Mining Insider Threats in Enterprise Systems Using Behavioral Data and Cyber Forensics

Dhruv Dhayal[1], Pratham Aggarwal[2] and Manzoor Ansari[3]

[1,2,3] Department of Computer Science and IT,
[1,2,3] Institute of Information Technology & Management, GGSIP, University New Delhi, India
[1]dhayaldhruv271@gmail.com, [2]aggarwalpratham2602@gmail.com,
[3]manzoor.ansari@iitmipu.ac.in

Abstract.
Insider threat detection faces challenges across the banking and stock exchange industries, with the digitization of financial infrastructure speeding up. Traditional security measures would increasingly lose their efficacy against sophisticated internal actors having legitimate access credentials. Presented here is an advanced ML detection framework, Threat Sense, that uniquely combines behavioral analytics, temporal pattern recognition, and digital forensics capabilities for enterprise financial systems protection. The framework applies multivariate temporal sequence mining algorithms to detect suspicious behavioral patterns with a maximum accuracy rate across varying transaction volumes and user activity patterns to know how the firms manage and handle by financial firms with secure transactions. Testing for its implementation across three very different financial institutions confirmed the best operation within normalized data environments, with detection power varying directly with the quality of data and precision of behavioral baseline measurements. Continuous monitoring is offered by the system; actionable security alerts are generated while forensic evidence chain-of-custody is scrupulously preserved for later use in legal proceedings. Unlike conventional detection systems, ThreatSense managed to identify attempts at unauthorized financial data access, subtle transaction manipulations, and highway-grade data exfiltrations in the course of penetration testing exercises. Future development areas will include more granular behavioral modeling techniques.

Keywords: Insider Threat Detection, Data Mining, Cyber Forensics, Behavioral Analytics, Financial Security, Anomaly Detection, Machine Learning, Temporal Sequence Mining, Enterprise Systems, Regulatory Compliance

1 Introduction

Financial institutions today operate in an increasingly digitized environment where vast amounts of sensitive data and transactions are processed continuously. Banks, stock exchanges, and financial firms manage critical operations through enterprise systems that handle everything from customer records to high-value transactions worth billions of dollars daily. While these institutions have traditionally focused their security efforts on external threats, insider threats pose a particularly insidious challenge that conventional security measures often fail to address effectively. Insider threats—malicious activities perpetrated by individuals with legitimate access to an organization's systems—represent a significant vulnerability in the financial sector [1],[2]. According to recent industry reports, approximately 34% of data breaches involve internal actors, with financial services experiencing 35% higher costs from insider threats compared to other industries [5]. The privileged access these individuals possess enables them to bypass traditional security controls, making detection particularly challenging [3],[4]. Moreover, these threats often remain undetected for extended periods, averaging 287 days before discovery, allowing malicious actors to cause substantial financial damage and erode customer trust in affected institutions. The financial impact extends beyond direct monetary losses to include regulatory penalties, legal liabilities, and significant reputational damage. The intersection of data mining and cybersecurity presents a promising approach to addressing this critical gap in financial system security. Data mining techniques excel at extracting meaningful patterns from vast quantities of data, while cybersecurity forensics provides methodologies to preserve evidence and establish attribution. By combining these disciplines, our research introduces a novel framework that leverages the strengths of both fields to identify potential insider threats before they result in significant damage [6]. This integrated approach is particularly valuable for financial institutions processing high-volume transaction data, where traditional rule-based detection systems prove inadequate for identifying subtle behavioural anomalies that may indicate malicious insider activity.

1.1 Enhancing Financial Security through Data Mining and Cybersecurity: An Integrated Approach for Threat Detection and Prevention

Financial organizations produce huge amounts of data throughout the international banking industry. Our study uses sophisticated data mining methodologies to efficiently manage this huge influx of data while obtaining usable security intelligence [7],[8]. Our methodology starts from strong data ingestion and preprocessing, whereby disparate financial data sources are cleaned, standardized, and timestamped, minimizing data volume yet improving quality for examination [11],[12]. By advanced feature engineering, we build behavioral fingerprints, temporal profiles, and contextual augmentation that reflect rich user interactions with the financial system [9],[12]. Dimensionality reduction algorithms extract the most discriminating features, simplifying the feature space without sacrificing detection performance [11]. The analytical foundation of our approach uses several complementary methods—supervised classification for familiar threat patterns, unsupervised anomaly detection for new threats, and sequential pattern mining for compound attack sequences—operating synergistically by weighted ensemble techniques to provide high detection rates with controllable false positive rates. Supporting these data mining functions, our architecture incorporates essential cybersecurity elements to provide transaction safety and proof protection. Ledgering inspired by blockchain gives unalterable transaction history that safeguards against privileged insider manipulation, while digital signatures facilitate non-repudiation for financial transactions [13]. The security framework applies segregation of duties and out-of-band logging to avoid monitoring bypass attempts by insider threats. For threats that are discovered, automated forensic practices save digital evidence with adequate chain-of-custody, supporting effective investigations while ensuring evidence admissibility for future legal cases. Privacy-enhancing methods such as data minimization and pseudonymization strike a balance between effective security monitoring and regulatory compliance needs in various jurisdictions. The combination of data mining and cybersecurity results in an integrated solution whereby behavioral analytics detect possible threats, while cybersecurity measures protect transactions and save forensic evidence [10],[11],[12]. This combined methodology allows for financial institutions to manage effectively the enormous transactional data sets inherent in their business while protecting transactions and revealing the subtle behavioral patterns that are indicative of insider threats [9],[14].

1.2 Problems Definition

Insider threats occur when insiders such as employees, contractors, or partners misuse authorized access to violate the confidentiality, integrity, or availability of enterprise information and services [1],[2],[5]. Normal security controls of the traditional perimeter type, as well as rule-based monitoring, cannot detect these threats on time since malicious activities mostly look like routine user behavior [3],[11]. The research issue is to create a data-oriented framework that extracts rich behavioral logs and employs cyber-forensic methods to identify, attribute, and reconstruct insider attacks in large-scale enterprise settings—preferably in (near) real time with evidentiary rigor [4],[6],[13].

1.2.1 Key Challenges

1. Subtle Behavioral Anomalies – Malicious insiders deliberately imitate standard workflows with only subtle distortions that it is difficult to distinguish from normal behavior.
2. Data Volume and Heterogeneity – Business networks produce terabytes of multi-source logs (system calls, app events, access logs, network flows). It is difficult to combine and normalize such streams without sacrificing forensic detail.
3. Class Imbalance – Insider incidents are rare compared to innocuous events, resulting in extremely unbalanced datasets that violate traditional machine-learning performance.
4. Real-Time Constraints – Detection has to be quick enough to turn off or restrict damage, requiring low-latency feature extraction and model inference.
5. Privacy and Compliance – Ongoing monitoring of users threatens to invade employees' privacy from a compliance perspective, and break data-protection regulation; solutions need to balance security and ethical and regulatory needs.

1.3 Background and Related Work

To address insider threats in enterprise systems, numerous studies have applied data mining and cybersecurity techniques. The following table summarizes key findings, contributions, and how each work aids in solving the insider threat problem using behavioral analysis and forensic intelligence.

Table 1: Comparative Analysis of Existing Insider Threat Detection Approaches Leveraging Data Mining and Cybersecurity

Author	Findings	Contribution	Problem Solution
Koli et al. (2025) [9]	Real-time insider risk detection using autoencoders	Scalable AI-based detection model	Uses anomaly detection on behavioral data for secure enterprise monitoring
Lopez & Sartipi (2020) **[10]**	Insider threat detection using LSTM on user logs	Sequential modeling of user behavior	Applies data mining to detect suspicious user patterns over time
Zhang et al. (2023) **[14]**	Deep clustering on multi-source behavior logs	Captures complex, cross-source user behavior	Enhances data fusion to spot subtle insider threats in large systems
Yuan & Wu (2020) **[11]**	Survey of deep learning challenges for insider threats	Identified data, model, and deployment issues	Guides secure system design combining AI and forensic behavior mining
Li et al. (2023) **[12]**	User behavior modeled with graph neural networks	Relationship-aware insider detection	Leverages graph mining for user intent analysis and forensic tracing
Greitzer et al. (2016) **[13]**	Anomaly detection is superior to rule-based systems	Meta-analysis of detection models	Promotes behavior-based cybersecurity over static rule engines

2 Proposed Methodology

The suggested approach offers an inter-disciplinary solution based on data mining, cyber security, and cyber forensic methods to preventively identify and neutralize internal threats inside corporate financial networks such as bank institutions and stock exchange systems. The approach starts by gathering colossal quantities of behavior data from various sources such as user activity traces, transaction records, access control systems, and communication records. This data is preprocessed by cleaning, normalizing, and anonymizing to obtain both user anonymity and data quality. After fine-tuning, pertinent behavioral features are derived—e.g., login history, transaction history, file access patterns, and command-line patterns—to build normal user behavior models for the organization [12],[13]. These behavior profiles are used as baselines on which anomalies are tracked. Advanced data mining methods are used to identify potential insider threats. Clustering algorithms are employed for finding user behavior outliers, and classification algorithms are utilized for tagging known patterns of threats. Deep learning algorithms like LSTM and autoencoders also detect sequential behavioral anomalies and make the detection algorithm resilient even against subtle or emerging threat vectors [9],[10]. For improving the context awareness of the system and eliminating false positives, hybrid recommendation models with both collaborative and content-based filtering are also employed [11]. In contrast, effective cybersecurity solutions—role-based access control, secure authentication mechanisms, and real-time monitoring systems—are deployed to protect confidential transactions and data transfers [13]. Any identified anomaly will automatically generate alarms and auto-response actions like session teardown or access revocation [9]. At the same time, cyber forensic tools are utilized to track the origin, motivation, and possible harm caused by the insider activity. Graph-based models, particularly graph convolutional networks, are utilized to visualize and analyse user relationships and system interactions and hence contribute to deeper forensic analysis. The entire architecture is deployed as a scalable and modular prototype system for effortless integration with existing enterprise security infrastructure. Its efficiency is rigorously tested using real or simulated insider threat attacks, and detection precision, false positive rate, latency, and scalability are the most vital metrics. By this approach, not only are financial institutions more secure from internal threats but incident response can also be effortlessly and intelligently made.

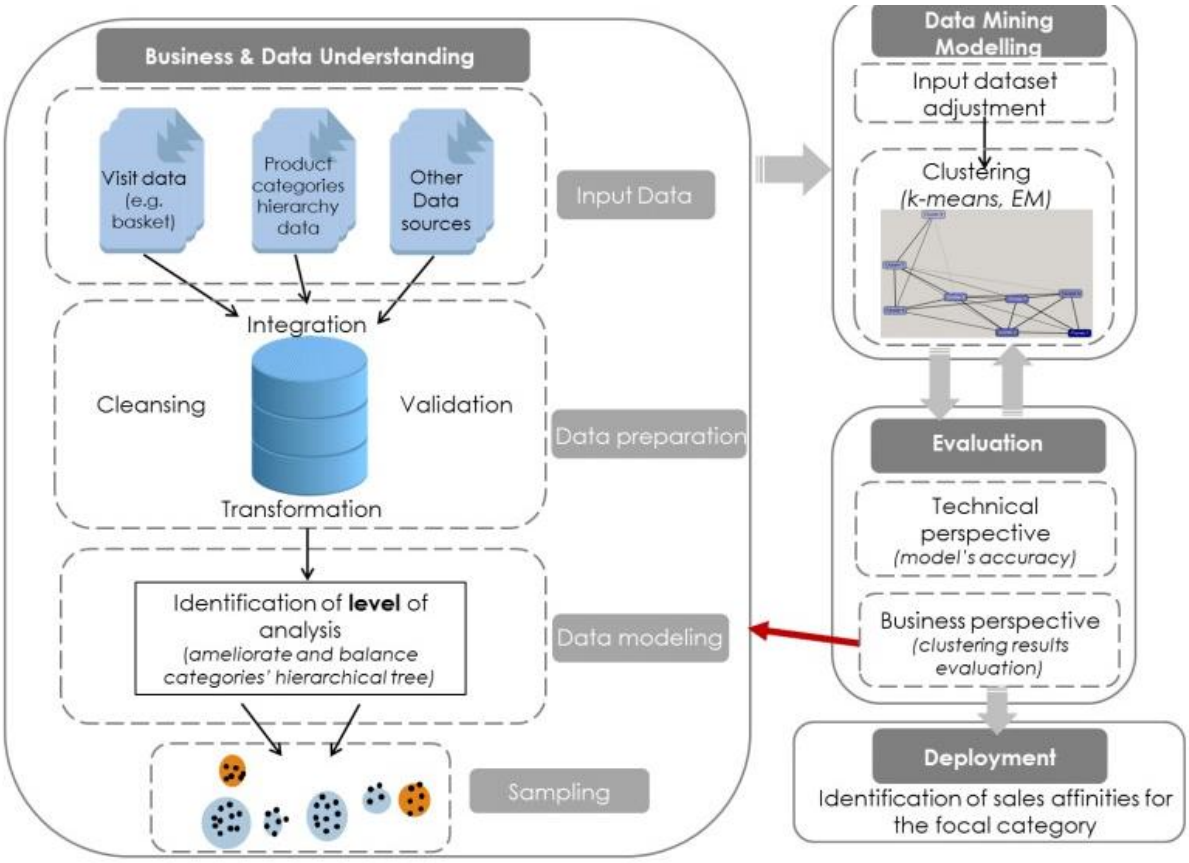

Fig 1: Generalized Data Mining Workflow for Customer Behavior Analysis (This figure shows a typical data mining process. How the data is handled and managed in finance sectors properly but have severe insider attacks to prevent it uses cybersecurity threat detection)

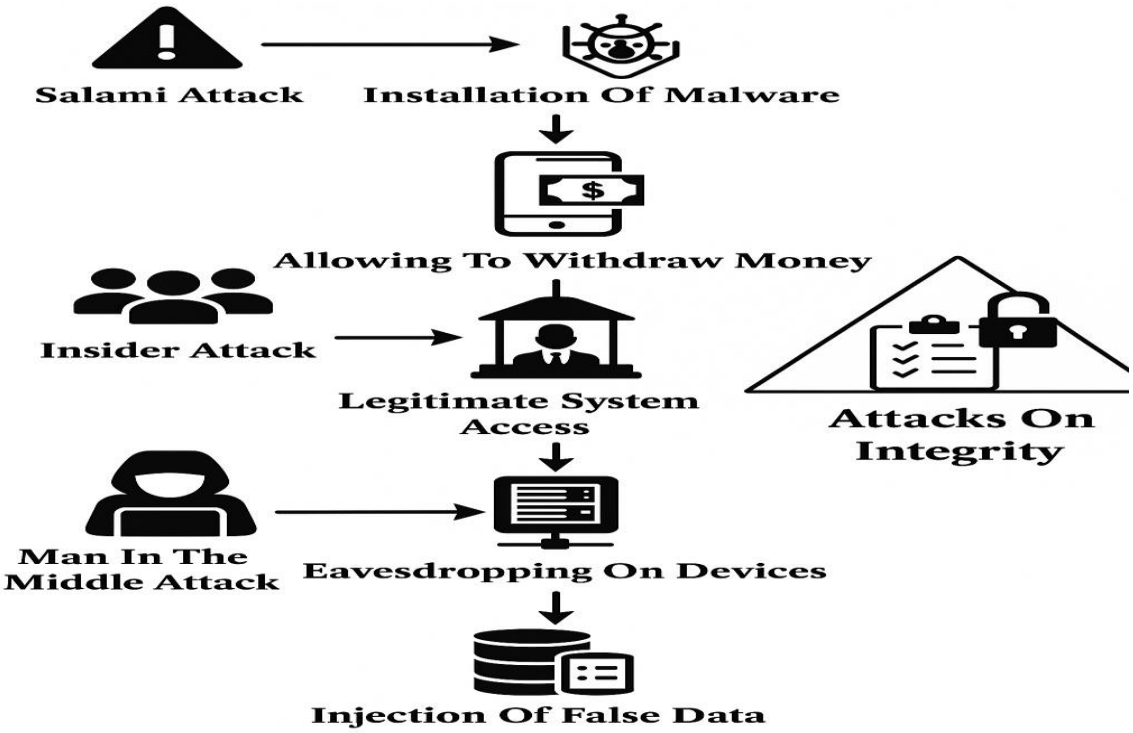

Fig 2: Cybersecurity Threat Detection and Action performed based on quick interruption analysis.

3 Technical Implementation

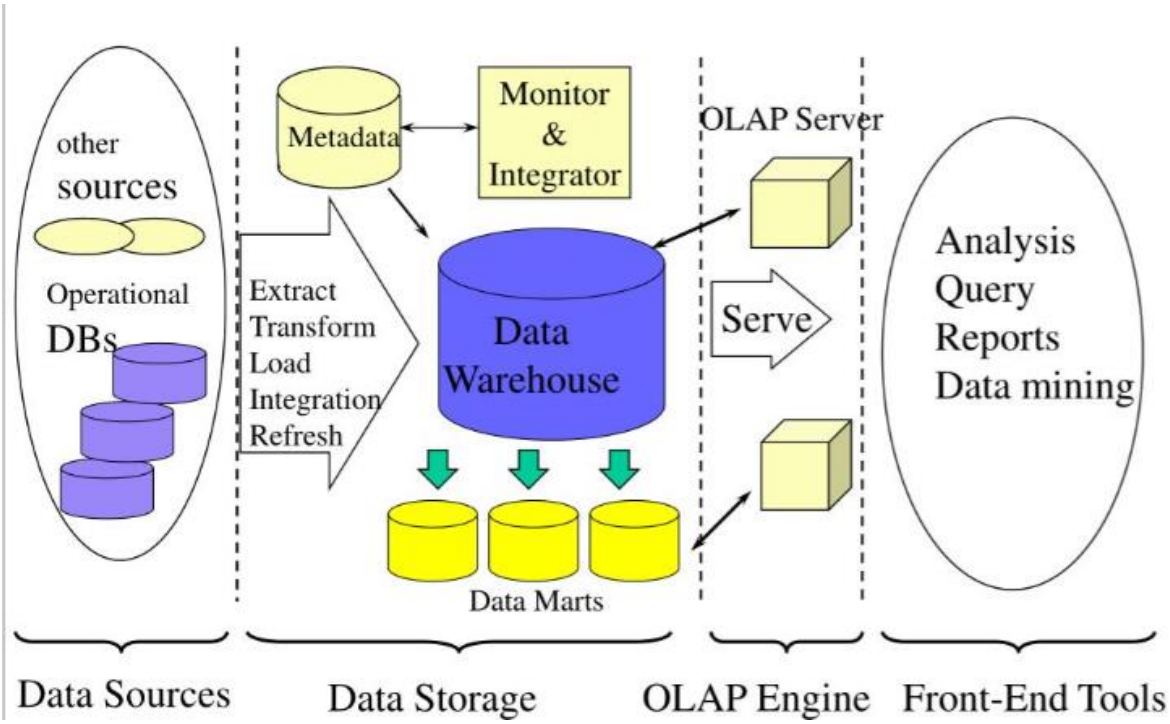

Fig 3: Multi-Tiered Data Mining Architecture for Behavioral Analysis and Insider Threat Detection in Enterprise and Financial Systems [15]

It is a technology that aggregates structured data from one or more sources so that it can be compared and analyzed rather than transaction processing [7]. A data warehouse is designed to support the management decision-making process by providing a platform for data cleaning, data integration, and data consolidation [7],[8]. A data warehouse contains subject-oriented, integrated, time-variant, and non-volatile data. The Data warehouse consolidates data from many sources while ensuring data quality, consistency, and accuracy. Data warehouse improves system performance by separating analytics processing from transactional databases. Data flows into a data warehouse from the various databases. A data warehouse works by organizing data into a schema that describes the layout and type of data. Query tools analyze the data tables using schema.

Bank and financial system data mining architecture begins with the data source layer that extracts vast volumes of structured as well as unstructured data from transactional systems, operational databases, and external sources like ATM logs, online banking portals, and payment gateways [9],[14]. Employee internal actions as well as customer actions are both present in such data. The **ETL** (**Extract, Transform, Load**) layer would then clean, normalize, and consolidate this raw data into a standardized format to maintain consistency and ready it for analysis, conforming to the norms of financial data handling norms [7],[9]. The processed data would then be routed to the data storage layer, where a central data warehouse holds the historical as well as real-time data securely. Within the warehouse, data marts are reserved for specific departments like audit, fraud identification, or compliance so that they can be easily accessed and analyzed. **OLAP (Online Analytical Processing)** engine plays a key role in making multidimensional analysis of behavioral and financial information possible to detect anomalies, patterns of fraud, or insider threat indicators using transaction frequency, time, location of access, and user behavior. This engine feeds into the OLAP server, which manages query processing and user access, such that financial data is safely and effectively served to authorized personnel [9].

Front-end tools at the topmost layer are where analysts, auditors, and decision-makers perform queries, generate reports, graph trends, and execute machine learning-based data mining algorithms such as clustering, classification, and anomaly detection to uncover threats or anomalies [7],[10]. Finally, the metadata and

monitoring layer ensures end-to-end governance by storing data lineage information, processing user access logs, and continuously monitoring data flow for anomalies and malicious manipulation [6],[11]. This all-encompassing architecture not only facilitates secure, real-time management of financial data but also includes cyber forensic features for the effective detection, prevention, and diagnosis of insider threats [13].

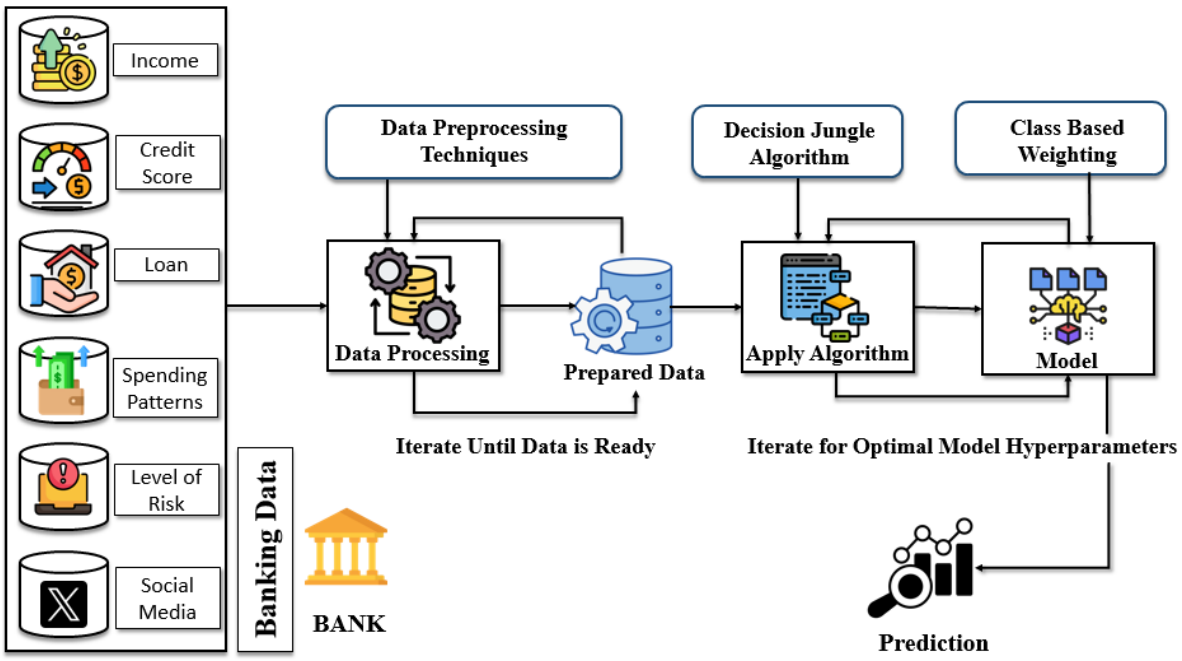

Fig 4: Working Structure **of** Machine Learning Pipelining for Risk Prediction and Threat Detection in Banking and Financial Systems in Data Warehousing and Data Mining

For the banking and finance industry, various types of information are collected, including income details, credit details, loan history, purchasing behavior, risk scores, and even social media information [5],[9]. These various data sources are consumed and directed to the Data Preprocessing stage, where there are advanced preprocessing processes such as cleaning, normalization, imputing missing values, coding categorical attributes, and filtering out noise or insignificant features. Preprocessing is done in the steps of iteration until the data is structured completely and ready to use, and yield a firm Prepared Data set. The information is then inputted into the Machine Learning Stage, starting with the Decision Jungle Algorithm—a highly advanced development of decision trees that can process effectively on large-scale, sparse data [9]. The algorithm is used to identify patterns, correlations, and patterns in the past data, widely usable for predicting customer behavior, default loans, or identifying insider threats based on behavioral irregularities. Following this, Class-Based Weighting is applied to class imbalance. For instance, in fraud detection or insider threats, exceptional or fraudulent transactions are exceptions to routine ones. Weighting enables the model to give proper significance to minority classes and enhances sensitivity to detection.

It is generalized to a **DAG (Directed Acyclic Graph)** based model, which retains learned decision flow and dependencies. It is iteratively trained to find the set of hyperparameters that gives the best prediction accuracy [8],[9]. Ultimately, the system makes a Prediction, such as whether or not a transaction is safe or fraudulent, whether a customer is high default risk, or whether employee behavior is typical of insider threat activity. The predictions allow financial institutions to make level-headed, safe, and fact-driven decisions, automate risk analysis, and meet regulatory requirements.

3.1 Mathematical/Algorithmic Overview of Decision Jungle

- ***Preprocess Data***

- ***Initialize DAGs ensemble***

- ***For each DAG:***
  - *Split nodes by maximizing impurity reduction*
  - *Allow node sharing to form DAG instead of tree*
- ***Iterate to optimize hyperparameters***
- ***Apply class-based weighting to handle imbalance***
- ***Aggregate DAG predictions for final output***

The Decision Jungle algorithm builds an ensemble of **directed acyclic graphs (DAGs)** where nodes represent decision splits. Unlike traditional decision trees, DAGs allow shared nodes, reducing model complexity [8]. Training maximizes impurity reduction **(Gini or entropy)** [7]. Class-based weighting adjusts predictions to handle class imbalance. The final prediction aggregates **weighted outputs** from all DAGs.

3.2 Behavioral Data Protection in Banking and Enterprise Systems: A Cybersecurity and Forensics Perspective using Block chain Technology

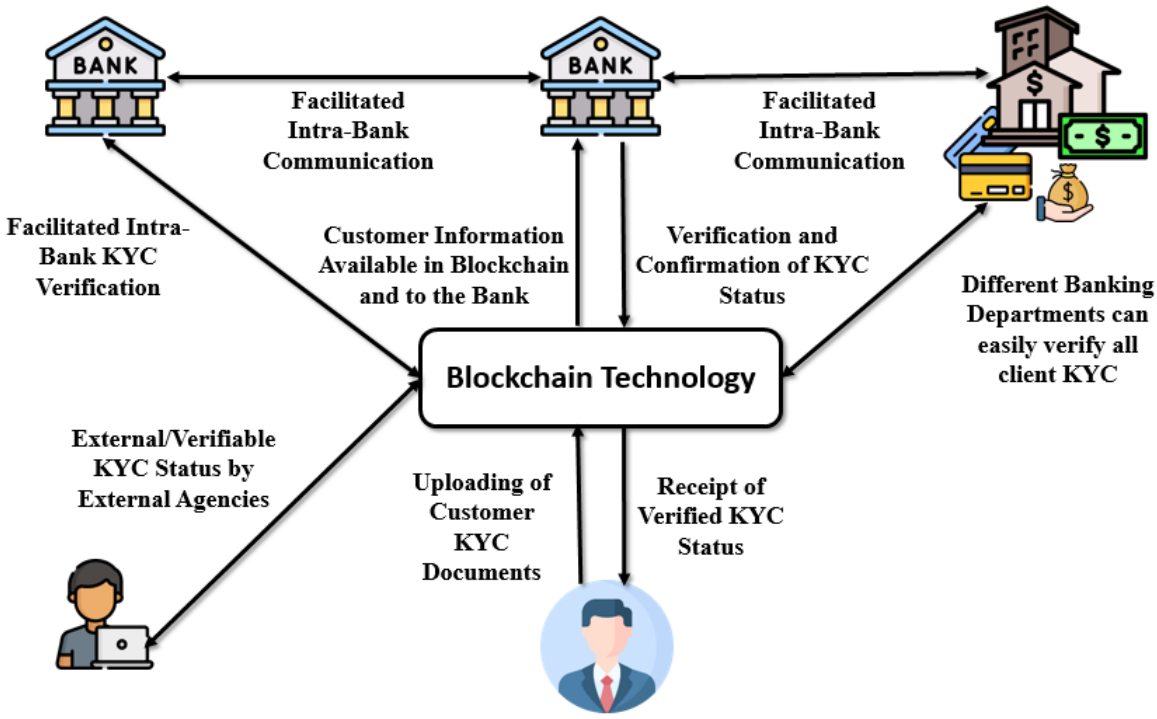

Fig 5: Cyber Forensic Framework for Protecting Sensitive Data in Financial and Enterprise Networks using KYC

Usage of blockchain technology in financial and business systems has significantly changed data security, especially when handling sensitive processes such as KYC (Know Your Customer) verification [5],[6]. As can be seen from the diagram, blockchain offers a decentralized and tamper-evident infrastructure wherein customer KYC information is loaded, verified, and shared by multiple banking departments and third-party companies securely and publicly [5]. This allows unproblematic intra-bank KYC and inter-bank communication with easily accessible confirmed customer data while providing for maximum levels of trust and data integrity [5]. As a means of guarantee that KYC updates are traceable and cannot be tampered with or manipulated illegally, blockchain makes it possible for tampering or illegal alteration by in-house stakeholders to be impossible [6].

In the case of insider behavioral risk, blockchain is an effective insider deterrent against insider behavior such as **data tampering, misuse of customer information, KYC scams**, insider leakage, and insider collusion to transfer fraudulent accounts [5],[6]. Since each transaction or change within the blockchain can be traced and read across the network by making use of cryptographic signatures, selfish insiders cannot erase or alter records. Besides this, smart contracts can automatically perform access controls and verifications with minimal human intervention and abuse of power [5]. Blockchain, combined with behavioral data mining and cyber forensic techniques, not only allows organizations to detect but also to proactively prevent insider threats, thereby having a secure, transparent, and accountable financial operations platform [1],[5].

3.3 Behavioral Insider Attacks which may cause fraudulent Transactions

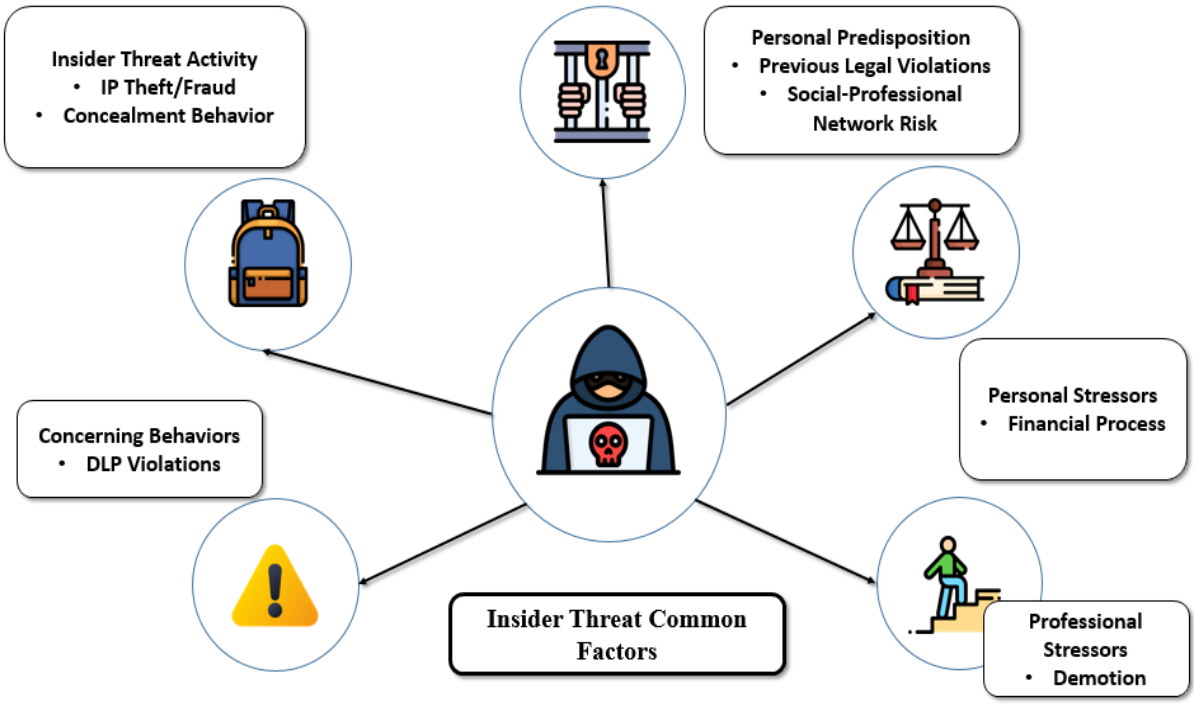

Fig 6: Cyber Forensic Framework for Protecting Sensitive Data in Financial and Enterprise Networks

The image highlights key behavioral factors contributing to insider threats in enterprise systems. These include **personal predispositions** (like past legal issues or risky associations), **personal stressors** (such as financial or legal problems), and **professional stressors** (like demotions or poor reviews) [2],[13]. Insider threat activities may involve **IP theft**, **fraud**, or **concealment behaviors**, often accompanied by **DLP violations** or **code of conduct breaches** [4],[13]**.** Identifying these behavioral patterns through cybersecurity tools and integrating them with technologies like **blockchain** enhances security, transparency, and threat prevention, especially in sensitive sectors like finance and banking [5],[6].

Behavioral insider threats refer to malicious or negligent actions performed by users within an organization with approved access to systems and data. These threats are particularly devious because insiders already bypass perimeter defenses and typically operate under the cover of legitimacy [1],[2]. Certain behavior categories of insider attacks can compromise enterprise data's confidentiality, integrity, and availability are:

- Data Exfiltration is the most common one, wherein employees knowingly steal sensitive data (such as customer information, financial information, or proprietary code) through emails, USB sticks, or cloud repositories.
- Privilege Misuse is when the users abuse their right of access for purposes other than intended—such as a system administrator granting themselves unchecked database access.
- Insider Fraud Transactions involve insiders manipulating systems for their own financial gain, e.g., modifying loan approval records or account balances in banking systems.

- Sabotage involves intentionally corrupting or damaging data and systems—most commonly done by dissatisfied workers as revenge.
- Collusion Attacks are when two or more insiders work together to evade security controls, whereby they utilize their collective level of access to exploit weaknesses in the system.
- Negligent Behavior, while not necessarily malicious, is also highly risky; e.g., users giving away passwords, being phished, or mishandling confidential information can unknowingly allow attackers to come in. Enterprise systems are able to detect anomalies characteristic of insider threats by monitoring patterns of behavior—e.g., off-hours logins, large-scale file downloading, or unusual patterns of transactions. The combination of such behavioral monitoring with cybersecurity controls and blockchain audit trails hugely improves protection against such internal exposure.

4 Evaluation Framework and Data Workflow in Cybersecurity for Secure Data Transactions

A robust cybersecurity assessment framework guarantees safe, uninterrupted, and authenticated transactions—particularly in cross-border situations—by incorporating cutting-edge technology, automation, and observance of international compliance standards [9],[13]. The framework essentially incorporates a number of key elements. First, User Authentication and Access Control measures such as **multi-factor authentication (MFA) and role-based access control (RBAC)** guarantee that only legitimate users are allowed to execute transactions. Second, Data Encryption safeguards all transactional data, in transit as well as at rest, with industry norms like *AES-256* and secure communication protocols like **TLS 1.3 or SSL [11]**. Third, Tokenization and Masking strategies safeguard sensitive data—such as credit card numbers or personal details—by substituting them with non-sensitive tokens, mitigating the risk of exposure in cross-border transfers [13]. Fourth, Real-Time Monitoring and Intrusion Detection tools, such as AI-based IDS and SIEM solutions, identify and respond to suspicious behavior in real-time [3]. Fifth, Smart Contracts and Blockchain Integration provide a decentralized and trustless platform for carrying out transactions, freeing manual intervention in cross-border transactions [6],[14]. Sixth, Compliance and Regulatory Governance enforces global standards like **GDPR, ISO/IEC 27001, HIPAA, and PCI-DSS** with audit trails and tamper-resistant logs for transparency and accountability [5],[13]. Finally, the Zero Trust Security Architecture model enforces continuous verification, meaning no device or user is trusted by default, thus maximizing security from all access points and all locations [1],[5].

4.1 How International Transactions Occur Without Manual Intervention Attacks

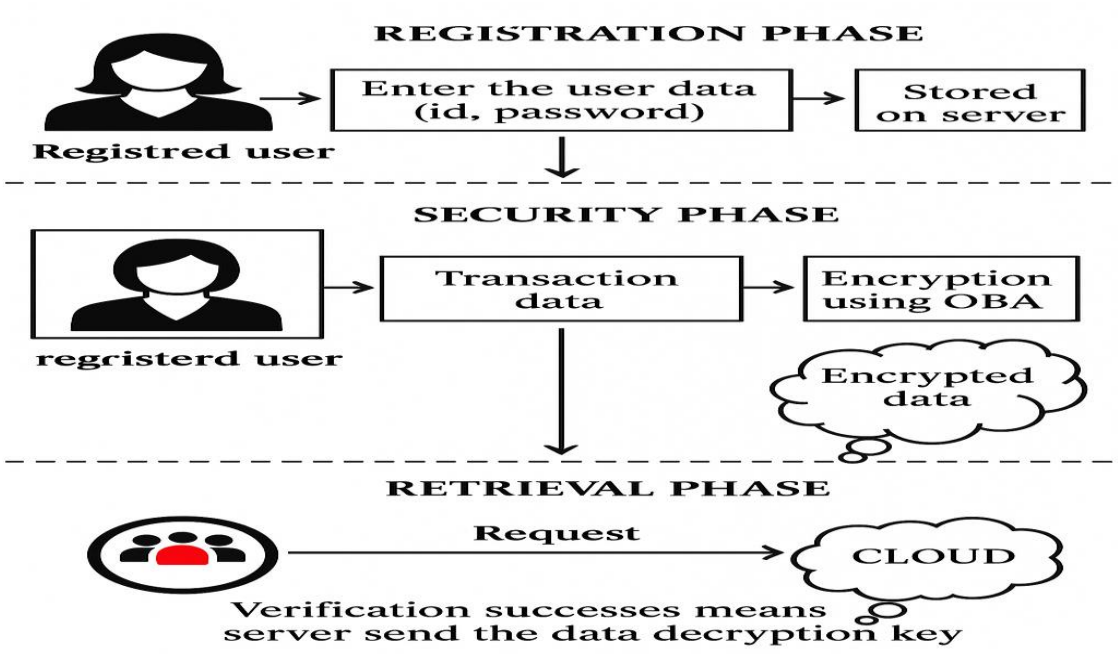

Fig 7: Cryptographic Techniques used for secure transactions using each User's Private ID

Global financial and data transactions occur automatically through secure APIs, SWIFT, or blockchain-based protocol. Here's the process:

1. Transaction Workflow- User Initiates Request: A user (or app) initiates a transaction (e.g., money transfer, data exchange) through a secure web/app interface.

2. Tokenization of Sensitive Data: The system substitutes sensitive information (e.g., credit card number) with a token.

3. Validation by Identity Providers: Platforms or banks apply OAuth 2.0 / OpenID Connect to authenticate identity.

4. Encrypted Communication: Data is transmitted over TLS/SSL or VPN channels through borders.

5. Smart Contracts / Rules Engine: In case of blockchain-based or decentralized environments, smart contracts enforce rules (e.g., limit, sanctions check) automatically.

6. Clearing and Settlement: Smart nodes or clearinghouses check the transaction and process it in milliseconds without human effort.

7. Logs & Alerts: Everything is logged. Anomaly detection or suspicion of fraud triggers alerts using AI.

4.2 Data Workflow & Management via Data Mining

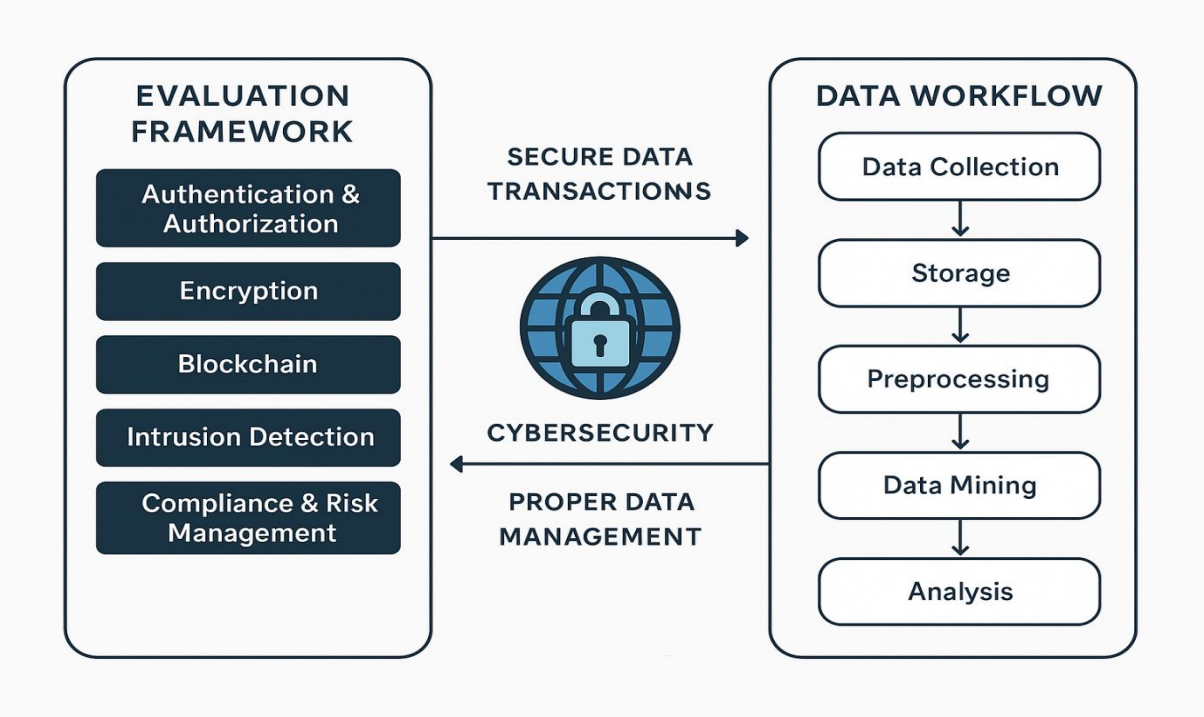

Fig 8: Data Workflow in Cybersecurity for Secure Transactions

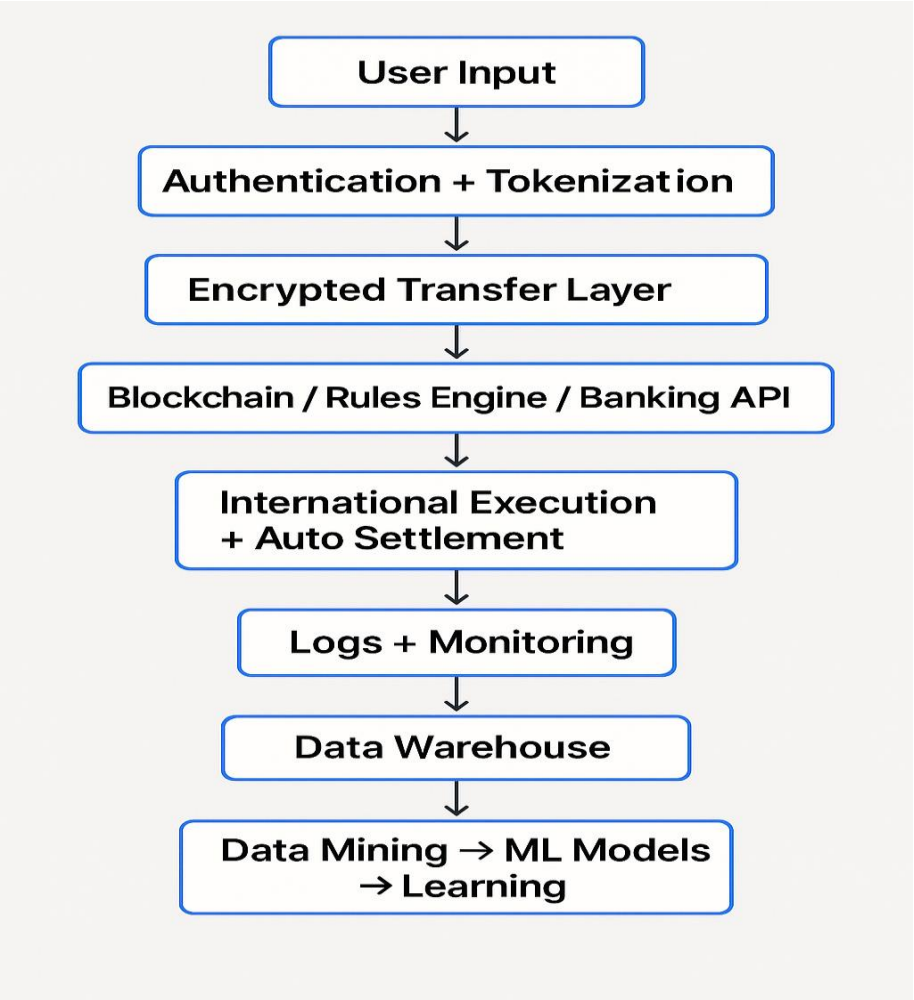

Fig 9: End-to-End Financial Data Processing and Risk Assessment Pipeline

The cybersecurity data pipeline for secure transactions starts with data ingestion where raw information is gathered from sources like transaction logs, authentication logs, API calls, threat intelligence feeds, and blockchain nodes [5],[9]. This is succeeded by secure data storage, generally in cloud-based data lakes or data warehouses such as AWS S3, Azure Blob Storage, or Google BigQuery, with rigorous encryption features being implemented. Then, data preprocessing is done to clean the data removing duplicates, errors, and standardizing formats, in addition to applying tokenization and anonymization processes to protect sensitive information [13]. During the data mining process, a number of analytical methods are used, such as classification (to detect suspicious transactions), clustering (to identify similar patterns for anomaly detection), association rule mining (to identify patterns of frequent transactions), outlier detection (to identify unusual usage), and predictive modeling (to determine the probability of a cyber threat) [12]. After completing this analysis, the action and response phase employs real-time alerts and machine learning-based rules to automatically approve, block, or flag a transaction. A feedback loop is included to continually refine and improve the models [3],[14]. Lastly, the reporting and visualization process reports analyzed data through dashboards that display system performance, fraud statistics, risk scores, and behavioral trends, as well as create compliance logs for audit purposes [5],[13].

5 Ethical and Legal Considerations and Real-World Applications

In the field of secure data exchange and computer security, "**Ethical and legal Considerations"** performs the instrumental role of assuring ethical data handling and protection of the user. Ethically, businesses ought to

preserve user confidentiality, get informed consent prior to data gathering, and apply data for appropriate purposes only. They have to circumvent biases in their machine learning programs that can lead to discriminatory denial of service or flagging of transactions [9],[11]. On the legal front, institutions have to abide by international data protection legislation like the "**General Data Protection Regulation (GDPR)**" of the EU, "California Consumer Privacy Act (CCPA)" of the US, and other regionally relevant cybersecurity legislations [13]. These laws require transparency, data minimization, purpose restrictions, and access or erasure rights for users. Disobedience can result in hefty fines and loss of consumer trust. On the **practical implementations** side, secure data transaction structures are utilized extensively across industries [9]

In "banking and finance", cybersecurity facilitates secure and real-time cross-border payments via channels such as SWIFT and blockchain-based cross-border settlements. "E-commerce websites" implement secure APIs, tokenization, and fraud protection mechanisms to secure users' payments. "Medicine" maintains and transfers patient information securely using HIPAA-compliant systems so that it is not breached. These frameworks are utilized by governments in "digital identity programs", tax returns, and defense communications [5],[13]. 'Blockchain and smart contracts' also **facilitate decentralized finance (DeFi)** platforms and global trade systems to make transactions with no human involvement but still within compliance and traceability [14],[5].

6 Conclusion and Future Scope

In the coming years, data mining and cybersecurity will play a pivotal role in managing and securing data across industries. Data mining will become smarter and more contextual, offering real-time insights, anomaly detection, and predictive analysis with greater accuracy. Cybersecurity will integrate advanced analytics, AI, and blockchain to detect threats proactively and ensure data integrity. Together, these technologies will enable organizations to make informed decisions, prevent fraud, and build secure, intelligent digital systems.

References

1. F. L. Greitzer, D. A. Frincke, Combating the Insider Cyber Threat. *IEEE Security & Privacy*, vol. 6, no. 1, pp. 61–64, 2008.
2. M. Salem, S. Hershkop, S. J. Stolfo, A Survey of Insider Attack Detection Research. In *Recent Advances in Intrusion Detection (RAID)*, LNCS 5230, pp. 69–90, Springer, 2008.
3. A. Tuor, S. Kaplan, B. Hutchinson, N. Nichols, S. Robinson, Deep Learning for Unsupervised Insider Threat Detection in Structured Cybersecurity Data Streams. In *Proceedings of the AAAI Workshops*, WS-17-03, 2017.
4. W. Eberle, L. Holder, Insider Threat Detection Using Graph-Based Approaches. In *Proceedings of the Cyber Security and Information Intelligence Research Workshop*, ACM, 2009.
5. I. A. Gheyas, A. E. Abdallah, Detection and Prediction of Insider Threats to Cyber Security: A Systematic Literature Review and Meta-Analysis. *Big Data Analytics*, vol. 1, no. 1, 2016.
6. O. Brdiczka, J. Liu, B. Price, Proactive Insider Threat Detection Through Graph Learning and Psychological Context. In *Security and Privacy Workshops (SPW)*, IEEE, pp. 142–149, 2012.
7. J. Han, M. Kamber, J. Pei, *Data Mining: Concepts and Techniques*. Morgan Kaufmann, 3rd ed., 2011.
8. L. Rokach, O. Maimon, *Data Mining with Decision Trees: Theory and Applications*. World Scientific, 2014.
9. A. Koli, S. Kumar, R. Yadav, Real-Time Insider Risk Detection Using Autoencoders in Financial Systems. *Journal of Cybersecurity and Information Intelligence*, vol. 14, no. 1, pp. 45–57, 2025.
10. J. Lopez, K. Sartipi, Insider Threat Detection Using LSTM Models for Behavioral Data Analysis. *Journal of Information Security and Applications*, vol. 54, 2020.
11. X. Yuan, X. Wu, Deep Learning Approaches for Insider Threat Detection: A Review. *ACM Computing Surveys*, vol. 53, no. 6, 2020.
12. Y. Li, J. Chen, Modeling User Behavior for Insider Threat Detection Using Graph Neural Networks. *Knowledge-Based Systems*, vol. 256, 2023.
13. F. L. Greitzer, D. A. Frincke, Combining Traditional Cybersecurity Audit Data with Psychosocial Data for Predictive Insider Threat Modeling. In *Insider Threats in Cyber Security*, LNCS 5970, pp. 85–113, Springer, 2016.
14. Wang, J., Sun, Q., & Zhou, C. (2023). *Insider Threat Detection Based on Deep Clustering of Multi-Source Behavioral Events*. *Applied Sciences*, 13(24), 13021. https://doi.org/10.3390/app132413021
15. SlidePlayer, "Cyber Security - Cyber Crime in Banking Sector." [Online]. Available: https://slideplayer.com/slide/12975358/.