© MAR 2018 | IRE Journals | Volume 1 Issue 9 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV1I9-1713778

Conceptual Model for Insider Threat Classification and Risk Modeling in Complex Digital Systems

BISOLA AKEJU, JOSEPH EDIVRI[2], JOLLY I. OGBOLE[3], PRECIOUS OSOBHALENEWIE OKORUWA[4], OLADAPO FADAYOMI[5], TOYOSI O ABOLAJI[6]

[1]*Independent Researcher*
[2]*Microsoft Canada*
[3]*University of California, Berkeley, USA*
[4]*Independent Researcher*
[5]*ND Western Limited, Lagos, Nigeria*
[6]*Independent Researcher*

Abstract: ***Insider threats remain one of the most persistent and complex challenges in contemporary cybersecurity, particularly within highly interconnected, data-intensive, and adaptive digital environments. Unlike external attacks, insider threats originate from trusted identities with legitimate access, making detection, attribution, and mitigation inherently difficult. This proposes a conceptual model for insider threat classification and risk modeling tailored to complex digital systems, including cloud-native platforms, distributed enterprise architectures, and cyber–physical ecosystems. The model addresses critical limitations of existing approaches, which often rely on static classifications, isolated behavioral indicators, or retrospective analysis, and therefore struggle to capture the dynamic, contextual, and systemic nature of insider risk. The proposed framework integrates two tightly coupled layers: an insider threat classification layer and a dynamic risk modeling layer. The classification layer systematically categorizes insiders based on intent (malicious, negligent, or compromised), capability, access privilege, behavioral patterns, and temporal characteristics, leveraging multi-source data such as activity logs, system context, and behavioral deviations. The risk modeling layer conceptualizes insider risk as a probabilistic and continuously evolving construct, driven by the interaction between insider behavior, asset criticality, system interdependencies, and organizational controls. Advanced modeling approaches, including probabilistic inference, temporal risk scoring, and scenario-based analysis, are incorporated to account for uncertainty, nonlinearity, and cascading effects within complex digital systems. A central contribution of the model lies in its integration mechanism, where classification outcomes dynamically inform risk scores, while evolving risk profiles feedback into reclassification and monitoring priorities. This closed-loop design supports real-time risk awareness, adaptive control strategies, and proactive intervention. Additionally, the model explicitly incorporates governance, ethical, and privacy considerations to ensure responsible deployment within enterprise and critical infrastructure contexts. By providing a unified, system-oriented perspective, the conceptual model advances insider threat research and practice, offering a foundation for resilient security architectures, improved decision-making, and future empirical validation in high-velocity digital environments.***

Keywords: ***Insider Threat, Risk Modeling, Threat Classification, Complex Digital Systems, Cybersecurity Governance, Behavioral Analytics, Enterprise Security***

I. INTRODUCTION

Insider threats represent a critical and enduring challenge in contemporary cybersecurity, particularly within modern digital ecosystems characterized by extensive connectivity, data sharing, and automation (Buchanan, 2016; Livingstoneand Lewis,, 2016). An insider threat can be broadly defined as the risk posed by individuals or entities with legitimate access to an organization's information systems, data, or physical assets who intentionally or unintentionally cause harm. In modern contexts, insiders are no longer limited to direct employees but include contractors, third-party partners, service providers, and non-human identities such as applications and automated agents (Morris, 2015; Lemley, 2015). Insider threats may be malicious, driven by financial gain, espionage, or sabotage; negligent, resulting from human error or policy violations; or compromised, where legitimate credentials are exploited by external adversaries (Sandberg, 2015; Kennedy, 2017). The scope of insider threats thus spans technical, behavioral, and organizational dimensions, making them

fundamentally different from traditional external attacks.

Conventional security approaches have historically relied on perimeter-based defenses and signature-driven detection mechanisms (Heckmanet al., 2015Smithet al., 2017). These models assume a clear boundary between trusted internal environments and untrusted external networks, focusing on preventing unauthorized access through firewalls, intrusion detection systems, and known attack signatures. However, such approaches are increasingly inadequate for addressing insider threats. Since insiders operate within trusted boundaries and often use legitimate credentials, perimeter defenses provide limited protection, while signature-based systems struggle to detect novel, subtle, or context-dependent behaviors (Wittkop, 2016; Omopariola, 2017). Moreover, these models are predominantly reactive, identifying threats only after predefined patterns are matched or damage has occurred, thereby limiting their effectiveness against adaptive and low-and-slow insider activities.

The limitations of traditional security models are further amplified by the growing complexity of digital systems. Modern organizations operate within heterogeneous environments that integrate cloud computing, artificial intelligence, Internet of Things (IoT) devices, and cyber–physical systems (Heet al., 2016; Mourtzisand Vlachou, 2016). These environments are highly distributed, dynamically reconfigured, and data-intensive, with access privileges and system states changing continuously. Cloud-native architectures and microservices introduce ephemeral workloads and identity sprawl, while AI-driven systems automate decision-making processes that may amplify the impact of insider misuse. IoT and cyber–physical systems extend digital access into physical domains, increasing the potential for cascading and systemic consequences (Humayedet al., 2017; Blaschet al., 2017). In such settings, insider threats are no longer isolated events but can propagate across interconnected components, creating nonlinear and emergent risk patterns that are difficult to anticipate and manage.

These developments motivate the need for a unified conceptual model that integrates insider threat classification with dynamic risk modeling. Existing approaches often treat classification and risk assessment as separate or static processes, failing to capture the evolving nature of insider behavior and system context (Punithavathaniet al., 2015; Böseet al., 2017). A unified model enables the systematic categorization of insider threat types while simultaneously assessing their likelihood and potential impact within a specific operational environment. By linking behavioral indicators, access privileges, and system criticality to probabilistic risk representations, such a model supports continuous monitoring, adaptive prioritization, and proactive intervention (Zio, 2016; Mohsinet al., 2017).

The primary objective of this, is to develop a conceptual framework that addresses insider threats as dynamic, system-level risks rather than isolated security incidents. The proposed model contributes by (i) providing a structured classification of insider threats grounded in intent, capability, and context; (ii) introducing a dynamic risk modeling approach that accounts for uncertainty, temporal evolution, and system interdependencies; and (iii) integrating these components into a feedback-driven architecture suitable for complex digital ecosystems. Collectively, these contributions aim to enhance organizational resilience, improve decision quality, and advance the theoretical foundations of insider threat management in modern cybersecurity.

II. METHODOLOGY

The PRISMA methodology was applied to systematically identify, evaluate, and synthesize existing research relevant to the development of a conceptual model for insider threat classification and risk modeling in complex digital systems. The review process was designed to ensure transparency, reproducibility, and methodological rigor while capturing interdisciplinary insights from cybersecurity, information systems, risk management, behavioral science, and organizational studies.

A comprehensive literature search was conducted across multiple academic databases, including Scopus, Web of Science, IEEE Xplore, ACM Digital Library, SpringerLink, and ScienceDirect. These sources were selected to capture both technical and socio-organizational perspectives on insider threats. The

search strategy combined controlled vocabulary and free-text keywords related to insider threat, insider risk, malicious and non-malicious insiders, privilege misuse, behavioral analytics, risk modeling, complex digital systems, socio-technical systems, and cybersecurity governance. Boolean operators and truncation were used to ensure broad coverage while maintaining relevance. The search was limited to peer-reviewed journal articles, conference proceedings, and authoritative review papers published in English to ensure quality and comparability.

Eligibility criteria were defined prior to screening. Studies were included if they addressed insider threat classification, insider risk assessment, behavioral or technical indicators of insider activity, or risk modeling approaches applicable to complex or distributed digital environments. Both qualitative and quantitative studies were considered, provided they contributed conceptual, empirical, or methodological insights. Excluded were studies focused solely on external threats, purely legal or policy discussions without analytical relevance, opinion pieces lacking methodological grounding, and papers that addressed insider threats only at a superficial or anecdotal level. Duplicate records across databases were identified and removed during the initial screening phase.

The screening process followed the PRISMA flow logic, beginning with title and abstract review to assess topical relevance. Potentially eligible studies then underwent full-text assessment to confirm alignment with the inclusion criteria. Disagreements during screening were resolved through iterative reassessment based on predefined criteria, ensuring consistency and minimizing selection bias. The final corpus represented a balanced set of studies spanning technical detection mechanisms, behavioral frameworks, organizational risk factors, and probabilistic or qualitative risk modeling techniques.

Data extraction focused on capturing key attributes relevant to conceptual model development. Extracted information included definitions and typologies of insider threats, classification dimensions such as intent, access level, role, and behavioral patterns, data sources used for insider risk analysis, modeling approaches, and identified limitations. Additional attention was given to how studies addressed system complexity, interdependencies, and dynamic environments, as well as how uncertainty and incomplete information were treated in risk assessments.

The synthesis phase followed a qualitative thematic analysis approach. Extracted data were iteratively coded to identify recurring concepts, relationships, and gaps in the literature. Themes emerging across studies were integrated to inform the structure of the conceptual model, particularly the linkage between insider classification schemes, contextual risk factors, and dynamic risk modeling processes. Rather than aggregating findings statistically, the synthesis emphasized conceptual coherence and explanatory power, consistent with the goal of developing a unifying model.

Methodological quality and relevance were assessed qualitatively by considering clarity of definitions, transparency of assumptions, robustness of analytical methods, and applicability to real-world complex digital systems. This assessment informed the weighting of insights during synthesis, with greater emphasis placed on studies demonstrating empirical grounding or well-articulated theoretical frameworks.

By following the PRISMA methodology, this review provides a systematic and defensible foundation for the proposed conceptual model. The approach ensures that the model is grounded in existing evidence while explicitly addressing fragmentation, inconsistencies, and gaps in current insider threat classification and risk modeling research, thereby supporting both academic rigor and practical relevance.

2.1 Theoretical Foundations of Insider Threats

Insider threats occupy a unique position in cybersecurity theory and practice because they arise from trusted identities operating within legitimate organizational boundaries. Unlike external attackers, insiders possess varying degrees of authorized access, contextual knowledge, and operational familiarity, which fundamentally alters threat dynamics and complicates detection and mitigation. A rigorous theoretical foundation is therefore essential to understand the nature of insider threats, the mechanisms through which they manifest, and the

limitations of existing models in complex digital systems (Wanget al., 2015; Costaet al., 2016).

An insider threat can be defined as the risk of harm to an organization's information assets, systems, or operations caused by an entity with authorized or trusted access. This definition extends beyond direct employees to encompass contractors, partners, service providers, and non-human agents operating under delegated credentials. Insider threats are commonly categorized into several typologies based on intent, awareness, and method of exploitation.

Malicious insiders are individuals who intentionally misuse their access to cause harm. Their motivations may include financial gain, ideological alignment, revenge, or corporate espionage. Malicious insiders often plan their actions strategically, exploiting privileged access, system knowledge, and trust relationships to evade detection. From a theoretical standpoint, malicious insiders represent adversarial agents embedded within the system, blurring the distinction between internal users and external attackers.

Negligent insiders pose unintentional threats resulting from human error, poor judgment, or failure to follow security policies. Examples include misconfiguring systems, falling victim to phishing attacks, or mishandling sensitive data. Although lacking malicious intent, negligent insiders can cause damage comparable to deliberate attacks. Theoretical models increasingly recognize negligence as a systemic risk influenced by usability, training, and organizational culture rather than solely individual failure.

Compromised insiders occupy an intermediate category in which legitimate credentials or identities are exploited by external actors through coercion, social engineering, or malware (Soodet al., 2015; Onovo, 2015). In this case, the insider may be unaware of the misuse or may act under duress. This typology challenges traditional insider–outsider distinctions and highlights the importance of identity-centric and behavior-based detection approaches.

Third-party and privileged insiders represent a particularly high-risk group. Third-party insiders, such as vendors and contractors, often operate outside core governance structures while retaining significant access. Privileged insiders, including system administrators and executives, possess elevated rights that can amplify the impact of misuse. Theoretical frameworks emphasize that risk is not uniformly distributed across insider categories but is shaped by privilege concentration, access scope, and accountability mechanisms.

Understanding insider threats requires an interdisciplinary perspective that integrates behavioral science, technical analysis, and organizational theory. From a behavioral standpoint, insider threat research often draws on the "fraud triangle," which conceptualizes harmful behavior as the interaction of motivation, opportunity, and rationalization. Motivation may arise from personal stressors, perceived injustice, or ideological beliefs. Opportunity is created by excessive privileges, weak controls, or lack of monitoring. Rationalization allows individuals to justify harmful actions, often influenced by organizational norms or perceived inequities. Behavioral theories thus frame insider threats as socio-technical phenomena rather than purely technical exploits.

From a technical perspective, insider threats manifest through specific attack vectors and system abuse pathways. These include unauthorized data exfiltration, privilege escalation, sabotage of systems or data integrity, and misuse of legitimate tools for malicious purposes. In modern digital environments, insiders may exploit cloud management interfaces, application programming interfaces (APIs), machine learning pipelines, or cyber–physical control systems. Technical analysis highlights that insider attacks often mimic normal usage patterns, making anomaly detection and contextual analysis essential components of effective defense (Agrafiotiset al., 2016; Mehan, 2016).

Organizational factors play a decisive role in shaping insider threat risk. Security culture, governance structures, and access management practices influence both the likelihood and impact of insider actions. Weak governance, opaque decision-making, and inconsistent enforcement of policies can create environments where harmful behavior is more easily rationalized or overlooked. Conversely, strong ethical

norms, transparent oversight, and well-designed access structures can reduce opportunity and increase deterrence. Organizational theory therefore positions insider threats as emergent properties of institutional design, incentives, and control mechanisms.

Several conceptual and operational models have been proposed to structure insider threat analysis. Classical frameworks, such as the CERT Insider Threat Model, focus on lifecycle stages of insider activity, including predisposing factors, behavioral indicators, and attack execution. Other approaches adapt models like the Diamond Model to incorporate insider actors, assets, and capabilities. These models have contributed valuable insights into threat categorization and investigative processes.

However, significant gaps remain. Many existing models rely on static classifications and retrospective analysis, limiting their ability to capture the evolving nature of insider behavior in real time. Dynamic risk assessment is often underdeveloped, with limited incorporation of temporal changes, uncertainty, and system interdependencies. Contextual awareness—such as shifting access rights, workload sensitivity, and organizational changes—is frequently treated as ancillary rather than central to risk evaluation.

Most critically, there is a lack of integration between insider threat classification and real-time risk modeling. Classification schemes identify types of insiders, while risk models estimate potential impact, but these processes are rarely unified into a continuous, feedback-driven framework. As a result, organizations struggle to translate classification insights into actionable, prioritized risk responses. Addressing this gap requires conceptual models that explicitly link insider typologies to dynamic, system-aware risk representations suitable for complex digital environments.

2.2 Characteristics of Complex Digital Systems

Complex digital systems form the backbone of modern enterprises, critical infrastructure, and digital platforms (Oughtonet al., 2016; Barnset al., 2017). These systems are no longer monolithic or static; instead, they are highly distributed, adaptive, and deeply intertwined with organizational processes and physical environments. Their structural and operational characteristics fundamentally shape how risks emerge and propagate, with significant implications for insider threat detection and management.

Structural complexity in modern digital systems arises primarily from distributed architectures and heterogeneous technology stacks. Distributed architectures, particularly those based on microservices, decompose applications into loosely coupled services that communicate through APIs and messaging layers. While this modularity enhances scalability and resilience, it also increases the number of components, interactions, and trust relationships that must be secured. Each microservice may have its own access controls, dependencies, and data stores, creating a dense web of interconnections that complicates system-wide visibility.

Hybrid and multi-cloud environments further amplify structural complexity. Organizations increasingly operate across on-premises infrastructure, private clouds, and multiple public cloud providers. These environments differ in security models, logging capabilities, identity management mechanisms, and control granularity. As a result, security controls and monitoring data are often fragmented across platforms, making unified risk assessment and consistent policy enforcement difficult. From an insider threat perspective, this fragmentation can obscure anomalous behavior that spans multiple environments.

Cyber–physical system integration introduces another layer of complexity. Digital systems are now tightly coupled with physical processes in domains such as manufacturing, energy, healthcare, and transportation. Software actions can have direct physical consequences, and physical states can influence digital behavior. Insiders operating within such environments may exploit both cyber and physical access, blurring traditional boundaries and expanding the potential impact of malicious or negligent actions.

Operational complexity reflects how complex digital systems function and evolve over time. High-volume, high-velocity data flows are a defining feature, driven by pervasive logging, telemetry, user interactions, and

machine-to-machine communication. While this data is essential for security analytics, its scale and speed can overwhelm monitoring systems and analysts, increasing the risk that subtle insider indicators are lost in noise.

Continuous deployment and DevSecOps pipelines further contribute to operational complexity. Rapid release cycles, automated infrastructure provisioning, and frequent configuration changes mean that system states are constantly evolving. Security controls must adapt in near real time, and historical baselines can become obsolete quickly (Luoet al., 2015; McLaughlinet al., 2016). Insiders with knowledge of deployment processes may exploit short-lived misconfigurations or gaps introduced during rapid change.

Dynamic access rights and role evolution also characterize modern operations. Users frequently change roles, projects, and privilege levels, and access is increasingly granted on a just-in-time or context-aware basis. While this flexibility supports agility, it complicates the definition of "normal" behavior. Legitimate changes in access patterns can resemble malicious activity, while improper privilege accumulation may go unnoticed, challenging traditional rule-based detection approaches.

These structural and operational characteristics have profound risk implications for insider threat detection. Reduced visibility and attribution challenges are among the most significant. Distributed components, federated identities, and inconsistent logging make it difficult to reconstruct user actions end to end or attribute behavior to specific individuals with high confidence. Insiders may exploit these blind spots to mask intent or distribute actions across systems.

Cascading failures and systemic risk propagation are also heightened in complex digital systems. An insider action affecting a seemingly minor component can trigger downstream effects across interconnected services or physical processes. Such cascading impacts may far exceed the scope of the initial action, transforming localized misuse into systemic incidents.

Finally, complex systems exhibit nonlinear and emergent threat behaviors. Interactions between components, users, and controls can produce outcomes that are not predictable from individual elements alone. Insider threats may emerge gradually through the interaction of benign actions, organizational pressures, and technical vulnerabilities, rather than through overt malicious acts. This nonlinearity challenges static threat models and underscores the need for adaptive, context-aware, and system-level approaches to insider risk detection.

Together, these characteristics demonstrate why complex digital systems require fundamentally different analytical and governance approaches to insider threat management than traditional, centralized environments.

2.3 Insider Threat Classification Layer

The Insider Threat Classification Layer constitutes a foundational component of advanced security and risk management architectures, particularly in complex digital and cloud computing systems. Its primary function is to systematically identify, categorize, and characterize insider-related risks in a manner that supports early detection, proportional response, and accountable decision-making. Unlike traditional perimeter-focused security controls, this layer acknowledges that insiders—authorized users with legitimate accesscan pose risks that are diverse in motivation, capability, and manifestation. A rigorous classification framework therefore enables organizations to move beyond binary notions of "trusted" versus "untrusted" users toward a nuanced, evidence-driven understanding of insider behavior (Büchelet al., 2016; Canbeket al., 2017).

A robust insider threat classification model is multidimensional, integrating technical, behavioral, and contextual factors. One core dimension is intent, which differentiates between malicious insiders who deliberately seek to cause harm, negligent insiders whose actions unintentionally create vulnerabilities, and compromised insiders whose credentials or devices have been exploited by external adversaries. This distinction is critical, as each category implies different mitigation strategies, ranging from disciplinary and legal actions to training interventions or credential recovery.

A second dimension concerns capability and privilege level. Insiders vary significantly in their technical skills, system knowledge, and access rights. Highly privileged users such as system administrators or cloud architects can exert disproportionate impact, making even low-frequency misuse potentially catastrophic. Classification must therefore consider both formal privileges and informal capabilities, such as deep system familiarity or the ability to bypass controls.

The scope of access and asset sensitivity represents a third dimension. Insider activities should be assessed in relation to the criticality of the data, systems, or processes involved. Access to personally identifiable information, intellectual property, or safety-critical infrastructure carries higher inherent risk than access to low-sensitivity resources. Classification frameworks that incorporate asset sensitivity enable risk-based prioritization rather than uniform treatment of all anomalies.

Finally, temporal patterns provide insight into the persistence and evolution of insider behavior. Some threats manifest as persistent, long-term patterns of gradual misuse, while others are episodic, triggered by specific events such as organizational change or personal stressors. Temporal analysis helps distinguish between isolated anomalies and sustained campaigns, improving both detection accuracy and response proportionality.

Effective classification depends on the integration of diverse and high-quality data sources. User activity logs and audit trails form the technical backbone of insider threat analysis, capturing authentication events, data access, configuration changes, and transaction histories. These records provide objective, time-stamped evidence of actions taken within digital systems.

Complementing technical logs are behavioral and psychometric indicators, where ethically permissible and legally compliant. Such indicators may include deviations from established work patterns, abrupt changes in productivity, or indicators of heightened stress. While potentially valuable, the use of these data sources requires strict governance, transparency, and safeguards to prevent misuse or unjust profiling.

System context and role-based metadata further enrich classification by situating user actions within organizational structures and operational expectations. Role definitions, job functions, project assignments, and approval hierarchies help distinguish legitimate deviations from suspicious behavior (Azariaet al., 2015; Kingori and Gerrets, 2016). For example, elevated data access may be appropriate during a sanctioned audit but anomalous otherwise.

Finally, external signals such as threat intelligence feeds, industry benchmarks, and anomaly baselines provide contextual awareness beyond the organization's internal environment. These sources help calibrate classification models against known attack patterns and emerging risks, reducing blind spots caused by purely inward-looking analysis.

Given the scale and complexity of modern digital systems, manual insider threat classification is neither feasible nor reliable. Rule-based and expert systems offer an initial layer of automation, encoding organizational policies and expert knowledge into deterministic rules. While transparent and interpretable, these systems struggle with novel or evolving threat patterns.

Supervised and unsupervised learning models address this limitation by identifying statistical regularities and anomalies across large datasets. Supervised models can classify known threat types with high accuracy, while unsupervised approaches are particularly valuable for detecting previously unseen behaviors. However, their effectiveness depends on data quality, representativeness, and continuous tuning.

Increasingly, organizations adopt hybrid human–AI classification mechanisms, combining machine efficiency with human judgment. In such models, automated systems surface risk signals and preliminary classifications, which are then reviewed and contextualized by trained analysts. This approach balances scalability with accountability and reduces the risk of false positives.

Across all machine-assisted approaches, explainability and accountability are essential. Classification decisions can have significant organizational and personal consequences, making it

imperative that models provide interpretable rationales and are subject to governance, auditability, and ethical oversight. An effective Insider Threat Classification Layer thus integrates advanced analytics with principled design, supporting security objectives while respecting individual rights and organizational trust.

2.4 Insider Risk Modeling Layer

The insider risk modeling layer represents a critical component of a comprehensive framework for managing insider threats in complex digital systems. While the classification layer focuses on categorizing insiders according to intent, behavior, and access privileges, the risk modeling layer translates these classifications into actionable insights by quantifying the likelihood, potential impact, and systemic consequences of insider activities. This layer enables organizations to prioritize monitoring, allocate security resources effectively, and implement targeted mitigation strategies within dynamic operational environments.

Risk, in the context of insider threats, is most effectively conceptualized as a function of likelihood, impact, and exposure. Likelihood refers to the probability that a specific insider, or class of insiders, will engage in harmful activity, while impact denotes the potential severity of consequences, including data breaches, operational disruption, financial loss, or reputational damage. Exposure represents the extent to which organizational assets are accessible or vulnerable to insider actions. By integrating these dimensions, risk modeling provides a multidimensional perspective that goes beyond binary threat detection, allowing organizations to evaluate both the probability and severity of potential events (Jouiniet al., 2015; Zuechet al., 2015).

Given the dynamic and stochastic nature of insider behavior, risk representation must be probabilistic and adaptive rather than deterministic. Insider actions are influenced by evolving motivations, system interactions, and contextual variables, creating uncertainty that requires continuous risk assessment. Risk scores must therefore incorporate time-sensitive inputs, such as changing access privileges, real-time behavioral anomalies, and system dependencies, to provide an up-to-date view of organizational vulnerability. Additionally, risk assessments can be asset-centric, focusing on individual critical resources and their sensitivity, or system-wide, considering cascading effects, interdependencies, and potential systemic failures arising from insider misuse. This dual perspective ensures both granular and holistic understanding of risk across complex digital ecosystems.

The risk modeling layer leverages multiple categories of factors and variables to quantify insider threat potential. Behavioral deviations and anomaly scores form a primary input, capturing unusual patterns of activity that may indicate intentional or inadvertent misuse. Such indicators can include abnormal file access, atypical login times, or irregular communication patterns, which are interpreted relative to baseline behavioral models.

Access privilege concentration and escalation paths are another critical determinant of insider risk. Users with elevated privileges, or those capable of escalating privileges through system misconfigurations, pose higher potential risk due to their ability to bypass standard controls. Risk modeling must account for privilege distribution, access hierarchies, and potential pathways for lateral movement.

System criticality and interdependencies further influence risk quantification. The potential impact of insider actions depends on the importance of the assets involved and their connectivity to other components. Highly interdependent systems, such as cloud-based platforms, IoT networks, or integrated operational technology, can amplify the effects of a single insider incident, creating cascading failures.

Finally, organizational controls and deterrence mechanisms modify risk outcomes. Policies, monitoring tools, auditing protocols, and ethical culture act as mitigating factors, reducing the likelihood or potential impact of insider activity. A robust risk model incorporates both technical controls and organizational influences to provide a more accurate, context-aware assessment.

Effective insider risk modeling relies on advanced analytical and probabilistic techniques capable of capturing uncertainty and system complexity.

Bayesian networks and probabilistic graphical models allow for representation of dependencies among multiple variables, enabling dynamic updating of risk estimates as new information becomes available (Farasatet al., 2015; Sperottoet al., 2017). These models can integrate behavioral, technical, and organizational inputs to compute posterior probabilities of harmful insider events.

Dynamic risk scoring and temporal models extend these approaches by incorporating time-sensitive factors, such as changes in behavior, access privileges, or system states. Temporal modeling captures the evolution of risk over time, allowing organizations to identify emerging threats before they manifest.

Scenario-based and simulation-driven assessment further enriches risk modeling by exploring hypothetical attack vectors, privilege escalations, or cascading failures. Monte Carlo simulations, agent-based models, and system dynamics techniques allow practitioners to quantify potential impacts under varying assumptions, providing insights into both expected and extreme outcomes.

Finally, the integration of uncertainty and incomplete information is critical in realistic operational environments. Insider actions may be partially observable, and behavioral signals can be noisy or ambiguous. Probabilistic models, stochastic simulations, and Bayesian updating provide mechanisms to estimate risk under incomplete knowledge, supporting informed decision-making even in complex and high-velocity digital systems.

By combining these conceptual foundations, variables, and modeling techniques, the insider risk modeling layer translates classification outputs into actionable risk intelligence, enabling continuous, adaptive, and context-aware management of insider threats across modern enterprises.

2.5 Integration of Classification and Risk Modeling

The integration of insider threat classification and risk modeling represents a critical evolution in cybersecurity for complex digital systems. Rather than treating threat identification and risk assessment as separate processes, contemporary approaches recognize that combining these functions can enhance both accuracy and operational effectiveness (Aven, 2016; Patriarcaet al., 2017). By linking classification outcomes to quantifiable risk measures, organizations can develop dynamic, context-aware, and prioritized mitigation strategies that adapt to evolving system states and user behaviors.

At the core of this integration are feedback loops between classification outcomes and risk scores. Insider threat classification categorizes user behavior into patterns such as malicious, negligent, or anomalous but non-malicious. Each classification outcome carries an associated risk profile that reflects potential impact, likelihood of occurrence, and exposure within the organizational environment. Risk scores derived from these outcomes are not static; they are continuously refined as additional behavioral data and system context become available. Feedback loops enable iterative learning: when risk scores indicate elevated likelihood or potential impact, classification models can adjust thresholds, incorporate new indicators, or recalibrate weights assigned to behavioral features. This continuous refinement ensures that classification outputs remain sensitive to both known attack patterns and emerging, previously unobserved behaviors, enhancing predictive accuracy and reducing false positives (Awad and Khanna, 2015; Junejo and Goh, 2016).

Continuous updating through real-time monitoring is essential to operationalizing the integration of classification and risk modeling. Modern distributed systems generate massive streams of telemetry, logs, and contextual data. By leveraging this data in real time, risk scores can reflect the current state of the system and the evolving behavior of users. For example, a sudden access attempt to a high-value repository, anomalous data exfiltration patterns, or deviations from typical operational workflows can immediately trigger reclassification and risk reassessment. This dynamic updating allows security teams to move beyond periodic, static assessments that quickly become outdated. Furthermore, real-time integration supports early detection of complex insider attack scenarios that unfold over time and across multiple system components, enabling proactive intervention before minor anomalies escalate into significant incidents.

A key advantage of this integrated approach is risk-driven prioritization of insider threat categories. Not all anomalies or classified behaviors carry equal risk. By combining classification outputs with quantitative or probabilistic risk measures, organizations can rank insider threats according to potential harm, systemic impact, or strategic relevance. For instance, a low-level misconfiguration by a junior employee may be classified as anomalous but carries minimal risk, whereas unauthorized access to sensitive financial data by a privileged administrator represents a high-risk category requiring immediate attention. Prioritization ensures that limited security resources are focused on the most consequential threats, improving operational efficiency and enabling faster remediation. Additionally, prioritization can account for dependencies within distributed systems, recognizing that seemingly minor actions may propagate risk through interconnected services or critical infrastructure (Petitet al., 2015; Korkaliet al., 2017).

The alignment with security operations and response workflows completes the integration. Risk-informed classification outputs must translate into actionable insights within the organization's security operations framework. Integration with incident response, vulnerability management, and access control workflows allows for automated or semi-automated interventions, such as enforcing temporary access restrictions, triggering forensic investigation, or adjusting monitoring sensitivity. By embedding classification and risk outputs directly into operational workflows, organizations create a closed-loop system in which detection, assessment, and response are continuously informed by real-time data and evolving threat context. This alignment not only improves response speed but also ensures that risk management decisions are consistent with organizational policies, regulatory requirements, and broader enterprise risk strategies.

Together, these elements—feedback loops, continuous updating, risk-driven prioritization, and alignment with operational workflows—form a cohesive framework for integrating insider threat classification and risk modeling. This integration transforms reactive security measures into adaptive, predictive, and resource-optimized strategies. By connecting behavioral insights to quantified risk and embedding them into operational processes, organizations can detect, prioritize, and mitigate insider threats more effectively, even within complex, dynamic, and distributed digital environments (Chenet al., 2015; Ravi and Kamaruddin, 2017). The approach also establishes a foundation for ongoing improvement, as each incident, anomaly, or near miss informs subsequent iterations of the model, reinforcing resilience and strategic cyber risk management.

2.6 Governance, Ethics, and Trust Considerations

In modern digital and cloud computing systems, effective security engineering extends far beyond technical safeguards to encompass governance, ethics, and trust considerations. These dimensions are critical for ensuring that organizational practices not only protect information assets but also uphold legal obligations, societal norms, and stakeholder confidence. Governance and ethical frameworks establish the boundaries within which technical solutions operate, providing accountability, fairness, and transparency while guiding responsible use of sensitive data. As organizations increasingly adopt data-intensive technologiesincluding machine learning-driven classification systems and behavioral analyticsthe integration of these considerations becomes indispensable for sustainable and trustworthy security operations (Ramprasadet al., 2017; Lockwoodet al., 2017).

A cornerstone of ethical security governance is privacy-preserving data collection and analysis. Organizations must ensure that data acquisition aligns with principles of minimization, purpose limitation, and proportionality, collecting only information necessary for defined objectives. Techniques such as data anonymization, pseudonymization, differential privacy, and secure multiparty computation enable organizations to perform meaningful analysis without exposing sensitive individual information. In practice, these approaches reduce the risk of re-identification and data breaches while maintaining analytical utility for detecting insider threats or anomalous behaviors. Privacy-preserving strategies also support regulatory compliance with frameworks such as GDPR, CCPA,

and NDPR, which mandate the protection of personal information throughout its lifecycle.

Ethical governance further requires deliberate attention to bias mitigation and fairness in automated classification models. Machine learning systems trained on historical data may inadvertently perpetuate biases, leading to disproportionate risk assessments for particular individuals or groups (Kim, 2016; Barocas and Selbst, 2016). For example, models that interpret behavioral deviations without contextual awareness may unfairly flag employees with atypical work patterns as potential threats. Addressing these issues involves both technical and organizational interventions: algorithmic fairness techniques, such as reweighting, counterfactual modeling, or adversarial debiasing, can reduce skewed outcomes, while ongoing monitoring and validation ensure models remain equitable over time. Embedding fairness as a design principle reinforces trust, demonstrates ethical stewardship, and mitigates reputational and legal risks associated with discriminatory practices.

Legal and regulatory compliance forms the structural backbone of governance in digital and cloud environments. Security programs must adhere to a growing landscape of obligations encompassing privacy, cybersecurity, labor law, and sector-specific regulations. Compliance requires organizations to establish policies for data retention, access control, breach reporting, and employee monitoring that are consistent with statutory frameworks. Regulatory standards such as ISO 27001, NIST SP 800-53, and the Cloud Security Alliance's Cloud Controls Matrix provide guidance on governance structures, risk management practices, and control implementation. Proactive compliance not only prevents legal penalties but also aligns organizational processes with industry best practices, reinforcing accountability and providing defensible positions in audit or litigation scenarios.

Transparency and explainability are vital for sustaining organizational trust in security operations. Stakeholders including employees, customers, auditors, and regulators must be able to understand how classification decisions are made, particularly when automated analytics or AI-driven systems are involved. Explainable models offer interpretable rationales for risk assessments, enabling validation and reducing the perception of arbitrariness or bias. Organizations can further enhance trust through clear communication of data collection policies, consent mechanisms, and monitoring practices, ensuring that users understand their rights and the purposes of data processing. Establishing an ethical governance culture, where accountability is explicit and traceable, strengthens confidence in security programs and supports a collaborative environment where insider threat mitigation does not erode morale or engagement.

Integrating governance, ethics, and trust considerations requires a multidisciplinary approach combining policy, technical controls, and organizational culture. Governance structures should define roles and responsibilities for privacy, compliance, and ethical oversight, while ethics committees or data stewardship teams can provide review and guidance on sensitive analytical practices. Training programs and awareness campaigns help embed ethical and privacy-conscious behavior across the workforce, complementing technical measures. By systematically aligning operational practices with ethical principles and regulatory requirements, organizations can achieve a security posture that is not only effective but also socially responsible, legally sound, and trusted by stakeholders.

Governance, ethics, and trust are essential pillars of privacy-centric security engineering. Privacy-preserving analytics, fairness in classification models, compliance with regulatory frameworks, and transparent decision-making collectively ensure that security operations are effective, accountable, and aligned with societal expectations. These considerations transform security from a purely technical challenge into a holistic organizational capability, enabling digital and cloud computing systems to operate securely, responsibly, and with the confidence of all stakeholders. By embedding these principles into design and operational practices, organizations can reconcile the tension between robust security, privacy protection, and ethical responsibility, fostering sustainable trust in complex technological environments (Grayand Boling, 2016; Andersonet al., 2017).

2.7 Research and Practical Implications

The conceptual model for insider threat classification and risk modeling in complex digital systems offers significant contributions to both cybersecurity theory and enterprise practice, bridging the gap between abstract threat understanding and operational risk management. From a theoretical perspective, the model advances existing frameworks by integrating classification and dynamic risk assessment into a unified, feedback-driven architecture. Traditional approaches often treat insider threats in isolation, focusing either on behavioral typologies or risk quantification. By combining these dimensions, the model enhances our understanding of insider threats as dynamic, context-dependent phenomena, enabling a richer conceptualization of risk propagation, threat interdependencies, and emergent behaviors within complex digital systems. This integration contributes to risk science by offering a systematic methodology to quantify and predict threat likelihood, potential impact, and cascading consequences in environments characterized by uncertainty, high connectivity, and rapid operational change. Furthermore, the incorporation of probabilistic, temporal, and scenario-based modeling advances the epistemological foundations of cybersecurity, providing a robust framework for studying threats that cannot be captured through static or deterministic models (Simonand de Goede, 2015; Modarreset al., 2017).

The model also carries important implications for security architecture and policy design. By mapping insider threat classifications to risk profiles and organizational controls, it supports the development of identity-aware, context-sensitive architectures that go beyond perimeter-based defenses. Security controls can be strategically aligned with the most critical assets and the highest-risk insider categories, ensuring efficient allocation of monitoring, auditing, and response resources. In practical terms, this enables organizations to implement adaptive access controls, dynamic monitoring policies, and just-in-time interventions that respond to evolving risk conditions rather than relying solely on preconfigured rules or historical patterns. Policy design benefits similarly: the model provides a structured methodology for defining risk thresholds, prioritizing mitigation strategies, and linking operational security measures to enterprise risk appetite and compliance requirements. As such, the framework serves as a bridge between technical implementation, governance oversight, and regulatory alignment, offering a blueprint for policy that is both enforceable and responsive to real-time threat dynamics.

A further practical implication is the model's capacity to support proactive and adaptive insider risk management. Unlike conventional reactive approaches, which detect threats post-incident, this framework enables continuous risk assessment and early warning. Behavioral anomalies, privilege escalations, and system interdependencies are continuously analyzed within a probabilistic risk context, allowing organizations to anticipate high-risk scenarios and intervene before harm occurs. The adaptive nature of the model also accommodates evolving operational environments, such as hybrid cloud infrastructures, AI-driven automation, and dynamic workforce models. By continuously updating threat classifications and risk scores, organizations can maintain situational awareness, prioritize high-impact threats, and tailor mitigation strategies to the most relevant insiders, thereby reducing exposure and enhancing operational efficiency (Allenand Derr, 2015; Mennenand Van Tuyll, 2015).

Finally, the model contributes directly to resilience and digital trust enhancement. Resilience in complex digital systems depends not only on preventing incidents but also on the capacity to withstand, absorb, and recover from insider-induced disruptions. By integrating dynamic risk modeling with classification insights, the framework facilitates rapid detection of emerging threats, informed prioritization of mitigation efforts, and scenario-based planning for potential impacts. In turn, this supports organizational trust, both internally and externally. Employees, customers, and partners gain confidence that sensitive information and critical operations are safeguarded through structured, evidence-based, and responsive security practices. Moreover, the explicit consideration of governance, ethical, and compliance factors strengthens confidence in the responsible and accountable management of insider risk.

The conceptual model advances cybersecurity theory, informs architectural and policy design, enables

proactive and adaptive risk management, and strengthens enterprise resilience and digital trust. By providing a unified, system-aware, and context-sensitive framework, it offers both theoretical and operational value, laying the foundation for more effective insider threat mitigation in increasingly complex and interconnected digital ecosystems.

2.8 Future Research Directions

As digital systems grow increasingly distributed, dynamic, and critical to organizational operations, the field of insider threat classification and risk modeling faces both unprecedented challenges and transformative opportunities (Johnson, 2016; Porterand Heppelmann, 2015). While contemporary approaches have advanced through risk-informed classification, real-time monitoring, and integrated response workflows, emerging technologies, organizational trends, and complex socio-technical interactions highlight several directions for future research. These directions aim to enhance predictive accuracy, operational efficiency, and strategic resilience against insider threats.

A key area for exploration is the development of autonomous and self-learning insider risk systems. Current risk models often rely on static rules, manually curated indicators, or periodic updates informed by historical data. Autonomous systems, leveraging artificial intelligence (AI) and machine learning (ML), can continuously adapt to evolving user behaviors, environmental contexts, and threat landscapes. Self-learning models can detect previously unobserved patterns of risk, identify subtle precursors to insider misuse, and dynamically recalibrate risk scores based on outcomes from interventions or incident investigations. Future research can investigate techniques for online learning in high-velocity, high-volume environments, hybrid human–AI decision-making architectures, and the mitigation of algorithmic biases that could lead to false positives or discriminatory outcomes. In particular, reinforcement learning and adversarial simulation may provide pathways for modeling complex insider behaviors and anticipating attack vectors before they manifest.

Another promising avenue is the integration with zero-trust and continuous authentication models. Zero-trust architectures challenge traditional perimeter-based security by assuming that no actor or device should be inherently trusted, instead requiring continuous verification of identity, context, and behavior. Integrating insider risk models with zero-trust systems enables dynamic adjustment of access privileges and risk mitigation strategies in real time. Future studies can explore how behavioral classification outputs, anomaly detection, and risk scoring can be embedded into continuous authentication mechanisms, session management, and adaptive access control policies. Such integration also raises important questions regarding the trade-offs between usability, security, and privacy, necessitating rigorous evaluation frameworks that balance risk reduction with operational efficiency.

A further critical research direction involves cross-organizational and supply-chain insider risk modeling. Modern enterprises operate within complex ecosystems, relying on third-party vendors, contractors, cloud providers, and collaborative platforms. Insider threats may not be confined to internal employees but can originate from partners with privileged access or indirect influence over critical systems. Future research should examine methods for federated risk modeling, secure data-sharing protocols, and distributed analytics that preserve confidentiality while enabling holistic assessment of insider risk across organizational boundaries (Fabianet al., 2015; Malikireddyand Algubelli, 2017). Techniques such as privacy-preserving machine learning, secure multiparty computation, and standardized incident taxonomy frameworks can provide avenues for robust modeling in multi-stakeholder contexts.

Equally important are human-centered and socio-technical extensions to existing models. Insider threats are fundamentally rooted in human behavior, motivation, and organizational context, yet many current models emphasize technical or quantitative indicators. Future research can focus on integrating psychological, organizational, and social factors into risk modeling, such as employee stress, job dissatisfaction, role ambiguity, and cultural influences on security compliance. Multi-modal data sources—including communication patterns, workflow interactions, and social network analytics—can enrich predictive models while ensuring ethical and privacy-

compliant implementation. Socio-technical extensions can also explore intervention strategies that combine behavioral nudges, training, and organizational redesign with automated detection, creating holistic mitigation frameworks that address both technical and human dimensions of insider risk.

Finally, future research should emphasize empirical validation and longitudinal studies of these emerging approaches. Autonomous systems, zero-trust integration, supply-chain modeling, and human-centered extensions all require real-world testing across diverse environments to assess predictive performance, operational feasibility, and ethical implications. Comparative studies across sectors, such as finance, healthcare, and critical infrastructure, can illuminate contextual dependencies and generalizability, while simulation-based studies can explore rare or high-impact scenarios that are difficult to observe in practice.

The next frontier in insider threat classification and risk modeling lies in the convergence of autonomous learning, continuous verification, ecosystem-wide awareness, and socio-technical understanding (O'Brolcháinet al., 2016; Lawless and Sofge, 2017). Research in these areas promises to transform insider risk management from reactive detection to proactive, adaptive, and resilient strategies, capable of addressing both technical vulnerabilities and human factors. By advancing these directions, the field can better equip organizations to navigate the growing complexity of digital systems, safeguard critical assets, and foster trust in increasingly interconnected operational environments.

III. CONCLUSION

The conceptual model for privacy-centric insider threat classification and security engineering provides a structured, multi-layered framework for managing risks posed by insiders in complex digital and cloud computing environments. By integrating dimensions of intent, capability, access scope, and temporal behavior, the model enables organizations to systematically categorize and assess insider threats, moving beyond simplistic binary notions of trusted versus untrusted users. Its incorporation of diverse data sources—including system logs, behavioral indicators, role metadata, and external threat intelligence—supports a comprehensive, evidence-based classification strategy. Furthermore, the model emphasizes the role of machine-assisted approaches, combining rule-based systems, supervised and unsupervised learning, and hybrid human–AI mechanisms to achieve scalable, accurate, and accountable classification outcomes. This layered approach allows organizations to align technical detection capabilities with privacy-preserving principles, ethical governance, and regulatory compliance, ensuring that insider threat management respects both organizational and individual rights.

Compared to existing insider threat approaches, the proposed model offers several notable advancements. Traditional frameworks often rely on either purely technical controls or post-incident response, lacking integration with behavioral analysis, temporal patterns, or contextual metadata. In contrast, this model embeds privacy, ethics, and trust considerations throughout the classification process, mitigating biases and promoting transparency. Its use of hybrid machine-assisted classification enables adaptive learning from evolving patterns of behavior while retaining human oversight, thereby reducing false positives and enhancing operational confidence. By bridging technical, organizational, and ethical dimensions, the model provides a holistic solution that is both proactive and resilient, addressing the limitations of conventional insider threat programs.

In final reflection, managing insider risk in complex digital systems requires a shift from reactive monitoring to strategic, privacy-conscious, and ethically governed risk management. The conceptual model demonstrates that effective insider threat mitigation is not solely a technical challenge but a socio-technical endeavor, integrating analytics, governance, and trust. Its implementation empowers organizations to detect, classify, and respond to insider risks responsibly, preserving system integrity while maintaining stakeholder confidence. As digital and cloud ecosystems continue to evolve, such comprehensive frameworks will be essential for ensuring that insider threat management remains robust, fair, and sustainable, supporting secure and trustworthy operations in increasingly complex technological landscapes.

REFERENCES

[1] Agrafiotis, I., Nurse, J.R., Buckley, O., Legg, P., Creese, S. and Goldsmith, M., 2015. Identifying attack patterns for insider threat detection. Computer Fraud & Security, 2015(7), pp.9-17.

[2] Allen, G. and Derr, R., 2015. Threat assessment and risk analysis: an applied approach. Butterworth-Heinemann.

[3] Anderson, C., Baskerville, R.L. and Kaul, M., 2017. Information security control theory: Achieving a sustainable reconciliation between sharing and protecting the privacy of information. Journal of Management Information Systems, 34(4), pp.1082-1112.

[4] Aven, T., 2016. Risk assessment and risk management: Review of recent advances on their foundation. European journal of operational research, 253(1), pp.1-13.

[5] Awad, M. and Khanna, R., 2015. Efficient learning machines: theories, concepts, and applications for engineers and system designers (p. 268). Springer nature.

[6] Azaria, A., Richardson, A., Kraus, S. and Subrahmanian, V.S., 2015. Behavioral analysis of insider threat: A survey and bootstrapped prediction in imbalanced data. IEEE Transactions on Computational Social Systems, 1(2), pp.135-155.

[7] Barns, S., Cosgrave, E., Acuto, M. and Mcneill, D., 2017. Digital infrastructures and urban governance. Urban Policy and research, 35(1), pp.20-31.

[8] Barocas, S. and Selbst, A.D., 2016. Big data's disparate impact. Calif. L. Rev., 104, p.671.

[9] Blasch, E., Kadar, I., Grewe, L.L., Brooks, R., Yu, W., Kwasinski, A., Thomopoulos, S., Salerno, J. and Qi, H., 2017, May. Panel summary of cyber-physical systems (cps) and internet of things (iot) opportunities with information fusion. In Signal Processing, Sensor/Information Fusion, and Target Recognition XXVI (Vol. 10200, pp. 171-188). SPIE.

[10] Böse, B., Avasarala, B., Tirthapura, S., Chung, Y.Y. and Steiner, D., 2017. Detecting insider threats using radish: A system for real-time anomaly detection in heterogeneous data streams. IEEE Systems Journal, 11(2), pp.471-482.

[11] Buchanan, B., 2016. The cybersecurity dilemma: Hacking, trust, and fear between nations. Oxford University Press.

[12] Büchel, F., Humprecht, E., Castro-Herrero, L., Engesser, S. and Brüggemann, M., 2016. Building empirical typologies with QCA: Toward a classification of media systems. The international journal of press/politics, 21(2), pp.209-232.

[13] Canbek, G., Sagiroglu, S., Temizel, T.T. and Baykal, N., 2017, October. Binary classification performance measures/metrics: A comprehensive visualized roadmap to gain new insights. In 2017 International Conference on Computer Science and Engineering (UBMK) (pp. 821-826). IEEE.

[14] Chen, W.J., Kamath, R., Kelly, A., Lopez, H.H.D., Roberts, M. and Yheng, Y.P., 2015. Systems of insight for digital transformation: Using IBM operational decision manager advanced and predictive analytics. IBM Redbooks.

[15] Costa, D.L., Albrethsen, M.J. and Collins, M.L., 2016. Insider threat indicator ontology (No. CMUSEI2016TR007).

[16] Fabian, B., Ermakova, T. and Junghanns, P., 2015. Collaborative and secure sharing of healthcare data in multi-clouds. Information Systems, 48, pp.132-150.

[17] Farasat, A., Nikolaev, A., Srihari, S.N. and Blair, R.H., 2015. Probabilistic graphical models in modern social network analysis. Social Network Analysis and Mining, 5(1), p.62.

[18] Gray, C.M. and Boling, E., 2016. Inscribing ethics and values in designs for learning: a problematic. Educational technology research and development, 64(5), pp.969-1001.

[19] He, H., Maple, C., Watson, T., Tiwari, A., Mehnen, J., Jin, Y. and Gabrys, B., 2016, July. The security challenges in the IoT enabled cyber-physical systems and opportunities for evolutionary computing & other computational intelligence. In 2016 IEEE congress on evolutionary computation (CEC) (pp. 1015-1021). IEEE.

[20] Heckman, K.E., Stech, F.J., Thomas, R.K., Schmoker, B. and Tsow, A.W., 2015. Cyber denial, deception and counter deception. Advances in Information Security, 64.

[21] Humayed, A., Lin, J., Li, F. and Luo, B., 2017. Cyber-physical systems security—A survey. IEEE Internet of Things Journal, 4(6), pp.1802-1831.

[22] Johnson, M., 2016. Cyber crime, security and digital intelligence. Routledge.

[23] Jouini, M., Rabai, L.B.A. and Khedri, R., 2015. A multidimensional approach towards a quantitative assessment of security threats. Procedia Computer Science, 52, pp.507-514.

[24] Junejo, K.N. and Goh, J., 2016, May. Behaviour-based attack detection and classification in cyber physical systems using machine learning. In Proceedings of the 2nd ACM international workshop on cyber-physical system security (pp. 34-43).

[25] Kennedy, K.A., 2017. Management and mitigation of insider threats. In Handbook of Behavioral Criminology (pp. 485-499). Cham: Springer International Publishing.

[26] Kim, P.T., 2016. Data-driven discrimination at work. Wm. & Mary L. Rev., 58, p.857.

[27] Kingori, P. and Gerrets, R., 2016. Morals, morale and motivations in data fabrication: Medical research fieldworkers views and practices in two Sub-Saharan African contexts. Social science & medicine, 166, pp.150-159.

[28] Korkali, M., Veneman, J.G., Tivnan, B.F., Bagrow, J.P. and Hines, P.D., 2017. Reducing cascading failure risk by increasing infrastructure network interdependence. Scientific reports, 7(1), p.44499.

[29] Lawless, W.F. and Sofge, D.A., 2017. Evaluations: autonomy and artificial intelligence: a threat or savior?. In Autonomy and artificial intelligence: a threat or savior? (pp. 295-316). Cham: Springer International Publishing.

[30] Lemley, M.A., 2015. IP in a World without Scarcity. NyUL Rev., 90, p.460.

[31] Livingstone, D. and Lewis, P., 2016. Space, the Final Frontier for Cybersecurity?. Chatham House. The Royal Institute of International Affairs.

[32] Lockwood, G.K., Hazen, D., Koziol, Q., Canon, R.S., Antypas, K., Balewski, J., Balthaser, N., Bhimji, W., Botts, J., Broughton, J. and Butler, T.L., 2017. Storage 2020: A vision for the future of hpc storage.

[33] Luo, F., Zhao, J., Dong, Z.Y., Chen, Y., Xu, Y., Zhang, X. and Wong, K.P., 2015. Cloud-based information infrastructure for next-generation power grid: Conception, architecture, and applications. IEEE Transactions on Smart Grid, 7(4), pp.1896-1912.

[34] Malikireddy, S.K.R. and Algubelli, B.R., 2017. Multidimensional privacy preservation in distributed computing and big data systems: Hybrid frameworks and emerging paradigms. International Journal of Scientific Research in Science and Technology, 3(4), pp.2395-602.

[35] McLaughlin, S., Konstantinou, C., Wang, X., Davi, L., Sadeghi, A.R., Maniatakos, M. and Karri, R., 2016. The cybersecurity landscape in industrial control systems. Proceedings of the IEEE, 104(5), pp.1039-1057.

[36] Mehan, J., 2016. Insider threat: A guide to understanding, detecting, and defending against the enemy from within. IT Governance Ltd.

[37] Mennen, M.G. and Van Tuyll, M.C., 2015. Dealing with future risks in the Netherlands: the National Security Strategy and the National Risk Assessment. Journal of Risk Research, 18(7), pp.860-876.

[38] Modarres, M., Kim, I.S., Ganguly, A. and Assessment, R., 2017. 4.2 Methodological Approaches in PRA for Critical Infrastructure. School of Social Sciences, p.33.

[39] Mohsin, M., Sardar, M.U., Hasan, O. and Anwar, Z., 2017. IoTRiskAnalyzer: A probabilistic model checking based framework for formal risk analytics of the Internet of Things. IEEE Access, 5, pp.5494-5505.

[40] Morris, J.W., 2015. Curation by code: Infomediaries and the data mining of taste. European journal of cultural studies, 18(4-5), pp.446-463.

[41] Mourtzis, D. and Vlachou, E., 2016. Cloud-based cyber-physical systems and quality of services. The TQM Journal, 28(5), pp.704-733.

[42] O'Brolcháin, F., Jacquemard, T., Monaghan, D., O'Connor, N., Novitzky, P. and Gordijn, B., 2016. The convergence of virtual reality and social networks: threats to privacy and autonomy. Science and engineering ethics, 22(1), pp.1-29.

[43] Omopariola, M., 2017. AI-Enhanced Threat Detection for National-Scale Cloud Networks: Frameworks, Applications, and Case Studies. ResearchGate Preprint.

[44] Onovo, A.A., Nta, I.E., Onah, A.A., Okolo, C.A., Aliyu, A., Dakum, P., Atobatele, A.O. and Gado, P., 2015. Partner HIV serostatus disclosure and determinants of serodiscordance among prevention of mother to child transmission clients in Nigeria. BMC public health, 15(1), p.827.

[45] Oughton, E.J., Tran, M.A.R.T.I.N.O., Jones, C.B. and Ebrahimy, R.A.Z.G.A.R., 2016. Digital communications and information systems. In The Future of National Infrastructure (p. 181). Cambridge University Press.

[46] Patriarca, R., Bergström, J. and Di Gravio, G., 2017. Defining the functional resonance analysis space: Combining Abstraction Hierarchy and FRAM. Reliability Engineering & System Safety, 165, pp.34-46.

[47] Petit, F., Verner, D., Brannegan, D., Buehring, W., Dickinson, D., Guziel, K., Haffenden, R., Phillips, J. and Peerenboom, J., 2015. Analysis of critical infrastructure dependencies and interdependencies (No. ANL/GSS-15/4). Argonne National Laboratory (ANL), Argonne, IL (United States).

[48] Porter, M.E. and Heppelmann, J.E., 2015. How smart, connected products are transforming companies. Harvard business review, 93(10), pp.96-114.

[49] Punithavathani, D.S., Sujatha, K. and Jain, J.M., 2015. Surveillance of anomaly and misuse in critical networks to counter insider threats using computational intelligence. Cluster Computing, 18(1), pp.435-451.

[50] Ramprasad, R., Batra, R., Pilania, G., Mannodi-Kanakkithodi, A. and Kim, C., 2017. Machine learning in materials informatics: recent applications and prospects. npj Computational Materials, 3(1), p.54.

[51] Ravi, V. and Kamaruddin, S., 2017, November. Big data analytics enabled smart financial services: opportunities and challenges. In International conference on big data analytics (pp. 15-39). Cham: Springer International Publishing.

[52] Sandberg, J., 2015. Human element of corporate espionage risk management: literature review on assessment and control of outsider and insider threats. University of Tampere.

[53] Simon, S. and de Goede, M., 2015. Cybersecurity, bureaucratic vitalism and European emergency. Theory, Culture & Society, 32(2), pp.79-106.

[54] Smith, O., Johnson, J. and Oscar, E., 2017. Rethinking Cyber Defense: Zero-Trust Implementation in Nigeria's Cloud Ecosystem.

[55] Sood, A.K., Zeadally, S. and Bansal, R., 2015. Exploiting trust: stealthy attacks through socioware and insider threats. IEEE Systems Journal, 11(2), pp.415-426.

[56] Sperotto, A., Molina, J.L., Torresan, S., Critto, A. and Marcomini, A., 2017. Reviewing Bayesian Networks potentials for climate change impacts assessment and management: A multi-risk perspective. Journal of environmental management, 202, pp.320-331.

[57] Wang, J., Gupta, M. and Rao, H.R., 2015. Insider threats in a financial institution. MIS quarterly, 39(1), pp.91-112.

[58] Wittkop, J., 2016. Building a comprehensive IT security program: practical guidelines and best practices. Apress.

[59] Zio, E., 2016. Challenges in the vulnerability and risk analysis of critical infrastructures. Reliability Engineering & System Safety, 152, pp.137-150.

[60] Zuech, R., Khoshgoftaar, T.M. and Wald, R., 2015. Intrusion detection and big heterogeneous data: a survey. Journal of Big Data, 2(1), p.3.