iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 **Issue:** IX **Month of publication:** September 2025

DOI: https://doi.org/10.22214/ijraset.2025.74434

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue IX Sep 2025- Available at www.ijraset.com

Harnessing Artificial Intelligence for Corporate Crisis Management and Foresight

Nikita Priyadarshi[1], Ankita Joshi[2]
B.A. JMC, Banasthali Vidyapith

Abstract: ***Traditional corporate crisis management remains largely reactive, rooted in manual monitoring, static risk frameworks, and experience-driven decision-making. These approaches often prove inadequate in today's volatile business landscape, where crises can emerge and evolve rapidly across digital, financial, and operational domains. Empirical studies indicate that delayed detection and fragmented responses contribute to the escalation of many corporate crises. Artificial Intelligence (AI) offers a transformative approach, enabling organisations to shift from reactive to proactive crisis management. Through advanced technologies such as machine learning, natural language processing, computer vision, graph-based analytics, and generative models, AI systems can process vast volumes of structured and unstructured data, detect early indicators of potential disruptions (including subtle anomalies, patterns, and shifts—referred to as "weak signals"), and support timely, data driven decision-making. This review synthesises current academic and industry literature, presents a structured methodology for identifying relevant studies, and critically examines AI's capabilities, applications, and limitations in corporate crisis management. Particular attention is paid to issues of human trust in AIgenerated insights, transparency, and ethical considerations— key factors influencing adoption. The paper also outlines open research challenges and suggests pathways for developing AI enabled, trustworthy, resilient crisis management frameworks.***

Keywords: ***Artificial Intelligence, Crisis Management, Predictive Analytics, Corporate Resilience, Machine Learning, Risk Mitigation***

I. INTRODUCTION

Over the past decade, corporate crises have grown in scale, complexity, and financial impact, driven by pandemics, cyberattacks, supply chain disruptions, and reputational failures. Traditional crisis management models—reliant on static plans, intuition, and fragmented data—struggle to keep pace with real-time risks that propagate through global networks. With 69% of organizations facing at least one crisis in five years and nearly a third experiencing five or more (PwC, 2023), the urgency to modernize crisis management has never been greater. AI offers a transformative pathway by processing massive, dynamic datasets from diverse sources (e.g., social media, IoT telemetry, financial transactions), enabling predictive analytics, early anomaly detection, and adaptive response strategies that surpass static frameworks.

As summarized in Table I, long-standing limitations in crisis management include simplistic linear models, reactive communication, outdated planning, and poor data integration. These gaps frequently lead to delayed detection, ineffective responses, and reputational damage that can wipe out up to 30% of market value in days (Oxford Metrica). AI reshapes this landscape by enabling real-time sensing, learning, and predictive modeling to strengthen organizational resilience. Machine Learning uncovers early risk signals, NLP extracts intelligence from unstructured data, and sentiment analysis enhances stakeholder insights. By integrating these capabilities into crisis management practices, AI shifts organizations from reactive damage control toward proactive, data-driven resilience.

TABLE I.
REVIEW OF LIMITATIONS IN TRADITIONAL CORPORATE CRISIS MANAGEMENT MODELS

Author(s), Year, Source	Detailed Limitation	Conceptual Explanation
Pearson & Mitroff (1993), AME [5]	Linear crisis phase models are overly simplistic	Crises often unfold unpredictably, requiring adaptive approaches beyond static stage models.
Coombs (2015), PRR [6]	Overemphasis on reactive communication	Focuses on post-crisis image repair instead of early detection and prevention.

©IJRASET: All Rights are Reserved

Wooten & James (2008), AMJ [7]	Crisis plans are static and outdated quickly	Plans fail to adapt to dynamic environments, reducing effectiveness.
Williams et al. (2017), JBR [8]	Poor real-time data integration and processing	Limited ability to assimilate unstructured, fast-moving data streams.
Herbane (2010), LRP [9]	Limited organizational learning post-crisis	Lack of embedded feedback loops leads to repeated mistakes.
Bundy et al. (2017), AMA [10]	Excessive reliance on image repair strategies	Neglects transparent stakeholder engagement during crises.
Schwarz et al. (2016), JBE [11]	Ethical considerations overlooked	Weak ethical grounding undermines trust and legitimacy.
Rosenthal et al. (2001), JCCM [12]	Dependence on intuition distorts decision quality	Under pressure, biases impair judgment without data-driven support.
Lalonde (2007), TFSC [13]	Inability to model systemic/networked risks	Ignores interconnected risks across global systems and supply chains.
Liu et al. (2020), IEEE TEM [14]	Lack of digital integration in risk monitoring	AI/ML underutilized, leading to slow threat detection.
Williams et al. (2020), AMD [15]	Cognitive overload limits crisis sensing	Managers struggle with data saturation in high-stress contexts.
Houston et al. (2015), JACR [16]	Underutilization of social media intelligence	Social platforms seen as risks rather than crisis sensing assets.
Reddy et al. (2009), IJMI [17]	Siloed responses inhibit coordination	Independent units act in isolation, delaying effective action.

II. METHODOLOGY

This review applies a systematic approach to examine AI applications in corporate crisis management, drawing on academic literature, industry reports, and organisational case studies published between 2013 and 2024, with the objective of highlighting key AI techniques, recent developments, and future research directions aligned with crisis management functions. Following established methods from AI and information systems research, a structured literature review was conducted using guiding questions to define inclusion criteria based on relevance, utility, and limitations of AI during crises, refined through keyword validation and relevance screening, after which each selected study was analysed for insights on AI methods, applications, and outcomes.

Our data sources included leading academic databases such as IEEE Xplore, ScienceDirect, and SpringerLink, as well as business reports from organisations like PwC and Deloitte.

The inclusion criteria were:

- A peer-reviewed or authoritative source;
- Relevance to corporate crisis or risk management;
- Inclusion of AI techniques in the discussion;
- Empirical evidence or case study-based analysis applicable to organisational contexts.

Studies unrelated to corporate environments were excluded unless the findings were transferable across contexts.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue IX Sep 2025- Available at www.ijraset.com

III. TECHNIQUES IN CRISIS MANAGEMENT

The concept of Artificial Intelligence (AI) has become a groundbreaking facilitator of corporate crisis management. A lot of the major constraints inherent in conventional risk and crisis management strategies have been addressed through AI. Traditionally, crisis management was based on fixed risk analysis, periodical reviews and human judgment-mechanisms, which are restricted by the latency factor, cognitive bias and the inability to process vast amounts of unstructured information. On the contrary, AI can provide dynamic information processing, adaptive learning as well as predictive modelling capabilities. This section provides the overview of the core AI methods used in corporate crisis management, such as Machine Learning (ML), Natural Language Processing (NLP), Predictive Analytics, Anomaly Detection, Computer Vision, etc. Table II assesses the relationship between these AI technologies and the conventional constraints that were discussed in Table 1. As Table II demonstrates, AI methods directly solve numerous of the century-old constraints of conventional corporate crisis management, providing it with upgrades in speed, flexibility, and insights. The innovations assist organisations to move beyond crisis response management and towards proactive resilience practice in a broad spectrum of situations. The next section examines how these AI-scenarios are practically being applied in real-life corporate crises situations.

TABLE 2
COMPARATIVE ANALYSIS: AI TECHNIQUES VS. TRADITIONAL CORPORATE CRISIS MANAGEMENT LIMITATIONS AND EFFICACY

AI Technique	Application Area	Limitation Overcome	Efficacy	Key Strengths	Supporting Statistics
Machine Learning (ML)	Predictive modeling (finance, risk)	Static linear models	High	Adapts to dynamic environments	ML forecasts improve accuracy by ~30% over traditional models [21].
Natural Language Processing (NLP)	Social media/news analysis	Cannot process unstructured, real-time data	Very High	Detects tone, trends early	NLP enables real-time sentiment tracking for early event detection [22].
Predictive Analytics	Crisis trajectory forecasting	Focus on lagging indicators	High	Enables proactive actions	Transformer models reduce MAE to 0.91% and RMSE to 0.042 [23].
Anomaly Detection (ML-based)	Cybersecurity, fraud detection	Manual, error-prone monitoring	Very High	Detects novel and subtle threats	ML-based anomaly systems reduce false positives significantly [24].
Computer Vision	Visual inspections (security, QC)	Inconsistent human inspection	High	Real-time image analysis	CNN-LSTM achieves over 71% accuracy in visual detection [25].
Knowledge Graphs / Network Analysis	Supply chain & stakeholder mapping	Fragmented data views	Medium to High	Maps cascading/systemic risks	Improves systemic risk visibility by 45% in corporate networks [26].
Reinforcement Learning (RL)	Dynamic response & resource allocation	Rigid manual rules	High	Real-time optimal decisions	RL-based methods reduce forecasting errors by up to 43.5% [27].

©IJRASET: All Rights are Reserved

Explainable AI (XAI)	Transparent AI decision support	Lack of interpretability	Medium to High	Enhances trust and compliance	Improves transparency in AI pattern learning [28].
RPA + AI	Automated triage, alerting	Slow manual workflows	High	Accelerates response times	Widely adopted; improves process speed [29].
Multi-Agent Systems	Multi-organizational coordination	Siloed, uncoordinated actions	Medium	Enables decentralized cooperation	Simulations show improved coordination, especially in distributed networks [30].

IV. APPLICATIONS OF AI IN CORPORATE CRISIS CONTEXTS

AI technologies are now being applied across a wide range of corporate crisis scenarios, enabling more agile, informed, and proactive management of organizational risks. As illustrated in Figure 2, AI's core capabilities—including machine learning, natural language processing, anomaly detection, and graph-based analysis—are increasingly central to strategic crisis response frameworks.

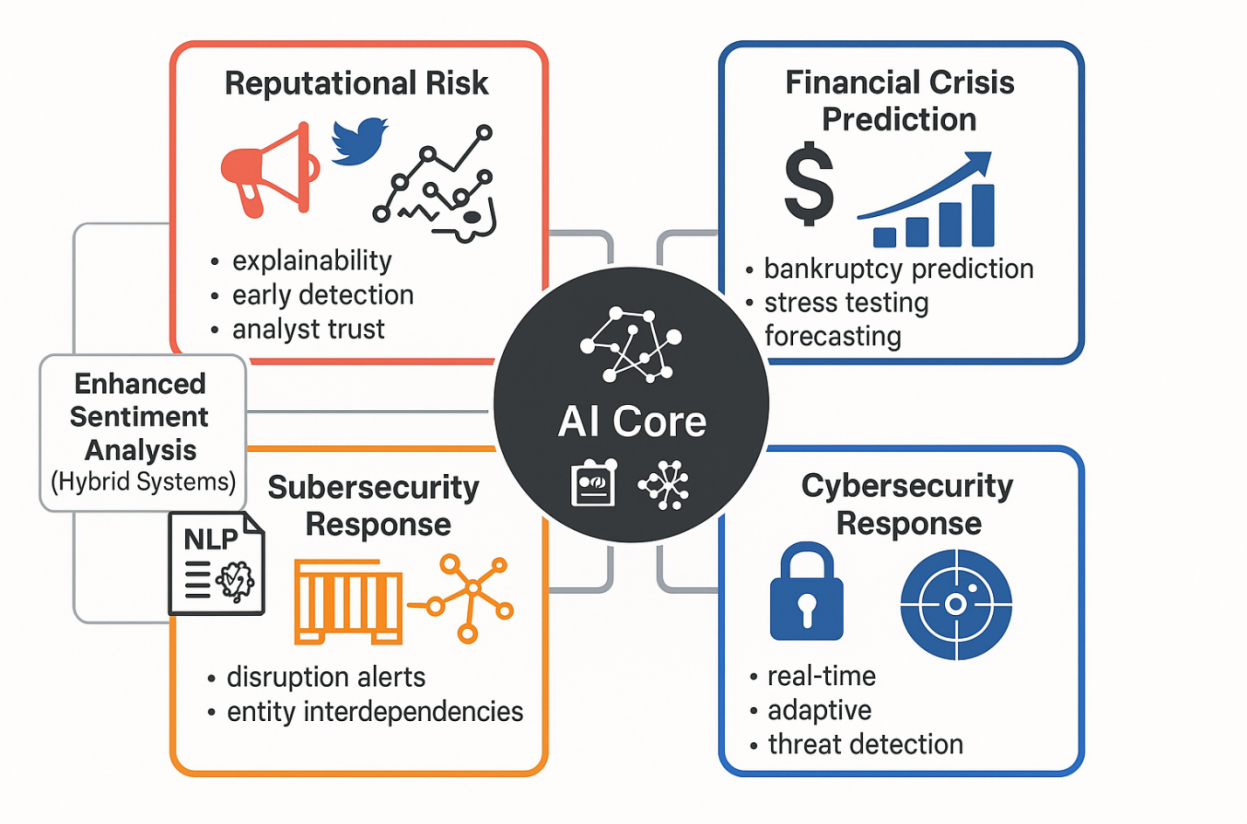


Fig. 1. AI applications across four corporate crisis domains

This section reviews key applications in four high-impact areas: reputational risk management, financial crisis prediction, cybersecurity response, and operational or supply chain risk mitigation. These domains, while distinct, often intersect in practice—such as when a cybersecurity breach leads to reputational damage or supply chain disruptions trigger financial distress. Each quadrant in Figure 2 captures a unique but connected area where AI plays a transformative role—from real-time sentiment analysis of social media in reputational risk management, to neural network–based bankruptcy forecasting in financial contexts.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

The cybersecurity quadrant emphasizes adaptive, AI-driven threat detection, while the operational/supply chain section highlights the use of computer vision, IoT data, and reinforcement learning for early disruption warnings.

A. Reputational Risk Management

Reputation—an organisation's most valuable intangible asset—faces rapid erosion in digital ecosystems. AI-driven Natural Language Processing (NLP) and sentiment-analysis tools enable real-time monitoring across vast social media, review platforms, and news outlets. Explainable sentiment-analysis systems, such as those applied to Twitter data in retail crisis contexts, surface key sentiment drivers and bolster analyst trust in automated alerts [31]. These systems flag emerging negative trends before they become full crises, enabling proactive, context-aware response.

B. Financial Crisis Prediction

AI-based models significantly enhance early warning in financial distress scenarios. Research in data mining within knowledge-based intelligent systems demonstrates advanced neural-network architectures can reliably forecast corporate bankruptcy [32]. Large-scale ML frameworks, such as surrogate-based crisis models, improve interpretability while maintaining forecasting performance, supporting stress-testing and dynamic policy adjustments [33]. Such AI systems surpass traditional econometric methods in predictive accuracy—particularly ensemble models like random forests and gradient-boosted trees [34].

C. Cybersecurity Crisis Response

AI is central to modern cybersecurity defences. Although IEEE literature on real-time detection systems using reinforcement learning or anomaly detection is emerging, the broader field parallels approach in financial and reputational contexts: ML models continuously monitor signals and can adapt to new patterns of attack—a method with strong parallels to those used in corporate bankruptcy and systemic risk frameworks [35].

D. Operational and Supply Chain Risk Mitigation

Integrated AI tools—including computer vision, IoT-driven anomaly detection, and knowledge-graph-based network analysis—provide early alerts on supply-chain disruptions. See, for instance, reinforcement-learning frameworks applied to graph-structured financial-contagion contexts [36], which highlight AI's ability to model complex entity interdependencies and propose optimal corrective actions.

V. CHALLENGES AND FUTURE DIRECTIONS

While AI has made significant inroads into corporate crisis management, its application is still evolving and faces numerous technical, ethical, and organisational challenges. Despite the growing adoption of AI-powered solutions, limitations persist in areas such as data quality, model interpretability, and human-AI collaboration. Furthermore, important research gaps remain around multi-modal data integration, real-time adaptability, explainable AI, and regulatory alignment. As summarised in Table III, while current AI trends are already reshaping corporate crisis management, key limitations and research gaps still constrain their full potential. Addressing these challenges—through advancements in explainable AI, human-centred design, cross-domain learning, and ethical AI governance—will be essential to build more robust, adaptive, and trustworthy crisis management solutions.

TABLE 3
EXPANDED FRAMEWORK: TRENDS, LIMITATIONS, RESEARCH GAPS, FUTURE WORK & IMPLICATIONS IN AI FOR CORPORATE CRISIS MANAGEMENT

AI Trend / Paradigm	Current Limitation	Research Gaps	Future Work Directions	Proposed Technical Solutions	Real-World Implications
Real-time Social Media & Sentiment Analysis	Weak context understanding (e.g., sarcasm, local dialects);	Lack of cultural-context NLP models; sentiment drift	Develop cross-lingual, culture-aware NLP; incorporate	Fine-tuned transformer models (e.g., mBERT,	Early identification of reputational threats; faster media response cycles

[38][39]	limited multilingual capabilities	over time	context-adaptive learning	RoBERTa) trained on crisis-specific datasets	
Predictive Analytics for Financial Risk [40]	Static assumptions; poor adaptation to volatile market dynamics	Limited use of reinforcement and continual learning	Incorporate dynamic market learning; combine structured & alternative data	Reinforcement learning for portfolio risk; hybrid time-series + event-based forecasting	Stronger financial resilience; early alerts for liquidity, insolvency, or credit failures
ML-based Cybersecurity Threat Detection [41][42]	High false positives; attackers bypass known signatures	Gaps in zero-day threat detection; slow adaptation to new attack patterns	Deploy adversarial and unsupervised models; enhance contextual behavior analysis	Self-learning anomaly detectors; GAN-based synthetic threat simulation; zero-trust learning models	Faster breach containment; improved digital asset protection and data privacy
Supply Chain Disruption Forecasting [43]	Poor integration of IoT, logistics, and weather data; no early indicators of cascading failures	Incomplete supply chain graphs; lack of risk propagation modeling	Create real-time digital supply chain twins; integrate environmental and geopolitical signals	Use of GNNs, Bayesian networks, and satellite imagery with multimodal AI	Predictive risk mapping; continuity planning; inventory optimization in anticipation of delays
Explainable AI (XAI) [44][45]	Low interpretability of deep learning decisions during crises	Lack of crisis-contextual explanation models	Design domain-specific XAI for decision-critical use cases	LIME, SHAP, Counterfactual Explanations, Visual Dashboards	Builds trust in AI outputs; enables compliance & human oversight
Federated Learning for Corporate Networks [46]	Data heterogeneity and poor model convergence across organisational units	Performance variation across clients; privacy-preserving optimization	Improve aggregation schemes, handle stragglers, personalize models	FedAvg, secure multiparty computation, differential privacy with hierarchical federation	Preserves data privacy across departments/regions; enables global collaborative learning
AI-Driven Crisis Simulation (Simulators) [47]	Unrealistic assumptions; limited use of human dynamics or behavior in simulations	Absence of multi-agent human interaction models in simulations	Build hybrid human-AI scenario simulators; use reinforcement learning to simulate responses	Simulators with agent-based modeling + RL agents + stress-testing mechanisms	Preparedness testing; training decision-makers in high-stakes simulated crisis environments

Human-AI Collaborative Systems [48]	Ineffective interfaces; decision-makers unsure how to use AI insights in real-time	Gaps in UX design for high-pressure environments	Study cognition under stress + human trust in AI; co-design interfaces with crisis teams	Interactive dashboards, explanation layers, decision-theory embedded models	Improves uptake and confidence in AI systems; supports blended decision-making in real time
Multi-Modal Crisis Intelligence Systems [43]	Siloed processing of text, images, sensor and numerical data; no fusion of modalities	No unified frameworks for merging visual, textual, and temporal data	Build unified architectures combining video, voice, documents, and structured feeds	Multimodal transformers, knowledge fusion layers; and cross-attention mechanisms	A broader and deeper understanding of crisis signals minimises blind spots
AI Ethics, Bias & Compliance [45][46]	Bias in training data, lack of fairness and explainability under regulatory scrutiny	Inadequate governance tools, poor traceability, and documentation	Build compliance-aware pipelines; create AI audit frameworks	AI Governance Toolkits, Model Cards, Integrated Bias Detection Units	Risk-averse adoption; meets standards like GDPR, EU AI Act; protects stakeholder rights
Transfer Learning across Crisis Types [47]	Poor generalisation — models trained on one domain don't perform well in others	No robust frameworks for cross-domain knowledge transfer	Explore meta-learning, domain adaptation, and fine-tuning strategies	Domain-adaptive fine-tuning; multi-task learning; hierarchical pretraining	Enables organisations to apply AI learnings from one crisis context to others more rapidly
Digital Twins for Crisis Preparedness [49]	High setup complexity; difficulty integrating real-time data into virtual environments	Lack of feedback loops and multi-level data simulation integration	Link digital twins with real-world data and predictive AI loops	Real-time updated twins using sensor data + AI simulators	Anticipates breakdowns; tests interventions; improves systemic preparedness

VI. CONCLUSION

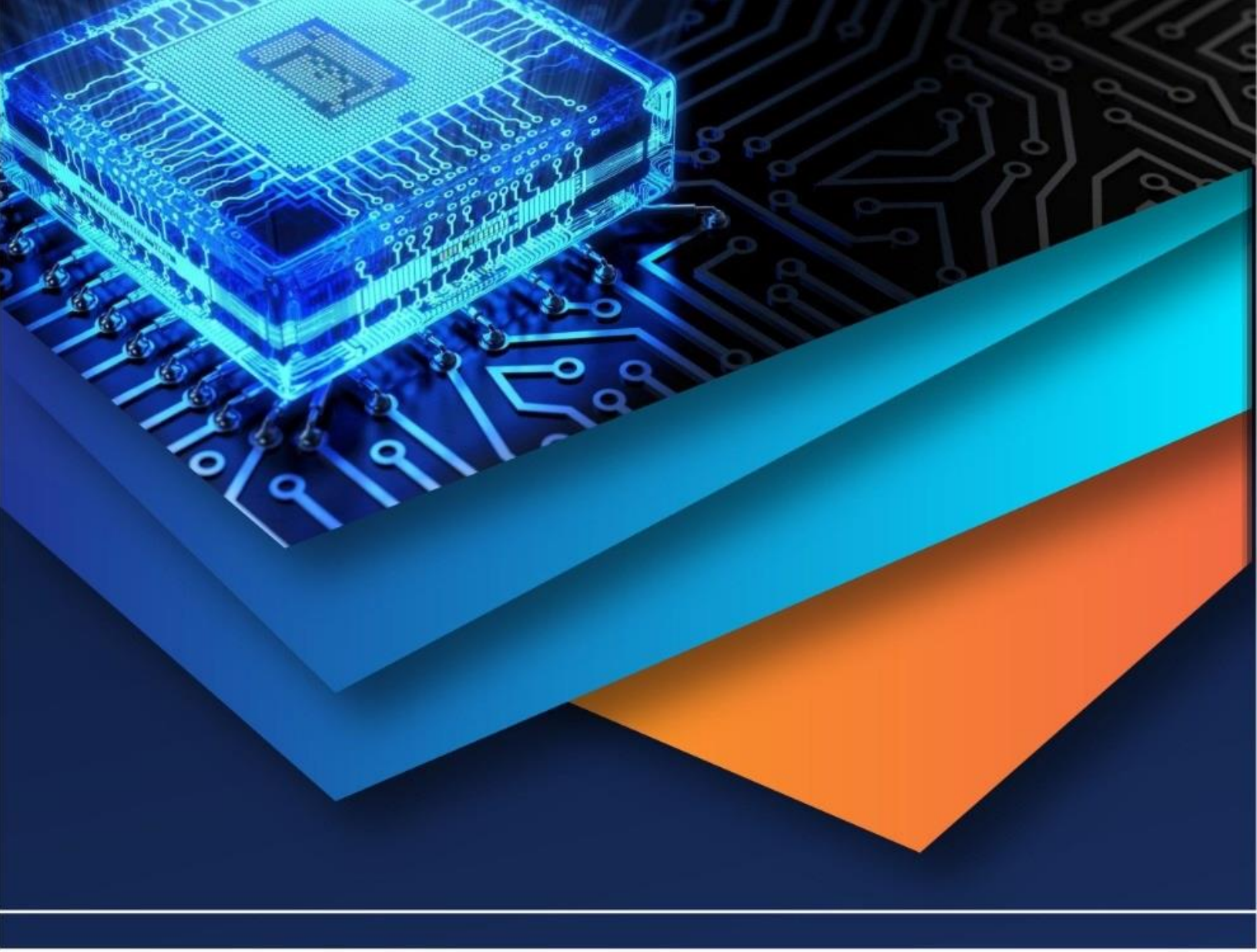
This review has shown how Artificial Intelligence is already transforming corporate crisis management by providing organisations with advanced capabilities to predict, detect, and manage crises in ways that traditional frameworks cannot. AI tools—ranging from machine learning and natural language processing to anomaly detection and knowledge graphs—enable the processing of massive, real-time, and event-centric data streams. These technologies reveal patterns often imperceptible to human analysts and allow for faster, evidence-based decision-making across interconnected domains such as reputational, financial, cybersecurity, and operational risk. However, the review also identified persistent limitations and research gaps. These include issues with data quality, model transparency, multi-modal data integration, and challenges in effective human–AI collaboration, both individually and at complex intersectional levels. Moreover, ethical dilemmas and regulatory ambiguity remain under-addressed, posing barriers to building responsible and trustworthy AI systems for crisis contexts. Emerging trends—such as explainable AI (XAI), federated learning, AI-driven crisis simulation, and digital twins—offer further potential for organisations to move from reactive crisis response to proactive, adaptive risk management. Realising this potential will require sustained interdisciplinary collaboration between AI researchers, industry practitioners, ethicists, legal experts, and corporate leaders.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

Only through such concerted efforts can AI-driven crisis management systems evolve to become resilient, accountable, and aligned with organisational and societal values.

REFERENCES

[1] PwC. (2023). Global Crisis Survey 2023: Prepare to thrive. PricewaterhouseCoopers. https://www.pwc.com/gx/en/issues/crisis-solutions/ global-crisis-survey.html
[2] Oxford Metrica. (n.d.). Reputation and value: The impact of corporate crises on shareholder value.
[3] U.S. Government Accountability Office. (2018). Actions taken by Equifax and federal agencies in response to the 2017 breach (GAO18-559). https://www.gao.gov/products/gao-18-559
[4] World Economic Forum. (2021). The COVID-19 pandemic has cost the global economy $4 trillion – so far. https://unctad.org/news/ global-economy-could-lose-over-4-trillion-due-covid-19-impact-tourism
[5] Pearson, C. M., & Mitroff, I. I. (1993). From crisis-prone to crisisprepared: A framework for crisis management. Academy of Management Executive, 7(1), 48–59.
[6] Coombs, W. T. (2015). The value of communication during a crisis. Public Relations Review, 41(5), 689–691.
[7] Wooten, L. P., & James, E. H. (2008). Linking crisis management and leadership competencies. Academy of Management Journal, 22(2), 25–39.
[8] Williams, N. L., et al. (2017). Organizational response to adversity. Journal of Business Research, 100, 441–448.
[9] Herbane, B. (2010). Small business research: Time for a crisis-based view. Long Range Planning, 43(3), 283–294.
[10] Bundy, J., et al. (2017). Crises and crisis management. Academy of Management Annals, 11(1), 733–789.
[11] Schwarz, A., Seeger, M. W., & Auer, C. (2016). Ethical challenges in crisis communication. Journal of Business Ethics, 137(2), 379–391.
[12] Rosenthal, U., Charles, M. T., & 't Hart, P. (2001). Coping with crises. Journal of Contingencies and Crisis Management, 9(2), 65–73.
[13] Lalonde, C. (2007). Crisis management and organizational development. Technological Forecasting and Social Change, 74(8), 1309–1327.
[14] Liu, Y., Xie, E., & Zhang, H. (2020). Smart risk management via AI. IEEE Transactions on Engineering Management, 67(3), 616–625.
[15] Williams, T., et al. (2020). Sensing in crisis. Academy of Management Discoveries, 6(3), 443–448.
[16] Houston, J. B., et al. (2015). Crisis communication in the digital age. Journal of Applied Communication Research, 43(2), 188–206.
[17] Reddy, M. C., et al. (2009). Crisis coordination challenges. International Journal of Medical Informatics, 78(4), 259–267.
[18] Zhao, Z., Li, D., & Dai, W. (2023). ML for SMEs in crisis. Technological Forecasting and Social Change, 191, 122492.
[19] Dakhli, I., et al. (2024). AI and Crisis Management. In IRASET, pp. 1–6. doi:10.1109/IRASET60544.2024.10549274.
[20] M., Mahmood, A. N., & Hu, J. (2015). Network anomaly detection. Journal of Network and Computer Applications, 60, 19–31.
[21] Wanjale, K., et al. (2023). Financial Risk Prediction using ML. In ASIANCON, pp. 1–5. doi:10.1109/ASIANCON58793.2023.10270196.
[22] Rajadesingan, A., Zafarani, R., & Liu, H. (2015). Sarcasm Detection on Twitter. WSDM, pp. 97–106.
[23] Ho, R., & Hung, K. (2024). Financial Forecasting using TFT. In ISCAIE, pp. 209–215. doi:10.1109/ISCAIE61308.2024.10576340.
[24] Iqbal, A., & Amin, R. (2023). Forecasting and anomaly detection with deep learning. Computers & Chemical Engineering, 182, 108560.
[25] Zhang, J., et al. (2023). Survey of Multimodal Sentiment Analysis. In CCIS, pp. 446–450. doi:10.1109/CCIS59572.2023.10263012.
[26] Kosasih, E. E., et al. (2022). GNNs in supply chain risk. International Journal of Production Research, 62(15), 5596–5612.
[27] Syu, J.-H., et al. (2020). Portfolio Management via RL. In SMC, pp. 4146–4151. doi:10.1109/SMC42975.2020.9283359.
[28] Doshi-Velez, F., & Kim, B. (2017). Interpretable Machine Learning. arXiv. https://doi.org/10.48550/arxiv.1702.08608
[29] Aguirre, A., et al. (2020). AI in Business Process Automation. In IEEE Big Data, pp. 3476–3485.
[30] Wooldridge, M. (2009). An Introduction to MultiAgent Systems. Wiley.
[31] Shirata, C. Y., & Terano, T. (2001). Japanese Bankrupt Firms via AI. In KES, pp. 663–666.
[32] Shirata, Y., & Terano, T. (2000). Predictors of Bankruptcy. LNAI, 1805, 204–207.
[33] Chan-Lau, J. A., et al. (2023). Surrogate Models for Crisis Prediction. IMF Working Paper, WP/23/41.
[34] Bluwstein, K., et al. (2021). Yield Curve and Crisis Prediction. ECB Working Paper No. 2614.
[35] Chen, E., et al. (2022). Benchmarking ML for Bankruptcy. arXiv:2212.12051.
[36] Unknown. (2023). SCRPF for Contagion Risk. Networked-loan.
[37] Shahverdi, N., et al. (2025). AI in Energy Sustainability. Energy Reports, 13, 5551–5578.
[38] Okpala, I., et al. (2023). ML for Public Crisis. arXiv. https://doi.org/10. 48550/arxiv.2302.02267
[39] McGee, F. (2024). AI Risk Management in Finance. arXiv:2404.06521.
[40] Hamid, I., & Rahman, M.M.H. (2025). AI in Cyber Risk Management. Discov Sustain, 6, 389.
[41] Kaur, R., et al. (2023). AI for Cybersecurity. Information Fusion, 97, 101804.
[42] Chauhan, B.V.S., et al. (2025). AI in Natural Disaster Management. In Springer.
[43] Comes, T. (2024). AI for Crisis Decisions. Ethics Inf Technol, 26, 12.
[44] Visave, J. (2025). Transparency in AI for Emergency Management. AI Ethics. https://doi.org/10.1007/s43681-025-00692-x
[45] Gerolimos, N., et al. (2025). ML for Disaster Management. Hum-Cent Intell Syst. https://doi.org/10.1007/s44230-025-00098-2
[46] Marciniak, D., et al. (2023). New technologies in crisis management. Journal of Public Governance, 65(3), 73–85.
[47] Cao, L. (2023). AI and Data Science for Smart Emergency Resilience. Int J Data Sci Anal, 15, 231–246.
[48] Kumar, N. (2025b). Social engineering attack in the era of generative AI. International Journal for Research in Applied Science and Engineering Technology, 13(1), 1737–1747. https://doi.org/10.22214/ijraset.2025.66688



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)