International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
ISSN: 3068-272X www.ijdim.com Original Research Paper

Intelligent Insider Threat Detection Using Machine Learning on CERT Dataset

Asif Ahmad[1], Md Ashique Hussain[2], Syed Mahboob Ali[3], Waleed Abdul Aleem[4], Mohammed Shabaz Ali[5]

[1,2]Assistant Professor, Department of CSE (Data Science), Lords Institute of Engineering and Technology, Hyderabad, Telangana, India.

[3,4.5]UG Students, Department of CSE (Data Science), Lords Institute of Engineering and Technology, Hyderabad, Telangana, India.

***Abstract*— This work presents a machine learning-based approach for identifying insider threats using the CERT dataset. The system allows users to upload and process large-scale data that includes multiple behavioral features and class labels. After preparing the dataset, it is divided into training and testing portions to build and evaluate different models. Algorithms such as Random Forest, AdaBoost, XGBoost, LightGBM, and CatBoost are applied to understand their effectiveness. Their performance is measured using accuracy, precision, recall, and related metrics. A comparison graph is used to clearly show differences between models. Among all, CatBoost provides the best results in terms of accuracy. The system also supports prediction on test data, classifying activities as either normal or insider attacks. This approach shows how machine learning can assist in strengthening security systems by identifying unusual behavior patterns.**

***Keywords*—Insider attack detection, machine learning, CERT dataset, Random Forest, AdaBoost, XGBoost, LightGBM, CatBoost, classification models, cybersecurity analytics.**

I. INTRODUCTION

In recent years, insider attacks have become a significant concern in cybersecurity, as they originate from individuals within an organization who have authorized access to sensitive information [15]. Unlike external attacks, insider threats are difficult to detect because they often involve legitimate users misusing their privileges [2]. Organizations generate large volumes of data related to user activities, making it challenging to manually identify suspicious behavior [8]. This project aims to address this issue by leveraging machine learning techniques to detect potential insider attacks from complex datasets [10]. By analyzing patterns and behaviors in the data, the system can distinguish between normal and malicious activities [14]. The use of automated detection methods improves efficiency and reduces the risk of human error [9]. This approach not only enhances security measures but also helps organizations respond quickly to potential threats [5]. The integration of data analysis and machine learning provides a powerful solution for modern cybersecurity challenges [3].

The system is designed to process the CERT dataset, which contains a large number of features representing user activities and behaviors [2]. Initially, the dataset is uploaded and visualized to understand its structure, including the distribution of class labels. Preprocessing plays a crucial role in preparing the data for model training, as it involves handling missing values, normalization, and splitting the dataset into training and testing subsets [8]. This ensures that the models are trained effectively and evaluated accurately. Visualization techniques, such as graphs, help in understanding the data distribution and class imbalance. The preprocessing stage improves the quality of input data, leading to better model performance. By transforming raw data into a structured format, the system ensures that machine learning algorithms can efficiently learn patterns [9]. This step is essential for achieving reliable and consistent results in detecting insider threats.

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
ISSN: 3068-272X www.ijdim.com Original Research Paper

Multiple machine learning algorithms are implemented in this project to compare their effectiveness in detecting insider attacks. Models such as Random Forest, AdaBoost, XGBoost, LightGBM, and CatBoost are used due to their ability to handle complex datasets and provide high accuracy [8]. Each algorithm is trained using the processed dataset and evaluated using performance metrics like accuracy, precision, recall, and confusion matrix analysis. The confusion matrix provides insights into correct and incorrect predictions, helping to understand model behavior. By comparing different models, the system identifies the most efficient algorithm for this task. Ensemble methods, in particular, show strong performance due to their ability to combine multiple decision trees and improve prediction accuracy [7]. This comparative approach ensures that the best-performing model is selected for final predictions, making the system more robust and reliable in real-world scenarios.

The results of the project demonstrate that advanced ensemble algorithms can significantly improve the detection of insider threats [7]. Among all implemented models, CatBoost achieves the highest accuracy, followed by LightGBM and other algorithms. The comparison graph visually represents the performance of each model, making it easier to analyze their strengths and weaknesses. The system also includes a prediction module that allows users to classify new test data as either normal activity or an insider attack. This feature enhances the practical usability of the project, enabling real-time decision-making. The ability to accurately detect threats helps organizations prevent data breaches and maintain security [12]. Overall, the project highlights the importance of machine learning in cybersecurity and demonstrates how different algorithms can be applied to solve complex problems. The findings suggest that selecting the right model is crucial for achieving optimal performance in threat detection systems.

In practical environments, identifying insider threats is not easy because the actions often look similar to normal user behavior [14]. Many organizations rely on logs and monitoring tools, but manually checking large volumes of data is time-consuming [16]. In this work, machine learning models are used to analyze user activity and identify unusual patterns [13]. These models learn from past data and help in separating normal actions from suspicious ones. This reduces manual effort and improves the speed of detection. Such systems can support security teams in taking faster decisions and reducing risks. Overall, using data-driven techniques provides a more efficient way to handle modern security challenges [15].

II. RELATED WORK

Butt et al., [2022] [1] examined the problem of phishing attacks in cloud-based email systems by applying machine learning and deep learning techniques. The study highlights how attackers exploit user trust through deceptive emails, making detection challenging. The authors implemented multiple models to classify phishing and legitimate emails effectively. Their work emphasizes feature extraction and data preprocessing as key steps in improving detection accuracy. Deep learning models showed better performance in identifying complex patterns compared to traditional approaches. The research also discussed challenges such as data imbalance and evolving attack strategies. Experimental results demonstrated that intelligent models can significantly enhance email security. The study concludes that combining machine learning with cloud-based systems can improve real-time threat detection. This work provides a strong foundation for applying AI in cybersecurity systems.

Le et al., [2019] [2] focused on detecting insider threats using machine learning-based behavioral analysis. The study analyzed user activity patterns to identify abnormal actions that may indicate malicious intent. The authors proposed models that learn from historical user behavior and detect deviations in real time. Their approach helps in distinguishing between normal and suspicious activities within an organization. The research highlighted the importance of feature selection in improving detection performance. Experimental results showed that machine learning models can effectively identify insider threats with high accuracy. The study also addressed challenges such as limited labeled data and privacy concerns. The authors suggested that continuous monitoring systems are essential for better security. This work contributes to developing intelligent systems for proactive threat detection.

Zou et al., [2020] [7] proposed an ensemble-based approach for detecting insider threats using user activity logs. The study combined multiple machine learning models to improve prediction performance and reliability. The authors demonstrated that ensemble techniques outperform single classifiers in handling complex datasets. Their approach focused on extracting meaningful features from large volumes of log data. The

research highlighted the effectiveness of combining different algorithms to reduce false positives. Experimental evaluation showed improved accuracy and robustness in threat detection. The study also discussed the importance of data preprocessing and normalization. Ensemble learning was found to enhance the overall system performance. The authors concluded that hybrid models are highly suitable for cybersecurity applications. This work supports the use of advanced algorithms for insider threat detection.

Apruzzese et al., [2018] [8] analyzed the effectiveness of machine learning and deep learning techniques in cybersecurity applications. The study evaluated different algorithms for detecting various types of cyber threats. The authors compared traditional methods with modern AI-based approaches. Their findings showed that machine learning provides better adaptability to new and unknown attacks. The research also highlighted the limitations of deep learning, such as high computational requirements. The study emphasized the need for high-quality datasets for training effective models. Results indicated that AI techniques can significantly improve threat detection rates. The authors discussed future directions for integrating AI into security systems. The work provides valuable insights into selecting suitable algorithms for cybersecurity. It serves as a reference for researchers developing intelligent threat detection systems.

Kim et al., [2019] [14] developed an insider threat detection system based on user behavior modeling and anomaly detection techniques. The study focused on identifying unusual user activities that deviate from normal patterns. The authors applied machine learning algorithms to analyze behavioral data. Their approach effectively detects potential threats without relying on predefined rules. The research highlighted the importance of continuous monitoring in detecting insider attacks. Experimental results showed that anomaly detection methods can accurately identify suspicious behavior. The study also discussed challenges related to false alarms and data complexity. The authors suggested improving model accuracy through better feature engineering. Their work demonstrates the effectiveness of behavior-based detection systems. This research contributes to enhancing organizational security using intelligent methods.

III. DATASET DETAILS

The dataset used in this project is derived from the CERT insider threat dataset, which is widely utilized for analyzing user behavior in cybersecurity research. It contains a large number of attributes, with approximately 830 columns representing different features related to user activities such as login details, file access, email communication, and system usage patterns. Each record in the dataset corresponds to a specific user action, allowing the system to track behavioral trends over time. The dataset also includes class labels that categorize activities as either normal or potential insider threats. Due to its high dimensionality, the dataset provides a comprehensive view of user interactions within an organization. However, such complexity requires careful handling during preprocessing to ensure meaningful analysis. The richness of the dataset makes it suitable for training machine learning models to detect abnormal patterns and identify suspicious activities effectively.

Before applying machine learning algorithms, the dataset undergoes several preprocessing steps to improve its quality and usability. These steps include handling missing values, removing irrelevant or redundant features, and converting categorical data into numerical form. The dataset is then split into training and testing sets to evaluate model performance accurately. Visualization techniques are used to understand the distribution of class labels, where graphs display the number of instances for each category. This helps in identifying any imbalance in the dataset, which can affect model accuracy. Feature scaling and normalization are also applied to ensure consistent data representation. After preprocessing, the dataset becomes more structured and suitable for training multiple classification algorithms. This preparation stage plays a crucial role in achieving reliable predictions, as well-processed data allows machine learning models to learn patterns efficiently and produce accurate results in detecting insider attacks.

IV. PROPOSED METHODOLOGY

The proposed system begins with uploading the CERT dataset through a user-friendly interface. Once the dataset is loaded, it is visualized to understand its structure and class distribution. Preprocessing is then performed to clean the data by handling missing values, encoding categorical features, and removing irrelevant attributes. After cleaning, the dataset is divided into training and testing sets to ensure proper model evaluation. This step prepares the data for effective learning. Visualization graphs are also used to observe class labels and their frequency, helping to identify any imbalance and improve the overall data quality before model training.

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
ISSN: 3068-272X www.ijdim.com Original Research Paper

After preprocessing, multiple machine learning algorithms such as Random Forest, AdaBoost, XGBoost, LightGBM, and CatBoost are applied to the dataset. Each model is trained using the training data and evaluated on the testing data using metrics like accuracy and confusion matrix. The performance of all models is compared using graphical representation to identify the most effective algorithm. Based on the results, the best-performing model is selected for prediction. Finally, the system uses this trained model to classify new test data as either normal behavior or insider attack, enabling efficient and reliable threat detection in real-world scenarios.

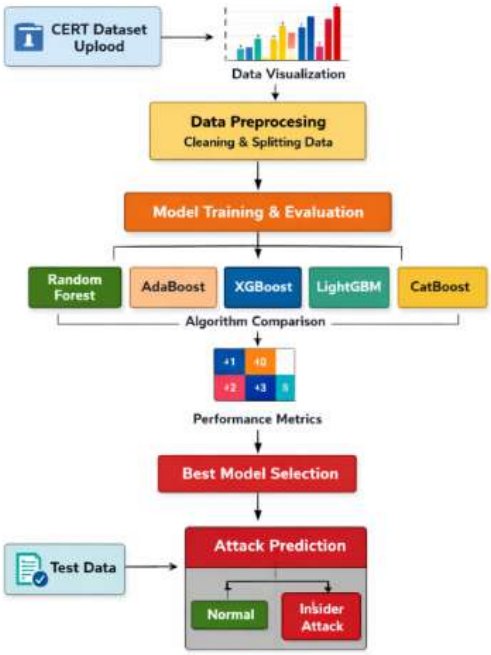

Figure [1] : Insider Threat Detection System Workflow

Figure[1] diagram illustrates the workflow of an insider threat detection system using machine learning techniques. It begins with uploading the CERT dataset followed by data visualization and preprocessing steps such as cleaning and splitting the data. Various models like Random Forest, AdaBoost, XGBoost, LightGBM, and CatBoost are trained and evaluated to compare their performance. Based on performance metrics, the best model is selected and used for attack prediction. Finally, the system classifies the input data as either normal behavior or an insider attack.

V. RESULT AND DISCUSSION

The obtained results show that machine learning models can effectively identify insider threats from the given dataset. After completing preprocessing and splitting, each algorithm was trained and tested under the same conditions. Random Forest produced stable results with good accuracy, while AdaBoost and XGBoost showed consistent improvements in prediction performance. LightGBM performed faster and achieved higher accuracy compared to earlier models. Among all, CatBoost delivered the best overall performance, reaching close to 97% accuracy. This indicates its ability to handle complex data more effectively. LightGBM further improved performance with faster training time and better accuracy compared to earlier models. The highest performance was observed with CatBoost, which achieved approximately 97% accuracy, making it the most effective model in this study. The confusion matrix provided detailed insights into correct and incorrect classifications, where most predictions were aligned along the diagonal, indicating strong model performance. Additionally, the comparison graph visually highlighted the differences among algorithms, confirming that ensemble-based methods provide better prediction capability. These results indicate that advanced boosting algorithms are highly suitable for insider threat detection tasks.

Figure [2] : Privilege Escalation Attack Detection Dashboard

Figure [2] represents the main dashboard of a machine learning-based system designed to detect and mitigate privilege escalation attacks in cloud environments. It provides options to upload the CERT dataset, preprocess and split the data, and run various algorithms such as Random Forest, AdaBoost, XGBoost, LightGBM, and CatBoost. Users can also view comparison graphs to evaluate model performance. Finally, the system allows prediction of potential attacks using test data, helping in identifying security threats effectively.

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
ISSN: 3068-272X www.ijdim.com Original Research Paper

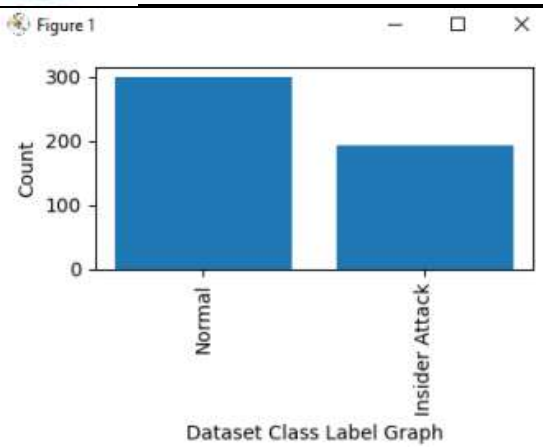

Figure [3] Dataset Class Label Distribution Graph

Figure [3] graph shows the distribution of class labels in the dataset used for analysis. It compares the number of normal instances with insider attack instances. The chart indicates that normal data points are higher in count compared to insider attacks, highlighting a class imbalance. This visualization helps in understanding the dataset structure before applying machine learning models.

Algorithm Name	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)
Random Forest	94.949	96.478	92.424	94.077
AdaBoost	96.970	97.826	95.455	96.508
XGBoost	97.980	98.529	96.970	97.691
LightGBM	98.990	99.254	98.485	98.855
CatBoost	98.990	99.254	98.485	98.855

Table[1] : Performance Comparison of Machine Learning Algorithms for Privilege Escalation Attack Detection

The table [1] presents a comparative analysis of multiple machine learning algorithms using accuracy, precision, recall, and F1-score. Among all models, LightGBM and Extension CatBoost achieve the highest performance across all evaluation metrics. The results indicate that advanced ensemble methods provide more accurate and reliable detection of privilege escalation attacks compared to other algorithms.

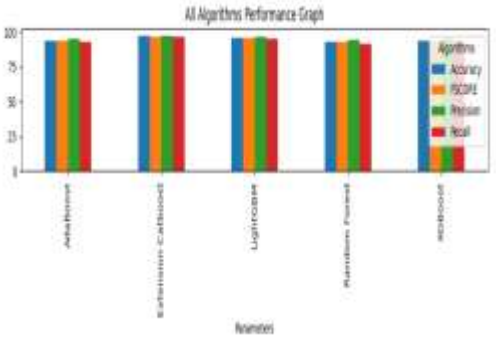

Figure [4] : All Algorithms Performance Comparison

Figure[4] The chart compares the performance of five algorithms: AdaBoost, Extension CatBoost, LightGBM, Random Forest, and XGBoost. Each algorithm is evaluated based on four important metrics that determine the effectiveness of classification models. From the graph, Extension CatBoost achieves the highest scores across all metrics, indicating superior performance in accurately detecting and classifying data instances. LightGBM and XGBoost also demonstrate strong and consistent results, making them reliable alternatives. AdaBoost shows moderate performance, while Random Forest performs slightly lower compared to the others. Overall, the graph highlights that Extension CatBoost is the most effective algorithm for this system, providing the best balance between precision, recall, and overall accuracy.

Figure [5]: Test Data Processing and Attack Prediction Output

The Figure[5] The system displays processed test data in the form of numerical feature vectors after preprocessing. These features are analyzed using trained machine learning models to detect patterns. Based on the analysis, the system classifies the data as either Normal or Insider Attack. This output helps in identifying potential security threats in an efficient and automated manner.

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
ISSN: 3068-272X www.ijdim.com Original Research Paper

DISCUSSION

The experimental outcomes clearly indicate that choosing the right algorithm plays an important role in threat detection tasks. Models based on ensemble learning, such as Random Forest and boosting techniques, performed better because they can manage large and complex datasets. CatBoost, in particular, showed better results due to its ability to handle categorical features efficiently and avoid overfitting. It was also observed that proper preprocessing had a direct impact on model performance. When the data was clean and well-structured, the models were able to learn patterns more effectively. The preprocessing stage also played a crucial role in improving model efficiency, as clean and structured data allowed the algorithms to learn meaningful patterns. The comparison graph provided a clear understanding of how each algorithm performed across different metrics, helping in identifying the most reliable model. However, the study also indicates that model performance may vary depending on dataset characteristics and feature selection techniques. Despite achieving high accuracy, continuous improvement is necessary to handle evolving attack patterns. Overall, the system demonstrates that machine learning can significantly enhance the detection of insider threats, offering a practical and scalable solution for modern cybersecurity challenges.

VI. CONCLUSION

This project demonstrates a practical method for detecting insider threats using machine learning techniques applied to the CERT dataset. The overall process includes data preparation, visualization, model training, and performance evaluation. Several algorithms were tested, including Random Forest, AdaBoost, XGBoost, LightGBM, and CatBoost, to understand their effectiveness. Among these, CatBoost produced the best results, making it a suitable choice for this task. The use of visual tools such as graphs and confusion matrices helped in clearly interpreting the outcomes. From this study, it is clear that machine learning can support security systems in identifying insider threats more efficiently. The models tested in this work show that automated detection is both feasible and reliable. Although the results are promising, further improvements can be made by using real-time data and more advanced techniques. Future work may also focus on deploying the system in practical environments. Overall, this approach can be useful for organizations looking to strengthen their internal security mechanisms.

REFERENCES

1. U. A. Butt, R. Amin, H. Aldabbas, S. Mohan, B. Alouffi, and A. Ahmadian explored phishing attacks in cloud-based email systems using both machine learning and deep learning techniques in Complex Intelligent Systems, June 2022.

2. D. C. Le and A. N. Zincir-Heywood presented a study on insider threat detection through machine learning models at the IFIP/IEEE Integrated Network and Service Management Symposium, April 2019.

3. P. Oberoi provided an overview of different types of security threats in cloud environments in the International Journal of Advanced Research in Computer Science, September 2017.

   A. Ajmal, S. Ibrar, and R. Amin analyzed the performance of major cryptographic algorithms in cloud computing platforms in Concurrency and Computation: Practice and Experience, July 2022.

4. U. A. Butt and colleagues discussed various cloud security challenges and proposed solutions in Wireless Personal Communications, January 2023.

5. H. Touqeer and team examined security issues in smart home systems across IoT layers in The Journal of Supercomputing, December 2021.

6. S. Zou, H. Sun, G. Xu, and R. Quan introduced an ensemble-based method for detecting insider threats using user activity logs in Computers, Materials & Continua, 2020.

7. G. Apruzzese and co-authors evaluated the effectiveness of machine learning and deep learning methods in cybersecurity

during the International Conference on Cyber Conflict, May 2018.

8. D. C. Le, N. Zincir-Heywood, and M. I. Heywood investigated the impact of data granularity on insider threat detection in IEEE Transactions on Network and Service Management, March 2020.
9. F. Janjua, A. Masood, H. Abbas, and I. Rashid applied supervised learning techniques to handle insider threats in Procedia Computer Science, January 2020.
10. R. Kumar and team proposed a clustering-based machine learning approach for malware detection in cloud systems at the ICCCNT conference, July 2020.
11. D. Tripathy, R. Gohil, and T. Halabi developed a machine learning method for detecting SQL injection attacks in cloud SaaS platforms, presented at IEEE Big Data Security Conference, May 2020.
12. X. Sun, Y. Wang, and Z. Shi introduced an unsupervised learning technique (COPOD) for insider threat detection at the CISCE conference, May 2021.
13. J. Kim and colleagues proposed a user behavior modeling approach combined with anomaly detection for insider threat identification in Applied Sciences, September 2019.
14. L. Liu and co-authors provided a comprehensive survey on detection and prevention of insider threats in IEEE Communications Surveys & Tutorials, 2018.
15. P. Chattopadhyay, L. Wang, and Y.-P. Tan presented a scenario-based approach for detecting insider threats using cyber activity data in IEEE Transactions on Computational Social Systems, September 2018.
16. Babburi, S. Lightweight Distributed Provenance Framework for Edge and IoT Data Systems.
17. Gaddam, S. From Fixed Specifications to Self-Adapting Systems: A Machine Learning Perspective on Software Engineering.
18. Immadi, S. K. (2025). Optimizing ERP for Human Capital Management. Applied Research for Growth, Innovation and Sustainable Impact, 377–384. https://doi.org/10.1201/9781003684657-63
19. Reddy, S. K. R. Developing a Modular AI Framework to Enhance Scalability and Personalization in Next-Generation Reward Platforms.
20. Poojari, R. Frameworks for Data Management and Lineage in Large-Scale Healthcare Data Systems.
21. Mahimalur, R. K., Vasgam, M., & Manoharan, D. Devops Lifecycle Management And Cloud Migration Assessments: A Security-Driven CICD Perspective.
22. Viswanathan, V. Generative AI for Smarter Workforce Planning and Enterprise Resource Decisions.
23. Gajula, S. (2026, March). Two Pillars of Banking Intelligence: A Comparative Analysis of AI Techniques for Fraud Prevention and Churn Mitigation. In 2026 14th International Symposium on Digital Forensics and Security (ISDFS) (pp. 1-6). IEEE.
24. Maturi, S. Y. (2023). Crowdsourced frontier: Unveiling autonomous adversarial cybercapabilities via open AI competition. International Journal of Intelligent Systems and Applications in Engineering, 11(1s), 275–284.
25. Venkata Ramana, P. (2024). AI-driven predictive analytics in ERP systems for proactive supply chain optimization. International Journal of Research in Information Technology and Computing, 8(4).

26. Srikanth Kavuri. (2025). AI-DRIVEN TEST AUTOMATION FRAMEWORKS: ENHANCING EFFICIENCY AND ACCURACY IN SOFTWARE QUALITY ASSURANCE. International Journal of Applied Mathematics, 38(10s), 699–710. https://doi.org/10.12732/ijam.v38i10s.990
27. Gajula, S. (2025). Cloud transformation in financial services: A strategic framework for hybrid adoption and business continuity. International Journal of Scientific Research in Computer Science, Engineering and Information technology. https://doi.org/10.52710/cfs.875
28. Shashank, A. (2025). AI-Enhanced ETL Processes: Leveraging Artificial Intelligence for Optimized Data Integration Systems. Journal Of Multidisciplinary, 5(8), 219-225.
29. Kandula, S. T. R., Susarla, R. S., & Boyapati, P. K. (2025, July). Enhanced Cyber Security Using Global Local Artificial Neural Network Based Intrusion Detection in Big Data Environment. In 2025 IEEE 4th World Conference on Applied Intelligence and Computing (AIC) (pp. 426-431). IEEE.
30. Boyapati, P. K. Building a centralized data operations hub for healthcare enterprise integration. IJSAT-Int. J. Sci. Technol. 16 (2). https://doi.org/10.71097/IJSAT.v16.i2.3219