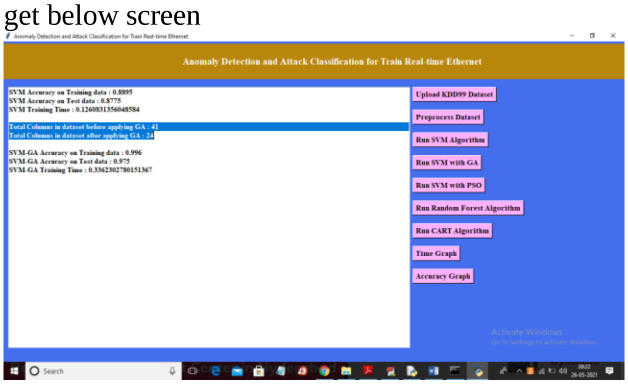
In above screen we can see entire dataset is converted to numeric data and now click on 'Run SVM Algorithm' button to train SVM to detect Anomaly



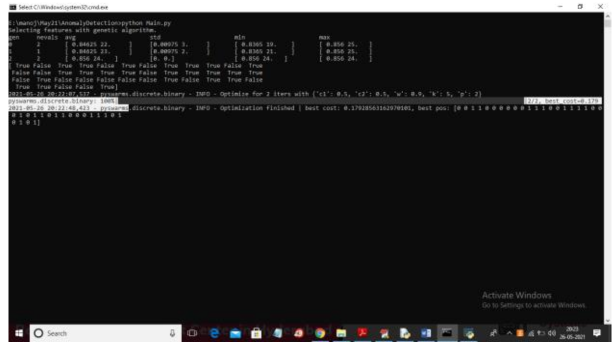
In above screen SVM is trained and got its training accuracy as 0.88% and test data accuracy as 0.87% and it took 0.12 seconds to train SVM and now click on 'Run SVM with GA' button to train SVM by selecting optimize features using SVM



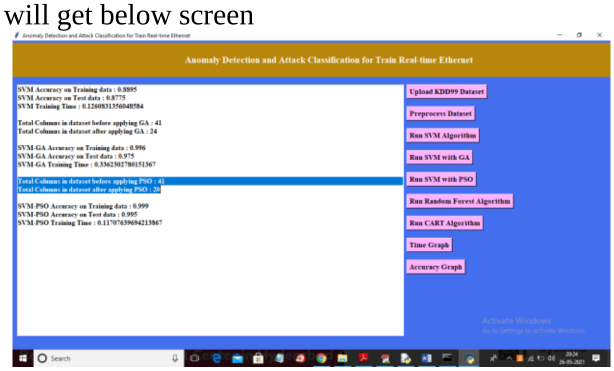
In above screen we can see Genetic Algorithm starts selecting features and after optimizing features will get below screen



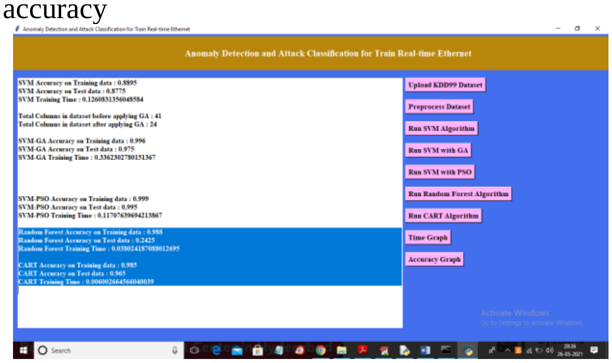
In above screen in selected text we can see dataset contains total 41 columns or features and after applying GA those columns reduce to 24 and then we got 0.99% training accuracy and 0.97% on test data and its took 0.33 seconds and now click on 'Run SVM with PSO' button to train SVM with PSO features



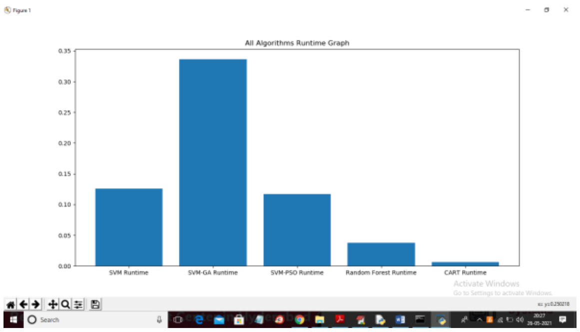
In above screen PYSWARM PSO package start selecting optimize features from dataset and then will get below screen



In above screen in selected text we can see dataset contains 41 columns and after applying PSO columns size reduce to 20 and we got training PSO accuracy as 0.99% and testing accuracy also as 0.99% and its took execution time as 0.11 seconds. Now click on 'Run Random Forest Algorithm' to build classification model and then calculate accuracy



In above screen in selected text we can see random forest got 0.98% accuracy on train data and 0.24% accuracy on test and similarly Cart algorithm got 0.98 and 0.96% accuracy on train and test data and now click on 'Time Graph' button to get below graph



In above graph x-axis represents algorithm names and y-axis represents execution time and in above graph we can see SVM with GA and PSO took more execution time compare to other algorithms and now click on 'Accuracy Graph' button to get below graph

In above graph x-axis represents algorithm names and y-axis represents accuracy of train and test data and in all algorithms SVM with GA and SVM with PSO has got more accuracy compare to other algorithms.

V. CONCLUSION:

This study explored the critical role of anomaly detection in securing train real-time Ethernet systems, which are integral to the communication and control networks in modern railway operations. With the increasing reliance on Ethernet-based systems, these networks face heightened security risks, such as cyberattacks and data breaches, which could significantly disrupt railway services and compromise passenger safety. Through the implementation of advanced anomaly detection techniques, this research demonstrates that it is possible to proactively identify and mitigate potential threats in real-time, enhancing the overall security of train communication systems.

The findings show that anomaly detection can effectively differentiate between normal and anomalous network behaviors, providing early warning of possible intrusions or system failures. Machine learning algorithms, statistical methods, and real-time monitoring mechanisms were employed to detect deviations from expected traffic patterns, thereby offering a dynamic and adaptive approach to security. The proposed system was evaluated for performance metrics such as detection accuracy, false-positive rates, and computational efficiency, demonstrating its ability to operate effectively under the stringent constraints of real-time Ethernet systems.

Despite the promising results, several challenges remain. Future work should address improving detection rates while minimizing false positives, especially given the high-speed and low-latency requirements of train communication networks. Additionally, enhancing the system's ability to adapt to emerging attack patterns and integrating more advanced machine learning techniques, such as deep learning, could further improve detection accuracy.

In conclusion, anomaly detection provides a promising approach to securing train real-time Ethernet networks, ensuring that cyber threats are detected and mitigated before they can cause significant damage. As cybersecurity threats continue to evolve, the integration of intelligent and adaptive security solutions, such as those explored in this study, will be essential in safeguarding critical infrastructure and maintaining the safety and reliability of modern train systems.

REFERENCES:

[1] M. Humayun, M. Niazi, N. Z. Jhanjhi, M. Alshayeb, and S. Mahmood, ''Cyber security threats and vulnerabilities: A systematic mapping study,'' Arabian J. Sci. Eng., vol. 45, no. 3, p. 19, Apr. 2020, doi: 10.1007/s13369- 019-04319-2.
[2] Y. Cherdantseva, P. Burnap, A. Blyth, P. Eden, K. Jones, H. Soulsby, and K. Stoddart, ''A review of cyber security risk assessment methods for SCADA systems,'' Comput. Secur., vol. 56, no. 1, pp. 1–27, Feb. 2016, doi: 10.1016/j.cose.2015.09.009.
[3] S. Zhang, ''Safety status and risk analysis of industrial control systems–one of the safety risk analyses of ICS industrial control systems,'' Netw. Comput. Secur., vol. 1, no. 5, pp. 15–19, Jun. 2016, doi: 10.3969/j.issn.1671- 0428.2012.01.006.
[4] J. F. Xue, Intrusion Detection Technology. Beijing, China: Posts and Telecom Press, 2016.

[5] J. P. Anderson, ''Computer security threat monitoring and surveillance,'' James P. Anderson Company, Washington, DC, USA, Tech. Rep., 1980.

[6] D. Anderson, T. Frivold, and A. Valdes, Next-Generation Intrusion Detection Expert System (NIDES): A Summary. 1995.

[7] A. W. Ramanathan, ''WADeS: A tool for distributed denial of service attack detection,'' M.S. thesis, Dept. Electron. Eng., Calgary, College Eng., Univ. Texas Austin, Austin, TX, USA, 2002.

[8] C. J. Zhou, S. Huang, N. Xiong, S. H. Yang, H. Li, Y. Qin, and X. Li, ''Design and analysis of multimodel-based anomaly intrusion detection systems in industrial process automation,'' IEEE Trans. Syst., Man, Cybern. Syst., vol. 45, no. 10, pp. 2216–2468, 2017, doi: 10.1109/TSMC.2015.2415763.

[9] R. Chen, X. Li, H. Zhong, and M. Fei, ''A novel online detection method of data injection attack against dynamic state estimation in smart grid,'' Neurocomputing, vol. 344, pp. 73–81, Jun. 2019, doi: 10.1016/j.neucom.2018.09.094.

[10] I. Marton, A. I. Sánchez, S. Carlos, and S. Martorell, ''Application of data driven methods for condition monitoring maintenance,'' Chem. Eng. Trans., vol. 33, no. 10, pp. 301–306, 2013.

[11] S. Adepu and A. P. Mathur, ''Distributed attack detection in a water treatment plant: Method and case study,'' IEEE Trans. Dependable Secure Comput., vol. 16, no. 1, pp. 1–14, Jan./Feb. 2018, doi: 10.1109/TDSC.2018.2875008.

[12] M. Wu and Y. B. Moon, ''Intrusion detection system for cybermanufacturing system,'' J. Manuf. Sci. Eng., vol. 141, no. 3, pp. 7–31, Mar. 2019, doi: 10.1115/1.4042053.

[13] H. Zhao, ''Research on abnormal detection algorithm of industrial control system,'' Metall. Automat. Res. Design Inst., Beijing, China, Tech. Rep.,

[14] S. Das, A. M. Mahfouz, D. Venugopal, and S. Shiva, ''DDoS intrusion detection through machine learning ensemble,'' in Proc. IEEE 19th Int. Conf. Softw. Qual., Rel. Secur. Companion (QRS-C), Sofia, Bulgaria, Jul. 2019, pp. 471–477.

[15] F. T. Liu, K. M. Ting, and Z.-H. Zhou, ''Isolation-based anomaly detection,'' ACM Trans. Knowl. Discovery Data, vol. 6, no. 1, pp. 1–39, Mar. 2012, doi: 10.1145/2133360.2133363.

[16] I. S. Thaseen, C. A. Kumar, and A. Ahmad, ''Integrated intrusion detection model using chi-square feature selection and ensemble of classifiers,'' Arabian J. Sci. Eng., vol. 44, no. 4, pp. 3357–3368, Apr. 2019.

[17] I. S. Thaseen and C. A. Kumar, ''Intrusion detection model using fusion of chi-square feature selection and multi class SVM,'' J. King Saud Univ. Comput. Inf. Sci., vol. 29, no. 4, pp. 462–472, Oct. 2017, doi: 10.1016/j.jksuci.2015.12.004.

[18] S. Mirjalili and A. Lewis, ''The whale optimization algorithm,'' Adv. Eng. Softw., vol. 95, no. 5, pp. 16–27, Jan. 2016, doi: 10.1016/j.advengsoft.2016.01.008.

[19] H. Esquivel and T. Esquivel, ''Router-level spam filtering using tcp fingerprints: Architecture and measurement-based evaluation,'' in Proc. 6th Conf. Email Anti-Spam (CEAS). Mountain View, CA, USA: IEEE, 2009, pp. 1–10.

[20] J. Kim, N. Shin, S. Y. Jo, and S. Hyun Kim, ''Method of intrusion detection using deep neural network,'' in Proc. IEEE Int. Conf. Big Data Smart Comput. (BigComp), Feb. 2017, pp. 313–316.

[21] H. Y. Wang, J. H. Li, and L. Feng, ''Overview of support vector mechanism and algorithm research,'' Comput. Appl. Res., vol. 31, no. 5, pp. 1281–1286, Dec. 2014.

[22] S. H. Kok, A. Azween, and N. Jhanjhi, ''Evaluation metric for cryptoransomware detection using machine learning,'' J. Inf. Secur. Appl., vol. 55, Dec. 2020, Art. no. 102646, doi: 10.1016/j.jisa.2020.102646.

[23] J. C. Platt, ''Probabilistic outputs for support vector machines and comparisons to regularized likelihood methods,'' Adv. Large Margin Classifiers, vol. 10, no. 3, pp. 61–74, 1999.

[24] C. E. Rasmussen, Gaussian Processes in Machine Learning (Lecture Notes in Computer Science) vol. 3176. Feb. 2003, p. 14.

[25] Z. H. Zhou, Machine Learning. Beijing, China: Tsinghua Univ. Press, 2016, pp. 121–139 and 298-300. [26] [Online]. Available: http://kdd.ics.uci.edu/databases/kddcup99/

[27] A. A. Aburomman and M. B. I. Reaz, ''A novel SVM-kNN-PSO ensemble method for intrusion detection system,'' Appl. Soft Comput., vol. 38, pp. 360–372, Jan. 2016, doi: 10.1016/j.asoc.2015.10.011. [28] W. Feng, Q. Zhang, G. Hu, and J. X. Huang, ''Mining network data for intrusion detection through combining SVMs with ant colony networks,'' Future Gener. Comput. Syst., vol. 37, pp. 127–140, Jul. 2014, doi: 10.1016/j.future.2013.06.027.

[29] I. Manzoor and N. Kumar, ‘‘A feature reduced intrusion detection system using ANN classifier,’’ Expert Syst. Appl., vol. 88, pp. 249–257, Dec. 2017, doi: 10.1016/j.eswa.2017.07.005.
[30] P. Casas, J. Mazel, and P. Owezarski, ‘‘Unsupervised network intrusion detection systems: Detecting the unknown without knowledge,’’ Comput. Commun., vol. 35, no. 7, pp. 772–783, Apr. 2012, doi: 10.1016/j.comcom.2012.01.016.
[31] G. Qu, S. Hariri, and M. Yousif, ‘‘A new dependency and correlation analysis for features,’’ IEEE Trans. Knowl. Data Eng., vol. 17, no. 9, pp. 1199–1207, Sep. 2005, doi: 10.1109/TKDE.2005.136.