iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 14 **Issue:** IV **Month of publication:** April 2026

DOI: https://doi.org/10.22214/ijraset.2026.81544

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue IV Apr 2026- Available at www.ijraset.com

A Comprehensive Survey on Context-Aware InsiderThreat Detection Systems: Bridging the Gap Using Deep Learning, NLP, and Time-Series Analysis

Hemalatha K, Hugar Renuka Prasad, Kusuma D, Mahanth DM, Nehal SP
Department o fCSE, Sapthagiri College of Engineering, Bengaluru, India

Abstract: ***Insider threats represent a criticalchallenge in modern cybersecurity due to the misuse of legitimate access by authorized users. Conventional detection approaches, including rule-based and signature-based systems, are limited in identifying unknown and evolving threats because they lack adaptability and contextual awareness. This paper presents a comprehensive survey of recent advancements in insider threat detection and introduces CogniShield, a context-aware detection framework. Existing methods are categorized into behavioural analytics, anomaly detection, deep learning-based techniques, and sequence modelling approaches. A detailed analysis highlights key limitations such as high false positive rates, insufficient temporal modelling, and limited integration of heterogeneous data sources. To address these issues, the proposed framework integrates Deep Learning, Natural Language Processing (NLP), and Time-Series Analysis to enable intelligent, scalable, and real-time threat detection.***

Thesystemfurtherincorporatescontextual understanding and dynamic risk scoring to enhance accuracy and support proactive security management.

Keywords: Insider Threat Detection, Deep Learning, Natural Language Processing, Time-Series Analysis, Anomaly Detection, Behavioural Analytics, Risk Scoring.

I. INTRODUCTION

With the increasing dependence on digital infrastructures, organizations are facing a growing number of cybersecurity challenges. Among these, insider threats are particularly difficult to detect, as they originate from individuals who already have authorized access to systems and data. Unlike external attackers, insiderscan operate within normal system boundaries, making malicious activities harder to distinguish from legitimate behaviour.

Traditional security systems, such as rule-based monitoring and signature-based detection, are primarily designed to identify known attack patterns. However, these approaches are ineffective in detecting subtle behavioural changes and previously unseen threats. As a result, there is a growing need for intelligent systems capable of analysing user behaviour, contextual information, and temporal patterns.

This paper presents a survey of existing insider threat detection techniques and proposes CogniShield, a context-aware system designed to overcome the limitations of conventional approaches by leveraging advanced AI technologies.

II. THEMATIC LITERATURE REVIEW

To understand the current research landscape, existing studies are categorized into three major themes: behavioural analytics, deep learning and sequence modelling, and context-aware hybrid approaches.

A. Behavioural Analytics and Anomaly Detection:

Early research in insider threat detection focused on analysing user activity logs to identify deviations from normal behaviour. These methods often rely on unsupervised learning techniques, clustering algorithms, and statistical models to establish baseline user profiles. While such approaches are effective in detecting obvious anomalies, they often fail to capture complex behavioural patterns and lack contextual understanding.

B. Deep Learning and Sequence Modelling:

Recent advancements have introduceddeep learning techniques such as Autoencoders, Long Short-Term Memory (LSTM) networks, and Transformer-based models. These approaches are capable of learning complex patterns and capturing temporal dependencies in user behaviour.

Sequence modelling techniques enable the system to analyse the order and timing of user actions, making it possible to detect subtle and long-term anomalies. Although these models significantly improve detection accuracy, they often require large datasetsandhighcomputationalresources.

C. Context-Aware and Hybrid Approaches:

Modern research emphasizes theintegration of multiple data sources, including system logs, user behaviour, and textual data. Natural Language Processing (NLP) techniques are used to analyse emails and communication logs, providing insights into user intent.

Hybrid systems that combine behavioural analysis, deep learning, and contextual information have shown improved performance. However, challenges related to scalability, real-time processing, and interpretability still remain.

III. COMPARATIVE ANALYSIS AND RESEARCH GAPS

A critical evaluation of existing approaches reveals several limitations:

1) Lack of Context Awareness: Many systems do not consider contextual information, limiting their ability to interpret user intent.
2) Limited Temporal Modelling: Traditional models fail to capture long-term dependencies in user behaviour.
3) High False Positive Rates: Rule-based and basic machine learning systems often generate excessive false alerts.
4) DataImbalance: Insider threat datasets typically contain very few malicious instances, affecting model performance.
5) ScalabilityIssues: Many systems struggle to process large-scale data in real time.

These challenges highlight the need for a more comprehensive and intelligent detection framework.

IV. PROPOSED SYSTEM: COGNISHIELD

To address the identified gaps, this paper proposes CogniShield, a context-aware insider threat detection system.

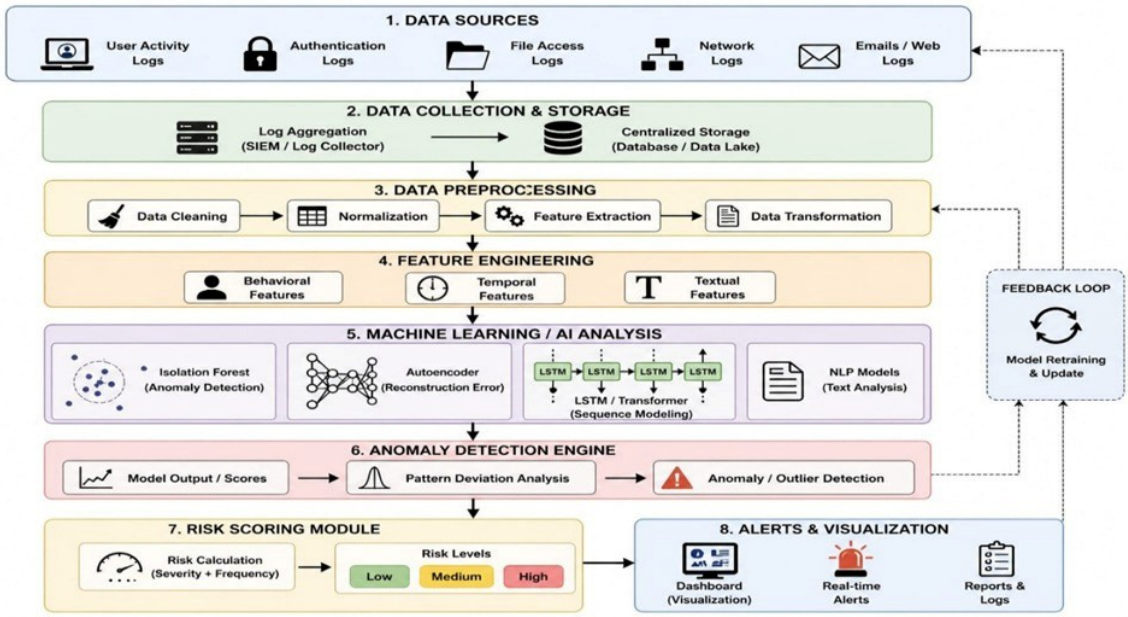
A. System Architecture

CogniShieldfollowsalayeredarchitectureconsistingof:

- DataCollectionLayer
- DataPreprocessingLayer
- BehaviourModellingLayer
- AI-BasedDetectionLayer
- RiskScoringModule
- AlertandVisualizationLayer

B. Key Features

- Integration of multi-source data (logs, user activities, textual data).
- Context-aware behaviouralanalysis.
- Real-timeanomalydetection.
- Dynamicriskscoringmechanism.
- Scalableandadaptivearchitecture.



This architecture enables the system to process data efficiently and detect threats in real time.

V. METHODOLOGY

Thesystemoperatesinfourmajorphases:

1) DataCollectionandPreprocessing: Data is collected from multiple sources, including logs, user activity records, and textual data. The data is then cleaned, normalized, and transformed into structured features.
2) BehaviourModelling; The system learns normal user behaviour patterns using historical data and establishes a baseline for comparison.
3) AnomalyDetection: Advanced models such as Isolation Forest, Autoencoders, and LSTM networks are applied to identify deviations from normal behaviour.
4) RiskScoringandAlertGeneration: Detected anomalies are evaluated and assigned risk levels.Alerts are generated to notify administrators in real time.

VI. ADVANTAGES OF THE PROPOSED SYSTEM

1) Detects unknown and evolving threats.
2) Reduces false positives through contextual analysis.
3) Captures temporal and sequential patterns.
4) Supportsreal-timemonitoring.
5) Scalable for organizational deployment.

VII. FUTURE RESEARCH DIRECTIONS

Futureworkcanfocuson:

1) Integration of Large Language Models (LLMs).
2) Development of explainableAI models.
3) Privacy-preserving machine learning techniques.
4) Cross-platform deployment and cloud integration.

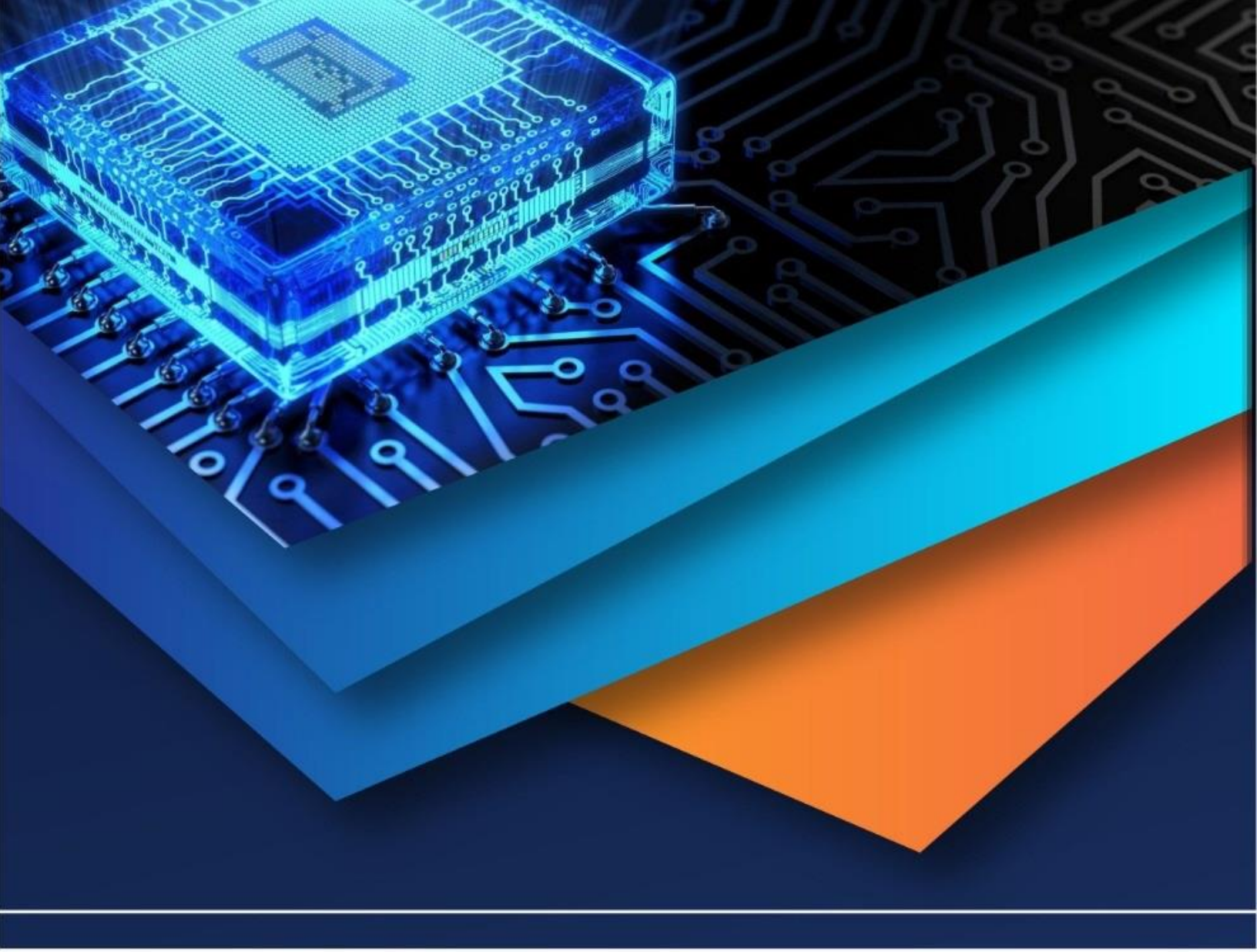
VIII. CONCLUSION

This paper presents a comprehensive survey of insider threat detection techniques and introduces CogniShield, a context-aware detection framework. By integrating Deep Learning, NLP, and Time-SeriesAnalysis, the proposed system addresses key limitations of traditional approaches and provides an effective solution for modern cybersecurity challenges.

The framework enables proactive threat detection, improved accuracy, and real-time decision-making, making it suitable for practical deployment in organizational environments.

REFERENCES

[1] F. R. Alzaabi and A. Mehmood, "A Review of Recent Advances, Challenges, and Opportunities in Malicious Insider Threat Detection Using Machine Learning Methods," IEEE Access, vol. 12, 2026.
[2] K. C. Roy and G. Chen, "GraphCH:ADeep Framework forAssessing Cyber-Human Aspects in Insider Threat Detection," IEEE Transactions on Dependable and Secure Computing, 2026.
[3] X.Tao, J. Liu,Y.Yu, H. Zhang, andY. Huang, "An InsiderThreat Detection Method Based on Improved Test-Time Training Model," High-Confidence Computing, 2025.
[4] O. Nikiforova,A. Romanovs, V. Zabiniako, and J. Kornienko, "Detecting and Identifying Insider Threats Based on Advanced Clustering Methods," IEEE Access, 2025.
[5] T.Al-Shehari et al., "Enhancing Insider Threat Detection in Imbalanced Cybersecurity Settings Using the Density-Based Local Outlier Factor Algorithm," IEEE Access, 2025.
[6] J. P. Ribeiro and E. Petrova, "AI-Based BehaviouralAnalytics for Insider Threat Detection in Enterprise Information Systems," 2025.
[7] T. Tian, C. Zhang, B. Jiang, H. Feng, and Z. Lu, "Insider Threat Detection for Specific Threat Scenarios," Cybersecurity Journal, 2024.
[8] M. Elbasheer and A. Akinfaderin, "User-Based Sequential Modelling with Transformer Encoders for Insider Threat Detection," 2024.
[9] J.Yang andY. Xia, "Coverage and Routing Optimization of Wireless Sensor Networks Using Improved Cuckoo Algorithm," IEEE Access, 2024.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY