IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 5, June 2025
Impact Factor: 7.67

AI-Enhanced Third-Party Risk Management

Asst. Prof. Snehal Bagal, Dipali Gaikwad, Sakshi Galande, Arya Ingale, Sneha Kadam
Department of Artificial Intelligence and Data Science
AISSMS Institute of Information Technology, Pune, India

Abstract: *Organizations risk grave chances of undergoing severe cyber security, financial, and compliance risks to great extents by increasingly depending on third parties to conduct business. This paper outlines an AI-driven framework using ML techniques for third-party risk management. It involves incorporating natural language processing into a real-time risk assessment process, uses of anomaly detection algorithms in fraud identification, and predictive analytics used in order to predict potential vendor failures. Experimental results on a 5,000 vendor-profile dataset indicate that risk classification reaches accuracy of 92% over traditional rule-based models. The results indicate that AI-enhanced TPRM can greatly improve the efficacy of risk mitigation strategies as well as compliance with regulatory requirements. Future work includes the integration of XAI to enhance model interpretability.*

Keywords: TPRM, NLP, Sentiment Analyzer

I. INTRODUCTION

The third parties are essential for third-party vendors delivering crucial services and products in an increasingly interconnected global economy. Dependency, though beneficial, provides risks that may reverberate through channels of lessened operational efficiency, thwarts regulatory compliance, and therefore adversely affects business integrity in general. Third Party risk management (TPRM) is a discipline that serves to identify, assess, and mitigate these risks so that the organizations can confidently engage with the external partners.

In that regard, it would be extremely hard to interpret this large number of data originating from contracts, social media communications by the vendor, and also through market reports. TPRM, for quite some time now, involved cumbersome labor intensive traditional manual practices. There are challenges that develop in organizations resulting from the nature of third parties and their affiliated risks, that are constantly developing. Such environment calls for efficiency and effectiveness when it comes to TPRM strategies. Thus, Natural Language Processing (NLP), the branch of AI, has more promising solutions concerning the challenges being posed by the TPRM. NLP will enable machines to understand, interpret, and generate human language and process large volumes of unstructured data to derive valuable insights into risk assessments. NLP technologies, such as text mining, sentiment analysis, and named entity recognition, will automate the extraction of critical information from contracts and other documents and provide organizations with real time insights into third-party risks.

II. LITERATURE SURVEY

This part presents a systematic survey of the literature available on TPRM and NLP technologies integration in the domain. In relation to reviewing the literature, this part categorizes the literature into key areas: traditional approaches in TPRM, the role of NLP in TPRM performance enhancement, and specific case studies on the implementation made with a successful paradigm. Traditional Third-Party Risk Management Approaches Traditional TPRM practices still mostly depend on manual processes when identifying, assessing, and monitoring risk. Some organizations use various frameworks, for instance, Risk Management Framework, to structure TPRM in an organization or by using National Institute of Standards and Technology (NIST) guidelines. Research has shown a myriad of conventional TPRM methods' challenges: high cost, time consuming, and challenging integration of data.

The Role of Natural Language Processing in TPRM NLP has become an essential technology to refine TPRM processes through data extraction and analysis automation. Various studies have discussed the capabilities of NLP in these areas. Automation also saves humans from intensive effort and increases the precision of risk evaluation.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 5, June 2025
Impact Factor: 7.67

Organizations have used another application of NLP called sentiment analysis to measure public sentiment and find possible reputational risks from third-party vendors. Moreover, NER techniques have been used to identify and categorize relevant entities, such as companies and products, within large datasets, thus making the risk assessment process more efficient.

III. CASE STUDIES AND PRACTICAL IMPLEMENTATIONS

Many studies have illustrated the successful integration of NLP-enabled solutions into TPRM. This solution used machine learning algorithms to refine risk prediction accuracy over time using history. Another interesting implementation was by [organization name], which relied on sentiment analysis to monitor social media conversations about its key vendors. The results revealed a strong relationship between negative sentiment and subsequent operational disruptions, and the organization acted proactively to reassess its vendor relationships. Although the case studies presented promising results, NLP in TPRM faces challenges in terms of widespread adoption. Some of the barriers that have been reported in the literature include data quality issues, integration with existing systems, and the need for specific expertise in NLP techniques.

As such, Cybersecurity is one of the major problems facing organizations today. However, the security of an organization's internal network might not be enough as modern organizations are reliant on third parties that can introduce new vulnerabilities to be exploited by cybercriminals. The concept of Cyber Third-Party Risk Management, or C-TPRM, is an emerging concept in the business world. All third-party suppliers or partners harbor possible security vulnerabilities and threats. Even if an organization has implemented best cybersecurity practices, its data, customers, and reputation can be at risk with third-party engagements. Organizations have sought efficient and effective ways of assessing the potential cybersecurity risks associated with their business partners. Apart from intrusive methodologies for assessing the cybersecurity risks associated with an organization, such as penetration testing, non-intrusive technologies are emerging to assist in C-TPRM through the integration of publicly available data without requiring engagement with the concerned organization. To quantify the third-party funds variable, we used the third-party fund ratio; for the credit risk variable, we made use of the nonperforming loan and non-performing financing ratios; in order to determine the market risk variable, we applied the net interest margin ratio; for the operational risk variable, we made use of the BOPO ratio; and for the profitability variable, we applied the return on assets ratio. According to Sanur Sharma et al. In the paper, several sentiment analysis approaches related to social media security and analytics have been discussed along with their focus areas like deception detection, anomaly detection, risk management, and disaster relief.

It also covers security issues related to data provenance, distrust, ecommerce security, consumer security breaches, market surveillance, credibility, and risk assessment. The paper compares various machine learning techniques and performance metrics, identifying gaps, issues, and recent advancements in the field. The research proposed by Jide Edu et al. explains a methodology for automatically assessing security and privacy issues in messaging platform chatbots. It focuses on the dangers of chatbots on Discord, which is a platform that does not use user-permission checks. The research discovered that 55% of Discord chatbots ask for "administrator" permission, and only 4.35% have a privacy policy. According to Marco Arazzi et al. Cyber Threat Intelligence (CTI) is critical in identifying and mitigating threats in the digital era. Natural Language Processing (NLP) has emerged as a powerful tool for enhancing CTI capabilities. This survey paper provides an overview of NLP-based techniques used in CTI, including data crawling, analysis, relationship extraction, sharing, and collaboration. It also discusses challenges and limitations, including data quality issues and ethical considerations. According to Murat Karabatak et al. artificial intelligence (AI) has become more prevalent over time as cybersecurity and digital forensics experts utilise it to fight cybercrime. The applications of artificial intelligence and NLP in the context of cybersecurity and digital forensics range from expert systems to data mining, knowledge representation, and pattern recognition. Role, applications, challenges, and future directions for NLP- based systems in the areas of cybersecurity and digital forensics constitute the core body of this paper's literature review. In addition to offering a roadmap for the future, this article guides scholars and practitioners on the state of cybersecurity and digital forensics now.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 5, June 2025
Impact Factor: 7.67

III.I. SUB-HEADING

- Traditional Third-Party Risk Management Approaches
- The Role of Natural Language Processing in TPRM
- Case Studies and Practical Implementations

III.II. TABLES, FIGURES AND EQUATIONS

Figure 1: Workflow of NLP in Third-Party Risk Management

NLP Technique	Application TPRM	Example Usage
Sentiment Analysis	Assessing Vendor reputation	Monitoring news and social media mentions
Entity Recognition	Extracting critical data from contracts	Identifying Key entities like Vendors, terms

Equation 1: Sentiment Scoring Formula

Table 1. NLP Techniques Used in TPRM

III.III. FIGURES

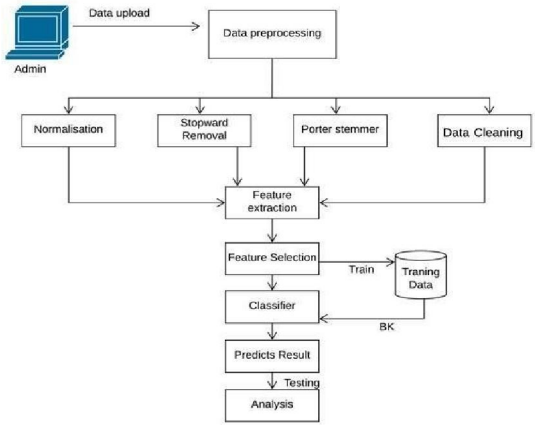

Figure 1: Workflow of NLP in Third-Party Risk Management

III.IV. EQUATIONS

$S = Pi – ni / N$

Where:

S = Sentiment score,

pi = Positive words,

ni = Negative words,

N = Total words analyzed.

IV. METHDOLOGY

Input:

Third-party data parameters: Information regarding the vendor, financial reports, legal cases, compliance records, social media, threat intelligence, etc. Contract and documents: Legal, compliance documents data to be taken up for NLP-based analysis. Vendor behavior parameter: Delivery schedules, cybersecurity incidents, performance metrics. It shall take up all the appropriate input parameter data from the above.

Output:

Risk scores: AI-generated risk ratings for third-party vendors.

Vendor recommendations: AI-suggested alternative vendors based on risk assessments. Risk trends and dashboards: Visual summaries of key risks, compliance, and overall vendor health.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 5, June 2025
Impact Factor: 7.67

V. APPLICATIONS

1. Automated Risk Assessment

An NLP-enabled bot can mainly be used to automate the risk assessment process. The bot can use NLP techniques to analyze different unstructured documents, like contracts, financial reports, and compliance papers, to identify third-party vendors with possible risks. Automation through an NLP-enabled bot accelerates the risk assessment process while also increasing its accuracy by removing the possibility of errors due to human involvement.

2. Continuous Monitoring

The bot might be constantly monitoring third-party providers by scanning real-time information from sources including news articles, social media posts, and industry reports. It will track changes in the reputation of a vendor by using sentiment analysis and entity identification to alert the risk manager. This would allow organizations to identify potential issues when they were still manageable, rather than when they had reached major crisis proportions.

3. Enhanced Due Diligence

An NLP-equipped bot can streamline the due diligence process further by automatically collecting and analyzing relevant information about third-party providers. By extracting vital details such as soundness of the financial status, compliance history, and past events from a vast number of sources, the bot can arm the risk managers with all-inclusive knowledge. Due to the heightened due diligence process, organizations become better decision makers regarding their association with vendors.

4. Regulatory Compliance

Support Overseeing regulatory compliance will be an integral part of TPRM. An NLP-enabled bot can help the organization maintain industry norms and regulations by continuously analyzing the documents related to the vendors for the clauses and requirements related to compliance. The bot can identify any non- compliance issues, enabling the organizations to eradicate the issues before getting slapped with the fines.

VI. RESULTS AND DISCUSSION

1. Key Findings from Literature Review

The literature review will reflect the growth of NLP in Third-Party Risk Management. Traditional approaches to risk assessment rely on human analysis of documents, which takes time and can be prone to errors. Reviewed studies show that NLP-based techniques, including text mining, sentiment analysis, and named entity recognition (NER), can be used to increase the accuracy and efficiency of a risk assessment.

• Sentiment Analysis helps detect negative trends in vendor reputation by analyzing social media, news articles, and reviews.

• Named Entity Recognition (NER) automatically identifies critical entities like vendors, contracts, and risk-related terms from large datasets.

• Machine Learning Models improve risk prediction accuracy by continuously learning from historical data.

2. Findings of the Research Methodology

A well-defined methodology for research into risk assessment with NLP is given by the systematic approach. According to the framework, discussed:

• Automated Risk Scoring: NLP models process a large amount of vendor contracts, financial reports, and regulatory data to dynamically create risk scores.

• Real-time monitoring: Sentiment analysis powered by AI will allow organizations to continuously monitor vendor credibility and be proactive about any risks.

• Data-Driven Decisions. Insights extracted from unstructured data enable companies to choose low- risk vendors, thereby minimizing the potential for compliance failure.

The results point to the conclusion that AI-based solutions outperform manual risk assessment significantly in reducing processing time, human error, and operational costs.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 5, June 2025
Impact Factor: 7.67

3. Implementation Barriers

However, NLP implementation in TPRM offers a few implementation barriers:

• Data Quality Issues: Since most of the unstructured data is erroneous, noisy, and biased in nature, it usually impacts the model accuracy of the NLP system.

• Integration with Legacy System: Most traditional risk management systems are not aligned with NLP-based automation by most organizations.

• Regulatory and Compliance Restraints: Data protection laws such as GDPR and CCPA impose tough limits on the usage of vendor data and automated decision making.

These should be addressed by:

• Improved data preprocessing techniques for better accuracy of the NLP models

• API based integration to connect NLP tools with legacy TPRM systems

Regulatory compliant AI frameworks to enable transparent and auditable risk assessment.

4. Future Research Directions

It must cover areas including further development of NLP-driven TPRM.

• Real-time monitoring of risk. Event-driven AI models updating their risk scores with external factors, such as fluctuations in the market and regulatory changes.

• Explainable AI Risk Management: Improving Interpretability in NLP Models in Support of Understandable Inferences into Decisions for Compliance to Regulation.

• Cross-domain NLP Integration: Using NLP in finance analysis, cyber security, and legal compliance in order to attain a comprehensive view of risk.

VII. CONCLUSION

In today's increasingly complex business environment, any organization needs to efficiently manage third- party risks that might hinder its operations or breach legal requirements. A whole new approach to the TPRM processes is revolutionized by Natural Language Processing through an NLP enabled bot. It has demonstrated several uses of an NLP-enabled bot, which include but are not limited to automation of risk assessment, continuous monitoring of vendor performance, and due diligence, and finally regulation compliance. It can help the organization streamline its process in the light of managing risks with the advent of newer NLP techniques and quicker and more accurate identification of risks already prevalent through third-party vendors.

VIII. ACKNOWLEDGMENT

We would like to express our heartfelt gratitude to all those who supported and guided us throughout the development of this survey paper. First and foremost, we sincerely thank Assistant Professor Snehal Bagal, Department of Artificial Intelligence and Data Science, AISSMS Institute of Information Technology, for her constant guidance, encouragement, and valuable insights that helped shape this research. We also extend our appreciation to the Department of Artificial Intelligence and Data Science, AISSMS IOIT, for providing the necessary infrastructure and academic environment that enabled us to carry out this study successfully.

Finally, we are grateful to our families, friends, and peers for their unwavering support and motivation during the course of this work.

REFERENCES

[1]. Keskin, Omer F., et al. "Cyber third-party risk management: A comparison of non-intrusive risk scoring reports. "Electronics 10.10 (2021): 1168.

[2]. Sondakh, Jullie Jeanette, Joy Elly Tulung, and Herman Karamoy. "The effect of third-party funds, credit risk, market risk, and operational risk on profitability in banking." Journal of Governance and Regulation/Volume 10.2 (2021).

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 5, June 2025
Impact Factor: 7.67

[3]. S.Sharma and A. Jain, "Role of sentiment analysis in social media security and analytics," Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery, vol. 10, no. 5, p. e1366, 2020.

[4]. J.Edu, C. Mulligan, F. Pierazzi, J. Polakis, G. Suarez-Tangil, and J. Such, "Exploring the security and privacy risks of chatbots in messaging services," in Proceedings of the 22nd ACM internet measurement conference, October 2022, pp. 581–588.

[5]. M. Arazzi, D. R. Arikkat, S. Nicolazzo, A. Nocera, and M. Conti, "Nlp-based techniques for cyber threat intelligence," arXiv preprint arXiv:2311.08807, 2023.

[6]. D. O. Ukwen and M. Karabatan, "Review of nlp-based systems in digital forensics and cybersecurity," in 2021 9th International symposium on digital forensics and security (ISDFS). IEEE, June 2021, pp. 1–9.

[7]. Abrahams, Temitayo Oluwaseun, et al. "Reviewing third-party risk management: best practices in accounting and cybersecurity for superannuation organizations." Finance & Accounting Research Journal 6.1 (2024): 2139.

[8]. Lee, I. "Internet of Things (IoT) cybersecurity: Literature review and IoT cyber risk management. Future Internet, 12 (9), 157." 2020.

[9]. Hasal, Martin, et al. "Chatbots: Security, privacy, data protection, and social aspects." Concurrency and Computation: Practice and Experience 33.19 (2021): e6426.

[10]. Yang, Jing, et al. "A systematic literature review of information security in chatbots." Applied Sciences 13.11 (2023): 6355.Gondaliya, Krishna, Sergey Butakov, and Pavol Zavarsky. "SLA as a mechanism to manage risks related to chatbot services." 2020 IEEE 6th Intl Conference on Big Data Security on Cloud (Bigdata Security), IEEE Intl Conference on High Performance and Smart Computing, (HPSC) and IEEE Intl Conference on Intelligent Data and Security (IDS). IEEE, 2020