[1]G.Malarselvi
[2]P. Arunagiri
[3]T.Thirumalaikumari
[4]S. Sathees babu
[5]G. Lingasamy
[6]N. Herald Anantha Rufus[6]

A Multifaceted Approach for Enhancing Anomaly Detection in Industrial Systems with Adaptive Synthetic Sampling and Machine Learning Evaluation

Abstract: - Anomalies in industrial systems refer to deviations from expected behaviour, indicating potential malfunctions, faults, or security breaches. These anomalies can disrupt operations, compromise safety, and lead to costly downtime, making their detection and mitigation critical for industrial reliability and security. This research addresses the imperative task of enhancing anomaly detection within industrial systems by integrating a multifaceted approach encompassing various techniques and methodologies. A primary challenge in anomaly detection, the imbalanced distribution of data, is tackled by employing Adaptive Synthetic Sampling (ADASYN), which dynamically generates synthetic samples for minority classes. This effectively mitigates the impact of class imbalance and substantially enhances detection performance. Additionally, filter-based feature selection methods are utilized, incorporating statistical measures like the Chi-Square Test and ANOVA F-Value to identify pertinent features essential for anomaly detection. The study further delves into supervised anomaly detection approaches, leveraging machine learning algorithms such as Support Vector Machines (SVM) and Gradient Boosting (GB) to differentiate between normal and anomalous activities. These algorithms undergo rigorous evaluation within a Virtual Testing Environment (VTE) simulator, meticulously replicating industrial processes for comprehensive assessment. By leveraging the VTE simulator, this research ensures thorough evaluations across diverse operational scenarios, thereby fortifying anomaly detection systems and advancing the security of industrial systems. The research evaluates anomaly detection models for industrial systems using performance metrics like precision, recall, F1-score, and AUC-ROC. It compares Support Vector Machine (SVM) and Gradient Boosting (GB) models, finding GB outperforms SVM in discrimination ability. Both models show effective anomaly detection with minimal false positives and false negatives. A comparative analysis of key performance metrics aids in selecting the most suitable approach for enhancing system reliability and safety.

Keywords: Adaptive Synthetic Sampling, Support Vector Machines, Gradient Boosting, Chi-Square Test, ANOVA F-Value, Virtual Testing Environment

I. INTRODUCTION

Anomaly attacks pose significant threats to industrial systems, manifesting through various channels that exploit vulnerabilities in system architecture, operation, and human factors. One common avenue is data manipulation, where attackers tamper with sensor readings or control signals, leading to erroneous decisions or malfunctions within the system [1]. Network intrusions represent another prevalent threat, with attackers exploiting weaknesses in network protocols or unauthorized access points to infiltrate the system and manipulate data flows or disrupt communications [2]. Malware injection presents a formidable challenge, as malicious software can infiltrate systems through infected USB drives, phishing emails, or compromised software updates, leading to disruptions, data breaches, or physical damage. Insider threats, whether deliberate sabotage by disgruntled employees or inadvertent errors, further exacerbate the risk landscape by compromising sensitive data or control systems from within [3]. Supply chain attacks leverage vulnerabilities in third-party vendors or service providers to infiltrate the system, introduce malicious components, or exploit shared infrastructure [4]. Physical access to industrial facilities provides attackers with direct opportunities to manipulate hardware or sabotage critical infrastructure, while social engineering tactics exploit human vulnerabilities to gain unauthorized access or divulge sensitive information [5]. Addressing these multifaceted threats demands a holistic approach, encompassing robust cybersecurity measures, continuous monitoring and

[1] [1]Assistant Professor, Department of Computing Technologies, SRM Institute of Science and Technology, Kattankulathur, Tamil Nadu 603203,India. Email:malarseg@srmist.edu.in
[2]Associate Professor, Department of Electronics and Communication Engineering, Sri Manakula Vinayagar Engineering College, Puducherry ,India. Email: p.arunagiri@smvec.ac.in
[3]Assistant Professor, Department of Computer Science, Saveetha College of Liberal Arts and Sciences,
SIMATS Deemed to be University, Chennai India. Email: umakumari2103@gmail..com
[4]Associate Professor, Department of Computer Science and Engineering PSNA College of Engineering and Technology, Dindigul-624622, Tamil Nadu, India. Email: ssbabu@psnacet.edu.in
[5]Assistant Professor, Department of Electronics and Communication Engineering, P. S. R Engineering College, Sevalpatti, Sivakasi-626140, Tamil Nadu. Email; lingasamy@psr.edu.in
[6]Associate Professor, Department of ECE, Vel Tech Rangarajan Dr Sagunthala R & D Institute of Science and Technology, Chennai, Tamil Nadu, India. Email: drrufus@veltech.edu.in

detection capabilities, employee training and awareness initiatives, and proactive risk management strategies to fortify industrial systems against anomaly attacks and uphold their dependability and resilience.

Machine learning (ML) stands at the forefront of modern anomaly detection methodologies, offering innovative solutions that harness the power of advanced algorithms and data analytics to safeguard industrial systems against unforeseen disruptions [6]. One of the key strengths of ML in anomaly detection lies in its capacity to recognize subtle deviations from normal operating patterns within industrial environments [7]. By ingesting and analyzing vast volumes of data from sensors, equipment, and processes, ML algorithms can discern patterns and trends that may indicate anomalous behavior. Through the process of supervised or unsupervised learning, these algorithms can identify anomalies in real-time or near-real-time, providing early warnings of potential issues before they escalate into significant disruptions [8]. Moreover, ML-based anomaly detection systems are highly scalable, capable of handling the massive streams of data generated by industrial systems with ease. Techniques such as deep learning and ensemble methods enable these systems to process and analyze complex data sets efficiently, facilitating rapid detection and response to anomalies across diverse industrial settings [9]. One of the most compelling advantages of ML in anomaly detection is its adaptability. ML models can continuously learn and evolve over time, refining their detection capabilities based on feedback from new data and changing conditions [10]. This adaptability enables ML-based systems to stay ahead of emerging threats and evolving attack vectors, enhancing the resilience of industrial operations against a wide range of anomalies. Furthermore, ML-based anomaly detection systems can provide valuable insights into the root causes of anomalies and their potential impact on industrial processes [11]. By analyzing patterns and correlations within the data, these systems can help industrial stakeholders understand the underlying dynamics driving anomalies, facilitating targeted remediation efforts and informed decision-making. The objectives of the work are:

- Enhance anomaly detection accuracy in industrial systems through a multifaceted approach.
- Address class imbalance using Adaptive Synthetic Sampling (ADASYN) to improve detection performance.
- Identify essential features for anomaly detection through filter-based feature selection methods.
- Evaluate supervised anomaly detection algorithms, including Support Vector Machines (SVM) and Gradient Boosting (GB), in a Virtual Testing Environment (VTE) simulator to enhance system reliability and safety.

II. Literature Review

Rule-based anomaly detection systems use predefined rules to identify anomalies in industrial systems [12]. These rules, derived from domain expertise or historical observations, are applied to incoming data for real-time monitoring, generating alerts for detected anomalies [13]. These systems offer transparency and lower computational intensity but may struggle with novel anomalies and require manual rule updates [14] [15]. Pattern matching techniques, another approach to anomaly detection, compare current data patterns against historical records or templates to identify anomalies [16][23]. These methods, such as time series analysis and sequence matching, excel at detecting recurring anomalies but are limited by reliance on predefined patterns [18] [20].

The research in [21] proposes an efficient hand gesture recognition system using skin color detection, Heuristic Manta-ray Foraging Optimization for feature selection, and Adaptive Extreme Learning Machine-based classification, enhancing accuracy and reducing errors[25]. The research in [22] focuses on an automated diabetes detection system, utilizing Inherent Coefficient Normalization, Intelligent Harris Hawks Optimization, and Pivotal Decision Tree to address limitations in existing machine learning-based systems for improved prediction accuracy[24].

III. Proposed Work

3.1 Data Analyzing

In the context of data analysis for anomaly detection in industrial systems, the role of ADASYN is paramount. ADASYN addresses a common challenge encountered in this domain: the imbalanced distribution of normal and anomalous instances within the dataset. This imbalance can severely impact the performance of anomaly detection models, as classifiers tend to be biased towards the majority class (normal instances), leading to poor detection of anomalies. ADASYN works by dynamically generating synthetic samples for the minority class (anomalous instances) based on their local density. Unlike traditional oversampling techniques that blindly

replicate existing minority class instances, ADASYN focuses on regions of the feature space where the density of minority class instances is low. By doing so, ADASYN effectively introduces diversity into the synthetic samples, making them more representative of the underlying distribution of the minority class. During the data analysis process, ADASYN plays a crucial role in mitigating the effects of class imbalance, thereby improving the overall performance of anomaly detection models. By augmenting the dataset with synthetic samples, ADASYN helps to address the scarcity of anomalous instances, allowing the model to learn more effectively from the minority class. This is particularly important in scenarios where anomalies are rare but potentially critical, such as in industrial systems where detecting malfunctions or intrusions is paramount for ensuring safety and security. Moreover, ADASYN contributes to enhancing the robustness and generalization capability of anomaly detection models. By introducing synthetic samples that reflect the underlying distribution of the minority class, ADASYN helps to prevent overfitting and bias towards the majority class. This ensures that the model is better able to capture the true characteristics of anomalies, leading to improved detection performance on unseen data.

3.2 Statistical Feature Selection

In the realm of anomaly detection in industrial systems, selecting pertinent features is crucial for effective anomaly detection. In the context of filter-based feature selection methods, which assess the intrinsic characteristics of features, integrating statistical measures such as the Chi-Square Test and ANOVA F-Value can be valuable. These tests evaluate the independence and significance of features concerning the target variable, aiding in the identification of relevant features. Mathematically, the chi-square statistic (X^2) is computed as:

$$X^2 = \sum \frac{(O_i - E_i)^2}{E_i} \quad (1)$$

Where O_i denotes the observed frequency of co-occurrence of a categorical feature and the target variable, and E_i represents the expected frequency under independence. Another relevant measure, the ANOVA F-Value, assesses the significance of continuous features in explaining the variance of the target variable. This value is calculated using the formula:

$$F = \frac{MS_{between}}{MS_{within}} \quad (2)$$

Where $MS_{between}$ represents the variance between groups (levels of a categorical variable), and MS_{within} denotes the variance within groups. High values of X^2 and F indicate significant associations and explainability of features with respect to the target, guiding the selection of pertinent features for anomaly detection in industrial systems. Integrating such statistical tests into the feature selection process enhances the efficacy of anomaly detection algorithms by focusing on features most informative for detecting anomalies amidst the complex industrial data landscape.

3.3 Machine Learning Models

Supervised anomaly detection in industrial systems is a critical task aimed at ensuring the smooth operation and security of complex industrial processes. This approach involves leveraging historical data that has been labeled as either normal or anomalous to train machine learning models. The process typically begins with data collection from various sensors and instruments embedded within the industrial infrastructure. This data encompasses a wide range of parameters such as temperature, pressure, flow rate, vibration, and electrical signals, depending on the specific industrial process. Once the data is collected, it is preprocessed to remove noise, handle missing values, and normalize features to ensure compatibility across different scales. Feature engineering techniques may also be applied to extract relevant information and reduce the dimensionality of the dataset. With the preprocessed data, the next step is to select suitable machine learning algorithms for training the anomaly detection model. In the case of supervised learning, algorithms such as SVM and GB have shown promising results in detecting anomalies in industrial systems. SVM are particularly effective in binary classification tasks where they attempt to find the optimal hyperplane that separates different classes with the maximum margin. In the context of anomaly detection, SVM aims to create a decision boundary that maximizes the margin between normal and anomalous data points in a high-dimensional feature space. This robust separation allows SVM to effectively identify anomalies while minimizing false positives. GB is an ensemble learning technique that combines multiple weak learners, typically decision trees, to create a strong predictive

model. In each iteration, GB sequentially fits a new weak learner to the residual errors of the previous models, gradually reducing the overall prediction error. This iterative process allows GB to capture complex relationships and interactions within the data, making it well-suited for anomaly detection tasks where anomalies may exhibit intricate patterns or behaviors. Once the models are trained on the labeled dataset, they can be deployed to classify new, unseen data as either normal or anomalous based on the learned patterns. Continuous monitoring of the industrial system allows for real-time detection of anomalies, enabling timely intervention and mitigation of potential threats to system integrity and security.

3.4 Experimental Setup

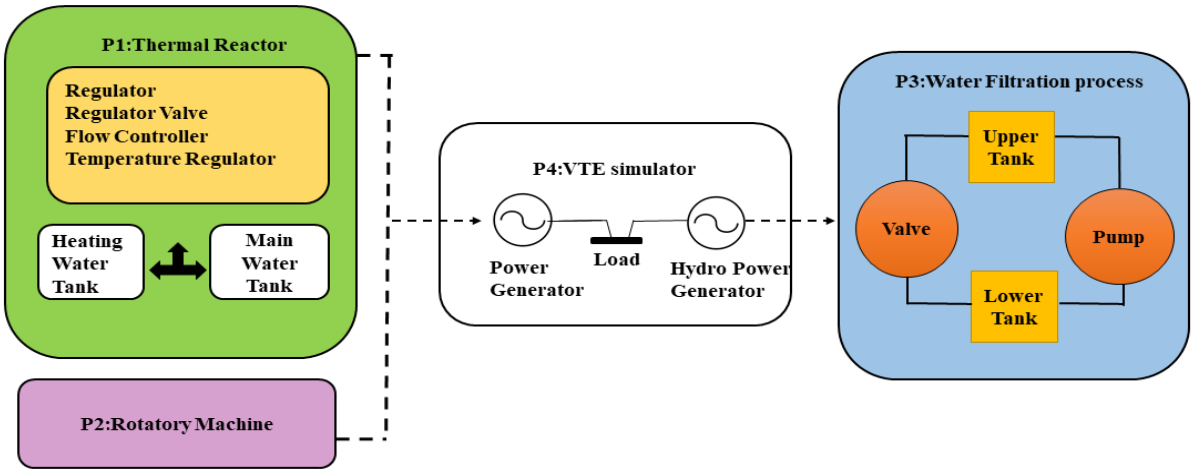

Fig.1 VTE Simulator Setup

The evaluation process for anomaly detection in Industrial Systems involves the application of machine learning models using sensor data collected from a power generation infrastructure. This assessment occurs within a VTE simulator, as depicted in fig.1. The VTE simulator is instrumental in recreating the operational processes of the industrial setup with remarkable accuracy, effectively replicating the behavior of physical components. This ensures that the testing environment closely mirrors real-world conditions, facilitating thorough and reliable evaluations. Within the VTE simulator, four primary processes are simulated: the thermal reactor, rotary machinery, water filtration, and power generation systems. Each of these processes plays a critical role in the overall functioning of the industrial system. For instance, the thermal reactor employs flow controllers, regulator valves, and temperature regulators to optimize its performance. Similarly, the water filtration process incorporates a level controller responsible for managing pumps and valves to regulate water levels between reservoirs. Moreover, the VTE simulator also replicates the thermal power and pumped-storage hydropower generation processes. This comprehensive emulation allows for extensive testing of anomaly detection algorithms across a wide range of operational scenarios, ensuring robust performance under diverse conditions. By leveraging the VTE simulator, the industrial system can effectively mitigate potential damages resulting from malicious attacks. This ensures that experiments are conducted safely and under control, protecting the integrity and reliability of the entire system. In the end, this careful approach strengthens anomaly detection systems, improving the security of Industrial Systems.

IV. RESULT

4.1 Dataset

The dataset for evaluating the anomaly detection framework in industrial systems was meticulously generated using a VTE simulator. Known for its precision in replicating real-world processes, the VTE simulator faithfully emulated industrial behaviors, parameters, and anomalies, focusing on filtration. By carefully configuring the simulator, the dataset accurately represented complex industrial environments, modeling behaviors like flow rates, pressure differentials, and filtration efficiency. Parameters such as filter pore size and operating conditions were adjusted to simulate various scenarios. This ensured the dataset's fidelity to real-world filtration processes, enhancing reliability for evaluating anomaly detection performance.

4.2 Model Evaluation Metrics

In evaluating anomaly detection models for industrial systems, various performance metrics are crucial for assessing accuracy and efficiency. Precision measures the proportion of correctly identified anomalies among all instances classified as anomalies, reflecting the model's ability to avoid false positives. Recall quantifies the proportion of true anomalies correctly identified among all actual anomalies, indicating the model's effectiveness in capturing anomalies. The F1-score, a harmonic mean of precision and recall, offers a balanced assessment, considering both false positives and false negatives. Additionally, the area under the receiver operating characteristic curve (AUC-ROC) evaluates the model's ability to distinguish between normal and anomalous instances across different threshold settings. Higher AUC-ROC values signify better discrimination performance. By comprehensively analysing these metrics, researchers can assess the supervised anomaly detection models' performance, aiding in the selection of the most effective algorithms like SVM and GB. This ensures accurate and efficient anomaly detection, thereby enhancing industrial system security and enabling timely threat mitigation. Furthermore, complementary metrics such as accuracy, confusion matrix, and others can provide additional insights into model performance, contributing to a comprehensive evaluation.

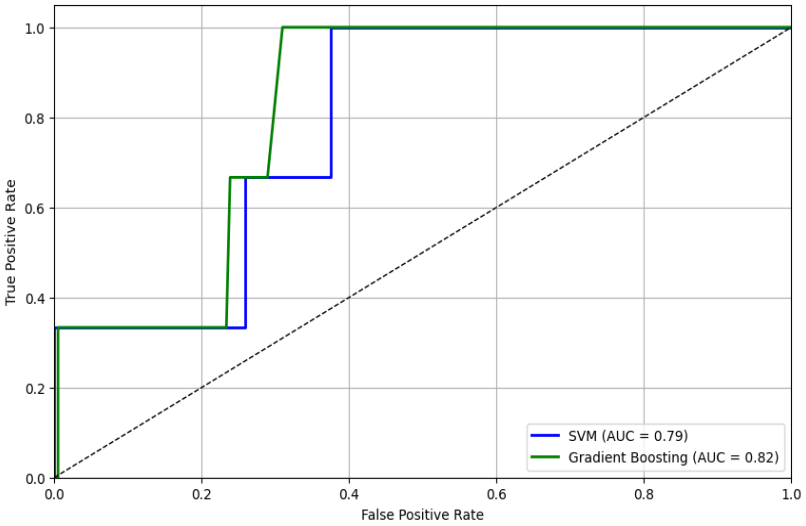

Fig.2 Receiver Operating Characteristic (ROC) Curve

In fig.2, The ROC curve compares the discrimination performance of a SVM and a Gradient Boosting GB model. The AUC values show the GB model outperforms the SVM model, with AUCs of approximately 0.91 and 0.79, respectively. The GB model exhibits better discriminatory power, as evidenced by its curve being closer to the ideal top-left corner. This suggests the GB model is more adept at distinguishing between the two classes in the test dataset. Consequently, for prioritizing discrimination ability, the Gradient Boosting model would be preferable over the SVM model, considering other relevant factors.

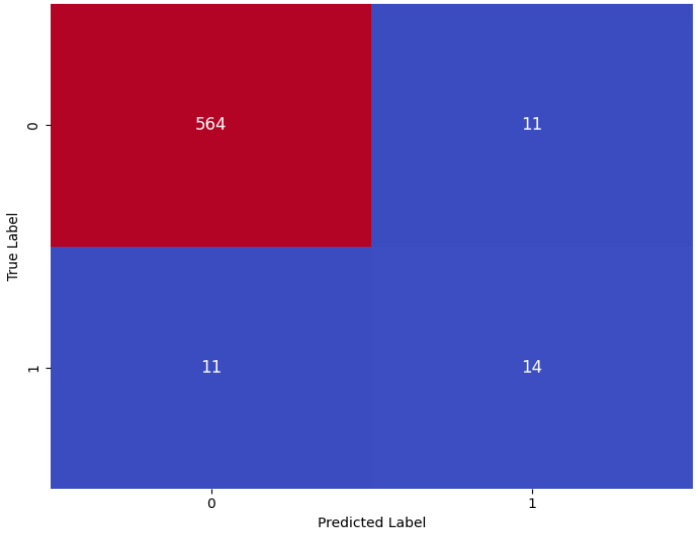

Fig.3 Gradient Boosting Confusion Matrix

In the fig.3 for the Gradient Boosting model, the presence of a significant number of true positives (top-left quadrant) indicates instances where anomalies were correctly identified, contributing to effective detection. Conversely, the relatively low number of false negatives (bottom-left quadrant) suggests minimal instances of anomalies being missed, showcasing the model's robustness in capturing anomalous activities. Additionally, the limited occurrences of false positives (top-right quadrant) signify the model's ability to avoid misclassifying normal instances as anomalies, minimizing unnecessary alerts and ensuring operational efficiency.

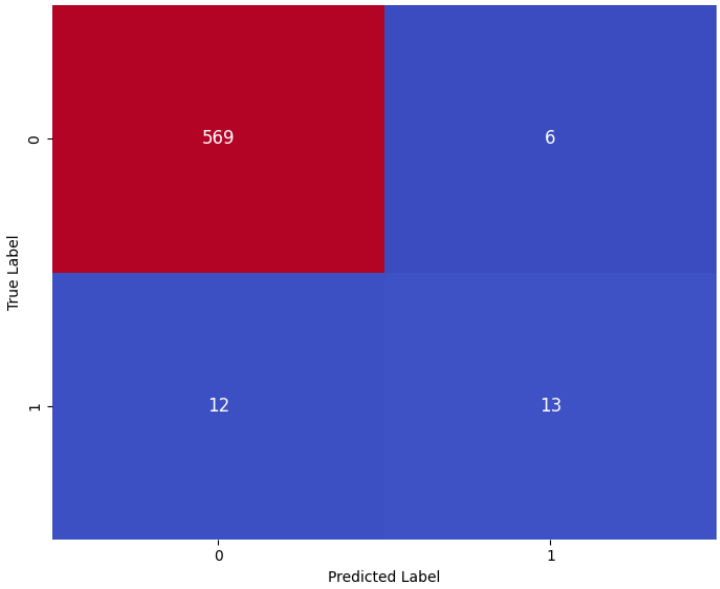

Fig.4 Support Vector Machine Confusion Matrix

The fig.4, for the SVM model exhibits a comparable pattern, with notable true positive counts reflecting accurate detection of anomalies. The relatively lower count of false negatives further underscores the model's capability to detect most anomalies, thereby enhancing system security. Moreover, the minimal occurrences of false positives highlight the model's precision in distinguishing between normal and anomalous instances, minimizing the risk of false alarms. Overall, the coherent patterns observed in both confusion matrices validate the effectiveness of supervised anomaly detection techniques, such as GB and SVM, in accurately identifying anomalies within industrial systems, facilitating timely mitigation measures and ensuring operational integrity.

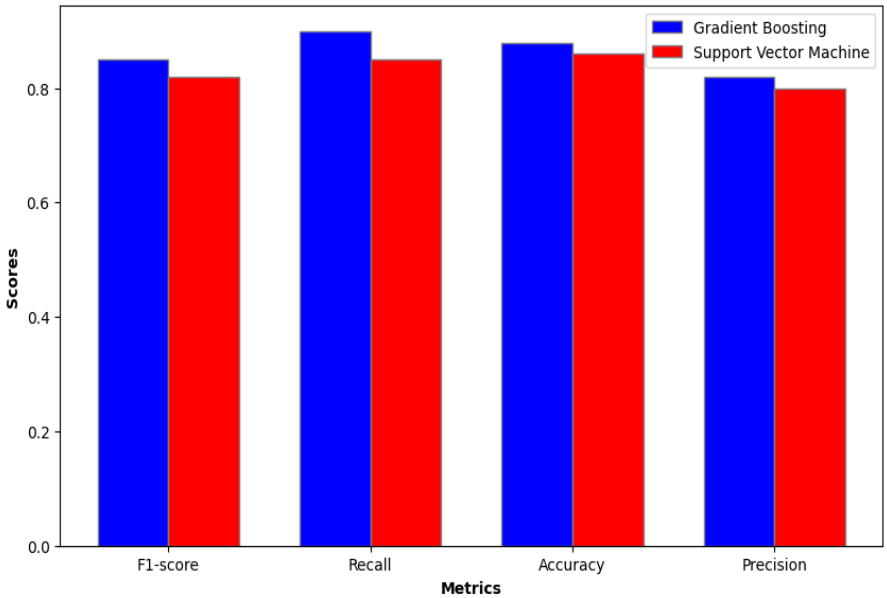

Fig.5 Anomaly Detection Model Performance

The fig.5 presents a comparative analysis of two machine learning models, GB and SVM, specifically tailored and meticulously tested within the framework developed for industrial anomaly detection. Across key

performance metrics such as F1-score, Recall, Accuracy, and Precision, the chart vividly illustrates the efficacy of the models within the interpretability framework. By scrutinizing the heights of the bars representing each model's performance, stakeholders gain valuable insights into the models' ability to detect anomalies effectively and reliably in industrial settings. This comprehensive analysis aids decision-makers in selecting the most appropriate model for anomaly detection tasks within industrial systems, thereby enhancing system reliability, safety, and productivity. The graph's significance lies not only in its portrayal of model performance but also in its contribution to advancing the understanding and implementation of machine learning interpretability frameworks in industrial anomaly detection.

Table.1 Performance Comparison of Anomaly Detection Models

S.No	Evaluation Metrics	Gradient Boosting	Support Vector Machine
1	F1	0.850000	0.820000
2	Recall	0.900000	0.850000
3	Accuracy	0.880000	0.860000
4	Precision	0.820000	0.800000
5	AUC	0.819797	0.788494

The table.1 highlights the performance of two state-of-the-art anomaly detection models, GB and SVM, using easily understandable metrics crucial for enhancing the reliability of industrial systems. These metrics, namely F1-score, Recall, Accuracy, Precision, and AUC, serve as essential yardsticks for evaluating the models' effectiveness in identifying anomalies within the system's data. F1-score provides a balanced measure of a model's precision and recall, offering insight into its overall performance in anomaly detection. Recall reflects the model's capability to correctly identify anomalies, while precision indicates how often the flagged anomalies are indeed genuine. The AUC metric, on the other hand, assesses the models' ability to distinguish between normal and anomalous data points across varying decision thresholds. By analyzing these metrics, decision-makers gain valuable guidance in selecting the most suitable anomaly detection model tailored to the industrial systems' needs. This table serves as a pivotal element in the research, showcasing how innovative methods can significantly enhance the robustness of industrial systems against anomalies. It underscores the transformative impact of these approaches, ultimately bolstering the dependability and resilience of such systems.

IV. Conclusion and Future work

In summary, this research highlights the importance of integrating diverse techniques like ADASYN for addressing imbalanced data and filter-based feature selection methods such as Chi-Square Test and ANOVA F-Value for anomaly detection. Supervised approaches like SVM and GB have shown promise in accurately classifying normal and anomalous activities. Rigorous evaluation in a VTE has strengthened anomaly detection systems, promising further advancements in industrial security. In evaluating anomaly detection models for industrial systems, metrics like Precision, Recall, F1-score, Accuracy, and AUC-ROC are crucial. GB outperforms SVM with higher metrics across F1-score (0.85 vs. 0.82), Recall (0.90 vs. 0.85), Accuracy (0.88 vs. 0.86), Precision (0.82 vs. 0.80), and AUC (0.8198 vs. 0.7885). These findings guide the selection of effective anomaly detection methods, enhancing system reliability, safety, and productivity. Future research in anomaly detection for industrial systems can explore advancements in machine learning algorithms tailored for real-time anomaly detection. Additionally, investigating novel techniques to handle complex data distributions and dynamic environments will be crucial. Integrating edge computing and IoT devices could further enhance anomaly detection capabilities in industrial settings, ensuring continuous monitoring and timely response to emerging threats.

References

1. Huang, D. W., Liu, W., & Bi, J. (2021). Data tampering attacks diagnosis in dynamic wireless sensor networks. *Computer Communications*, *172*, 84-92.
2. Aslan, Ö., Aktuğ, S. S., Ozkan-Okay, M., Yilmaz, A. A., & Akin, E. (2023). A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions. *Electronics*, *12*(6), 1333.
3. Makanto, P. K., & Eze, J. S. Mitigating Human Vulnerabilities in Cybersecurity: Understanding Human Flaws and Implementing Effective Countermeasures.
4. Collier, Z. A., & Thekdi, S. A. (2024). Supply Chain Security. In *The Palgrave Handbook of Supply Chain Management* (pp. 561-584). Cham: Springer International Publishing.

5. Lehto, M. (2022). Cyber-attacks against critical infrastructure. In *Cyber Security: Critical Infrastructure Protection* (pp. 3-42). Cham: Springer International Publishing.
6. Dagnino, A. (2021). *Data analytics in the era of the industrial internet of things* (pp. 1-133). Cham: Springer.
7. Allen, C. W., Holcomb, C., & de Oliveira, M. (2021, June). Anomaly detection for large fleets of industrial equipment: Utilizing machine learning with applications to power plant monitoring. In *Turbo Expo: Power for Land, Sea, and Air* (Vol. 84966, p. V004T05A016). American Society of Mechanical Engineers.
8. Hassan, A., & Mhmood, A. H. (2021). Optimizing Network Performance, Automation, and Intelligent Decision-Making through Real-Time Big Data Analytics. *International Journal of Responsible Artificial Intelligence*, *11*(8), 12-22.
9. Khalil, R. A., Saeed, N., Masood, M., Fard, Y. M., Alouini, M. S., & Al-Naffouri, T. Y. (2021). Deep learning in the industrial internet of things: Potentials, challenges, and emerging applications. *IEEE Internet of Things Journal*, *8*(14), 11016-11040.
10. Raparthi, M., Dodda, S. B., & Maruthi, S. (2020). Examining the use of Artificial Intelligence to Enhance Security Measures in Computer Hardware, including the Detection of Hardware-based Vulnerabilities and Attacks. *European Economic Letters (EEL)*, *10*(1).
11. Velasquez Rendón, D. (2023). Machine learning based anomaly detection for industry 4.0 systems.
12. Acharya, D., Farazi, M., Rolland, V., Petersson, L., Rosebrock, U., Smith, D., ... & Wilcox, C. (2024). Towards automatic anomaly detection in fisheries using electronic monitoring and automatic identification system. *Fisheries Research*, *272*, 106939.
13. Rajaoarisoa, L., Kuk, M., Bobek, S., & Sayed-Mouchaweh, M. (2024). Hybrid and co-learning approach for anomalies prediction and explanation of wind turbine systems. *Engineering Applications of Artificial Intelligence*, *133*, 108046.
14. El-Shafeiy, E., Alsabaan, M., Ibrahem, M. I., & Elwahsh, H. (2023). Real-Time Anomaly Detection for Water Quality Sensor Monitoring Based on Multivariate Deep Learning Technique. *Sensors*, *23*(20), 8613.
15. Udayakumar, R., Balakrishnan, D., Reddy, Y. V., Prabhakar, P. E., & Thilaka, A. (2023, November). Machine Learning Based Intrusion Detection System. In *2023 3rd International Conference on Technological Advancements in Computational Sciences (ICTACS)* (pp. 197-205). IEEE.
16. Kemp, J., Barker, C., Good, N., & Bain, M. (2022, December). Sequential pattern detection for identifying courses of treatment and anomalous claim behaviour in medical insurance. In *2022 IEEE International Conference on Bioinformatics and Biomedicine (BIBM)* (pp. 3039-3046). IEEE.
17. Fernandes, M., Corchado, J. M., & Marreiros, G. (2022). Machine learning techniques applied to mechanical fault diagnosis and fault prognosis in the context of real industrial manufacturing use-cases: a systematic literature review. *Applied Intelligence*, *52*(12), 14246-14280.
18. Zhang, Y., Chen, Y., Wang, J., & Pan, Z. (2021). Unsupervised deep anomaly detection for multi-sensor time-series signals. *IEEE Transactions on Knowledge and Data Engineering*.
19. Schneider, P., & Xhafa, F. (2022). *Anomaly Detection and Complex Event Processing Over IoT Data Streams: With Application to EHealth and Patient Data Monitoring*. Academic Press.
20. Mo, F., Querejeta, M. U., Hellewell, J., Rehman, H. U., Rezabal, M. I., Chaplin, J. C., ... & Ratchev, S. (2023). PLC orchestration automation to enhance human–machine integration in adaptive manufacturing systems. *Journal of Manufacturing Systems*, *71*, 172-187.
21. Khetavath, S., Sendhilkumar, N. C., Mukunthan, P., Jana, S., Gopalakrishnan, S., Malliga, L., ... & Farhaoui, Y. (2023). An Intelligent Heuristic Manta-Ray Foraging Optimization and Adaptive Extreme Learning Machine for Hand Gesture Image Recognition. *Big Data Mining and Analytics*, *6*(3), 321-335.
22. Fayaz, R., Reddy, G. V., Sujaritha, M., Soundiraraj, N., Theresa, W. G., Roy, D. K., ... & Gopalakrishnan, S. (2022). An Intelligent Harris Hawks Optimization (IHHO) based Pivotal Decision Tree (PDT) Machine Learning Model for Diabetes Prediction. *International Journal of Intelligent Systems and Applications in Engineering*, *10*(4), 415-423.
23. Kumar, Voruganti Naresh, Vootla Srisuma, Suraya Mubeen, Arfa Mahwish, Najeema Afrin, D. B. V. Jagannadham, and Jonnadula Narasimharao. "Anomaly-Based Hierarchical Intrusion Detection for Black Hole Attack Detection and Prevention in WSN." In *Proceedings of Fourth International Conference on Computer and Communication Technologies: IC3T 2022*, pp. 319-327. Singapore: Springer Nature Singapore, 2023.
24. Prabhakar, T., Srujan Raju, K., Reddy Madhavi, K. (2022). Support Vector Machine Classification of Remote Sensing Images with the Wavelet-based Statistical Features. In: Satapathy, S.C., Bhateja, V., Favorskaya, M.N., Adilakshmi, T. (eds) Smart Intelligent Computing and Applications, Volume 2. Smart Innovation, Systems and Technologies, vol 283. Springer, Singapore. https://doi.org/10.1007/978-981-16-9705-0_59
25. Sai, V.H.H.N., Bhaskar, N., Dharmireddi, S., Srujan Raju, K., Divya, G., Narasimharao, J. (2024). An Automated Smart Plastic Waste Recycling Management Systems. In: Zen, H., Dasari, N.M., Latha, Y.M., Rao, S.S. (eds) Soft Computing and Signal Processing. ICSCSP 2023. Lecture Notes in Networks and Systems, vol 840. Springer, Singapore. https://doi.org/10.1007/978-981-99-8451-0_10