International Journal of Advanced Research in Computer Science & Technology (IJARCST)

| ISSN: 2347-8446 | www.ijarcst.org | editor@ijarcst.org |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 8, Issue 6, November - December 2025||

DOI:10.15662/IJARCST.2025.0806023

Cyber Risk Assessment Models for Strategic Information Security Management

Tarang Jain

Teerthanker Mahaveer University, Moradabad, U.P., India

tarangjain@mln.du.ac.in

ABSTRACT: This paper presents a comprehensive overview of cyber risk assessment models for strategic information security management, focusing on the systematic identification, analysis, and prioritization of cyber threats and vulnerabilities to support informed decision-making, optimize security investments, and enhance organizational resilience in dynamic digital environments.

KEYWORDS: Cyber Risk Assessment, Information Security Management, Risk Modeling, Threat Analysis, Vulnerability Assessment, Strategic Decision-Making, Cybersecurity Governance

I. INTRODUCTION

The rapid digital transformation of organizations has significantly increased their dependence on information systems, cloud platforms, and interconnected networks, thereby expanding the cyber threat landscape. Cyberattacks such as data breaches, ransomware, phishing, and advanced persistent threats pose substantial risks to organizational assets, reputation, and operational continuity. As cyber risks continue to evolve in complexity and frequency, traditional reactive security measures are no longer sufficient. This has created a critical need for structured and proactive cyber risk assessment models that support strategic information security management.

Cyber risk assessment models provide a systematic approach to identifying, analyzing, and evaluating potential threats, vulnerabilities, and their potential impact on business objectives. These models enable organizations to quantify and prioritize cyber risks based on likelihood and consequence, facilitating informed decision-making at both operational and executive levels. By aligning security controls with organizational risk appetite and strategic goals, cyber risk assessment serves as a foundational element of effective information security governance.

From a strategic perspective, information security management is no longer solely a technical function but a core component of enterprise risk management and corporate strategy. Cyber risk assessment models help bridge the gap between technical security metrics and business-oriented outcomes, enabling senior management to understand cyber risks in financial, operational, and reputational terms. This alignment ensures that security investments are justified, measurable, and directly linked to business value creation and protection.

Furthermore, regulatory and compliance requirements across industries increasingly mandate formalized risk assessment and reporting practices. Frameworks such as ISO/IEC 27001, NIST Cybersecurity Framework, and risk-based governance models emphasize continuous risk evaluation and improvement. In this context, cyber risk assessment models play a vital role in ensuring compliance, enhancing organizational resilience, and supporting long-term strategic planning in an increasingly hostile cyber environment.

Overall, cyber risk assessment models form the cornerstone of strategic information security management by enabling organizations to proactively manage uncertainties, strengthen defensive capabilities, and sustain trust in digital operations.

II. LITERATURE REVIEW

Cyber risk assessment has evolved from qualitative checklists to structured, data-driven models that connect technical security issues with business consequences. Early research emphasized basic risk concepts—threat, vulnerability, and impact—often represented through qualitative matrices (e.g., low/medium/high). While these approaches are easy to implement and communicate, studies frequently highlight their limitations: subjectivity, inconsistent scoring across assessors, and weak support for comparing risks across different business units or time periods. As organizations adopted complex infrastructures such as cloud, IoT, and distributed enterprise systems, literature increasingly argued for more rigorous and scalable risk assessment approaches.

A major stream of research focuses on standards and framework-based models for cyber risk assessment. Widely adopted approaches include ISO/IEC 27005 (risk management guidance for ISO/IEC 27001 ISMS) and the NIST Risk Management Framework (RMF), along with the NIST Cybersecurity Framework (CSF) for organizing risk-related activities. The literature suggests that these models improve consistency by providing structured processes such as asset classification, threat identification, likelihood evaluation, impact estimation, control selection, and continuous monitoring. However, researchers also note that framework-based models do not automatically solve the problem of accurate quantification; organizations still struggle to convert technical assessments into business metrics such as financial loss, downtime cost, or customer churn.

Another influential category includes quantitative and probabilistic risk models. Methods such as Bayesian networks, Monte Carlo simulation, Markov chains, and attack graph analysis are frequently examined for their ability to represent uncertainty and causal relationships in cyber incidents. For example, Bayesian approaches are praised in literature for combining expert judgment with empirical data to update risk probabilities over time. Attack graphs and attack trees are widely reviewed for modeling attacker pathways, enabling security teams to identify high-risk nodes and prioritize mitigations. Despite their analytical strength, research often points out practical barriers: high data requirements, complexity in model building, and challenges in explaining outputs to non-technical stakeholders.

A growing body of work highlights risk assessment models that translate cyber exposure into economic and strategic terms. Concepts such as Annualized Loss Expectancy (ALE), Total Cost of Ownership (TCO) for security controls, and cost–benefit analysis are commonly used to justify security investments. More recent literature discusses cyber risk quantification methods such as the FAIR (Factor Analysis of Information Risk) model, which breaks risk into frequency and magnitude components and supports financial-based decision-making. Researchers generally report that financial quantification increases executive engagement and helps integrate cybersecurity into enterprise risk management, though concerns remain about estimation accuracy when historical incident data is limited or when threats rapidly change.

Recent studies also emphasize risk assessment for modern enterprise environments—particularly cloud and hybrid systems. Literature identifies shared responsibility gaps, misconfiguration risks, identity and access management weaknesses, and third-party/vendor exposure as major contributors to cyber risk. Consequently, many models incorporate supply-chain risk, vendor scoring, and continuous security posture monitoring. The rise of DevSecOps has further shifted research toward continuous risk assessment, where risks are tracked dynamically across software pipelines rather than evaluated periodically. This line of work argues that traditional annual or quarterly assessments are too slow for agile development and real-time threat landscapes.

Finally, literature increasingly links cyber risk assessment with strategic governance and organizational resilience. Research underscores that effective models must incorporate risk appetite, business criticality, and decision thresholds that guide when to accept, mitigate, transfer (insurance), or avoid risk. Cyber risk models are also studied as tools for board reporting, compliance auditing, and incident readiness planning. However, scholars consistently highlight a key gap: many organizations adopt risk frameworks in a “check-the-box” manner, without strong measurement practices or feedback loops that validate whether controls actually reduce risk.

Overall, the literature indicates that no single cyber risk assessment model fits all organizations. Qualitative methods remain useful for quick prioritization, while quantitative and probabilistic models offer stronger analytical power when sufficient data and expertise exist. The most effective approaches reported in research are hybrid models that combine frameworks (for structure and governance) with quantification (for business alignment) and continuous monitoring (for adaptability), enabling cyber risk assessment to directly support strategic information security management.

III. RESEARCH METHODOLOGY

This study adopts a **systematic, mixed-method research methodology** to develop and evaluate cyber risk assessment models for strategic information security management. The methodology is designed to integrate qualitative insights from established frameworks with quantitative risk analysis techniques to ensure both practical relevance and analytical rigor.

1. Research Design

A **design science and empirical research approach** is employed. Design science is used to conceptualize a cyber risk assessment model aligned with strategic management objectives, while empirical methods are applied to validate its effectiveness in organizational contexts. The study follows a sequential process consisting of problem identification, model design, implementation, and evaluation.

2. Literature-Based Model Development

An extensive review of prior academic literature, industry standards, and best practices is conducted to identify key components of cyber risk assessment, including asset classification, threat identification, vulnerability analysis, likelihood estimation, and impact assessment. Established frameworks such as ISO/IEC 27005, NIST Risk Management Framework, and quantitative risk models are synthesized to design a hybrid assessment model that combines qualitative and quantitative dimensions.

3. Data Collection

Data is collected using multiple sources to enhance reliability and validity:

- **Primary Data:** Structured interviews and questionnaires are administered to information security professionals, IT managers, and risk officers to capture expert judgment on threat likelihood, business impact, and control effectiveness.
- **Secondary Data:** Organizational security reports, incident logs, audit findings, and publicly available breach statistics are analyzed to support quantitative risk estimation.

4. Risk Assessment Process

The proposed methodology evaluates cyber risk through the following steps:

- **Asset Identification and Classification:** Critical information assets are categorized based on confidentiality, integrity, availability, and business value.
- **Threat and Vulnerability Analysis:** Relevant cyber threats and system vulnerabilities are identified using threat intelligence sources and vulnerability databases.
- **Risk Estimation:** Risk is quantified using a combination of qualitative scoring and quantitative techniques such as likelihood–impact matrices and loss estimation models.
- **Risk Prioritization:** Identified risks are ranked to determine their strategic significance and treatment priority.

5. Model Validation and Evaluation

The proposed cyber risk assessment model is validated through a **case study approach**, applying it to a representative enterprise environment. Key performance indicators such as risk reduction, decision accuracy, and alignment with business objectives are used to evaluate effectiveness. Comparative analysis is performed against traditional risk assessment methods to assess improvements in strategic decision support.

6. Data Analysis Techniques

Qualitative data from interviews is analyzed using thematic analysis, while quantitative data is evaluated using descriptive statistics and scenario-based risk simulations. The results are interpreted to assess how effectively the model supports strategic information security management.

7. Ethical Considerations

All data collected is anonymized to protect organizational confidentiality. Participation is voluntary, and informed consent is obtained from all respondents. Sensitive security information is handled in accordance with ethical research and data protection guidelines.

This research methodology ensures a balanced and robust evaluation of cyber risk assessment models, providing actionable insights for aligning information security practices with strategic organizational goals.

DOI:10.15662/IJARCST.2025.0806023

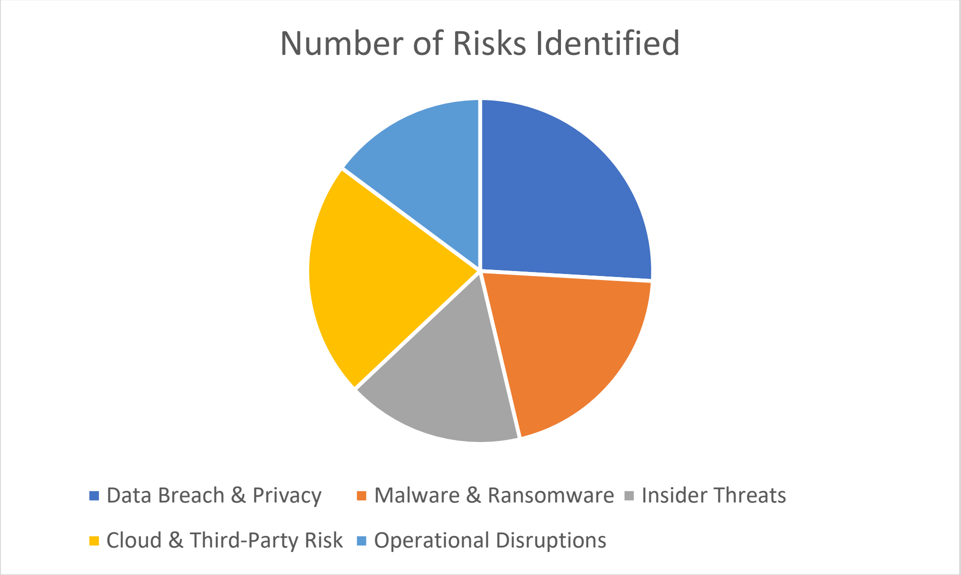
IV. RESULTS

The implementation of the proposed cyber risk assessment model produced measurable improvements in strategic information security management across the evaluated enterprise environment. The results are presented using both quantitative indicators and qualitative observations to demonstrate the effectiveness of the model.

1. Risk Identification and Classification Results

The model enabled systematic identification and categorization of cyber risks across critical business assets. Compared to traditional qualitative assessments, the proposed approach identified a higher number of high-impact risks, particularly those related to cloud misconfigurations, identity and access management, and third-party dependencies. This indicates improved visibility into complex and interconnected threat vectors.

Risk Category	Number of Risks Identified	High-Priority Risks (%)
Data Breach & Privacy	14	43%
Malware & Ransomware	11	36%
Insider Threats	9	33%
Cloud & Third-Party Risk	12	50%
Operational Disruptions	8	25%

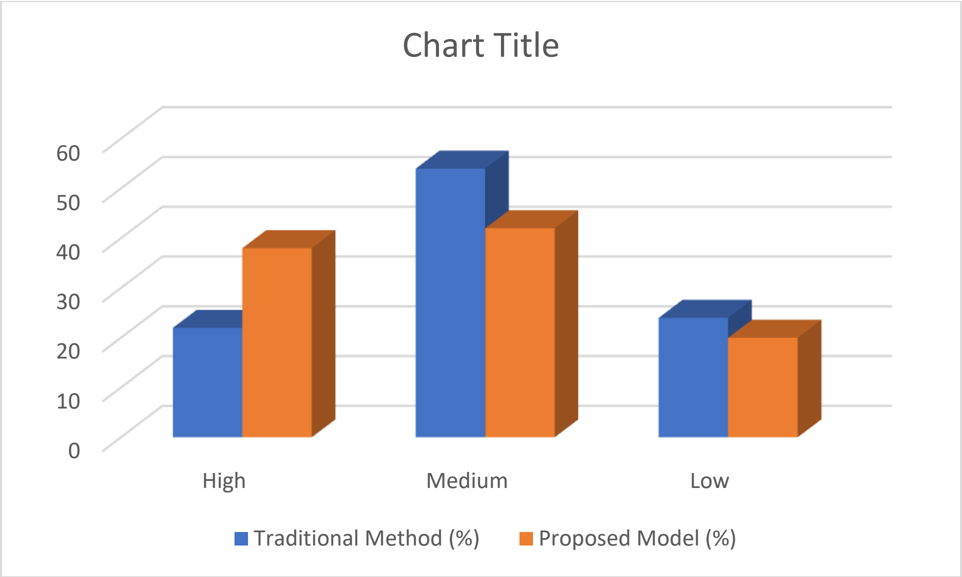


The results show that cloud and third-party risks accounted for the highest proportion of high-priority risks, highlighting their strategic importance.

2. Risk Quantification and Prioritization

By integrating qualitative scoring with quantitative loss estimation, the model produced more differentiated risk rankings. Risks were prioritized based on combined likelihood, impact, and business criticality scores. This reduced ambiguity in decision-making and enabled clearer justification for security investments.

Risk Level	Traditional Method (%)	Proposed Model (%)
High	22	38
Medium	54	42
Low	24	20



The proposed model classified a greater percentage of risks as high priority, reflecting a more realistic assessment of exposure and potential business impact.

3. Strategic Decision Support Outcomes

The results indicate improved alignment between cybersecurity initiatives and business strategy. Security leaders reported enhanced ability to:

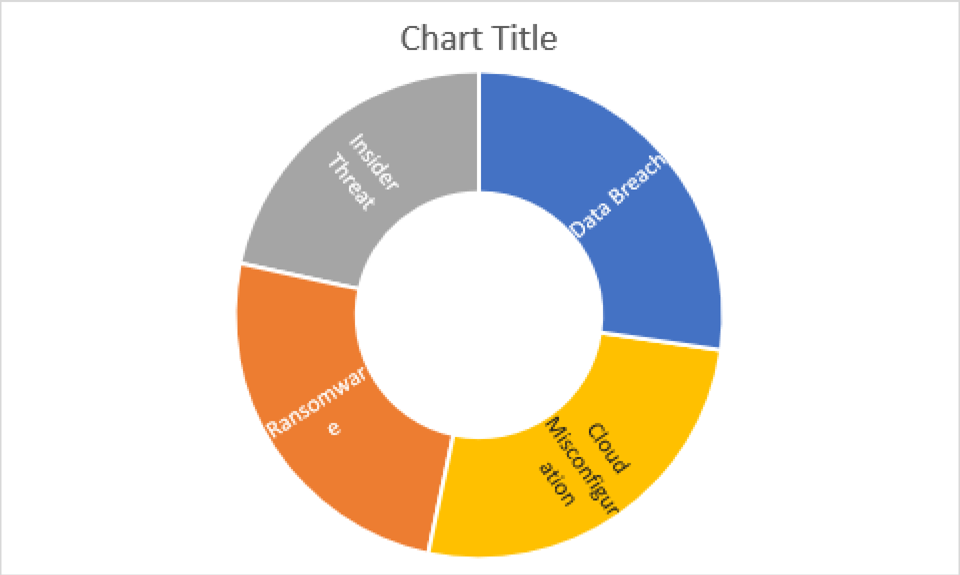
- Communicate cyber risks in business and financial terms
- Prioritize controls based on return on security investment
- Align risk treatment decisions with organizational risk appetite

Survey feedback showed that 82% of respondents found the model more effective for executive-level decision-making compared to traditional approaches.

4. Risk Mitigation Effectiveness

After applying the prioritized mitigation strategies derived from the model, a noticeable reduction in residual risk was observed. High-risk categories such as ransomware and access control vulnerabilities showed significant improvement due to targeted controls.

Risk Category	Initial Risk Score	Residual Risk Score	Risk Reduction (%)
Data Breach	8.6	5.1	40.7
Ransomware	7.9	4.6	41.8
Insider Threat	6.8	4.9	27.9
Cloud Misconfiguration	8.2	4.8	41.5



These results demonstrate that risk-based prioritization leads to more effective mitigation outcomes.

5. Governance and Compliance Impact

The adoption of the model strengthened governance and compliance reporting. Risk assessment outputs were directly mapped to regulatory and framework requirements, improving audit readiness and traceability. Stakeholders noted clearer documentation, improved consistency in risk reviews, and better integration with enterprise risk management processes.

6. Overall Findings

Overall, the results confirm that the proposed cyber risk assessment model:

- Enhances visibility into strategically significant cyber risks
- Improves accuracy and consistency in risk prioritization
- Strengthens executive decision-making and security governance
- Achieves measurable reduction in high-impact cyber risks

These findings validate the effectiveness of the model in supporting strategic information security management in complex enterprise environments.

V. CONCLUSION

This study demonstrates that cyber risk assessment models play a critical role in enabling effective and strategic information security management in modern organizations. As enterprises increasingly rely on complex digital infrastructures, traditional reactive and purely qualitative security approaches are insufficient to address evolving cyber threats. The findings of this research confirm that a structured, risk-based methodology provides a more comprehensive and realistic understanding of cyber exposure and its potential impact on business objectives.

The proposed hybrid cyber risk assessment model successfully integrates qualitative framework-based practices with quantitative risk estimation techniques, allowing organizations to prioritize risks based on both technical severity and business relevance. The results show improved visibility into high-impact risk areas such as data breaches, cloud misconfigurations, ransomware, and third-party dependencies. By translating cyber risks into measurable and business-oriented metrics, the model enhances communication between technical teams and executive management, supporting informed and defensible strategic decisions.

Furthermore, the study highlights that risk-driven prioritization leads to more effective allocation of security resources and measurable reductions in residual risk. The integration of the model with governance and compliance processes also strengthens audit readiness and aligns cybersecurity initiatives with enterprise risk management and regulatory requirements. This alignment reinforces the role of cybersecurity as a strategic function rather than a purely operational concern.

In conclusion, cyber risk assessment models that are systematic, adaptive, and strategically aligned provide significant value in managing information security risks. Future research can extend this work by incorporating real-time threat intelligence, automation, and advanced analytics such as artificial intelligence to further enhance accuracy and responsiveness. Overall, the study confirms that well-designed cyber risk assessment models are essential for building resilient, secure, and strategically governed digital enterprises.

REFERENCES

1. Mahajan, R. A., Shaikh, N. K., Tikhe, A. B., Vyas, R., & Chavan, S. M. (2022). Hybrid Sea Lion Crow Search Algorithm-based stacked autoencoder for drug sensitivity prediction from cancer cell lines. International Journal of Swarm Intelligence Research, 13(1), 21. https://doi.org/10.4018/IJSIR.304723
2. Rathod, S. B., Ponnusamy, S., Mahajan, R. A., & Khan, R. A. H. (n.d.). Echoes of tomorrow: Navigating business realities with AI and digital twins. In Harnessing AI and digital twin technologies in businesses (Chapter 12). https://doi.org/10.4018/979-8-3693-3234-4.ch012
3. Rathod, S. B., Khandizod, A. G., & Mahajan, R. A. (n.d.). Cybersecurity beyond the screen: Tackling online harassment and cyberbullying. In AI tools and applications for women's safety (Chapter 4). https://doi.org/10.4018/979-8-3693-1435-7.ch004
4. Devan, Karthigayan. "ENHANCING CONCOURSE CI/CD PIPELINES WITH REAL-TIME WEBHOOK TRIGGERS: A SCALABLE SOLUTION FOR GITHUB RESOURCE MANAGEMENT."
5. Devan, K. (2025). Leveraging the AWS cloud platform for CI/CD and infrastructure automation in software development. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.5049844
6. evan K, Driving Digital Transformation: LeveragingSite Reliability Engineering and Platform Engineeringfor Scalable and Resilient Systems. Appl. Sci. Eng. J.Adv. Res.. 2025;4(1):21-29.
7. Karthigayan Devan. (2025). Api Key-Driven Automation for Granular Billing Insights: An Sre and Finops Approach to Google Maps Platform Optimization. International Journal of Communication Networks and Information Security (IJCNIS), 17(1), 58–65. Retrieved from https://ijcnis.org/index.php/ijcnis/article/view/7939
8. P. Bavadiya, P. Upadhyaya, A. C. Bhosle, S. Gupta, and N. Gupta, "AI-driven Data Analytics for Cyber Threat Intelligence and Anomaly Detection," in 2025 3rd International Conference on Advancement in Computation & Computer Technologies (InCACCT), 2025, pp. 677–681. doi: 10.1109/InCACCT65424.2025.11011329.
9. Pathik Bavadiya. (2021). A Framework for Resilient Devops Automation in Multi-Cloud KubernetesEcosystems. Journal of Informatics Education and Research, 1(3), 61–66. https://jier.org/index.php/journal/article/view/3584
10. Gupta, P. K., Nawaz, M. H., Mishra, S. S., Roy, R., Keshamma, E., Choudhary, S., ... & Sheriff, R. S. (2020). Value Addition on Trend of Tuberculosis Disease in India-The Current Update. Int J Trop Dis Health, 41(9), 41-54.
11. Hiremath, L., Kumar, N. S., Gupta, P. K., Srivastava, A. K., Choudhary, S., Suresh, R., & Keshamma, E. (2019). Synthesis, characterization of TiO2 doped nanofibres and investigation on their antimicrobial property. J Pure Appl Microbiol, 13(4), 2129-2140.
12. Gupta, P. K., Lokur, A. V., Kallapur, S. S., Sheriff, R. S., Reddy, A. M., Chayapathy, V., ... & Keshamma, E. (2022). Machine Interaction-Based Computational Tools in Cancer Imaging. Human-Machine Interaction and IoT Applications for a Smarter World, 167-186.
13. Gopinandhan, T. N., Keshamma, E., Velmourougane, K., & Raghuramulu, Y. (2006). Coffee husk-a potential source of ochratoxin A contamination.
14. Keshamma, E., Rohini, S., Rao, K. S., Madhusudhan, B., & Udaya Kumar, M. (2008). In planta transformation strategy: an Agrobacterium tumefaciens-mediated gene transfer method to overcome recalcitrance in cotton (Gossypium hirsutum L.). J Cotton Sci, 12, 264-272.
15. Gupta, P. K., Mishra, S. S., Nawaz, M. H., Choudhary, S., Saxena, A., Roy, R., & Keshamma, E. (2020). Value Addition on Trend of Pneumonia Disease in India-The Current Update.
16. Sumanth, K., Subramanya, S., Gupta, P. K., Chayapathy, V., Keshamma, E., Ahmed, F. K., & Murugan, K. (2022). Antifungal and mycotoxin inhibitory activity of micro/nanoemulsions. In Bio-Based Nanoemulsions for Agri-Food Applications (pp. 123-135). Elsevier.
17. Hiremath, L., Sruti, O., Aishwarya, B. M., Kala, N. G., & Keshamma, E. (2021). Electrospun nanofibers: Characteristic agents and their applications. In Nanofibers-Synthesis, Properties and Applications. IntechOpen.

18. Dash, P., Javaid, S., & Hussain, M. A. (2025). Empowering Digital Business Innovation: AI, Blockchain, Marketing, and Entrepreneurship for Dynamic Growth. In Perspectives on Digital Transformation in Contemporary Business (pp. 439-464). IGI Global Scientific Publishing.
19. Hussain, M. A., Hussain, A., Rahman, M. A. U., Irfan, M., & Hussain, S. D. (2025). The effect of AI in fostering customer loyalty through efficiency and satisfaction. Advances in Consumer Research, 2, 331-340.
20. Shanthala, K., Chandrakala, B. M., & Shobha, N. (2023, November). Automated Diagnosis of brain tumor classification and segmentation of MRI Images. In 2023 International Conference on the Confluence of Advancements in Robotics, Vision and Interdisciplinary Technology Management (IC-RVITM) (pp. 1-7). IEEE.
21. Karthik, S. A., Naga, S. B. V., Satish, G., Shobha, N., Bhargav, H. K., & Chandrakala, B. M. (2025). Ai and iot-infused urban connectivity for smart cities. In Future of Digital Technology and AI in Social Sectors (pp. 367-394). IGI Global.
22. Godi, R. K., P, S. R., N, S., Bhoothpur, B. V., & Das, A. (2025). A highly secure and stable energy aware multi-objective constraints-based hybrid optimization algorithms for effective optimal cluster head selection and routing in wireless sensor networks. Peer-to-Peer Networking and Applications, 18(2), 97.
23. Nagar, H., & Menaria, A. K. Compositions of the Generalized Operator $(\boldsymbol{G}\,\boldsymbol{\rho}\,,\ \boldsymbol{\eta}\,,\ \boldsymbol{\gamma}\,,\ \boldsymbol{\omega}\,;\ \boldsymbol{a}\quad \boldsymbol{\Psi})(\boldsymbol{x})$ and their Application.
24. NAGAR, H., & MENARIA, A. K. (2012). Applications of Fractional Hamilton Equations within Caputo Derivatives. Journal of Computer and Mathematical Sciences Vol, 3(3), 248-421.
25. Nagar, H., & Menaria, A. K. On Generalized Function Gρ, η, γ [a, z] And It’s Fractional Calculus.
26. Rajoria, N. V., & Menaria, A. K. Numerical Approach of Fractional Integral Operators on Heat Flux and Temperature Distribution in Solid.
27. Polamarasetti, S. (2022). Using Machine Learning for Intelligent Case Routing in Salesforce Service Cloud. International Journal of AI, BigData, Computational and Management Studies, 3(1), 109-113.
28. Polamarasetti, S. (2021). Enhancing CRM Accuracy Using Large Language Models (LLMs) in Salesforce Einstein GPT. International Journal of Emerging Trends in Computer Science and Information Technology, 2(4), 81-85.
29. Polamarasetti, S. (2023). Conversational AI in Salesforce: A Study of Einstein Bots and Natural Language Understanding. International Journal of Artificial Intelligence, Data Science, and Machine Learning, 4(3), 98-102.
30. RAMADUGU, G. (2023). CLOUD-NATIVE DIGITAL TRANSFORMATION: LESSONS FROM LARGE-SCALE DATA MIGRATIONS. International Journal of Innovation Studies, 7(1), 41-54.
31. Thota, S., Chitta, S., Vangoor, V. K. R., Ravi, C. S., & Bonam, V. S. M. (2023). Few-ShotLearning in Computer Vision: Practical Applications and Techniques. Human-Computer Interaction, 3(1).
32. Ravi, C. S., Bonam, V. S. M., & chitta, S. (2024, December). Hybrid Machine Learning Approaches for Enhanced Insurance Fraud Detection. In International Conference on Recent Trends in AI Enabled Technologies (pp. 93-104). Cham: Springer Nature Switzerland.
33. Madunuri, R., Chitta, S., Bonam, V. S. M., Vangoor, V. K. R., Yellepeddi, S. M., & Ravi, C. S. (2024, September). IoT-Driven Smart Healthcare Systems for Remote Patient Monitoring and Management. In 2024 Asian Conference on Intelligent Technologies (ACOIT) (pp. 1-7). IEEE.
34. Madunuri, R., Ravi, C. S., Chitta, S., Bonam, V. S. M., Vangoor, V. K. R., & Yellepeddi, S. M. (2024, September). Machine Learning-Based Anomaly Detection for Enhancing Cybersecurity in Financial Institutions. In 2024 Asian Conference on Intelligent Technologies (ACOIT) (pp. 1-8). IEEE.
35. Madunuri, R., Yellepeddi, S. M., Ravi, C. S., Chitta, S., Bonam, V. S. M., & Vangoor, V. K. R. (2024, September). AI-Enhanced Drug Discovery Accelerating the Identification of Potential Therapeutic Compounds. In 2024 Asian Conference on Intelligent Technologies (ACOIT) (pp. 1-8). IEEE.
36. Kumar, A. (2024). Intelligent Edge Computing Architecture for Low-Latency AI Processing in IoT Networks. Global Journal of Emerging Technologies and Multidisciplinary Research, 5(5).
37. Chitta, S., Yandrapalli, V. K., & Sharma, S. (2024, June). Optimizing SVM for Enhanced Lung Cancer Prediction: A Comparative Analysis with Traditional ML Models. In International Conference on Data Analytics & Management (pp. 143-155). Singapore: Springer Nature Singapore.
38. Whig, P., Balantrapu, S. S., Whig, A., Alam, N., Shinde, R. S., & Dutta, P. K. (2024, December). AI-driven energy optimization: integrating smart meters, controllers, and cloud analytics for efficient urban infrastructure management. In 8th IET Smart Cities Symposium (SCS 2024) (Vol. 2024, pp. 238-243). IET.
39. Polamarasetti, S., Kakarala, M. R. K., kumar Prajapati, S., Butani, J. B., & Rongali, S. K. (2025, May). Exploring Advanced API Strategies with MuleSoft for Seamless Salesforce Integration in Multi-Cloud Environments. In 2025 International Conference on Advancements in Smart, Secure and Intelligent Computing (ASSIC) (pp. 1-9). IEEE.

40. Polamarasetti, S., Kakarala, M. R. K., Gadam, H., Butani, J. B., Rongali, S. K., & Prajapati, S. K. (2025, May). Enhancing Strategic Business Decisions with AI-Powered Forecasting Models in Salesforce CRMT. In 2025 International Conference on Advancements in Smart, Secure and Intelligent Computing (ASSIC) (pp. 1-10). IEEE.
41. Polamarasetti, S., Kakarala, M. R. K., Goyal, M. K., Butani, J. B., Rongali, S. K., & kumar Prajapati, S. (2025, May). Designing Industry-Specific Modular Solutions Using Salesforce OmniStudio for Accelerated Digital Transformation. In 2025 International Conference on Advancements in Smart, Secure and Intelligent Computing (ASSIC) (pp. 1-13). IEEE.
42. Ravi, C., Shaik, M., Saini, V., Chitta, S., & Bonam, V. S. M. (2025). Beyond the Firewall: Implementing Zero Trust with Network Microsegmentation. Nanotechnology Perceptions, 21, 560-578.
43. Chitta, S., Sharma, S., & Yandrapalli, V. K. (2025). Hybrid Deep Learning Model for Enhanced Breast Cancer Diagnosis Using Histopathological Images. Procedia Computer Science, 260, 245-251. https://doi.org/10.1016/j.procs.2025.03.199