# Insider Threat Detection Methodologies

**SHREYA SREEKUMAR**
Department of Computer Science and Engineering (Cyber Security)
Vimal Jyothi Engineering College, Chemperi, Kannur shreyasreekumar6@gmail.com

**SARANG C**
Department of Computer Science and Engineering (Cyber Security)
Vimal Jyothi Engineering College, Chemperi, Kannur
sarangc438@gmail.com

**ALKA SAJEEVAN P**
Department of Computer Science and Engineering (Cyber Security)
Vimal Jyothi Engineering College, Chemperi, Kannur
alkasajeevan12@gmail.com

**VARNA O V**
Department of Computer Science and Engineering (Cyber Security) Vimal Jyothi Engineering College, Chemperi, Kannur
varnaov04@gmail.com

**ASWATHI V**
Assistant Professor
Department of Computer Science and Engineering (Cyber Security)
Vimal Jyothi Engineering College, Chemperi, Kannur
aswathiv2016@gmail.com

*Abstract*—**Insider threats, originating from individuals with legitimate access to sensitive systems and data, represent a significant cybersecurity challenge, unlike external attacks, insider threats are harder to detect, as they often exploit legitimate credentials to bypass conventional security measures. These threats can result in severe consequences such as data breaches, financial losses, and system disruptions. Traditional detection methods, such as rule-based approaches and classical ma- chine learning models, struggle to identify evolving and sophisticated insider behaviors due to their reliance on predefined patterns and static detection criteria. Recent advancements in artificial intelligence (AI), deep learning, cryptographic security and hybrid detection frame- works have significantly enhanced the ability to detect and mitigate insider threats. Deep learning models, such as Long Short-Term Memory (LSTM) networks and Generative Adversarial Networks (GANs), excel at identifying subtle behavioral anomalies, while cryptographic techniques, such as blockchain-based authentication and data encryption, reinforce security by preventing unauthorized access. Hybrid approaches that combine AI-driven anomaly detection with structured security control mechanisms have emerged as the most effective solution, offering multi-layered protection against insider attacks. The primary objective of this paper is to present a comprehensive review of insider threat detection methodologies, comparing traditional and AI- based approaches, including specification-based detection, behavioral monitoring, anomaly-based models and cryptographic security measures. The study highlights the strengths and limitations of each method and explores future research directions, including the development of self-supervised learning models, explainable AI and optimized real-time detection systems. A holistic security strategy, integrating AI, cryptographic security and policy-driven risk mitigation is necessary to enhance organizational resilience against insider threats.**

## I. INTRODUCTION

In today's digital landscape, organizations face an increasing risk of insider threats, which arise from employees, contractors, or partners misusing their legitimate access to sensitive data and systems. Unlike external cyberattacks, which rely on exploiting vulnerabilities from outside an organization's net- work, insider threats originate from within, making them more difficult to detect and prevent. Security threats can arise from both deliberate actions, like data theft, sabotage, or fraud, and unintentional errors, such as accidental data leaks or misconfigured security settings. Traditional security measures such as firewalls, intrusion detection systems (IDS), and access control policies are primarily designed to counter external threats, often leaving organizations vulnerable to insider attacks. Rule-based security approaches rely on predefined conditions, making them ineffective against evolving attack patterns. Classical ma- chine learning models, while improving detection accuracy often struggle with high-dimensional data, require extensive feature engineering, and are prone to false positives. The emergence of AI and deep learning has revolutionized insider threat detection by introducing models capable of autonomously identifying suspicious activities and learning behavioral patterns over time. Techniques such as LSTMs, Re- current Neural Networks (RNNs) and Graph Neural Networks (GNNs) have demonstrated promising capabilities in analyzing sequential data and identifying insider behaviors. Additionally, cryptographic advancements, such as blockchain-based access control and secure encryption techniques, provide enhanced security against unauthorized data access. This paper aims to provide a detailed analysis of insider threat detection methodologies, comparing traditional approaches with modern AI-based techniques. The study examines various models, including behavioral anomaly detection, cryptographic security solutions and hybrid works that integrate multiple detection strategies. By identifying existing challenges and limitations, this re- search explores future directions for improving detection accuracy, reducing false positives, and optimizing real-time threat prevention mechanisms. The ultimate goal is to establish a comprehensive, multi-layered defense system that effectively mitigates insider threats while maintaining organizational efficiency and security compliance.

*1) Traditional Machine Learning Approaches:* Traditional machine learning techniques focus on detecting anomalies and deviations in user behavior. These methods have been widely researched and applied in cybersecurity for their interpretability and efficiency in structured environments.

- **S**upport Vector Machines (SVM): SVMs have been effective in classifying normal and malicious behaviors based on predefined features. However, their reliance on manual feature engineering limits their adaptability to evolving insider threats.
- **H**idden Markov Models (HMMs): HMMs analyze sequential data patterns, making them useful in detecting behavior-based threats. However, they require significant computational resources and struggle with unseen patterns.
- **D**ecision Trees and Random Forests: These models are effective for classification tasks, providing interpretable decision rules. However, they tend to struggle with high-dimensional data and often require additional preprocessing techniques to re- main effective.
- **L**ogistic Regression: This technique is simple and interpretable but performs poorly in capturing complex behaviors associated with insider threats.
- **S**ynthetic Minority Oversampling Technique (SMOTE): Used to address class imbalance in datasets, SMOTE generates synthetic samples to improve model learning. However, it can intro- duce noise and overfitting, making it less effective in real-world applications.

*2) Deep Learning-Based Approaches:* Deep learning models have revolutionized insider threat detection by leveraging automated feature learning, reducing reliance on manual feature engineering. These models adapt dynamically to new threats and provide superior pattern recognition capabilities.

- **D**eep Feedforward Neural Networks (DNNs): DNNs learn intricate representations of insider threat behaviors but require large labeled datasets for optimal performance. Their application is limited by their need for significant computational power.
- **R**ecurrent Neural Networks (RNNs) And Long Short-Term Memory (LSTMs): These models are particularly effective in processing sequential data, making them valuable in detecting anomalous user behavior over time. However, training RNNs and LSTMs can be expensive, and they may suffer from vanishing gradient issues.
- **G**raph Neural Networks (GNNs): GNNs leverage relational data to identify patterns of malicious behavior within an organization's structure. While highly effective, they require graph-based data representations, which are not always available.
- **G**enerative Adversarial Networks (GANs): GANs generate synthetic insider threat scenarios to augment training data, improving model generalize ability. However, training GANs is complex and prone to mode collapse, limiting their widespread adoption.

## II. LITERATURE SURVEY

Insider threats pose a significant risk to organizations as traditional security measures often fail to detect malicious activities from authorized users. Re- cent research has focused on behavioral and anomaly detection methods using ML and DL techniques. In this paper [1] user behavior analytics plays a key role, with deep learning models like LSTMs, CNNs, and Autoencoders effectively identifying deviations in activity patterns. LSTM-based models, including hybrid LSTM-CNN and LSTM-RNN approaches, have shown high accuracy in detecting anomalous behaviors. ML models such as Random Forest, SVM, and XG Boost are also widely used for feature-based classification of user activity data. Graph-based methods analyze relationships and interactions within an organization, utilizing techniques like Gaussian Mixture Models (GMM) and Structural Anomaly Detection. Other approaches, including network-based anomaly detection and psychological profiling, provide additional insights. Despite advancements, challenges re- main in computational costs, dataset limitations, and model interpretability. The proposed study introduces an LSTM Autoencoder approach with session-based feature extraction, achieving high accuracy on the CMU CERT dataset. Future research should focus on real-world datasets and hybrid models integrating behavioral, psychological, and contextual analysis for enhanced security.

Unlike external attackers, insiders-employees, con- tractors, or business associates-blend malicious actions with routine activities. The 2019 Insider Threat Re- port found that 60 percentage of organizations faced insider-related incidents, with associated costs rising by 34 percentage in a year refer [2]. Traditional rule- based detection methods, relying on thresholds and known patterns, struggle with adaptability and high false positives. Machine learning (ML) approaches, such as Naive Bayes, SVMs, and decision trees, improve detection by analyzing user behavior on endpoints and networks. However, ML models often require manual feature engineering and fail to capture long-term patterns. Deep learning methods like LSTMs, CNNs and graph neural network, enhance detection but suffer from computational inefficiencies and complexity. Transformers, such as BERT and GPT-2, revolutionize insider threat detection by processing long-term dependencies and improving contextual awareness. Digital Twin technology further strengthens monitoring by creating real-time behavioral models of employees. Data augmentation techniques, like BERT-based modifications and GPT-2-generated syn- thetic data, help address imbalanced datasets. The introduction of Distilled Trans, a streamlined trans- former model, enhances accuracy, reduces training time, and outperforms traditional approaches. These advancements-self-attention-based deep learning, Digital Twin integration, and scalable AI solutions-offer organizations real-time, effective, and explainable insider threat detection, improving cybersecurity resilience.

Insiders-including employees, contractors, or partners-can misuse data, disrupt operations, or compromise system integrity. In the paper [3], research has evolved from theoretical discussions to empirical detection techniques. Cappelli et al. (CERT) define insiders as those who intentionally exceed or misuse access, while Pfleeger et al. extend this to include unintentional threats. Malicious insiders act deliberately for financial gain, ideology, or revenge, while accidental insiders expose data due to negligence. Industry reports highlight the growing impact of insider threats. The Ponemon Institute estimates annual losses at 8.76 million per organization, and IBM X-Force attributes 60 percentage of cyberattacks to insiders. Notable cases, such as Robert Hanssen's espionage and Societe Generale's 7 billion fraud, underscore the risks. Detection techniques include rule-based, machine learning (ML), and deep learning approaches. Rule- based systems rely on predefined thresholds but generate false positives. ML models like SVMs and Decision Trees analyze user behavior but require extensive feature engineering and struggle with imbalanced datasets. Deep learning, especially transformers and Digital Twin Technology, improves detection by modeling complex behaviors but raises privacy concerns. Future efforts should focus on hybrid approaches combining anomaly-based and signature-based detection while addressing dataset limitations, false positives, and ethical concerns.

A systematic approach to mitigating insider threats by mapping security controls to specific threat characteristics. Insider threats, involving individuals with legitimate access misusing their privileges, pose a significant challenge as they operate within an organization's trusted boundaries, making detection and prevention complex. According to the 2019 Insider Threat Report, 90% of enterprises feel vulnerable to insider threats and 53% have experienced insider-related security incidents. These threats have manifested as data exfiltration, sabotage, fraud and privilege abuse, leading to severe financial and reputational consequences. Existing mitigation strategies include security frameworks, behavioral analytics, and machine learning-based models. Studies from Carnegie Mellon's CERT Insider Threat Center highlight [4] best practices such as log-based monitoring, anomaly detection, and policy enforcement, while regulatory guidelines like ISO/IEC 27002:2013 and NIST SP 800-53 advocate for structured security governance. Traditional rule-based approaches, though effective in enforcing policies, suffer from high false positive rates and fail to detect evolving attack patterns. Mod- ern approaches, including User and Entity Behavior Analytics (UEBA), leverage social network analysis, semantic analysis, and role-based assessments to detect suspicious activities. However, these techniques require significant computational resources and raise privacy concerns. The study proposes a formalized threat-control mapping methodology, categorizing in- sider threats based on their impact, affected com- ponents, and security properties while aligning them with relevant security controls such as role-based access control, multi-factor authentication, and data loss prevention. By integrating these controls into Security Information and Event Management (SIEM) systems, organizations can automate threat mitigation. Future research should focus on expanding threat- control knowledge bases, AI-driven behavioral modeling, and Digital Twin Technology to enhance real- time monitoring and response capabilities, ensuring a proactive and structured approach to insider threat mitigation.

In Forensic Investigation, existing research on in- sider threat detection, highlighting gaps and contributions. Insider threats pose significant risks as they involve authorized individuals engaging in malicious activities. Traditional forensic investigations follow a reactive approach, analyzing evidence post-incident, but this fails to prevent damage. Proactive forensic solutions using AI and ML have gained attention for real-time threat detection. Existing methods include statistical models, rule-based systems, and supervised learning techniques, but they require large labeled datasets, which are often unavailable. Unsupervised methods like Deep Autoencoding Gaussian Mixture Models (DAGMM) show promise but suffer from data purification challenges and high false positive rates. The study introduces the Cascaded Autoencoder Purification and Joint Optimization Scheme (CPJOS), which refines anomaly detection using cascaded autoencoders (CAEs) for data purification and a joint optimization network for improved accuracy. A hyper-graph correction module further enhances precision by distinguishing malicious activities from benign anomalies. Additionally, a Bidirectional Long Short-Term Memory (BiLSTM) network automates feature extraction, capturing temporal dependencies in user behavior. Empirical evaluations on benchmark datasets show CPJOS outperforms state-of-the-art models, achieving high precision and recall were discussed in the [5]. Future research aims to extend the model to spatial data and integrate transformer-based techniques for improved feature learning.

Insider Threat Mitigation, analyzes prevention strategies, classifying insider threats into malicious (e.g., lone wolves, third-party collaborators) and negligent (human error, lack of awareness). Attack types include data breaches, sabotage, espionage, Advanced Persistent Threat (APT), credential theft, and privilege escalation, violating confidentiality, integrity, and availability (CIA triad).Detection and prevention techniques fall into six categories: network-based methods (blockchain access control, centralized detection), behavior-based methods (ML-driven deterrence, adversarial detection), anomaly-based methods (AI and pattern recognition), analysis-based methods (semantic analysis, cryptographic security), access-based methods (biometric security, risk-based authentication), and intention-based methods (eye-tracking, behavioral assessments). Despite these advancements, existing frameworks remain reactive, struggling against emerging threats like deepfake fraud and AI-powered insider attacks. The study proposes [6] a multi-tiered activity monitoring model: Tier I (SIEM, XDR for real-time intelligence), Tier II (IAM for access control), and Tier III (security training to prevent accidental breaches). Future research should explore AI-driven threat intelligence, real-time monitoring, and adaptive access control to strengthen security. A proactive, multi-layered approach integrating behavioral analytics, anomaly detection, and access regulation is essential for mitigating evolving insider risks.

In [7] the expansion of the Internet of Things (IoT) has introduced significant cybersecurity risks, particularly insider threats, which are difficult to detect due to their authorized access. Recent advancements in artificial intelligence (AI), particularly deep learning and data augmentation, have shown promise in mitigating these threats. Insider Threat Detection (ITD) techniques have evolved from machine learning models like decision trees, random forests, and logistic regression to deep learning approaches such as Long Short Term Memory (LSTM) and Generative Adversarial Networks (GANs). However, machine learning models suffer from class imbalance, leading to high false positives. Oversampling techniques like SMOTE and ADASYN have been introduced but often generate redundant samples. GAN-based augmentation methods, including Conditional GANs and Wasserstein GANs, improve robustness but face mode collapse issues. Enhanced Bidirectional GANs (EBiGANs) address these limitations by improving data diversity. To optimize deep learning models, Bayesian hyperparameter tuning and dimensionality reduction techniques like PCA with k-means clustering have been integrated. These hybrid models improve accuracy and interpretability. Future research should focus on scalability, computational efficiency, and real-time adaptability to enhance ITD performance in IoT-enabled environments.

The use of deep learning techniques for insider threat detection has gained significant attention due to the challenges faced. Traditional machine learning methods struggle with capturing such complexities, but deep learning, with its ability to learn end-to- end representations, offers promising solutions. Key datasets like the CERT dataset are used to simulate insider threats in synthetic environments, facilitating model training. Deep learning models, including deep feedforward neural networks (DFNNs), recurrent neural networks (RNNs), convolutional neural networks (CNNs), and graph neural networks (GNNs), have outperformed conventional techniques in detecting suspicious behaviors from various data sources such as user activity logs and network interactions from [8]. Despite their advantages, challenges remain, such as the scarcity of labeled insider threat data, the subtlety of malicious activities, and the lack of model explain ability. Adaptive insider attacks further complicate detection. Future research directions include few- shot and self-supervised learning, multi-modal learning, deep survival analysis, and deep reinforcement learning, which can improve model robustness, pre- diction accuracy, and adaptability. Overcoming these challenges will enable deep learning to effectively safeguard organizations from insider threats, ensuring both security and operational efficiency.

Insider threat detection in Cyber-Physical Systems (CPS) has become a critical area of research as these systems integrate physical and digital infrastructures, introducing unique security challenges as we can see from the paper [9]. A systematic literature review (SLR) of 69 research papers highlights increasing research focus since 2016, with major contributions from the USA, China, and India, and a dominance of journal publications. The study categorizes in- sider threat detection methodologies into five key approaches: Specification-Based Methods, which rely on mathematical models, trust-based models, simulations, and security frameworks; Cryptographic Methods, including blockchain authentication, time synchronization, group key management, and anonymous authentication; Machine Learning and Deep Learning approaches, which leverage AI for threat detection and prediction; Game-Theoretic Approaches, which model strategic attacker-defender interactions; and Re- view and Survey Studies, summarizing CPS security literature. Insider threat impact multiple industries, including healthcare,

TABLE I
COMPARISON TABLE

| Reference | Methodologies | Strengths | Limitations |
|---|---|---|---|
| [1] | LSTM Autoencoder | - High detection accuracy with sequential dependency modeling.<br>- Handles large-scale session-based datasets effectively.<br>- Capable of detecting complex insider threat patterns | - Computationally expensive for large datasets and real-time monitoring.<br>- Lacks interpretability due to deep learning complexity.<br>- Dataset dependency may affect generalization to new threats. |
| [2] | Distilled Trans (Transformer-based model) | - Captures long-term dependencies for insider risk detection.<br>- Real-time monitoring with high adaptability.<br>- Improves contextual awareness of threats. | - Computationally expensive due to transformer-based architecture.<br>- Privacy concerns when monitoring user behaviors.<br>- Requires large-scale labeled data for training. |
| [3] | Hybrid ML + Deep Learning | - Captures both statistical and deep-learning-based threat signals.<br>- Highly adaptable to evolving attack patterns.<br>- Ensures robust insider attack mitigation. | - Struggles with dataset imbalance affecting model fairness.<br>- Potential for false positives leading to unnecessary alerts.<br>- Privacy concerns in real-world applications. |
| [4] | Structured Threat-Control Mapping | - Automated SIEM threat mitigation enhances security.<br>- Adaptive response to insider threats. -<br>- Detects anomalous access patterns. | - High computational resource demands for real-time processing.<br>- Privacy and ethical challenges in workplace monitoring.<br>- Difficult to implement across multiple security platforms. |
| [5] | CPJOS (Cascaded Autoencoder Purification and Joint Optimization Scheme) | - High precision and recall with anomaly identification.<br>- Reduces false positives with error correction.<br>- Ensures fine-tuned risk assessment | - Challenges in data purification impact accuracy.<br>- Difficulties in modeling spatial data.<br>- Scalability concerns for enterprise applications. |
| [6] | Multi-Tiered Activity Monitoring | - Provides real-time and multi-layered security.<br>- Detects sophisticated insider attacks.<br>- Enhances organizational cybersecurity resilience. | - Struggles with deepfake-based fraud risks.<br>- Emerging AI-powered threats challenge detection accuracy.<br>- Requires extensive cybersecurity infrastructure. |
| [7] | Enhanced Bidirectional GANs (EBiGANs) | - Improves diversity of training datasets.<br>- Reduces class imbalance issues significantly.<br>- Enhances robustness against adversarial attacks. | - Prone to mode collapse issues in GAN training.<br>- Challenges in ensuring model stability.<br>- Computationally expensive for large-scale datasets. |
| [8] | Self-Supervised and Few-Shot Learning | - Improves detection robustness in real-world applications.<br>- Reduces reliance on extensive labeled datasets.<br>- Enhances explain ability in AI-driven security models.<br>- Enhances Anomaly Detection and Behavioral Analysis.<br>- Reduces False Positives and Improves Accuracy. | - Limited availability of high-quality labeled data.<br>- Challenges in making AI models interpretable.<br>- Struggles with handling zero-day attacks.<br>- Difficulty in Capturing Contextual Insider Threats.<br>- Potential Privacy and Ethical Concerns. |

TABLE II
COMPARISON TABLE

| Reference | Description | Strengths | Limitations |
|---|---|---|---|
| [9] | CPS Insider Threat Detection | - Enhances security for Cyber-Physical Systems (CPS).<br>- Detects sophisticated insider threat strategies.<br>- Applicable across multiple industries | - Scalability issues in real-world deployment.<br>- Risk of adversarial ML-based evasion attacks.<br>- Requires real-world datasets for improved accuracy. |
| [10] | Multi-Model Inference Enterprise Modeling (MIEM) | - High accuracy in behavioral risk detection.<br>- Applicable to cross-sector enterprise security.<br>- Adapts well to evolving threats. | - Data privacy challenges with enterprise-wide deployment.<br>- Vulnerable to adversarial evasion tactics.<br>- Computational overhead in real-time scenarios. |

where medical devices and patient data face unauthorized access; transportation, particularly air traffic control and public transport security; nuclear facilities, which face sabotage and espionage risks; oil and gas, where remote system exploitation poses security threats; energy and smart grids, which are vulnerable to power grid hacking; water systems, where critical infrastructure faces cyber- physical attacks; smart cities, with risks to public infrastructure; and industrial automation, where IoT- based cyber threats endanger manufacturing processes. To enhance CPS security research, various datasets and simulation tools are used, including the CERT dataset for insider threat behavior, the TWOS dataset for SCADA system attacks, Network Simulator 2 (NS2) for attack scenario modeling, and Digital Twin Technology for real-time infrastructure modeling. However, several challenges remain, including the lack of real- world datasets, scalability issues in cryptographic and AI models, adversarial machine learning risks, and the absence of a standardized framework for insider threat detection. Future research should focus on developing real-time, adaptive security models, creating benchmark datasets, and enhancing AI resilience against adversarial attacks. In conclusion, insider threats in CPS remain a significant cybersecurity challenge, and while various methodologies have been explored, real-world applicability, scalability, and AI security vulnerabilities continue to be critical issues that require urgent attention to fortify CPS against emerging insider threats.

The paper [10], insider threats pose a significant security challenge across industries, involving fraud, data theft, sabotage, workplace violence, data exfiltration and shadow IT with the 2016 Ponemon Institute study estimating an annual loss of 4.3 million per company. To address this, Multi-Model Inference Enterprise Modelling (MIEM) integrates multiple in- dependent models to improve insider threat detection. The Inference Enterprise (IE) framework underpins this approach by monitoring and collecting various organizational activity data, processing it to generate behavioral indicators, and using these indicators to enhance detection algorithms. The research incorporates Bayesian Networks, Machine Learning Algorithms, Stochastic Optimization, Markov Models, and Monte Carlo Simulations, each independently assessing risks before their results are fused for improved accuracy. The SCITE competition tested various detection models, with Innovative Decisions, Inc. (IDI) outperforming competitors by leveraging MIEM, excelling in key performance metrics such as Mean Squared Error (MSE), Certainty Interval Calibration (CIC), and Interval Scoring Rule (ISR). The MIEM approach effectively detects insider threats by analyzing behavioral deviations, physical and digital activity correlations, and unusual workplace behaviors. Its applications extend across cybersecurity, enterprise security, immigration screening, and public safety, yet challenges remain, including data privacy concerns, scalability issues, and adversarial evasion risks. Future research should focus on developing AI-driven adaptive security models, refining behavioral risk indicators, and establishing cross-sector standardization. Ultimately, MIEM proves superior to single-model methods, offering enhanced accuracy and reliability in detecting high-risk individuals, with broader applications in border security, public safety, and enterprise risk management.

## III. CONCLUSION

Insider threats remain one of the most persistent and complex challenges in cybersecurity. Unlike ex- ternal attacks, which can often be mitigated through perimeter security measures, insider threats exploit legitimate access privileges, making them difficult to detect and prevent. Deep learning techniques, particularly LSTMs, RNNs and GANs, have significantly improved insider threat detection by capturing complex behavioral patterns and identifying deviations in real-time. Cryptographic methods, such as blockchain authentication and secure encryption, strengthen access control mechanisms and prevent data breaches. Hybrid models that integrate AI-driven anomaly detection with structured security control frameworks offer a multi-layered approach, enhancing detection accuracy and reducing false positives. However, several challenges persist in insider threat detection. Data imbalance remains a key issue, as insider attacks are relatively rare compared to normal user activities, making it difficult to train accurate models. Real- time computational constraints pose another limitation, particularly for large-scale enterprise networks and cyber-physical systems. Additionally, privacy concerns related to employee monitoring create ethical and regulatory challenges, limiting the extent to which behavioral analysis can be implemented. Future research should focus on developing self-supervised learning techniques to minimize reliance on labeled datasets, improving explainable AI to enhance trust and interpretability, and optimizing real-time processing for large-scale threat detection. Furthermore, organizations should adopt a holistic security strategy that combines AI, cryptographic security, behavioral monitoring, and structured mitigation policies. Regulatory frameworks should also be established to standardize insider threat detection methodologies while ensuring compliance with data protection laws. By implementing a multi-faceted defense strategy that leverages AI, crypto-graphic security, and structured risk mitigation, organizations can build a more resilient and adaptive security posture. This approach will not only enhance insider threat detection capabilities but also reduce security risks, improve response times, and strengthen overall organizational cybersecurity resilience.

## REFERENCES

[1] Rida Nasir, Mehreen Afzal, Rabia Latif, and Waseem Iqbal. Behavioral based insider threat detection using deep learning. *IEEE Access*, 9:143266–143274, 2021.

[2] Zhi Qiang Wang and Abdulmotaleb El Saddik. Dtitd: An intelligent insider threat detection framework based on digital twin and self-attention based deep learning models. *IEEE Access*, 2023.

[3] Rakan A Alsowail and Taher Al-Shehari. Empirical detection techniques of insider threat incidents. *IEEE Access*, 8:78385– 78402, 2020.

[4] Puloma Roy, Anirban Sengupta, and Chandan Mazumdar. A structured control selection methodology for insider threat mitigation. *Procedia Computer Science*, 181:1187–1195, 2021.

[5] Yichen Wei, Kam-Pui Chow, and Siu-Ming Yiu. Insider threat prediction based on unsupervised anomaly detection scheme for proactive forensic investigation. *Forensic Science International: Digital Investigation*, 38:301126, 2021.

[6] Usman Inayat, Mashaim Farzan, Sajid Mahmood, Muhammad Fahad Zia, Shahid Hussain, and Fabiano Pallonetto. Insider threat mitigation: Systematic literature review. *Ain Shams Engineering Journal*, page 103068, 2024.

[7] P Lavanya, H Anila Glory, and VS Shankar Sriram. Mitigating insider threat: A neural network approach for enhanced security. *IEEE Access*, 2024.

[8] Shuhan Yuan and Xintao Wu. Deep learning for insider threat detection: Review, challenges and opportunities. *Computers & Security*, 104:102221, 2021.

[9] Mohammed Nasser Al-Mhiqani, Tariq Alsboui, Taher Al-Shehari, Karrar hameed Abdulkareem, Rabiah Ahmad, and Mazin Abed Mohammed. Insider threat detection in cyber- physical systems: a systematic literature review. *Computers and Electrical Engineering*, 119:109489, 2024.

[10] David P Brown, Dennis Buede, and Sean D Vermillion. Improving insider threat detection through multi-modelling/data fusion. *Procedia Computer Science*, 153:100–107, 2019.