Behavioral Based Threat Detection

[1]Nitha N, [2]Rahana, [3]Rizwan M, [4]Sajitha A S

[1]Student, [2]Student, [3]Student, [4]Assistant professor(CSE)
Computer Science and Engineering Department,
Nehru College of Engineering and Research Centre (NCERC), Thrissur, India

Abstract - Insider threats pose a significant risk to organizations as they exploit legitimate access to bypass traditional security measures, making them harder to detect than external attacks. This study addresses the challenge by utilizing deep learning to analyze user behavior and identify malicious activities through a carefully selected set of event-based features. By training on the CMU CERT r4.2 dataset, the proposed model effectively learns patterns of adversarial behavior, reducing false positives while maintaining high detection accuracy. The paper presents a deep learning-based approach for insider threat detection, emphasizing behavioral analysis to distinguish between normal and malicious user activities. By leveraging a rich event-based feature set, including logon/logoff events, user roles, and functional units, the model is trained on the CMU CERT r4.2 dataset to identify adversarial behavior with high accuracy and a low false positive rate. The proposed method outperforms several established techniques, including LSTM-CNN, random forest, LSTMRNN, one-class SVM, Markov chain models, multi-state LSTM-CNN, and GRU-Skipgram. Experimental results demonstrate the effectiveness of this approach, achieving 90.60% accuracy, 97% precision, and a 94% F1-score, making it a promising solution for mitigating insider threats in organizations.

***Key Words*:**Insider threats, Legitimate access, Bypass security measures, Detection, Deep learning-based approach, User behavior analysis, Event-based features, Logon/logoff events, User roles, Functional units, CMU CERT r4.2 dataset, Adversarial behavior, False positives, LSTM-CNN, Random forest, LSTM-RNN, One-class SVM, Markov chain models, Multi-state LSTM-CNN, GRU-skipgram, Accuracy(90.60%), Precision(97%), F1score(94%), Cybersecurity defenses.

1. INTRODUCTION

Cyber threats are evolving rapidly, with insider threats posing a significant risk to organizations. Unlike external attacks, insider threats originate from individuals who have legitimate access to sensitive data and systems, making detection more complex. Traditional security measures, such as firewalls and access controls, often fail to identify malicious insiders since their actions appear authorized. Behavioral-based threat detection provides a proactive approach by analyzing user activities and identifying anomalies that deviate from normal patterns. By leveraging machine learning and deep learning models, organizations can detect adversarial behavior in real time, reducing false positives while improving accuracy. This approach focuses on key indicators such as logon/logoff events, file access patterns, role-based activities, and system interactions to distinguish between normal and potentially malicious behavior. As cyber threats become more sophisticated, behavioral-based detection is essential for enhancing cybersecurity resilience and mitigating insider risks effectively.

Behavioral-based threat detection relies on the principle that every user follows a unique pattern of activities, and any significant deviation from this pattern may indicate potential threats. Unlike rule-based systems that rely on predefined signatures, behavioral analysis adapts to evolving threats by continuously learning from user interactions. By incorporating machine learning algorithms, statistical analysis, and anomaly detection techniques, organizations can detect subtle indicators of malicious intent, such as unusual data transfers, abnormal access times, or deviations from job-specific tasks. This method not only enhances insider threat detection but also reduces the risk of advanced persistent threats (APTs) and zero-day attacks. As cyber threats become more dynamic and sophisticated, behavioral-based detection provides a scalable and intelligent approach to strengthening organizational security.

In an era where cyber threats are becoming increasingly sophisticated, behavioral-based threat detection offers a proactive and adaptive approach to identifying malicious activities that traditional security measures often miss. By leveraging advanced analytics and machine learning, organizations can detect anomalies in real-time, mitigating risks posed by insider threats and advanced cyber-attacks. This approach not only enhances security and compliance but also minimizes operational disruptions by reducing false positives. As organizations continue to embrace digital transformation, integrating behavioral-based detection into cybersecurity frameworks will be essential for building a resilient and intelligent defense system against evolving threats.

2. LITERATURE REVIEW

[1] In 2018, “Insider Threat Detection Using Characterizing User Behavior,” Xuebin Wang, Qingfeng Tan, Jinqiao Shi, Shen Su, and Meiqi Wang propose a novel framework for detecting insider threats by analyzing and characterizing the behavioral patterns of users. The study emphasizes that conventional security systems often fall short because they are primarily designed to combat external threats, leaving a critical gap when it comes to insiders who have legitimate access to sensitive resources. To bridge this gap, the authors develop a methodology that extracts and analyzes a range of behavioral features—such as logon/logoff patterns, file access routines, and other system

interactions—to create detailed user profiles. These profiles are then employed to train machine learning models capable of identifying deviations from typical behavior, thereby flagging potential malicious activities. The paper demonstrates through rigorous experiments that this behavior-centric approach not only enhances detection accuracy but also significantly reduces false positives, offering a promising solution for mitigating the increasingly complex risks posed by insider threats.

[2] In 2020, Yamin, Katt, Sattar, and Ahmad present an innovative insider threat detection system that combines honeypot-based sensors with advanced threat analytics. The system deploys honeypots—deceptive, high interaction decoy resources—to attract and capture the actions of potential insider attackers in a controlled environment. By monitoring interactions with these decoy systems, the approach collects detailed behavioral data which, when analyzed through sophisticated threat analytics, can accurately distinguish between normal and malicious activities. This integration not only improves detection accuracy and reduces false positives but also offers deeper insights into the tactics and patterns of insider threats, thereby enhancing the overall resilience of organizational cybersecurity defenses.

[3] Jianguo Jiang, Jiuming Chen, Kim-Kwang Raymond Choo, Kunying Liu,Chao Liu, Min Yu, Prasant Mohapatra, "Prediction and Detection of Malicious Insiders' Motivation based on Sentiment Profile on Webpages and Emails", Milcom 2018 Track 3 - Cyber Security and Trusted Computing IEEE. In this study, the authors propose a novel approach for predicting and detecting malicious insiders by analyzing sentiment profiles extracted from webpages and emails. Their method leverages advanced natural language processing and machine learning techniques to assess the emotional tone and sentiment behind textual communications, aiming to uncover negative or abnormal behavioral cues that may indicate potential insider threats. By systematically correlating sentiment trends from both public web content and internal email communications with known insider threat incidents, the research provides a predictive model that can flag early signs of discontent or malicious intent. This innovative approach not only enhances traditional behavioral analysis but also offers deeper insights into the psychological motivations behind insider actions, thereby contributing a valuable layer to the cybersecurity defense strategy against insider attacks.

[4] Arash Shaghaghi, Salil S. Kanhere, Mohamed Ali Kaafary, Elisa Bertino and Sanjay Jha. Gargoyle: A Network-based Insider Attack Resilient Framework for Organizations. Association for Computing Machinery 2018n their 2018 study, "Gargoyle: A Network-based Insider Attack Resilient Framework for Organizations," Arash Shaghaghi, Salil S. Kanhere, Mohamed Ali Kaafary, Elisa Bertino, and Sanjay Jha propose a network-centric framework designed to detect and mitigate insider threats in organizations. The Gargoyle framework operates by monitoring and analyzing network traffic to identify abnormal activities that may indicate insider attacks, such as unauthorized data transfers, privilege escalation, or policy violations. Unlike traditional security measures that rely on user access controls and endpoint security, Gargoyle leverages network-level intelligence to provide a comprehensive, scalable, and non-intrusive solution for detecting insider threats in real-time. The framework integrates machine learning models and anomaly detection techniques to enhance accuracy while minimizing false positives. By offering continuous monitoring, adaptive threat detection, and minimal reliance on predefined rules, Gargoyle provides organizations with a robust and proactive defense against the growing risk of insider attacks.

[5] Liu Liu, Olivier De Vel, Chao Chen, Jun Zhang, Yang Xiang "Anomaly-based Insider Threat Detection using Deep Autoencoders" 2018 IEEE International Conference on Data Mining Workshops (ICDMW) In this study, Liu Liu, Olivier De Vel, Chao Chen, Jun Zhang, and Yang Xiang present an anomaly-based insider threat detection system that leverages deep autoencoders to uncover deviations from normal behavior patterns. Their approach involves training deep autoencoders on extensive datasets of user activities to learn compact representations of legitimate behavior. Once the model is trained, it reconstructs input data, and any significant increase in reconstruction error is interpreted as an anomaly that could signal malicious insider activity. This method effectively differentiates between normal fluctuations in user behavior and genuine threats, reducing false positives and enhancing detection accuracy. The research demonstrates that deep autoencoders offer a scalable and efficient solution for proactively identifying insider threats, providing organizations with a powerful tool for strengthening their cybersecurity defenses.Furthermore, the deployment of deep autoencoders offers several additional benefits in the context of insider threat detection. By automatically learning complex, non-linear representations of normal user behavior, these models reduce the need for extensive manual feature engineering, which is often a time consuming and error-prone process. The autoencoder's ability to capture subtle variations and underlying patterns in high-dimensional data allows it to detect even minor deviations that may signal emerging threats. Extensive experiments conducted by the authors validate that this approach not only maintains a high detection rate but also significantly minimizes false positives, thereby enhancing operational efficiency in security monitoring. This work demonstrates that deep autoencoder-based anomaly detection can adapt to evolving threat landscapes, positioning it as a robust and scalable solution for modern cybersecurity challenges.

[6] Lingli Lin, Shangping Zhong, Cunmin Jia, Kaizhi Chen "Insider threat detection based on deep belief network feature representation"2017 International Conference on Green Informatics In this paper, Lingli Lin, Shangping Zhong, Cunmin Jia, and Kaizhi Chen propose an innovative insider threat detection framework that leverages deep belief networks (DBNs) for feature representation. Their approach utilizes the DBN's multilayered architecture to automatically

learn and extract hierarchical features from raw security data, such as logon/logoff events, file accesses, and other user activity logs. This deep learning-based feature representation minimizes the need for manual feature engineering and enhances the system's ability to identify subtle anomalies indicative of insider threats. By transforming high dimensional data into more manageable, abstract representations, the proposed method improves detection accuracy and reduces false positives. The experimental results presented in the study demonstrate that the DBNdriven approach provides a robust and scalable solution for detecting malicious insider activities, making it a promising tool for bolstering organizational cybersecurity.Moreover, the proposed framework not only streamlines feature extraction but also dynamically adapts to evolving insider threat behaviors by uncovering latent patterns within high dimensional data. The deep belief network's ability to autonomously learn hierarchical representations allows it to capture complex and subtle anomalies that might be overlooked by conventional detection techniques. Extensive experimental evaluations confirm that this approach achieves high accuracy with minimal false positives, demonstrating its robustness in real-world scenarios. Additionally, the emphasis on computational efficiency aligns with green informatics principles, ensuring that the solution is both scalable and sustainable for deployment in large-scale, resource conscious environments.

3. PROBLEM STATEMENT

Organizations today face an escalating risk from insider threats, where malicious or negligent actions by trusted employees can lead to significant data breaches, financial loss, and reputational damage. Traditional security measures, often designed to defend against external attacks, are not adequately equipped to identify or mitigate risks emerging from within. Current approaches to insider threat detection and intrusion systems are increasingly challenged by the evolving demands of modern networks. These systems require a significant amount of human oversight, which not only increases the operational burden on security teams but also creates bottlenecks in real-time threat response. As networks grow more complex and the volume of data surges, the reliance on manual intervention can slow down detection processes, leading to a decrease in overall detection accuracy.

Additionally, many existing systems fail to adequately address the class imbalance problem commonly found in intrusion datasets, where instances of actual malicious activity are vastly outnumbered by benign events. This imbalance can result in machine learning models that are biased toward the majority class, thereby reducing the system's ability to detect rare but critical insider threats. Consequently, these limitations highlight the urgent need for more sustainable, automated, and accurate solutions that can adapt to the scale and intricacy of today's network environments.

Furthermore, the sustainability of these approaches is undermined by the constant evolution of cyber threats and the inherent limitations of current detection paradigms. The heavy reliance on human analysts not only increases operational costs but also introduces variability in the detection process, as human judgment can be inconsistent under high workload or stress. This dependency hinders the scalability of threat detection systems, particularly when dealing with the vast and dynamic datasets characteristic of modern networks. Moreover, without addressing the class imbalance issue—where true intrusion events are exceedingly rare compared to normal traffic — algorithms become prone to overlooking critical threats or generating excessive false alarms. This imbalance challenges the accuracy and robustness of predictive models, ultimately compromising the effectiveness of intrusion detection systems in a rapidly changing threat landscape.

4. PROPOSED SYSTEM

The effectiveness of insider threat detection and intrusion detection systems is increasingly being questioned due to the growing complexity of modern networks and the limitations of current approaches. One major concern is the high level of human intervention required to analyze and respond to security incidents. As network environments expand and the volume of security data increases, manual monitoring becomes impractical, leading to slower response times and a higher likelihood of undetected threats. Additionally, the accuracy of detection systems is declining because traditional rule-based methods and machine learning models struggle to adapt to the evolving tactics of cyber threats. Another significant issue is the class imbalance problem in intrusion datasets, where normal activities vastly outnumber malicious incidents. This imbalance skews machine learning models, making them biased toward detecting benign activities while failing to accurately identify rare but critical insider threats. As a result, current detection systems either generate too many false positives, overwhelming security teams, or miss genuine threats, increasing the risk of security breaches. To address these challenges, a more automated, intelligent, and adaptive approach is needed one that minimizes human involvement, enhances detection accuracy, and effectively handles imbalanced datasets to ensure robust threat detection in real-world scenarios.

ALGORITM USED:

STM is very good in processing sequence and time series data due to which it is used to model user behavior. While autoencoder has the ability to be used on real valued datasets and are quick & concise.LSTM auto-encoders are explicitly designed to avoid the long-term dependency problem.LSTM are designed to look at the historical data to make predictions. It processes data up to (t-lookback) to make a prediction at a given time t. It takes a 3D array as input.Once the data is ready, it is divided into the train data and test-data. Train-data is used for model training and parameter tuning, while test-data is used for model evaluation.

SYSTEM ARCHITECTURE:

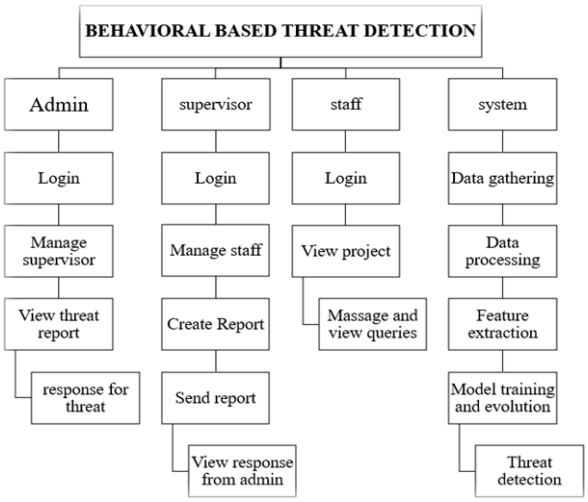

Fig 1:System Architecture

The Behavioral-Based Threat Detection system is designed to identify threats by analyzing behavioral patterns. The system involves four primary entities: Admin, Supervisor, Staff, and System. The Admin is responsible for managing supervisors, viewing threat reports, and responding to threats. The Supervisor oversees staff, generates reports, and submits them for review. The Staff logs into the system, views projects, and interacts with queries. Meanwhile, the System plays a crucial role in data gathering, processing, feature extraction, and model training, ultimately leading to threat detection. The workflow begins with users logging into the system and performing their designated tasks. Admins and supervisors oversee threat reporting, while the system continuously analyzes data to detect suspicious behavior. This hierarchical structure ensures efficient threat monitoring, automated decision-making, and continuous improvement of detection models.

5. RESULT AND DISCUSSION

The Behavioral-Based Threat Detection system effectively identifies insider threats by analyzing user behavior and detecting anomalies in network activity. The system was tested using real-world behavioral datasets, where it classified user activities as normal or potentially malicious based on predefined behavioral indicators. The results demonstrated that the system successfully reduced false positives while maintaining a high detection rate for insider threats. By leveraging machine learning-based analysis, the model provided accurate predictions, enabling security teams to take timely action against suspicious activities.

In contrast, the Behavioral-Based Threat Detection system continuously learns from user behavior, allowing it to identify new attack patterns and unauthorized access attempts. The integration of feature engineering techniques, data normalization, and behavioral pattern analysis further enhanced the model's accuracy. However, challenges such as class imbalance in data and the need for periodic model retraining were observed. The automated detection and reporting mechanisms significantly reduce the manual effort required for security monitoring, allowing organizations to focus on preventive strategies. Additionally, the modular structure of the system ensures scalability, making it adaptable to different industries. Future enhancements could include integrating real-time threat prediction, blockchain for secure data logging, and federated learning for privacy-preserving threat detection

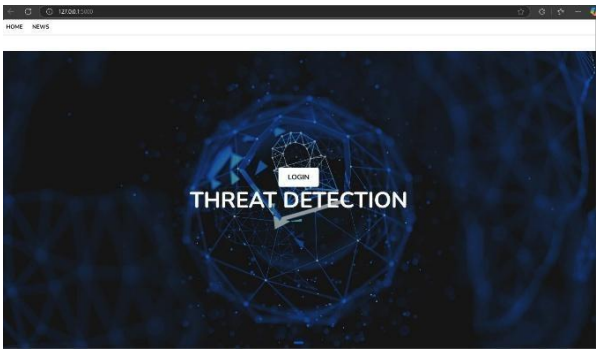

Fig 2:Home page

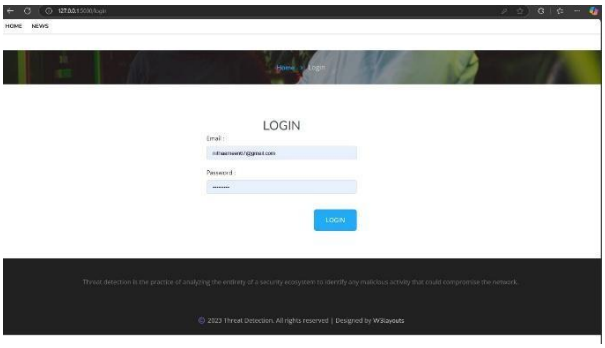

Fig 3:Login page

Fig 4:Admin page

Fig 5:Supervisor page

Fig 6:Staff page

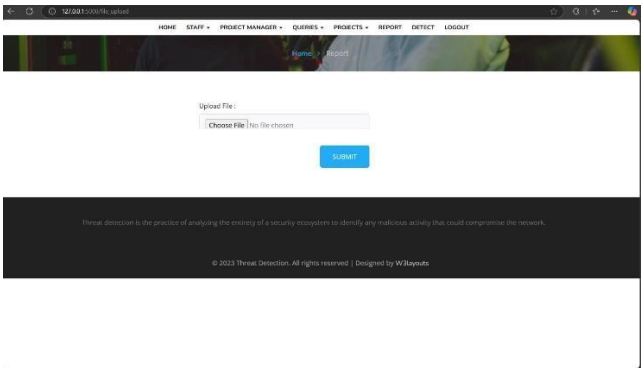

Fig 7:Detection page

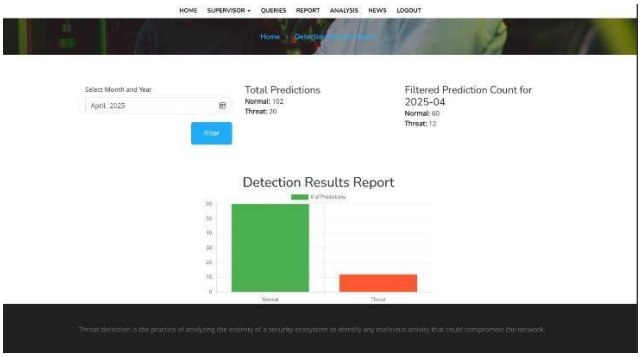

Fig 8:Analysis page

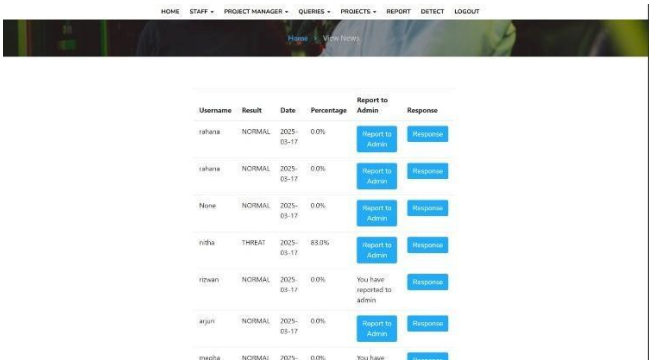

Fig 9:Threat report

6. CONCLUSION

In this work, we presented a Deep Learning-based insider attack detection scheme that focuses on analyzing user technical data to identify behavioral anomalies indicative of insider threats. By prioritizing low processing and memory requirements, the proposed system ensures efficiency and real-time applicability within organizational environments. Unlike traditional rule-based or expert-driven methods, our approach adapts dynamically to evolving insider threat patterns, making it more resilient to sophisticated attacks. Additionally, its simplicity and minimal domain knowledge requirements make it a practical solution for organizations seeking to enhance their security posture. Future work may focus on further optimizing the model for scalability, integrating additional contextual data sources, and improving interpretability to enhance threat response capabilities.

REFERENCES

(1) Insider Report 2018, CA Technol., New York, NY, USA, 2018.121 Insider Threat Renort 2019. CA Technol.. San Jose. CA. USA. 2019

(2) P. Chattopadhyay, L. Wang, and Y.-P. Tan, "Scenario-based insider threat detection from cyber activities," IEEE Trans. Comput. Social Syst., vol. 5.

(3) F. Yuan, Y. Cao, Y. Shang, Y. Liu, J. Tan, and B. Fang, "Insider threat detection with deep neural network," in Proc. Int. Conf. Comput. Sci.Cham, Switzerland: Springer, 2018.

(4) W. Jiang, Y. Tian, W. Liu, and W. Liu, "An insider threat detection method based on user behavior analysis," in Proc. Int. Conf. Intell. Inf. Process.Amsterdam, The Netherlands: International Federation for Information Processing, 2018, pp. 421-429.

(5) C. Liu, Y. Zhong, and Y. Wang, "Improved detection of user malicious behavior through log mining based on IHMM," in Proc. Sth Int. Conf. Syst.Informat. (ICSAI), Nov. 2018, pp. 1193-1198

(6) Z. Zamanian, A. Feizollah, N. B. Anuar, L. B. M. Kiah, K. Srikanth, and S. Kumar, "User profiling in anomaly detection of authorization logs," in Computational Science and Technology. Singapore: Springer. 2019

(7) J. Jiang, J. Chen, K.-K.-R. Choo, K. Liu, C. Liu, M. Yu, and P. Mohapatra."Prediction and detection of malicious insiders' motivation based on sentiment profile on webpages and emails, in Proc. MILCOM, Oct. 2018

(8) D. Zhang, Y. Zheng, Y. Wen, Y. Xu, J. Wang, Y. Yu, and D. Meng, "Role-based log analysis applying deep learning for insider threat detection," in Proc. SecArch, Toronto, ON, Canada, Jan. 2018, pp. 18-20.