Innovations

Third Party Risk Management and Data Privacy Leveraging AI

Samson, Adegbenro A.
Department of Informatics & Analytics
University of North Carolina, Greensboro

Abstract: *The application of artificial intelligence (AI) into third-party risk management (TPRM) has transformed processes for vendor risk assessment, anomaly detection, and contract review. This paper carefully examines the role of AI in addressing key challenges in Third-Party Risk Management while maintaining data privacy. A thorough search technique, compliant with PRISMA rules, retrieved 116 papers from databases including Google Scholar, Science Direct, and JSTOR, of which 36 were chosen for in-depth qualitative analysis. The findings of the study indicates that AI-driven predictive analytics improves accuracy of vendor risk assessments, whilst anomaly detection techniques strengthen operational resilience. In addition, AI-driven contract review solutions enhance the efficiency of due diligence and adherence to regulatory standards such as GDPR. However, the issues surrounding data privacy, algorithmic biases, and governance remain prevalent. Policy recommendations include promoting transparency, ethical governance of AI, and establishing effective compliance mechanisms. Finally, future research should look into AI scalability, inter-industry comparisons, and the possibilities of emerging technologies such as block chain in Third Party Risk Management (TPRM).*

Keywords: *Predictive Analytics, Artificial intelligence, Automation, Third-Party Risk Management, Cyber security*

1. Introduction

In today's interconnected and digitally-driven business environment, organizations increasingly rely on third-party vendors to provide essential services, software, and infrastructure. These partnerships offer significant benefits, including cost savings, specialized expertise, and operational efficiencies. However, they also introduce substantial risks, particularly in the realms of IT security and operational resilience. Third-Party Risk Management (TPRM) has emerged as a critical discipline, focusing on identifying, assessing, and mitigating the risks associated with outsourcing business processes and integrating third-party services (Chipeta, 2022). These risks are multiple, as they include cyber security threats, operational disruptions, regulatory compliance

failures, and reputational damage, all of which can have consequences for organizations (Park et al., 2015).

The advent of digital transformation has further amplified the complexity of managing third-party risks. Digital transformation, defined as the integration of disruptive technologies such as artificial intelligence (AI), block chain, cloud computing, and Internet of Things (IoT) into business operations, is reshaping traditional supply chains and enabling organizations to innovate rapidly (Dennehy et al., 2021; Anthony, 2021). While these technologies enhance operational efficiencies and risk analysis capabilities, they also expose organizations to some vulnerabilities, particularly in managing sensitive information and maintaining compliance with regulatory standards (Herold et al., 2021). As organizations embrace global e-commerce and digitized supply chains, the importance of TPRM practices becomes paramount to safeguard critical assets and ensure operational continuity.

One transformative force in TPRM is the adoption of AI-driven technologies, which have the potential to revolutionize risk management practices. AI applications in risk management enable predictive analytics, anomaly detection, and automated risk assessments, providing organizations with advanced tools to identify and mitigate third-party risks proactively (Adama & Okeke, 2024). However, the integration of AI into risk management introduces its own set of challenges, particularly in the area of data privacy. With AI systems requiring big amounts of data to operate effectively, organizations face often face risks related to unauthorized data access, breaches, and regulatory compliance (Quach et al., 2022). These risks are further exacerbated by the increasing sophistication of cyber attacks targeting sensitive data (Djenna et al., 2021).

Furthermore, the intersection of AI and data privacy in risk management highlights the dual role of AI as both a transformative tool and a source of potential vulnerabilities. On one hand, AI enhances risk identification and mitigation by enabling real-time monitoring, automated due diligence, and predictive modelling. On the other hand, its reliance on large-scale data processing makes it necessary for stringent safeguarding to protect data integrity, confidentiality, and availability (Rao et al., 2023). In addition, regulatory frameworks such as the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) highlights the importance of aligning AI-driven risk management practices with legal and ethical standards (Hartzog & Richards, 2020). As a result, organizations must strike a delicate balance between leveraging AI to strengthen third-party risk management and ensuring compliance with data privacy regulations to build trust and maintain resilience in an increasingly digital ecosystem. Due to this, this paper explores the growing importance of TPRM in the era of digital transformation, with a particular focus on the transformative role of AI and its implications for data privacy. By examining key trends, challenges, and opportunities, this study aims to provide a

comprehensive framework for leveraging AI to enhance risk management while upholding data privacy and regulatory compliance

1.2 Problem Statement

The reliance on third-party vendors for essential services, infrastructure, and processes has exposed organizations to a myriad of risks. These third-party relationships often serve as potential points of vulnerability, introducing threats such as data breaches, cyber attacks, compliance failures, and operational disruptions (Adama & Okeke, 2024; Jejeniwa et al., 2024). The opacity of modern supply chains makes these risks worse, as vendors have access to sensitive organizational information and critical systems. Supply chain attacks, which exploit vulnerabilities in vendor systems to infiltrate an organization's network, are becoming more problem, an example is the incidents of Saudi Aramco cyberattack and operations by groups such as Dragonfly (National Cyber Security Centre, 2018; Yeboah-Ofori & Islam, 2019). The financial and reputational costs of third-party risks are important. For instance, data reveals that 82% of organizations have experienced one or more data breaches caused by third-party vendors in the past two years, with an average cost of USD 4.33 million per breach which exceeds the cost of internal breaches (Thomas, 2024).

In addition, adhering to new privacy standards, such as GDPR and HIPAA, requires significant efforts. The annual hidden costs of managing vendor risk, including due diligence, legal expenses, and reputational damage, are estimated at USD 3.8 million (CENTRL, 2020). Despite all these investments, organizations lack the tools and frameworks necessary to proactively identify and mitigate risks associated with vendor bankruptcy, cyber security breaches, and other vulnerabilities (Rogoz, 2024). Conventional risk management methods frequently lack the capacity to deliver prompt insights into vendor performance and risk exposure, rendering organisations susceptible to disruptive events. Predictive analytics will offer a transformative solution which will enable organizations to forecast potential risks throughout their vendor relationship, identify patterns of vulnerabilities, and implement measures to mitigate these risk (Adeniran et al., 2024). This approach leverages advanced data-driven techniques to assess the likelihood of adverse events, such as vendor insolvency or targeted supply chain attacks, thereby enhancing situational awareness and decision-making (Wang et al., 2020; CENTRL, 2020).

Furthermore, procurement, an essential aspect of organisational functions, entails significant costs, frequently representing up to 60% of revenue in certain industries (Westerski et al., 2015). Financial frauds, including procurement fraud, cybercrime, and network intrusions, cause billions of dollars in annual losses globally, affecting organizations' financial stability, operational continuity, and reputational trust (Sánchez, et al 2009; Fischer, 2014). As a result, addressing these challenges requires adaptive, real-time, and security solutions that are capable of detecting anomalies and mitigating risks efficiently. As highlighted

earlier, traditional methods are limited in their ability to identify sophisticated and evolving threats, such as false positives, insider risks, and biases. However, the emergence of artificial intelligence (AI) offers transformative potential for overcoming these limitations. AI systems leverage machine learning (ML), especially unsupervised learning for anomaly detection and reinforcement learning for automated responses, to create a framework for real-time risk monitoring, identification, and response (Bhardwaj et al., 2024).

These systems can automate anomaly detection, score risks based on data, and streamline contract review processes through natural language processing (NLP). Despite this potential, integrating AI into risk management raises significant challenges, particularly regarding data privacy and regulatory compliance. This is because the integration of AI for anomaly detection, risk scoring, and contract review introduces policy and ethical implications. AI systems often require big amounts of data, which may include sensitive organizational and personal information, raising concerns about unauthorized data access, misuse, and compliance with privacy regulations like GDPR and HIPAA (Hartzog & Richards, 2020). Moreover, AI's inherent risks—such as biases, loss of privacy, false positives, and concentration of power compound these concerns, emphasizing the need for a policy framework to govern AI applications responsibly (Benjamins & Garcia, 2020; Jackson, 2020). The lack of clear regulatory guidance on AI's role in data processing and decision-making further complicates its adoption, posing risks of liability misattribution and erosion of stakeholder trust (Taddeo & Floridi, 2018). Given these challenges, this study will focus on three main objectives with the aim to; explore predictive analytics for vendor risk assessment (e.g., bankruptcy, cyber security breaches), investigate the role of AI in automating anomaly detection, risk scoring, and contract review, and examine policy implications for integrating AI with data privacy regulations.

1.3 Research Objectives

The aim of this research is to investigate third party risk management and data privacy leveraging artificial intelligence, as a result the research objectives of this study include;

i. Explore predictive analytics for vendor risk assessment (e.g., bankruptcy, cyber security breaches)
ii. Investigate the role of AI in automating anomaly detection, risk scoring, and contract review
iii. Examine policy implications for integrating AI with data privacy regulations.

1.4 Research questions

i. How can predictive analytics improve the accuracy of vendor risk assessment?

ii. What methodologies are most effective for AI-driven anomaly detection?
iii. What are the implications of AI adoption for data privacy and compliance?
iv. How can AI-based tools enhance due diligence and contract review processes?

2. Literature review

2.1 Conceptual Framework

Third-Party Risk Management and Its Components

Third-Party Risk Management (TPRM) is a critical aspect of organizational governance that ensures the identification, assessment, mitigation, and monitoring of risks associated with engaging external vendors, suppliers, service providers, and contractors (Abrahams et al., 2024). As organizations rely on third parties for essential operations, TPRM has become indispensable for maintaining operational continuity, financial stability, regulatory compliance, and reputational trust. The process begins with establishing a comprehensive inventory of all third-party relationships, including vendors involved in high-risk functions such as data handling, financial transactions, and critical service delivery (Bronson, 2022). Effective TPRM involves due diligence in vendor selection, prioritizing efforts based on the criticality and impact of the services provided, and ensuring vendors meet standards for security, compliance, and performance (Keskin et al., 2021).

A TPRM framework has numerous essential components. Risk identification is the foundation of Third-Party Risk Management (TPRM), which requires organisations to enumerate all third-party affiliations and identify vulnerabilities, including data breaches, supply chain attacks, or compliance failures. (Pham, 2023; Tummala & Schoenherr, 2011). This is then followed by risk assessment, where the likelihood and impact of these risks are evaluated. This phase involves analyzing vendor financial stability, operational reliability, and adherence to security protocols (Ahmed et al., 2021). Based on the outcomes of risk assessment, risk mitigation strategies are developed to reduce or eliminate vulnerabilities. These strategies involve the use of security measures to enforce strict contractual commitments and the preparation of contingency plans for unexpected disruptions. (Sen et al., 2020).

Continuous monitoring is another critical component of TPRM, enabling organizations to adapt to dynamic risk landscapes which involves real-time tracking of vendor performance, conducting regular audits, and updating risk assessments as circumstances change (Moyer, Walls & Phillips, 2020). Furthermore, governance and oversight provide the backbone for effective TPRM, establishing policies, roles, and responsibilities that ensure risks are managed proactively and consistently. In addition, contracts play a pivotal role in TPRM by clearly defining vendor responsibilities, performance expectations, and

liability (Khalef et al., 2021). However, the complexity of contractual arrangements, particularly in sectors such as financial services, requires standardization to provide sufficient safeguarding for monitoring and compliance (European Commission, 2020; Clausmeier, 2023).

Challenges and Risks in TPRM

Despite the structured approach offered by TPRM, challenges persist. For instance, data breaches are among the most prevalent risks, with vendors often serving as entry points for unauthorized access to sensitive organizational information (Adama & Okeke, 2024). Also, supply chain attacks, which capitalise on vulnerabilities in vendor systems to penetrate an organization's network, have become increasingly sophisticated (Benjamin, Amajuoyi & Adeusi, 2024). Furthermore, compliance failures by vendors can lead to regulatory sanctions and legal liabilities for the contracting organization (Jejeniwa, Mhlongo & Jejeniwa, 2024). Finally, over-dependence on vendors for critical services poses operational risks, with potential disruptions jeopardizing business continuity (Ikegwu et al., 2017). To address these challenges, TPRM frameworks must incorporate advanced practices such as risk-based vendor selection, comprehensive due diligence, and dynamic monitoring systems (Wang, Huo & Zhao, 2020).

The Role of AI in Modern Risk Management Frameworks

Artificial Intelligence (AI) is revolutionizing modern risk management frameworks by transforming traditional methods into adaptive, data-driven processes capable of addressing complex and evolving risks. Risk management, a fundamental aspect of corporate governance, has conventionally depended on manual procedures, fixed models, and the examination of historical data. However, the use of AI facilitates dynamic capabilities, allowing organisations to monitor, predict, and manage hazards in real time with improved accuracy and efficiency (Goodell et al., 2021). AI's role in risk management includes several transformative applications, including machine learning (ML), natural language processing (NLP), robotic process automation (RPA), and anomaly detection systems. These technologies work together to streamline workflows, enhance decision-making, and mitigate threats, improving organizational resilience (Kumar et al., 2022).

Predictive Analytics and Risk Forecasting

AI-driven predictive analytics leverages statistical models and machine learning algorithms to analyse big datasets, providing insights into patterns and trends that help forecast risks with outstanding precision. Unlike traditional models, which rely on static historical data, AI systems adapt to new inputs, making them ideal for identifying emerging threats (Schmitt, 2023). For instance, AI-powered algorithms can predict market fluctuations, assess credit risks, and identify

operational vulnerabilities, allowing organizations to develop mitigation strategies (Owen, 2024). As a result of continuously learning from these data's, these models evolve to address unforeseen challenges, such as economic downturns or supply chain disruptions, with greater agility.

Anomaly Detection and Fraud Prevention

Anomaly detection, a critical component of AI in risk management, involves identifying deviations from expected patterns in data. By employing advanced machine learning and deep learning techniques, AI systems can detect subtle irregularities that traditional methods often miss (Ajala, 2024). These capabilities are particularly valuable in detecting fraud, cyber security threats, and operational anomalies. For example, AI systems can analyze transaction data in real time to flag fraudulent activities, identify unusual trading patterns, or detect irregular behaviors in cloud computing environments (Bukhari et al., 2023). However, challenges such as false positives—triggered by noisy or incomplete data—highlight the need for robust contextualization and continual refinement of AI models (Montesinos López et al., 2022).

Automating Risk Scoring and Decision-Making

AI enhances risk scoring by dynamically analyzing multi-dimensional datasets to assign risk scores to entities, transactions, or processes. Machine learning models evaluate factors such as historical performance, financial stability, and compliance records, enabling organizations to prioritize risks and allocate resources effectively (Ahmed et al., 2022). Automated risk scoring accelerates decision-making processes, delivering relevant information that enable stakeholders to concentrate on strategic efforts instead of manual evaluations (Rizinski et al., 2024).

Enhancing Contract Review and Regulatory Compliance

Natural Language Processing (NLP) plays a pivotal role in automating contract review and ensuring compliance with regulatory requirements. AI-powered systems analyze complex legal documents, identify potential risks, and suggest amendments to align with regulatory standards (Cao & Zhai, 2023). By extracting actionable insights from unstructured textual data such as contracts, regulatory guidelines, and audit reports, NLP reduces human error and streamlines workflows, enabling organizations to maintain compliance while reducing operational overhead (Devarajan, 2018).

Real-Time Risk Monitoring and Mitigation

Traditional risk monitoring systems often suffer from delayed data processing, limiting their ability to respond to emerging threats. AI-driven systems overcome this limitation by leveraging real-time analytics to provide continuous monitoring of market conditions, operational performance, and cyber security environments

(Bello & Olufemi, 2024). In addition, advanced anomaly detection systems integrated with machine learning algorithms enable organizations to proactively address risks before they escalate into crises (Ji et al., 2024).

Integration with Cybersecurity Frameworks

In cyber security, AI systems provide a defense mechanism by identifying vulnerabilities and responding to threats in real time. AI-powered tools can analyze big amounts of network data to detect malicious activities, predict potential breaches, and recommend countermeasures. For example, AI-based anomaly detection systems in cloud computing environments ensure robust security by identifying suspicious behaviors and risks (Chatterjee & Ahmed, 2022). As a result, integrating AI into cyber security frameworks helps organizations enhance their security while reducing response times to critical incidents (Raparthi et al., 2020).

Addressing Ethical and Policy Challenges

Finally, the integration of AI in risk management frameworks introduces ethical and policy challenges, particularly around explainability, data privacy, and regulatory compliance. Algorithms must be transparent and auditable to ensure accountability for AI-driven decisions. Regulations such as the General Data Protection Regulation (GDPR) makes it mandatory for robust data protection measures and the need for explainability in automated decision-making (Wachter et al., 2017). This endeavours that organizations must strike a balance between leveraging AI's capabilities and adhering to ethical standards, so as to ensure that AI systems promote trust and fairness in risk management practices (Reed et al., 2016).

2.2 Theoretical Framework

The Technology-Organization-Environment (TOE) Framework

The Technology-Organization-Environment (TOE) paradigm, proposed by Tornatzky and Fleischer (1990), offers a theoretical foundation for understanding the acceptance and execution of technological breakthroughs within organisations. The framework classifies factors affecting technology adoption into three dimensions: technological, organisational, and environmental. The technological context includes the attributes of the technology, such as its perceived advantages, complexity, and compatibility with current systems. It analyses how the technology's capabilities fulfil organisational requirements and its potential to promote innovation. The organisational environment emphasises on internal elements, including size, structure, culture, and the availability of financial and human resources, which collectively impact the decision-making process. The environmental context encompasses external influences such as governments regulations, competitive forces, and industry standards that influence an organization's technology adoption strategy.

The TOE framework claims that the decision to embrace new technologies is impacted not only by technological capabilities but also by the interaction between organisational readiness and external environmental factors (Baker, 2012). This thorough approach allows a multidimensional understanding of the elements influencing adoption decisions. The TOE methodology is particularly pertinent in the realm of third-party risk management (TPRM) and data privacy leveraging artificial intelligence (AI). The technological aspect analyses AI's function in predictive analytics, anomaly detection, and the automation of activities such as contract approval. The organisational environment assesses the incorporation of AI into TPRM workflows, the allocation of resources for AI implementation, and the internal governance frameworks. The environmental aspect emphasises on the need of adhering to data protection rules, such as GDPR, and the imperative to conform to industry standards for ethical AI implementation.

Despite its positive aspects, the TOE structure possesses limits. It frequently faces criticism for its extensive scope, which may downplay the complicated process of technology adoption. Furthermore, it fails to clearly consider human and cultural aspects, including resistance to change and the impact of organisational culture on technological acceptability (Oliveira & Martins, 2011). Its holistic approach renders it an essential instrument for assessing the integration of AI in Third-Party Risk Management and data privacy, offering a systematic basis for exploring the interaction of technological, organisational, and environmental factors.

3. Methodological Approach

In the research approach and design, this study adopts the interpretivism philosophy, which is particularly well-suited for investigating the dynamic nature of third-party risk management (TPRM) and data privacy leveraging artificial intelligence (AI). Interpretivism enables an in-depth analysis of the complex connections of technological, organizational, and environmental elements, emphasizing on the understanding of AI's contribution to the enhancement of TPRM processes and the assurance of data privacy compliance. The study employs a secondary data approach that aligns with the research focus on analyzing existing literature, frameworks, and trends in TPRM, AI applications, and regulatory implications. This is because, secondary data offers a solid basis for assessing predictive analytics, AI-based anomaly detection, and automated tools for due diligence and contract review in organizational settings. This approach ensures a comprehensive analysis of AI’s transformative potential in addressing vendor risk and data privacy concerns.

Furthermore, an archival research methodology is used, involving a systematic review of scholarly articles, industry reports, regulatory guidelines, case studies, and historical documents, enabling the researcher to examine trends, methodologies, and frameworks adopted by organizations to integrate AI into TPRM processes. For data description and sources, the study conducts an in-

depth analysis of secondary data sources spanning from 2019 to 2024, including surveys and academic research. The selection criteria ensure that materials directly discussing connections between TPRM, artificial intelligence, and data privacy, enhancing the validity of the findings. Exclusion criteria are applied to filter out sources lacking relevance or methodological robustness, maintaining the study's rigor and integrity. Adherence to PRISMA standards enhances transparency and methodological rigor, providing a structured framework for conducting systematic reviews of the literature, thereby ensuring the validity and replicability of the research findings while offering guidance for future researchers.

Search Strategy:

A comprehensive review searched through electronic databases using keywords to find relevant literature on the topic, following the method of Kitchenham (2007) and Atkinson and Cipriani (2018). The search covered the period from 2019 to 2024 and included sources such as journals, government publications, and highly relevant websites from journal database such as: Google Scholar, Springer Link, Science Direct (Elsevier), Taylor and Francis Online, JSTOR, etc to reflect assess to investigate third party risk management and data privacy leveraging artificial intelligence as shown in the table below. The review used a systematic approach to select the publications that met the inclusion criteria (See Table 1).

Table 1: A 11-Year Search

Year under review	2019 -2024
Search Terms	These terms are used in combination using Boolean operators (AND, OR) to create search strings for databases like Google Scholar, Springer Link, Science Direct (Elsevier), Taylor and Francis Online, JSTOR. The search strategy was adjusted based on the specific requirements of each database and the focus of the study. This search term encompasses the key elements of interest: Third-party risk management and artificial intelligence, Contract review automation and natural language processing etc
	. Researchers used this term to identify relevant literature that focus on areas such as, predictive analytics for vendor risk assessment, AI methodologies for anomaly detection, automation of contract review, and the policy implications of integrating AI with data privacy frameworks. The result revealed empirical evidence and theoretical perspectives that underpin the role of AI in transforming third-party risk management and maintaining data privacy while addressing regulatory and ethical considerations.

Sample Journals	☒ Journal of Applied Science ☒ Journal of Enterprise Information Management ☒ Journal of Enterprise Information Systems ☒ Innovative Computer Sciences Journal ☒ International Journal of Management & Entrepreneurship Research ☒ Computer Science & IT Research Journal ☒ Journal of Behavioural and Experimental Finance ☒ Journal of Legal Affairs and Dispute Resolution in Engineering and Construction
Database	Google Scholar, Springer Link, Science Direct (Elsevier), Taylor and Francis Online, JSTOR

The study initially identified 116 articles related to the relationship between TPRM and data privacy leveraging AI, but after applying inclusion/exclusion criteria, 75 articles were excluded. After further filtering and skimming the full contents, about 36 relevant articles were retained for review on the assessment of third-party risk management (TPRM) and data privacy leveraging artificial intelligence (AI).

Table2: A 11-Year Assessment Inclusion and Exclusion Criteria

Inclusion criteria	Exclusion criteria
Studies published between the period of 2019–2023	Studied outside the domain of third-party risk management (TPRM) and data privacy leveraging artificial intelligence (AI).
Studied within the domain of third-party risk management (TPRM) and data privacy leveraging artificial intelligence (AI).	No full-length peer reviewed studies
Full-length peer reviewed studies	Not published in the English language
Published in the English language	Duplicated
Available in selected electronic databases	

The systematic review flow diagram, based on PRISMA guidelines, will display the number of records identified and included studies.as depicted in Figure 3.1

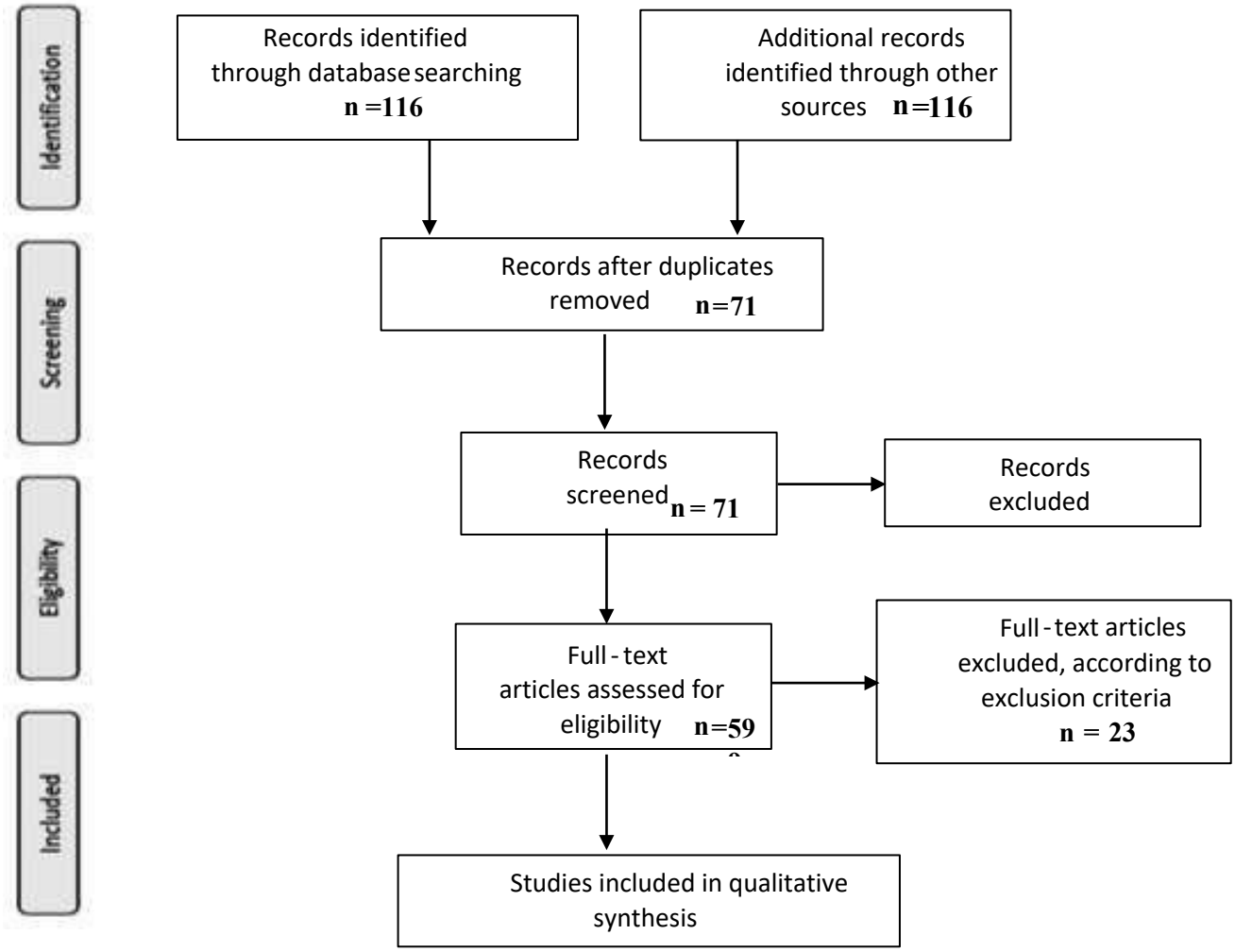

Figure 3.1: Systematic review flow diagram based on PRISMA guidelines

Only journals that are indexed in respected database such as Google Scholar, Springer Link, Science Direct (Elsevier), Taylor and Francis Online, and JSTOR were selected for this study as demonstrated in Table 3

Table 3: No of Selected Publications

SN	Publisher(s)	No of Papers Assessed for Eligibility [N=107]	No of Papers Selected for Qualitative Synthesis [N=36]
1	Google Scholar	46	13
2	Science Direct (Elsevier)	24	5
3	JSTOR	13	3
4	Taylor & Francis Online	19	7
5	Springer Link	14	8
	Total	**116**	36

4. Analysis of Research Questions

Four research questions were established to guide this study, delineating the scope of inquiry and objectives. These questions serve as focal points for investigating third party risk management and data privacy leveraging artificial intelligence.

The research questions for this study are as follows:

i. How can predictive analytics improve the accuracy of vendor risk assessment?
ii. What methodologies are most effective for AI-driven anomaly detection?
iii. What are the implications of AI adoption for data privacy and compliance?
iv. How can AI-based tools enhance due diligence and contract review processes?

4.1 Analysis of Research Question 1: How can predictive analytics improve the accuracy of vendor risk assessment?

This research question investigates the role of predictive analytics in improving the accuracy of vendor risk assessment, particularly in areas such as bankruptcy prediction and cyber security breach identification. Predictive analytics employs statistical techniques and machine learning algorithms to examine historical data and forecast future results, allowing organisations to identify and mitigate risks (Schmitt, 2023). Using extensive datasets, such as vendor financial stability, compliance records, and market behaviour, predictive algorithms can uncover patterns and trends that static risk assessments may miss (Ahmed et al., 2022).

For instance, predictive analytics systems can evaluate financial indicators including liquidity ratios, cash flow trends, and creditworthiness, enabling the early identification of possible vendor insolvencies (Samad, 2024). Likewise, AI-powered predictive algorithms examine cyber threat data and identify vendors with insufficient cyber security protocols or records of breaches (Owen, 2024). This approach aligns with the conclusions of Wang et al. (2020), who assert that predictive analytics offers dynamic insights into risk exposure, hence enhancing the precision of risk scoring and prioritisation.

Furthermore, Owen, (2024) highlights that predictive analytics systems integrated with machine learning capabilities consistently adjust to new data, improving their forecasts and increasing their relevance over time. This adaptability is essential for managing rapidly evolving hazards in complex vendor ecosystems. The use of predictive analytics in vendor risk assessment encounters hurdles such as data quality concerns and algorithmic biases, making it necessary for strong governance structures for successful deployment (Quah & Sriganesh, 2008). The findings highlight the revolutionary potential of predictive analytics in vendor risk assessment. These tools enable real-time, data-driven

insights that improve decision-making, reduce financial and operational risks, and offer a competitive advantage in managing third-party partnerships.

4.2 Analysis of Research Question 2: What methodologies are most effective for AI-driven anomaly detection?

This research question examines the methodologies of AI-driven anomaly detection, emphasising their effectiveness in identifying unusual patterns in third-party operations. Anomaly detection entails recognizing deviations from predicted behaviours, a vital function for identifying fraud, cybersecurity threats, and operational inefficiencies (Bukhari et al., 2023). Artificial intelligence techniques, especially machine learning and deep learning, are leading the progress of anomaly detection systems. Traditional anomaly detection methods, such as statistical techniques and rule-based systems, depend on established thresholds to flag irregularities. Nonetheless, these methodologies encounter difficulties with high-dimensional data and dynamic threats. Machine learning methodologies, for example, clustering algorithms (e.g., k-means) and support vector machines (SVM), have exhibited exceptional proficiency in managing complex datasets (Igwenagu et al., 2024). Furthermore, deep learning models, such as autoencoders and recurrent neural networks (RNNs), are competent in analysing time-series and unstructured data, rendering them optimal for detecting complex and dynamic anomalies (Ajala, 2024).

Research conducted by Saeed et al., (2023) demonstrates that the incorporation of historical data into anomaly detection algorithms diminishes false positives, a prevalent issue in AI applications. Furthermore, Ji et al., (2024) argue that reinforcement learning improves the adaptability of detection models, enabling ongoing learning and improvement in dynamic settings. Although effective, AI-driven anomaly detection systems encounter restrictions such as high computing expenses and the necessity for extensive, high-quality datasets. Olaniyi, (2024) highlights the significance of rigorous training procedures and frequent model validation to mitigate these challenges. In conclusion, AI-driven techniques, especially deep learning and reinforcement learning, provide the most efficient methods for anomaly identification. Their capacity to analyse large amounts of data and adjust to emerging risks improves the precision and dependability of third-party risk management frameworks.

4.3 Analysis of Research Question 3: What are the implications of AI adoption for data privacy and compliance?

This research question examines the effects of AI adoption on data privacy and regulatory compliance, emphasising the relationship between technological progress and legal structures. AI systems, especially those employed in third-party risk management, handle extensive volumes of sensitive data, hence generating a huge privacy concern (Hartzog & Richards, 2020). The General Data Protection Regulation (GDPR) and similar regulatory frameworks impose severe

data protection requirements, highlighting accountability, openness, and consent in data processing (Wachter et al., 2017). Nonetheless, AI's dependence on large amounts of data and unclear decision-making processes frequently contradicts these stipulations, resulting in a complicated regulatory environment (Reed, 2018). The absence of explainability in machine learning models presents challenges in proving adherence to the "right to explanation" mandated by GDPR (Selbst & Powles, 2018).

Benjamins and Garcia, (2020) identify ethical challenges related to AI adoption, such as biases, data exploitation, and surveillance hazards. Taddeo and Floridi, (2018) propose that organisations should establish extensive governance frameworks to reconcile AI's prospective advantages with ethical and legal responsibilities. These frameworks must have procedures for algorithmic accountability, data anonymisation, and frequent compliance audits. In summary, although AI implementation improves operational efficiency in TPRM, it requires thorough attention to data protection and regulatory issues. Organizations must synchronise AI operations with evolving regulations to promote trust and reduce legal and reputational risks.

4.4 Analysis of Research Question 4: How can AI-based tools enhance due diligence and contract review processes?

This research question investigates the extent to which artificial intelligence (AI) tools enhance the efficiency and precision of due diligence and contract review, which are critical elements of third-party risk management. Traditional approaches for these activities involve labour-intensive review processes that are inefficient, susceptible to errors, and limited in scalability (Cao & Zhai, 2023). Artificial Intelligence technologies, especially Natural Language Processing (NLP), automate and optimise workflow by extracting relevant information from large volume of textual data. NLP-driven system evaluates contracts to detect risks, including ambiguous terms, regulatory non-compliance, and liability concerns, by offering actionable mitigation recommendations (Devarajan, 2018). AI techniques can identify inconsistencies in financial agreements or highlight terms that varies from industry standards, so improving the efficacy of contract negotiation and management (Rizinski et al., 2024).

In addition, AI-driven due diligence tools evaluate vendor financial stability, compliance records, and cybersecurity protocols by synthesizing and scrutinizing data from various sources, such as financial statements and market news (Ahmed et al., 2022). Villar and Khan, (2021) assert that these technologies enhance decision-making by providing detailed risk profiles of third-party vendors in shorter timeframes. However, challenges persist, particularly in guaranteeing the accuracy of AI outputs and addressing biases within training datasets. Chatterjee and Ahmed, (2022) propose for regular checks and human supervision to verify AI-generated insights and ensure adherence to legal regulations. In summary, AI-driven technologies improve due diligence and

contract review by automating analysis, improving accuracy, and decreasing processing times. These improvements will enhance organizations' capacity to manage third-party risks efficiently while ensuring adherence to regulatory requirements.

5. Conclusion and Policy Implications

In conclusion, this study highlights the capacity of artificial intelligence (AI) in improving third-party risk management (TPRM) and protecting data privacy during digital transformation. By making use of predictive analytics, anomaly detection, and automated systems for due diligence and contract review, organisations can adopt a proactive and adaptive risk management strategy. This is because AI-driven approaches yield significant insights into vendor risk profiles, enabling the early identification of possible risks including bankruptcy, cybersecurity breaches, and compliance failures. These improvements enhance operational efficiency and strengthen organizational resilience against the growing complexities of global supply networks. The findings also have significant policy implications, that highlights the need for strong frameworks that balance AI use with ethical and regulatory adherence.

Policymakers and organizational leaders must prioritize the integration of AI applications with data privacy legislation, including the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA). Transparency and accountability in AI systems are very important for strengthening stakeholder trust and mitigating risks linked to biased or opaque algorithms. Furthermore, it is important to invest in AI governance frameworks, employee training, and ethical AI development to prevent risks related to data exploitation and privacy violations. As a result, by cultivating a framework of trust and compliance, organizations can fully leverage AI to transform risk management procedures while adhering to changing regulatory environments. This study advocates for a coordinated initiative to appropriately incorporate AI into TPRM processes, ensuring that technological advancements enhance organizational integrity and sustainability. The balance between technological progress and ethical governance will enable organizations to address the challenges of the digital age.

6. Contributions to Knowledge and Suggestions for Further Studies

This research advances the understanding of third-party risk management (TPRM) and data privacy by clarifying the function of artificial intelligence (AI) in tackling modern challenges. By examining predictive analytics, AI-based anomaly detection, and automation tools for due diligence and contract reviews, this study presents a thorough framework for leveraging AI to improve TPRM processes. The results emphasise the relationship between technology, organizational preparedness, and regulatory compliance, providing essential

insights for practitioners and academics aiming to refine risk management strategies.

The study examines methods using artificial intelligence and their potential to mitigate risks including data breaches, fraud, and vendor insolvencies. Furthermore, the integration of AI with compliance frameworks offers a blueprint for organizations to synchronize their technological advancements with ethical and regulatory requirements, hence enhancing the overall dialogue on responsible AI implementation. These are essential for organisations seeking to manage the complicated nature modern supply chains while maintaining data privacy and regulatory compliance. Further studies should expand upon this study by investigating the long-term effects of AI integration into TPRM processes, evaluating the sustainability and scalability of these measures. Comparative analysis across sectors and geographic areas may yield insight into the contextual elements affecting the effectiveness of AI-driven risk management strategies. In addition, qualitative study examining organizational cultures, leadership styles, and employee opinions of AI implementation may reveal the socio-psychological aspects of AI adoption. Finally, future research may explore the ramifications of upcoming technologies like blockchain and quantum computing on Third Party Risk Management (TPRM) and data privacy, offering a prospective view on the advancement of this critical field.

References

1. *Abrahams, T.O., Farayola, O.A., Kaggwa, S., Uwaoma, P.U., Hassan, A.O. and Dawodu, S.O., 2024. Reviewing third-party risk management: best practices in accounting and cybersecurity for superannuation organizations. Finance & Accounting Research Journal, 6(1), pp.21-39.*
2. *Adama, H.E. and Okeke, C.D., 2024. Comparative analysis and implementation of a transformative business and supply chain model for the FMCG sector in Africa and the USA. Magna Scientia Advanced Research and Reviews, 10(2), pp.265-271.*
3. *Adama, H.E. and Okeke, C.D., 2024. Harnessing business analytics for gaining competitive advantage in emerging markets: A systematic review of approaches and outcomes. International Journal of Science and Research Archive, 11(2), pp.1848-1854.*
4. *Adeniran, I.A., Efunniyi, C.P., Osundare, O.S. and Abhulimen, A.O., 2024. Enhancing security and risk management with predictive analytics: A proactive approach. International Journal of Management & Entrepreneurship Research, 6(8).*
5. *Ahmed, M.O., Abdul Nabi, M., El-adaway, I.H., Caranci, D., Eberle, J., Hawkins, Z. and Sparrow, R., 2021. Contractual guidelines for promoting integrated project delivery. Journal of construction engineering and management, 147(11), p.05021008.*

6. *Ahmed, S., Alshater, M.M., El Ammari, A. and Hammami, H., 2022. Artificial intelligence and machine learning in finance: A bibliometric review. Research in International Business and Finance, 61, p.101646.*
7. *Anthony Jnr, B., 2021. Managing digital transformation of smart cities through enterprise architecture–a review and research agenda. Enterprise Information Systems, 15(3), pp.299-331.*
8. *Baker, J., 2012. The technology–organization–environment framework. Information Systems Theory: Explaining and Predicting Our Digital Society, Vol. 1, pp.231-245.*
9. *Bello, O.A. and Olufemi, K., 2024. Artificial intelligence in fraud prevention: Exploring techniques and applications challenges and opportunities. Computer Science & IT Research Journal, 5(6), pp.1505-1520.*
10. *Benjamin, L.B., Amajuoyi, P. and Adeusi, K.B., 2024. Leveraging data analytics for informed product development from conception to launch. GSC Advanced Research and Reviews, 19(2), pp.230-248.*
11. *BenJaMins, V.R. and Salazar García, I., 2019. Towards a framework for understanding societal and ethical implications of Artificial Intelligence. Vulnerabilidad y cultura digital: riesgos y oportunidades de la sociedad hiperconectada, pp.89-100.*
12. *Bhardwaj, A.K., Dutta, P.K. and Chintale, P., 2024. AI-Powered Anomaly Detection for Kubernetes Security: A Systematic Approach to Identifying Threats. Babylonian Journal of Machine Learning, 2024, pp.142-148.*
13. *Bronson, H.E., 2022. Five Common Shortcomings of Third-Party Management Programs in Financial Organizations and Recommended Risk Management Strategies (Master's thesis, Utica University).*
14. *Bukhari, O., Agarwal, P., Koundal, D. and Zafar, S., 2023. Anomaly detection using ensemble techniques for boosting the security of intrusion detection system. Procedia Computer Science, 218, pp.1003-1013.*
15. *Cao, Y. and Zhai, J., 2023. Bridging the gap–the impact of ChatGPT on financial research. Journal of Chinese Economic and Business Studies, 21(2), pp.177-191.*
16. *CENTRL, (2020). INFOGRAPHIC: The hidden cost of vendor risk and compliance (no date) Centrl.ai. Available at: www.centrl.ai (Accessed: November 26, 2024).*
17. *Chatterjee, A. and Ahmed, B.S., 2022. IoT anomaly detection methods and applications: A survey. Internet of Things, 19, p.100568.*
18. *Chipeta, C. (2022). What is Third-Party Risk? | Up Guard. www.upguard.com.*
19. *Clausmeier, D. (2023) "Regulation of the European Parliament and the Council on digital operational resilience for the financial sector (DORA)," International Cybersecurity Law Review, 4(1), pp. 79–90.*
20. *Devarajan, Y., 2018. A study of robotic process automation use cases today for tomorrow's business. International Journal of Computer Techniques, 5(6), pp.12-18.*

21. *Djenna, A., Harous, S. and Saidouni, D.E., 2021. Internet of things meet internet of threats: New concern cyber security issues of critical cyber infrastructure. Applied Sciences, 11(10), p.4580.*
22. *Fischer, E.A., 2014. Cyber security issues and challenges: In brief [online]*
23. *Goodell, J.W., Kumar, S., Lim, W.M. and Pattnaik, D., 2021. Artificial intelligence and machine learning in finance: Identifying foundations, themes, and research clusters from bibliometric analysis. Journal of Behavioral and Experimental Finance, 32, p.100577.*
24. *Hartzog, W. and Richards, N., 2020. Privacy's constitutional moment and the limits of data protection. BCL Rev., 61, p.1687.*
25. *Herold, D.M., Ćwiklicki, M., Pilch, K. and Mikl, J., 2021. The emergence and adoption of digitalization in the logistics and supply chain industry: an institutional perspective. Journal of Enterprise Information Management, 34(6), pp.1917-1938.*
26. *Igwenagu, U.T.I., Salami, A.A., Arigbabu, A.S., Mesode, C.E., Oladoyinbo, T.O. and Olaniyi, O.O., 2024. Securing the digital frontier: Strategies for cloud computing security, database protection, and comprehensive penetration testing. Journal of Engineering Research and Reports, 26(6), pp.60-75.*
27. *Ikegwu, A.C., Nweke, H.F., Anikwe, C.V., Alo, U.R. and Okonkwo, O.R., 2022. Big data analytics for data-driven industry: a review of data sources, tools, challenges, solutions, and research directions. Cluster Computing, 25(5), pp.3343-3387.*
28. *Jackson, B.W., 2019. Cybersecurity, privacy, and artificial intelligence: an examination of legal issues surrounding the European union general data protection regulation and autonomous network defence. Minn. JL Sci. & Tech., 21, p.169.*
29. *Jejeniwa, T.O., Mhlongo, N.Z. and Jejeniwa, T.O., 2024. A comprehensive review of the impact of artificial intelligence on modern accounting practices and financial reporting. Computer Science & IT Research Journal, 5(4), pp.1031-1047.*
30. *Jejeniwa, T.O., Mhlongo, N.Z. and Jejeniwa, T.O., 2024. A comprehensive review of the impact of artificial intelligence on modern accounting practices and financial reporting. Computer Science & IT Research Journal, 5(4), pp.1031-1047.*
31. *Ji, I.H., Lee, J.H., Kang, M.J., Park, W.J., Jeon, S.H. and Seo, J.T., 2024. Artificial intelligence-based anomaly detection technology over encrypted traffic: a systematic literature review. Sensors, 24(3), p.898.*
32. *Keskin, O.F., Caramancion, K.M., Tatar, I., Raza, O. and Tatar, U., 2021. Cyber third-party risk management: A comparison of non-intrusive risk scoring reports. Electronics, 10(10), p.1168.*
33. *Khalef, R., El-Adaway, I.H., Assaad, R. and Kieta, N., 2021. Contract risk management: A comparative study of risk allocation in exculpatory clauses*

and their legal treatment. Journal of Legal Affairs and Dispute Resolution in Engineering and Construction, 13(1), p.04520036.

34. *Kumar, S., Sharma, D., Rao, S., Lim, W.M. and Mangla, S.K., 2022. Past, present, and future of sustainable finance: insights from big data analytics through machine learning of scholarly research. Annals of Operations Research, pp.1-44.*
35. *Montesinos López, O.A., Montesinos López, A. and Crossa, J., 2022. Overfitting, model tuning, and evaluation of prediction performance. In Multivariate statistical machine learning methods for genomic prediction (pp. 109-139). Cham: Springer International Publishing.*
36. *Moyer, D., Walls, K.E. and Phillips, C.V., 2020. An Analysis of Air Force Contract Management Personnel Competency and Internal Processes Using the National Contract Management Association's Third-Party Accredited Competency Standard (Doctoral dissertation, Monterey, CA; Naval Postgraduate School).*
37. *Olaniyi, O.O., 2024. Ballots and padlocks: Building digital trust and security in democracy through information governance strategies and blockchain technologies. Available at SSRN 4759942.*
38. *Oliveira, T. and Martins, M.F., 2011. Literature review of information technology adoption models at firm level. Electronic journal of information systems evaluation, 14(1), pp.pp110-121.*
39. *Owen, J., 2024. AI and ML in Financial Knowledge Management and Predictive Analytics.*
40. *Park, K., Davis, K., & Hoogmoed, W. (2015). Deloitte.com. Available at: www 2.deloitte.com (Accessed: November 25, 2024).*
41. *Pham, T., 2023. Risk identification and mitigation in data analytics outsourcing: the vendor's perspective.*
42. *Quach, S., Thaichon, P., Martin, K.D., Weaven, S. and Palmatier, R.W., 2022. Digital technologies: tensions in privacy and data. Journal of the Academy of Marketing Science, 50(6), pp.1299-1323.*
43. *Quah, J.T. and Sriganesh, M., 2008. Real-time credit card fraud detection using computational intelligence. Expert systems with applications, 35(4), pp.1721-1732.*
44. *Rao, P.S., Krishna, T.G. and Muramalla, V.S.S.R., 2023. Next-gen cybersecurity for securing towards navigating the future guardians of the digital realm. International Journal of Progressive Research in Engineering Management and Science (IJPREMS) Vol, 3, pp.178-190.*
45. *Raparthi, M., Dodda, S.B. and Maruthi, S., 2020. Examining the use of Artificial Intelligence to Enhance Security Measures in Computer Hardware, including the Detection of Hardware-based Vulnerabilities and Attacks. European Economic Letters (EEL), 10(1).*

46. *Rizinski, M., Jankov, A., Sankaradas, V., Pinsky, E., Mishkovski, I. and Trajanov, D., 2024. Comparative Analysis of NLP-Based Models for Company Classification. Information, 15(2), p.77.*
47. *Rogoz, R.D., 2024. Identifying Risks and Protecting Supply Chains. Innovative Computer Sciences Journal, 10(1).*
48. *Saeed, M.M., Saeed, R.A., Abdelhaq, M., Alsaqour, R., Hasan, M.K. and Mokhtar, R.A., 2023. Anomaly detection in 6G networks using machine learning methods. Electronics, 12(15), p.3300.*
49. *Samad, A., 2024. AI-Based Knowledge Extraction and Machine Learning for Predictive Financial Decision-Making.*
50. *Sánchez, D., Vila, M.A., Cerda, L. and Serrano, J.M., 2009. Association rules applied to credit card fraud detection. Expert systems with applications, 36(2), pp.3630-3640.*
51. *Schmitt, M., 2023. Automated machine learning: AI-driven decision making in business analytics. Intelligent Systems with Applications, 18, p.200188.*
52. *Selbst, A. and Powles, J., 2018, January. "Meaningful information" and the right to explanation. In conference on fairness, accountability and transparency (pp. 48-48). PMLR.*
53. *Sen, S., Kotlarsky, J. and Budhwar, P., 2020. Extending organizational boundaries through outsourcing: toward a dynamic risk-management capability framework. Academy of Management Perspectives, 34(1), pp.97-113.*
54. *Taddeo, M. and Floridi, L., 2018. Reed, C., 2018. How should we regulate artificial intelligence?. Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences, 376(2128), p.20170360.Science, 361(6404), pp.751-752.*
55. *Thomas, S. (2024) Challenges in vendor management: What finance teams need to know, Hiver. Available at: hiverhq.com (Accessed: November 26, 2024).*
56. *Tummala, R. and Schoenherr, T., 2011. Assessing and managing risks using the supply chain risk management process (SCRMP). Supply Chain Management: An International Journal, 16(6), pp.474-483.*
57. *Villar, A.S. and Khan, N., 2021. Robotic process automation in banking industry: a case study on Deutsche Bank. Journal of Banking and Financial Technology, 5(1), pp.71-86.*
58. *Wang, D.N., Li, L. and Zhao, D., 2022. Corporate finance risk prediction based on LightGBM. Information Sciences, 602, pp.259-268.*
59. *Westerski, A., Kanagasabai, R., Wong, J. and Chang, H., 2015. Prediction of enterprise purchases using Markov models in procurement analytics applications. Procedia Computer Science, 60, pp.1357-1366.*
60. *Yeboah-Ofori, A. and Islam, S., 2019. Cyber security threat modeling for supply chain organizational environments. Future internet, 11(3), p.63*