Towards More Effective Insider Threat Countermeasures: A Survey of Approaches for Addressing Challenges and Limitations

Omar Gonzales
Electrical Engineering and Computer Science
Florida Atlantic University
Boca Raton, FL, USA
ogonza16@fau.edu

Shihong Huang
Information Systems
Carnegie Mellon University
Pittsburgh, PA, USA
shihong@cmu.edu

KwangSoo Yang
Electrical Engineering and Computer Science
Florida Atlantic University
Boca Raton, FL, USA
yangk@fau.edu

2024 IEEE International Systems Conference (SysCon) | 979-8-3503-5880-3/24/$31.00 ©2024 IEEE | DOI: 10.1109/SysCon61195.2024.10553441

***Abstract*—This survey delves into challenges and limitations in addressing insider threats, utilizing both qualitative and quantitative questions to extract nuanced insights. It categorizes challenges based on characteristics and methodologies, conducting a comprehensive analysis across approaches to evaluate security control functions. The study systematically examines hurdles through targeted qualitative questions, providing a nuanced understanding of unique challenges. Additionally, quantitative questions assess each approach's adherence to security control functions. The findings underscore the complexity of addressing the human factor and emphasize the need for a unified approach integrating technical and behavioral factors. The paper highlights the urgency of implementing enhanced security measures and sets the stage for future research in insider threat mitigation.**

***Keywords*— Insider threat, human-eccentric, ontology, organizational culture, survey, security controls, threat mitigation, comprehensive security, behavioral analysis.**

I. Introduction

Insider threats are a growing concern in today's digital world, posing significant risks to organizations and individuals. Mitigating this problem is challenging due to large number of false positive errors and delayed processing. Insufficient datasets and a failure to consider human factors further complicate the issue. This survey aims to enhance the effectiveness of insider threat mitigation by addressing the challenges and limitations of existing approaches in academic research. The findings emphasize the need for a comprehensive approach to effectively tackle insider threats.

A. Definition of Insider Threat

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) [1] defines insider threats as potential or actual harm from employees, contractors, or business partners to an organization's critical assets. Addressing these threats necessitates a comprehensive approach involving various stakeholders and a mix of technical, administrative, and physical controls. CISA identifies four main insider threat types: (1) unintentional, (2) negligent, (3) malicious, and (4) outsider-influenced, each requiring specific countermeasures for effective protection.

B. Impact on Organizations and Industries

Attacks from within organizations have caused big problems for many industries. In the last two years, 67% of organizations have been affected by insider attacks, costing about $15.4 million on average [2]. They often target sensitive information like customer data and finances. Most of these incidents—56%—happen because of accidents or carelessness, while 44% involve people intentionally causing harm. The financial services sector is hit particularly hard, losing an average of $243,000 each year because of insider threats [4]. In 2021, the risk of insider incidents rose to 72%, with a high chance of industrial spying [5]. For example, in the 2015 Ukraine power grid cyber-attack, insiders used stolen credentials to cause a blackout, resulting in damages of around $15.6 million [6].

C. Factors Contributing to the Complexity of the problem

Detecting and responding to insider threats is a complex task for organizations due to various contributing factors. Insider threats arise from authorized individuals who carry out seemingly legitimate but harmful actions. They may use tactics to hide their activities and are influenced by human factors and legal considerations. Responding in real-time is challenging, especially when there are errors in identifying threats.

D. Search and Selection of Proposed Approaches

This survey uses strict criteria to find and select relevant papers. It focuses on works published in the last 10 years, sourced from respected academic databases like IEEE Xplore and ACM Digital Library, as well as relevant government and educational institutions. These platforms offer comprehensive coverage of computer science and cybersecurity literature. Searches use keywords like 'insider threat,' 'security controls,' and 'behavioral analysis' to refine results, ensuring papers address technical and/or behavioral aspects of mitigating insider threats. Selected papers must be recent, relevant to insider threat mitigation, and focus on real-world applications or empirical studies. Excluded are non-English papers, those lacking methodological details, and those mainly addressing external threats. Quality assessment considers the reputation of publishing venues and author credibility.

The remainder of this paper is organized as follows: Section 2 offers an overview of the technological approaches to mitigate insider threats. In Section 3, human-centric strategies, encompassing administrative controls, policies, and training programs, are examined. Section 4 describes integrated security control evaluation. Lastly, Section 5 discusses opportunities for further research and improvement to enhance the effectiveness of the proposed solutions, concluding with a summary of the survey findings.

II. Limitation and Challenge Evaluation

Based on insights from industry tools and reports by Ponemon Institute [2], Accenture[4], and DTEX [5], along with technical and behavioral indicators from the CISA insider threat guide, qualitative questions were developed to address key aspects in identifying limitations and challenges. Although not all questions may apply universally, they target crucial areas for analysis. See Fig. 1 for the survey's evaluation workflow. Below are questions aimed at analyzing related limitations or challenges:

- Adaptability: How does the approach handle diverse insider threat scenarios?
- Validation and Scalability: How is the approach validated, and how effectively does it scale?
- Implementation and Complexity: How complex is it to implement the approach?
- Privacy and Ambiguity: How does the approach manage privacy concerns and resolve ambiguities?
- Timeliness and External Dependency: How does the approach ensure timely responses and reduce reliance on external factors?
- Limited Scope and Heterogeneity: How does the approach handle various insider threat scenarios and organizational environments?

III. Technical Approaches

Various technical approaches have been proposed to prevent insider threats in information systems. These approaches can be categorized based on the insider threat activity they target, the technological solutions they suggest, the methodological approaches they adopt, and their limitations or weaknesses. Insider threat activities are defined using reliable sources, including industry standards and best practices from organizations such as the Cybersecurity and Infrastructure Security Agency (CISA) [1], Ponemon Institute [2], and Carnegie Mellon University CERT Insider Threat Center [3].

We group the approaches based on what kind of insider threat they deal with, like misuse of privileged access, stealing data, or tricking people. Each approach is designed to tackle specific challenges linked to these activities. While the solutions, such as using data analysis or access controls, can work for different types of threats, we won't go into the specific technical details here.

A. Unauthorized Access

This activity refers to the situation where an insider gains access to information or systems without proper authorization or permission. Several technical approaches have been proposed to mitigate this threat. Here is a category of the existing proposed approaches and description to mitigate this type of activity.

1) Cloud-based approaches: Approaches that specifically target unauthorized access in cloud environments. The paper [7] provide authentication mechanism based on facial feature recognition and KNN-based user classification and the paper [8] proposed a Mobile Edge Computing (MEC) approach that monitors and handles all insider requests at real-time.

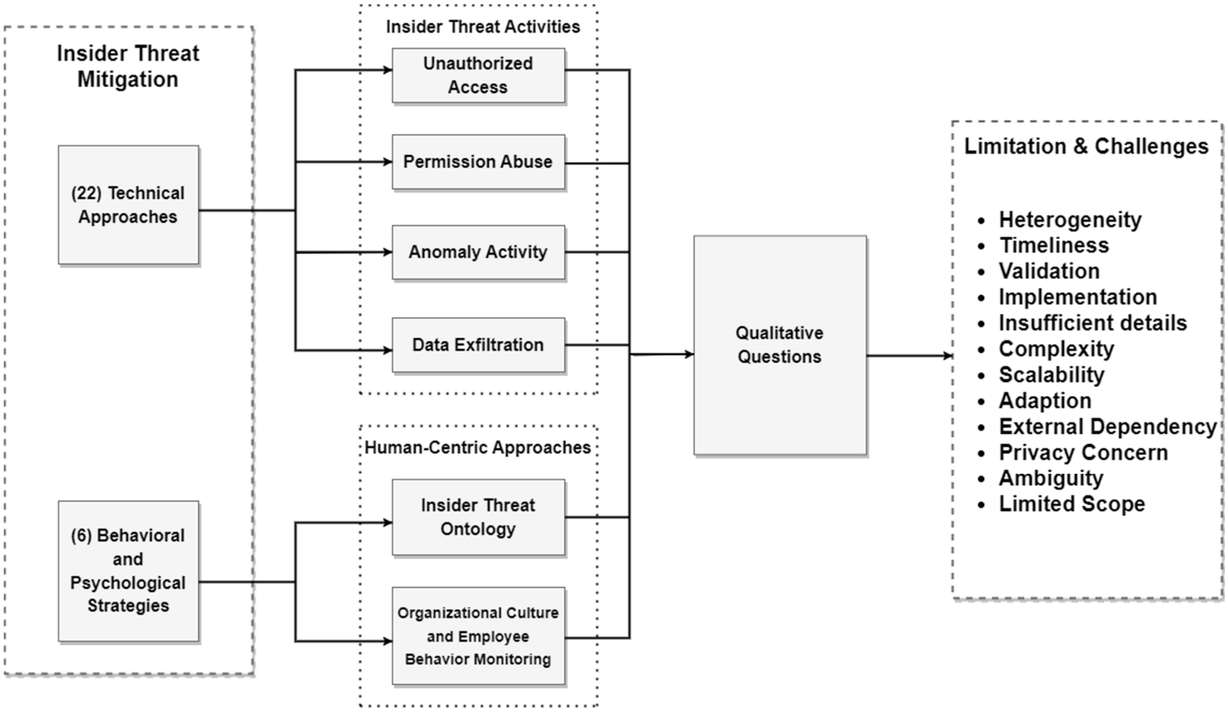

Fig. 1: Qualitative evaluation workflow to extract limitation and challenges from technical approaches and behavioral and psychological strategies

2) Deception techniques: Approaches utilizing deception as a strategy to detect and prevent unauthorized access. The paper [9] combines moving target defense, defensive deception, and attribute-based access control (ABAC).

3) Systematic Dynamic methods: Approaches employing system dynamics principles to mitigate unauthorized access. The paper [24] proposed a layered defense strategy consisting of policies, procedures, and technical controls.

These approaches provide promising contributions to mitigate unauthorized access events caused by insider threats. However, they also face challenges and limitations, as detailed in Table I.

B. Privileged Permission Abuse

This activity refers to the misuse of permissions or access rights granted to privileged users, such as system administrators or other high-level users. Several approaches have been made to mitigate this serious insider threat activity and they can be categorized as:

1) Attribute Based Access Control (ABAC) Policies: Approaches centered around the use of ABAC policies to mitigate privileged permission abuse. The proposed approach in [10] implements a rule mining algorithm for addressing policy-based access control (PBAC) or claims-based access control (CBAC) problem and a policy scoring algorithm for evaluating policies across multiple operation periods.

TABLE I. THE LIMITATIONS AND CHALLENGES OF FRAMEWORKS ADDRESSING UNAUTHORIZED ACCESS IN INSIDER THREATS

Approaches	Challenges and Limitations
Insider Threat detection with Face Recognition and KNN User Classification [7].	**Privacy Concerns:** Collection and storage of facial features. **Scalability:** High-quality image requirement, processing time, insider knowledge accumulation. **Limited scope:** Authentication mechanism solely relying on biometric face recognition, and its applicability extends only to cloud computing.
A Mobile Edge Mitigation Model for Insider Threats: A Knowledgebase Approach [8].	**Heterogeneity:** The coexistence of diverse configurations and resource sets across different versions of endpoints. **Timeliness:** Difficulties in timely processing of complex scenarios involving multiple versions of cloud environments. **Validation:** Accuracy indicates a 5% false positive rate. No statistical analysis was performed.
Insider Threat Mitigation Using Moving Target Defense and Deception [9].	**Implementation:** Complex integration of defensive deception, moving target defense and ABAC. **Validation:** No validation provided **Adaptability**: Framework should be adapted to different environments.
A Method of Evaluation for Insider Threat [24].	**Implementation:** Challenging to implement due to resource intensiveness. **Validation:** No accuracy assessment conducted, and assumptions are utilized. **Insufficient details:** Lack of low-level details in approach explanation.

2) Machine Learning ML-based methods: Approaches leveraging machine learning algorithms for detecting and preventing privileged permission abuse. The paper [11] employs logistic regression, random forest, neural network, and XGBoost algorithms to detect insider threat behavior in unseen data. Also the proposed approach in [12] extracts features by calculating statistical features of user and user group behaviors using unsupervised learning. Another approach in [14] proposes a hybrid deep learning architecture that combines Convolutional Neural Network (CNN) and Long-Short Term Memory (LSTM) on user behavior profiling.

3) Data packet analysis: Approaches incorporating DPI solutions to monitor and prevent permission abuse. The paper [13] proposes a approach that employs a combiantion of hierarchy-mapping based model, artificial intelligence, access control and graph theory to analyze network packets and estimate insider threat at real-time. Another approach. Lastly, the paper [25] employs Deep Packet Inspection (DPI) to identify source, destination and pathway of network traffic for forensic examination in cybercrime.

While useful, it's important to consider the challenges and limitations of these approaches, as outlined in Table II.

TABLE II. THE LIMITATIONS AND CHALLENGES OF FRAMEWORKS ADDRESSING PRIVILEGED PERMISSION ABUSE IN INSIDER THREATS

Approaches	Challenges and Limitations
Mining Least Privilege Attribute Based Access Control Policies [10].	**Complexity:** The mining algorithm's exponential nature and high uniqueness in attributes pose challenges in deriving rules. **Scalability:** With an expansive ABAC privilege space and diverse real-world data attributes, the dataset's size becomes practically limitless. **Validation:** Accuracy risks of overfitting to specific datasets, potentially resulting in suboptimal performance.
Analyzing Data Granularity Levels for Insider Threat Detection Using Machine Learning [11].	**Inherited limitation:** Any existing limitation from ML-based algorithms. **Validation:** Biased evaluation due to a restricted set of users. False positive alarms pose a challenge to analysts.
Towards a User and Role-Based Behavior Analysis Method for Insider Threat Detection [12].	**Inherited limitation:** Any existing limitation from isolation forest algorithm **Adaptation:** The model's ability to generalize to diverse organizational environments, job roles, and user behaviors may be limited **Privacy Concerns:** The collection and analysis of user behavior data for insider threat detection may involve sensitive personal information.
An Active Defense Model and Framework of Insider Threats Detection and Sense [13].	**Privacy concerns:** Detection measures may raise concerns about user privacy and monitoring. **Complexity:** Challenging to integrate all mechanisms—prediction, prevention, detection, response, recovery, and reinforcement. **Validation**: Questionable due to a limited dataset of 30 users and 5 roles.
User Behavior Profiling using Ensemble Approach for Insider Threat Detection [14].	**Privacy concerns:** Detection measures may raise concerns about user behavior. **Scalability:** Limited when applied to large-scale organizations with a high volume of user activities. **Inherited limitation:** Any limitation from Long Short-Term Memory and Convolutional neural network.

	Validation: There is detection rate of 85%.
Cybercrime Countermeasure of Insider Threat Investigation [25].	**Privacy concerns:** Detection measures may raise concerns about user privacy. **Timeliness:** Time-consuming analysis degrades real-time mitigation. **External dependency:** The need for cyber security expertise to confirm incidents. **Insufficient details:** Lack of low-level details in approach explanation.

C. *Anomaly User Activity*

This activity involves abnormal user actions deviating from typical behavior in a system or network. Various approaches aim to mitigate this risk, categorized by detection mechanisms:

1) Behavior-based detection: Approaches focusing on modeling and evaluating user behavior to detect anomalies. The paper [16] proposes an Artificial Immune System (AIS)-based algorithm called negative selection algorithm to predict anomalies. Another paper [18] introduces an detection method based on Gated Recurrent Unit (GRU) and multi-autoencoder techniques, employing an unsupervised anomaly detection approach. The method incorporates multi-level filter behavior learning. The paper [19] applies the implementation of Long Short-Term Memory (LSTM) Autoencoder for behavior learning and anomaly detection. The paper [22] proposes an Hidden Markov Model (HMM)-based model to learn the user behavior and to detect deviations to alert analysts. Lastly, the paper [20] contributes with novelty of a privacy preserving feature extraction to capture online behaviors and the usage of isolation forest to detect anomalies.

2) Rule-based detection: Approaches that utilize predefined security rules. The paper [23] proposes a detection mechanism that combines a rule matching with pre-set threholds for immediate response and iterative attention based on historical evants. Another paper [21] employs policy-based tripwires and known insider attack patterns, treating policy violations or pattern matches as anomalies.

It's important to recognize and explore the challenges and limitations of these approaches, as outlined in Table III.

TABLE III. THE LIMITATIONS AND CHALLENGES OF FRAMEWORKS ADDRESSING ANOMALY USER ACTIVITY IN INSIDER THREATS

Approaches	Challenges and Limitations
Insider Threat Detection using an Artificial Immune system Algorithm [16].	**Inherited limitation:** Any constraints arising from negative selection algorithms and artificial immune systems. **Validation:** Utilization of a synthetic dataset instead of real-world scenarios. Limited evaluation metrics were employed, excluding recall and F-1 score. The accuracy indicates 85%
GRU and Multi-autoencoder based Insider Threat Detection for Cyber Security [18].	**Timeliness:** Potential delays due to data events from multiple sources and a large set of behavioral features. **Adaptability:** Relied on a specific benchmark dataset, limiting generalization to unseen data. **Accuracy:** Experimental results show better performance than existing methods, but no accuracy metrics or values are provided.
User Behavior Analytics for Anomaly Detection Using LSTM Autoencoder: Insider Threat Detection [19].	**Limited scope:** Anomaly detection is constrained to within a user's session or extended periods. **Inherited limitation:** Constraints stemming from LSTM autoencoder. **Implementation:** Feature selection and engineering can be time-consuming, requiring domain expertise. **Adaptability:** Challenging to continuously monitor and update the model for changes in user behavior and new threat patterns.
Detecting Insider Threat from Enterprise Social and Online Activity Data [20].	**Validation:** Prioritizing high recall over precision due to broad feature selection, with ongoing efforts to enhance precision through adaptive anomaly detection algorithms. **External Dependency:** Relies heavily on data quality; incomplete or inaccurate data may impact effectiveness. **Complex analysis:** Challenges arise from the hierarchical structure, resulting in over 200 subtrees for analysis.
A Tripwire Grammar for Insider Threat Detection [21].	**Implementation:** Involves constant refinement and updates of policies and tripware. **Ambiguity:** Various thresholds to define suspicious or normal events may lead to different interpretations.
A new take on detecting insider threats: Exploring the use of hidden Markov models [22].	**Limited scope:** Unable to detect incidents occurring over an extended timeframe. **Implementation:** Selecting the right hyperparameters is challenging, with difficulties in quantifying vague features. **Validation:** Utilization of a synthetic dataset instead of real-world datasets. The Hidden Markov model demonstrates an area under the curve of 0.83.
A hybrid intelligent system for insider threat detection using iterative attention [23].	**Heterogeneity:** Challenging to process and analyze data from diverse sources like logs, user behavior, and psychological assessments. **Ambiguity:** Introducing psychological data into threat detection introduces multiple interpretations. **Privacy concerns:** Collecting and analyzing psychological data may raise privacy concerns among employees. **Validation:** Specific accuracy values or detailed performance metrics are not explicitly provided.

D. *Data exfiltration*

This activity refers to the unauthorized transfer of sensitive information from an organization to an external party, posing significant risks. Various approaches aim to detect and prevent this activity using multiple methods.

1) Game-theory method: Approach that analyzes user interaction, In paper [15], A two-player zero-sum stochastic game to model the interaction between insider and system administrator game theory approach to derive malicious actions in file systems.

2) Machine-learning methods: Approaches that utilzies machine learning algorithms to prevent data loss. The paper [17] introduces an Adaptive Deep Forest model (ADF) designed for SQL injection detection. The model incorporates feature transformation based on multi-grained scanning, employs a cascade structure for characterization learning, and integrates the AdaBoost algorithm into the deep forest model. A proposed approach in [33] presented a Data Loss Prevention (DLP) model utilizing statistical data analysis, including Term Frequency Inverse Document Frequency (TF-IDF), to cluster documents by topics and detect confidential data with restricted secrecy levels. The model's statistical analysis enables the approximation of confidential data semantics, facilitating the identification of existing sensitive information and newly created documents containing such data. Another approach proposed in [34] is to detect electronic data theft. It employs one-class learning algorithms trained on flow-oriented feature representations. This approach enables the system to detect unusual timing patterns, indicating potentially malicious data transfers.

3) Information leakage awareness: Approaches that employs prevention against data leakage. The paper [35] presents StoreSim, a multicloud storage system emphasizing information leakage awareness. StoreSim minimizes leakage by storing syntactically similar data on the same cloud, utilizing an approximate algorithm with MinHash and Bloom filter for similarity-preserving data chunk signatures.

The above papers provide methods against data exfiltration incidents. However, these proposed approaches exhibit various limitations as illustrated in Table IV.

TABLE IV. THE LIMITATIONS AND CHALLENGES OF FRAMEWORKS ADDRESSING DATA EXFILTRATION IN INSIDER THREATS

Approaches	Challenges and Limitations
Behavioral Analysis of Insider Threat: A Survey and Bootstrapped Prediction in Imbalanced Data [15].	**Limited scope**: Usage of a predefined set of possible actions, limiting the range of malicious actions. **Validation:** Utilizes a synthetic dataset. Good recall and precision but high false positive rate.
A SQL Injection Detection Method Based on Adaptive Deep Forest [17].	**Inherited limitation:** Constraints arising from adaptive deep forest algorithms. **Validation:** Limited use of real-world datasets, inadequate comparison evaluation with other deep learning models, and absence of specific accuracy values. **Insufficient details:** Lack of a detailed explanation of the AdaBoost algorithm and the integration of the raw feature vector.
Detecting Data Semantic: A Data Leakage Prevention Approach [33].	**Limited scope:** Real-time notifications are not feasible. **Scalability:** Increased data volume may elevate computational and processing requirements. **Validation:** Testing is limited to a small dataset and specific topics.
Malicious Overtones: Hunting Data Theft in the Frequency Domain with One-class Learning [34].	**External dependency:** The model relies on the distribution of normal traffic and the Dynamic Host Configuration Protocol (DHCP). **Limited scope:** Real-time notifications are not feasible. Applicable only to unencrypted packets, and effective for network-wide traffic rather than individual hosts.
Optimizing Information Leakage in Multi-cloud Storage Services [35] .	**Performance:** Less effective than encryption and may incur potential excessive CPU overhead. **Validation:** Used small datasets and the assumption of equal reliability and weight for all cloud service providers. No accuracy value is provided. **Limited scope:** No detection on specific types of sensitive data due to its reliance on syntactic similarity metrics instead of semantic measures.

IV. BEHAVIORAL AND PSYCHOLOGICAL STRATEGIES

While technical tools like access controls and monitoring systems are important for stopping insider threats, they might not address human and organizational issues. To fill this gap, we need non-technical solutions that focus on people, awareness, and company culture. This section looks at the challenges of using these non-technical methods to deal with insider threats. A big challenge is understanding and handling the complicated ways people act. Human-centric approaches, like changing company culture or training employees, face difficulties and pushback. Non-technical strategies include defining insider threat indicators and suggesting ways to improve company culture and how staff deal with insider threats.

A. Insider threat Ontology:

This section looks into how using ontology can help deal with insider threats. Ontology is like a formal map that shows different ideas, connections, and groups in a specific area. It helps organize and understand insider threats better, making it easier for everyone involved to talk and work together. Several approaches for insider threat ontologies are presented. The approach in [26] focuses on sharing indicators of insider threats without revealing sensitive information. The resulting ontology is machine-readable, human-understandable, and transferable, incorporating data-driven ontology bootstrapping and concept map extraction methods (See Fig. 2). Another approach in [27] introduces the Sociotechnical and Organizational Factors for Insider Threat (SOFIT) approach, which describes individual and organizational factors contributing to insider threats (See Fig. 3). This comprehensive ontology is characterized by a hierarchical arrangement and includes indicators of insider threat characteristics. Furthermore, a dictionary-based classification method [29] is proposed (See Fig. 4) to detect negative attitudes towards law enforcement on

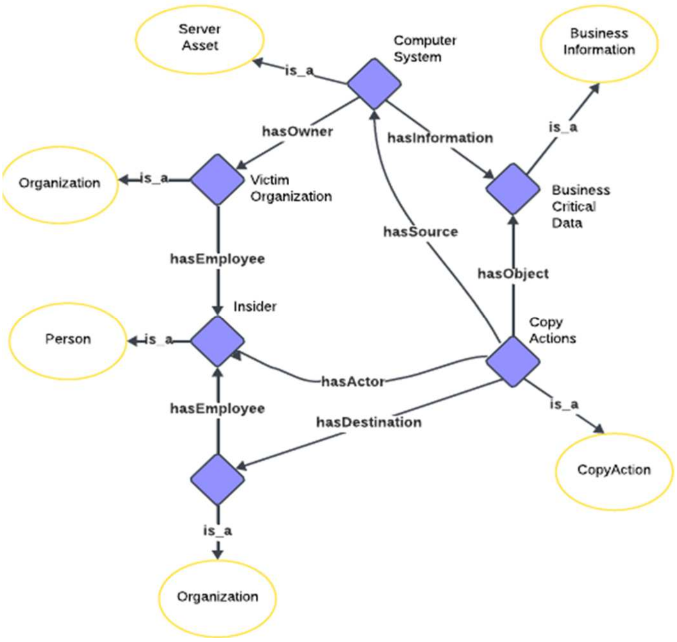

Fig. 2 shows an example illustrating the translation of data exfiltration events into ontology individuals and logical workflow [26].

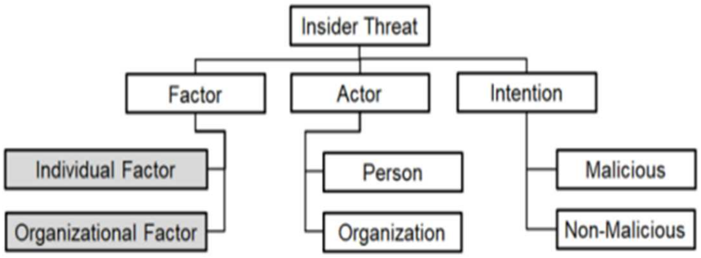

Fig. 3 shows the Sociotechnical and Organizational Factors for Insider Threat (SOFIT) Ontology at high-level classes [27].

social media platforms, particularly YouTube. Lastly, the paper [28] characterize insider attacks, identifying key elements such as events, motivations, and organizational characteristics. This approach provides a general understanding of insider threats and can be used to model past attacks (See Fig. 5).

It's important to explore the challenges and limitations of these ontology-based approaches, as explained in Table V.

B. *Organizational Culture and Employee Behavior Monitoring*

An organization's culture affects insider threats significantly. A positive culture, valuing ethics, and trust, reduces risks, while a negative one, marked by secrecy and distrust, increases them.

TABLE V. THE LIMITATIONS AND CHALLENGES OF APPROACHES DEFINING AN ONTOLOGY TO MITIGATE INSIDER THREATS

Approaches	Challenges and Limitations
An Ontology for Insider Threat Indicators [26].	Ambiguity: Real-world insider threat cases exhibit variable representations, with data gathered from legal judgments and outcomes showing highly variable documentation. Complexity: Formalizing an insider threat indicator ontology model demands domain experts, and translating it into a machine-readable format is challenging.
Modeling Expert Judgments of Insider Threat Using Ontology Structure [27].	Validation: Lack of testing in real operational settings and insufficient studies on the relationships among constructs and their influence on insider threat judgments. Complexity: The necessity for expert knowledge elicitation studies as proxies for empirically investigating the predictive strength of indicators in an operational setting.
Understanding Insider Threat: A Framework for Characterizing Attacks [28].	Validation: The psychological surveys to measure static traits are unreliable; only the dataset used has been assessed. Complexity: Characterizing the mindset of individuals conducting insider attacks with static and dynamic personality traits pose challenges. Limited scope: Focuses on specific factors, potentially overlooking other elements relevant to insider threats.
Proactive Insider Threat Detection Through Social Media [29].	Complexity: Analyzing user-generated content for psychosocial trait analysis poses challenges in drawing conclusions about behavior, beliefs, and attitudes toward specific topics. Privacy concerns: Users may be unaware of online monitoring and analysis, lacking explicit consent for data utilization. Limited scope: Limited to comment classification, focusing on user-generated content on social media platforms like comments, posts, likes, and shares.

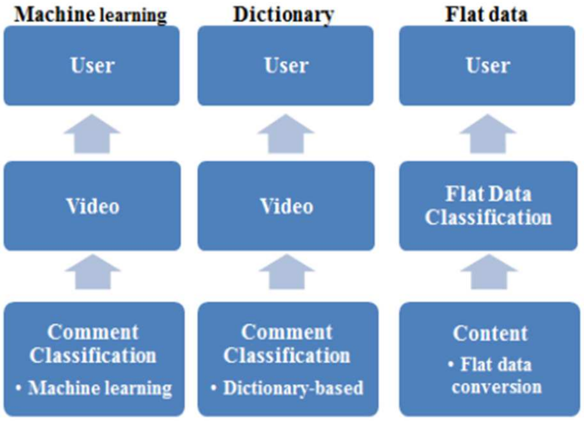

Fig 4. shows a dictionary-based classification to extract the attitude expressed in Youtube video comments [29]

Monitoring employee behavior, such as using data analysis, can spot potential threats. Establishing an ethical code, providing insider threat training, and enabling reporting channels are essential preventive measures. Various approaches tackle these issues. One suggests using positive incentives and addressing organizational vulnerabilities [30]. It focuses on deterring threats through theories like Social Exchange and Situational Crime Prevention. Another proposes a critical-path approach to assess insider risks [31], considering personal traits, stressors, behaviors, and organizational responses. However, these approaches face challenges and limitations. Refer to Table VI for more information.

V. INTEGRATED SECURITY CONTROL EVALUATION

This section evaluates the insider threat countermeasure approaches discussed earlier, recognizing their use of different methods to tackle specific issues within insider threat mitigation. Given this diversity, conducting a unified experimental analysis is challenging. Thus, the evaluation focuses on the common security control functions across these approaches. The following outlines the defined security control functions relevant to insider threats:

TABLE VI. THE CHALLENGES AND LIMITATIONS OF APPROACHES DEFINING AN ORGANIZATIONAL CULTURE TO MITIGATE INSIDER THREATS

Approaches	Challenges and Limitations
Balancing Organizational Incentives to Counter Insider Threat [30]	**Validation:** Inadequate testing with just three incidents and survey questions directed at insider threat program decision-makers may introduce inaccuracies and misinterpretations. **Complexity:** Challenges in interpretation and a reliance on subject matter experts are integral aspects. **Limited scope:** Constrained to demonstrating a correlational influence, rather than a causal one of perceived organizational support on insider misbehavior.
Application of the Critical-Path Method to Evaluate Insider Risks. Internal Security and Counterintelligence [31]	**Complexity:** challenging to uncover concerning behaviors in current circumstances due to privacy concerns. **Limited scope:** Effective in detecting general risks, it may not replace specialized evaluation methods for specific insider activities or violence risk assessments.

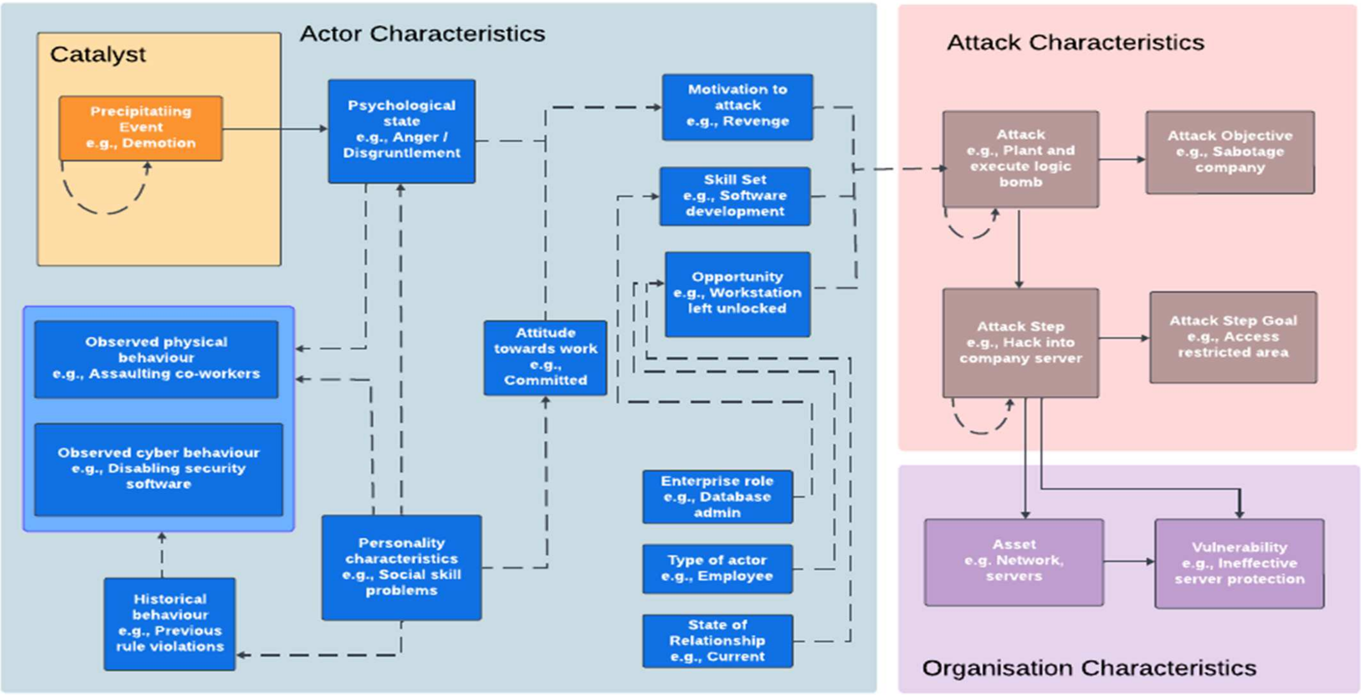
Actor Characteristics
Catalyst
Precipitatiing Event e.g., Demotion
Psychological state e.g., Anger / Disgruntlement
Motivation to attack e.g., Revenge
Skill Set e.g., Software development
Opportunity e.g., Workstation left unlocked
Attitude towards work e.g., Committed
Observed physical behaviour e.g., Assaulting co-workers
Observed cyber behaviour e.g., Disabling security software
Historical behaviour e.g., Previous rule violations
Personality characteristics e.g., Social skill problems
Enterprise role e.g., Database admin
Type of actor e.g., Employee
State of Relationship e.g., Current
Attack Characteristics
Attack e.g., Plant and execute logic bomb
Attack Objective e.g., Sabotage company
Attack Step e.g., Hack into company server
Attack Step Goal e.g., Access restricted area
Asset e.g. Network, servers
Vulnerability e.g., Ineffective server protection
Organisation Characteristics

Fig. 5 shows an ontology model and workflow for characterizing insider attacks [28].

1) Preventative Controls: Security measures, including those specific to insider threat mitigation, to prevent unauthorized activities, spanning physical, technical, and administrative controls.

2) Detective Controls: Measures to detect and alert unauthorized activities, including those initiated by insider threats, encompassing physical alerts and technical solutions like honeypots and IDSs.

3) Corrective Controls: Measures, both technical and administrative, to repair damage or restore resources after unauthorized or insider threat-related activities, including system patching and tailored incident response plans.

Furthermore, a set of three qualitative yes-or-no questions was formulated to assess the effectiveness of each security control function provided by each approach:

- Preventative: Does the mitigation approach include proactive measures against malicious insiders?
- Detective: Is the mitigation approach designed to identify and alert insider threats?
- Corrective: Does the mitigation approach have corrective actions in place to respond to insider threat incidents?

Table VII analysis reveals that no singular insider threat countermeasure approach comprehensively encompasses the entire set of security control functions. Notably, most current technological frameworks (blue color) focus on providing detection controls, while behavioral and psychological strategies (red color) predominantly support preventive controls.

VI. Conclusion and Future Work

The conclusion underscores the need for a holistic approach, considering both technical and behavioral factors, to effectively address the challenges and limitations in insider threat mitigation. Recommendations, such as those from the Insider Threat Mitigation Program [1] by CISA and the seven science-based commandments [32] from CITRAP, offer comprehensive strategies. Human behavioral factors, crucial yet challenging to identify due to their non-technical nature, play a significant role in insider threats. Future research directions include enhancing technological approaches, refining models for detecting insider threats, and exploring behavioral and psychological factors. This involves conducting studies on employee attitudes, expert knowledge elicitation, and evaluating the utility of approaches. Further research is suggested on classification methods, meta-training techniques, and the impact of national culture.

TABLE VII. The Evaluation Results of Security Control Functions of Insider Threat Countermeasure Approaches

Mitigation Approaches	Preventative	Detective	Corrective
[7] [9] [10] [21] [23] [24] [34][35]	No	Yes	Yes
[26][27][30] [31]	Yes	No	No
[28] [33]	Yes	No	Yes
[8] [13] [17]	Yes	Yes	No
[11] [12] [14] [15] [16] [18][19] [20] [22] [25] [29]	No	Yes	No

ACKNOWLEGMENT

The authors would like to thank the U.S. National Science Foundation under Grant #1844565.

REFERENCES

[1] U.S. Cybersecurity and Infrastructure Security Agency. (2022). Insider threat mitigation guide. Retrieved from https://www.cisa.gov/sites/default/files/2022-11/Insider%20Threat%20Mitigation%20Guide_Final_ 508.pdf

[2] Ponemon Institute. 2020. Insider Threat Report. www.observeit.com/wp-content/uploads/2020/01/Ponemon-Insider-Threat-Report-2020.pdf.

[3] CERT Insider Threat Center. Insider Threats: Reducing the Risk. Software Engineering Institute, Carnegie Mellon University, 2018, resources.sei.cmu.edu/library/asset-view.cfm?assetid=508099.

[4] Accenture. 2020. The Cost of Insider Threats in Financial Services. https://newsroom.accenture.com/news/cost-of-cybercrime-continues-to-rise-for-financial-services-firms-according-to-report-from-accenture-and-ponemon-institute.htm

[5] DTEX Systems .2022. Insider Risk Report. https://www.dtexsystems.com/wp-content/uploads/2022/02/DTEX_2022_Inside_Risk_Report_Infographic .pdf.

[6] Cybersecurity and Infrastructure Security Agency. Cyber-Attack Against Ukrainian Critical Infrastructure 2021, https://www.cisa.gov/news-events/ics-alerts/ir-alert-h-16-056-01

[7] Sarma, M., Srinivas, Y. & Abhiram, M. (2017). Insider Threat detection with Face Recognition And KNN User Classification. IEEE International Conference on Cloud Computing in Emerging Markets.

[8] Althebyan, Q. (2019) A Mobile Edge Mitigation Model for Insider Threats: A Knowledgebase Approach. Jordan University of Science and Technology & Al Ain University. IEEE International Arab Conference on Information Technology.

[9] Takabi, H. & Jafarian, H.J. (2017). Insider Threat Mitigation Using Moving Target Defense and Deception. MIST '17: Proceedings of the 2017 International Workshop on Managing Insider Security Threats.

[10] Sanders, M. & Yue, C. 2019. Mining Least Privilege Attribute Based Access Control Policies. ACM Annual Computer Security Applications Conference.

[11] D. C. Le, N. Zincir-Heywood and M. I. Heywood (2020). Analyzing Data Granularity Levels for Insider Threat Detection Using Machine Learning. IEEE Transactions on Network and Service Management.

[12] Q. Lv, Y. Wang, L. Wang and D. Wang (2018). Towards a User and Role-Based Behavior Analysis Method for Insider Threat Detection. IEEE International Conference on Network Infrastructure and Digital Content.

[13] Zhang, H., Ma. J., Wang, Y., & Pei, Q. (2019). An Active Defense Model and Framework of Insider Threats Detection and Sense. The Research Institute, China Electronic Equipment & Systems Engineering Corporation. IEEE Fifth International Conference on Information Assurance and Security.

[14] M. Singh, B. M. Mehtre and S. Sangeetha (2019). User Behavior Profiling using Ensemble Approach for Insider Threat Detection. IEEE 5th International Conference on Identity, Security, and Behavior Analysis (ISBA).

[15] Azaria, A., Richardson, A., Kraus, S. & Subrahmanian, V. (2014). Behavioral Analysis of Insider Threat: A Survey and Bootstrapped Prediction in Imbalanced Data. IEEE Transactions on Computational Social Systems.

[16] Igbe, O. & Saadawi, T. (2018). Insider Threat Detection using an Artificial Immune system Algorithm. Department of Electrical Engineering, University of New York. IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference.

[17] Li, Q., Li,W., Wang, J. and Cheng, M. (2019). A SQL Injection Detection Method Based on Adaptive Deep Forest. IEEE Access, vol. 7, pp. 145385-145394.

[18] Meng, F., Lu, P., Li, J., Hu, T., Yin, M., and Lou, F. (2021) GRU and Multi-autoencoder based Insider Threat Detection for Cyber Security. Institute of Computer Application China Academy of Engineer Physics. IEEE 6th International Conference on Data Science in Cyberspace.

[19] Balaram S., Prabhat P., and Basanta J. (2020). User Behavior Analytics for Anomaly Detection Using LSTM Autoencoder: Insider Threat Detection. ACM International Conference on Advances in Information Technology.

[20] Gavai, G., Sricharan, K., Gunning, D., Rolleston, R., Hanley, J. & Singhal, M. (2015). Detecting Insider Threat from Enterprise Social and Online Activity Data. ACM 7th CCS International Workshop on Managing Insider Security Threats.

[21] Agrafiotis, I., Erola, A., & Goldsmith, M. (2016). A Tripwire Grammar for Insider Threat Detection. Department of Computer Science. University of Oxford. ACM 8th CCS International Workshop on Managing Insider Security Threats.

[22] Rashid, T., Agrafiotis, I., & Nurse, J. R. C. (2017). A new take on detecting insider threats: Exploring the use of hidden Markov models. Department of Computer Science, University of Oxford. ACM 8th CCS International Workshop on Managing Insider Security Threats.

[23] Ren, X., & Wang, L. (2021). A hybrid intelligent system for insider threat detection using iterative attention. Institute of information engineering, Chinese academy of sciences. ACM 6th International Conference on Computing and Data Engineering.

[24] Wang, Y. & Yang, S. (2014) A Method of Evaluation for Insider Threat. School of Defense Science, CCIT, National Defense University. IEEE International Symposium on Computer, Consumer and Control.

[25] Kao, D. 2019. Cybercrime Countermeasure of Insider Threat Investigation. International Conference on Advanced Communications Technology. IEEE International Conference on Advanced Communications Technology.

[26] Costa, D., Collins, M., Perl, S., Albrethsen, J., Silowash, G. & Spooner, D. (2014). An Ontology for Insider Threat Indicators. Carnegie Mellon University. CERT Insider Threat Center.

[27] Greitzer, F., Purl, J., Becker, D., Sticha, P & Leong, Y. (2019). Modeling Expert Judgments of Insider Threat Using Ontology Structure: Effects of Individual Indicator Threat Value and Class Membership. 52nd Hawaii International Conference on System Sciences.

[28] Nurse, J., Buckley, O., Legg, P., Goldsmith, M., Creese, S., Wrigth, G., & Whitty, M. (2014). Understanding Insider Threat: A Framework for Characterizing Attacks. Cyber Security Centre, Department of Computer Science, University of Oxford. Workshops. IEEE Security and Privacy Workshops.

[29] Kandias, M., Stavrou, V., Bozovic, N. & Gritzalis, D. 2013. Proactive Insider Threat Detection Through Social Media: The YouTube Case. 12th ACM workshop on Workshop on privacy in the electronic society.

[30] Moore, A. Cassidy, T., Theis, M., & Bauer, D. (2018). Balancing Organizational Incentives to Counter Insider Threat. CERT National Insider Threat Center Software Engineering Institute.

[31] Shaw, E. & Sellers, L. (2015) Application of the Critical-Path Method to Evaluate Insider Risks. Internal Security and Counterintelligence. Central Intelligence Agency. Studies in Intelligence Vol. 59.

[32] Lang, E. (2020). Seven (science-based) commandments for understanding and countering insider threats. Counter-Insider Threat Research and Practice (CITRAP). Personnel and Security Research Center (PERSEREC).

[33] Alneyadi, S., Sithirasenan, E., and Muthukkumarasamy, V. Detecting Data Semantic: A Data Leakage Prevention Approach. 2015 IEEE Trustcom.

[34] Powell, B. (2019). Malicious Overtones: Hunting Data Theft in the Frequency Domain with One-class Learning. ACM Transactions on Privacy and Security.

[35] Zhuang, H., Pan, H & Aberer, K H. Zhuang, R. Rahman, P. Hui and K. Aberer. (2020). Optimizing Information Leakage in Multicloud Storage Services. IEEE Transactions on Cloud Computing.