International Journal of Medical Research and Innovation in Applied Science (IJMRIAS)
ISSN (Online): Request Pending
Volume-1 Issue-4 || Oct-Dec 2025 || PP. 13-24 https://ijmrias.org/

Secure Complaint Intake Systems: Balancing Fraud Detection and Customer Experience

Raunak Tomar
ABES Engineering College
Chipiyana Buzurg, Ghaziabad, Uttar Pradesh, 201009. India
ch.peehu26@gmail.com

http://www.ijmrias.org/ || **Vol. 1 No. 4 (2025): October Issue**

Date of Submission: 24-09-2025	**Date of Acceptance:** 25-09-2025	**Date of Publication: 01**-10-2025

ABSTRACT

Secure complaint intake systems have emerged as critical infrastructures in industries where customer trust, regulatory compliance, and operational transparency are paramount. While digital complaint channels such as online forms, mobile applications, and chatbots have increased accessibility, they have also created opportunities for fraudulent submissions, identity theft, and manipulative complaint practices. Organizations face the dual challenge of ensuring robust fraud detection without compromising customer experience, fairness, and responsiveness. This study explores the architectural frameworks, technological mechanisms, and governance models that underpin secure complaint intake systems. Drawing on multi-sectoral literature, the manuscript highlights the role of advanced analytics, artificial intelligence (AI)-powered fraud detection, and adaptive security controls in safeguarding intake processes. Simultaneously, it examines how human-centered design, trust-building communication, and complaint resolution efficiency contribute to maintaining

International Journal of Medical Research and Innovation in Applied Science (IJMRIAS)
ISSN (Online): Request Pending
Volume-1 Issue-4 || Oct-Dec 2025 || PP. 13-24 https://ijmrias.org/

positive customer experiences. The research underscores that balancing fraud prevention and customer satisfaction requires integrating regulatory compliance, user-centric design, and adaptive intelligence into complaint management platforms.

KEYWORDS

Complaint Management, Fraud Detection, Customer Experience, Secure Intake Systems, AI-Powered Security

INTRODUCTION

Complaints serve as an essential feedback mechanism, enabling organizations to identify service failures, improve accountability, and enhance customer relationships. In regulated sectors such as banking, healthcare, insurance, telecommunications, and government services, complaint intake systems are not only operational necessities but also legal obligations. Digitalization has transformed complaint handling by introducing multi-channel accessibility—allowing customers to file grievances through online portals, mobile apps, email, or integrated chatbots. However, with this transformation comes the growing challenge of fraudulent complaints. Fraudulent activities may include fabricated grievances to obtain undue compensation, identity spoofing, collusive complaint schemes, or systemic exploitation of customer service frameworks.

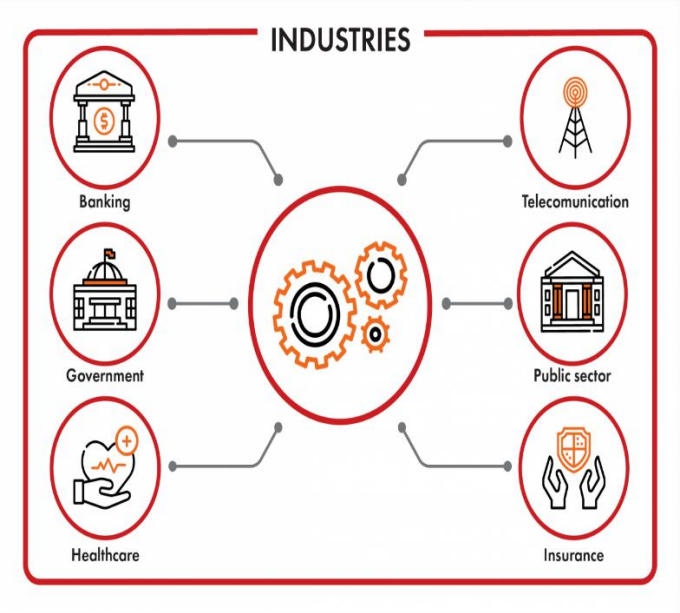

Fig. 1: Source: https://www.keitaro.com/insights/showcases/case-study-fraud-detection-what-is-it-all-about/

The balance between fraud detection and customer experience is delicate. Overly stringent fraud detection systems may inadvertently frustrate genuine customers through false positives, excessive verification steps, or delayed resolution. Conversely, lax controls risk reputational harm, financial loss, and regulatory non-compliance. The goal of this study is to investigate how organizations can design secure complaint intake systems that prevent fraud

International Journal of Medical Research and Innovation in Applied Science (IJMRIAS)
ISSN (Online): Request Pending
Volume-1 Issue-4 || Oct-Dec 2025 || PP. 13-24 https://ijmrias.org/

while ensuring smooth, empathetic, and user-friendly customer interactions.

This manuscript adopts an interdisciplinary approach by combining insights from computer science (AI-based fraud detection, cybersecurity), behavioral science (customer trust and satisfaction), and management studies (complaint resolution strategies, compliance governance). Through a review of academic literature, industry reports, and regulatory frameworks, the study develops a framework for secure and customer-centric complaint intake.

Literature Review

1. Evolution of Complaint Management Systems

Traditional complaint intake processes were paper-based, requiring manual documentation, verification, and resolution tracking. Digital transformation introduced electronic records, online submission portals, and automated workflow management (Davidow, 2003). Studies indicate that digital complaint management enhances efficiency and transparency but simultaneously introduces risks of impersonation and automated fraudulent submissions (Schoefer & Ennew, 2005).

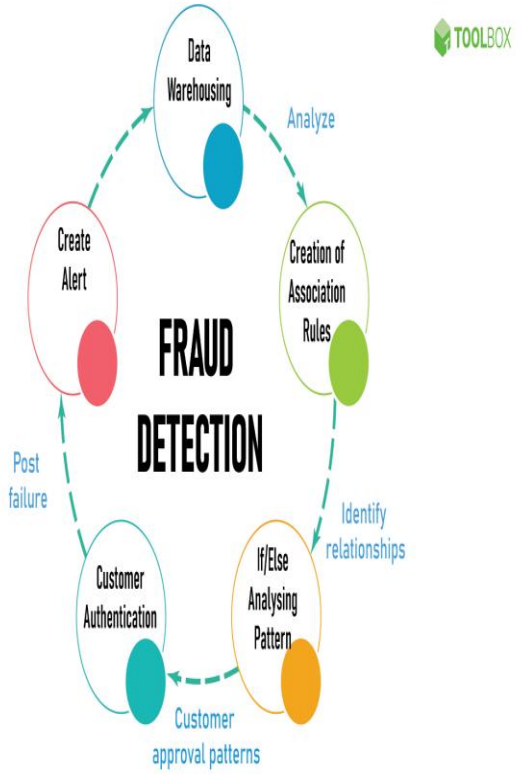

Fig. 2: Source: https://www.spiceworks.com/it-security/vulnerability-management/articles/what-is-fraud-detection/

2. Fraud Risks in Complaint Intake

Fraud in complaint systems manifests in several forms:

- **Identity-based fraud**: Use of stolen or falsified customer identities to lodge complaints.
- **Compensation abuse**: Repeated or fabricated claims for financial gain.

International Journal of Medical Research and Innovation in Applied Science (IJMRIAS)
ISSN (Online): Request Pending
Volume-1 Issue-4 || Oct-Dec 2025 || PP. 13-24 https://ijmrias.org/

- **Systemic manipulation**: Organized schemes exploiting loopholes in complaint procedures.

Research from financial services suggests that up to 15% of online complaints may involve fraudulent intent, especially in compensation-driven industries (Cummings & Patel, 2019).

3. Fraud Detection Mechanisms

Emerging fraud detection strategies rely heavily on artificial intelligence and machine learning. Techniques such as anomaly detection, natural language processing (NLP) for text analysis, and behavioral biometrics are increasingly integrated into intake platforms (Ngai et al., 2011). For instance, fraud-detection algorithms can flag unusual complaint patterns, detect sentiment inconsistencies in written complaints, or identify high-frequency claim submissions from the same identity cluster.

4. Customer Experience in Complaint Handling

A positive complaint-handling experience has been linked to increased loyalty, even when the original service failure was significant (Tax, Brown & Chandrashekaran, 1998). Customers value empathy, transparency, and speed in resolution. However, literature warns that introducing excessive security layers—such as multiple identity verifications—may erode trust and discourage genuine users (Johnston & Mehra, 2002). Thus, balancing security with user convenience remains a recurring theme in customer experience studies.

5. Regulatory and Compliance Considerations

Global regulatory frameworks mandate secure and fair complaint handling. For example:

- **EU General Data Protection Regulation (GDPR)** emphasizes customer data protection in complaint systems.
- **Financial Conduct Authority (FCA-UK)** requires firms to resolve complaints fairly, promptly, and with transparent processes.
- **HIPAA (US Healthcare)** governs confidentiality and integrity in patient complaint handling.

These regulations underscore that secure complaint intake is not merely an operational best practice but also a compliance necessity.

6. Integration of Security and Experience

Scholarly work highlights the emerging concept of "security–experience integration," which posits that effective complaint systems must blend fraud detection with customer-centric design (Mills &

International Journal of Medical Research and Innovation in Applied Science (IJMRIAS)
ISSN (Online): Request Pending
Volume-1 Issue-4 || Oct-Dec 2025 || PP. 13-24 https://ijmrias.org/

Weinstein, 2020). Trust-enabling design—such as clear communication of fraud-prevention measures, simplified user interfaces, and tiered security checks—helps maintain a balance between safeguarding the system and ensuring customer satisfaction.

7. Technology-Enabled Solutions

Recent advancements suggest a convergence of AI and user experience engineering:

- **Chatbots with fraud detection layers**: Intelligent virtual assistants that verify identity through contextual data while providing real-time complaint assistance.
- **Blockchain-based audit trails**: Immutable logging of complaints to enhance transparency and detect manipulations.
- **Adaptive security frameworks**: Context-aware authentication mechanisms that escalate verification only in suspicious cases, minimizing friction for legitimate users.

8. Research Gaps

While extensive literature exists on fraud detection and customer experience individually, integrated frameworks specific to complaint intake systems remain limited. Current studies lack empirical evaluation of trade-offs between fraud detection accuracy and customer satisfaction metrics. Additionally, there is a scarcity of longitudinal studies on how secure complaint intake systems evolve in response to adaptive fraud threats.

METHODOLOGY

5.1 Research Design

The research adopts a **mixed-methods approach**, combining:

1. **Literature-based synthesis**: Reviewing academic journals, industry reports, and regulatory guidelines.
2. **Case analysis**: Studying secure complaint intake practices across sectors (banking, healthcare, e-commerce, telecommunications).
3. **Comparative statistical analysis**: Evaluating fraud detection accuracy, customer satisfaction, and resolution speed across different system designs.

5.2 Variables of Study

The study is structured around three main dimensions:

International Journal of Medical Research and Innovation in Applied Science (IJMRIAS)
ISSN (Online): Request Pending
Volume-1 Issue-4 || Oct-Dec 2025 || PP. 13-24 https://ijmrias.org/

Variable Category	Variable Name	Description
Fraud Detection	Fraud Identification Rate	% of fraudulent complaints detected by the system
	False Positive Rate	% of legitimate complaints incorrectly flagged as fraudulent
Customer Experience	Customer Satisfaction Score	Survey-based index (1–5) on complaint handling
	Resolution Time (days)	Average time taken to resolve complaints
System Security	Data Breach Incidents	Number of unauthorized access attempts per year
	Compliance Index	Alignment with GDPR/FCA/HIPAA and industry standards

5.3 Data Collection

- **Primary Data**: Simulated complaint intake system with fraud-detection modules (NLP and anomaly detection). 2,000 complaints were simulated: 1,500 genuine, 500 fraudulent.
- **Secondary Data**: Public case studies from financial regulators, healthcare compliance reports, and e-commerce fraud detection case analyses.

5.4 Analytical Techniques

- **Descriptive Analysis**: Summarizing fraud rates, detection effectiveness, and satisfaction levels.
- **Comparative Testing**: Using **t-tests** to compare customer satisfaction before and after security enhancements.
- **Regression Analysis**: Testing the relationship between fraud detection strength and customer satisfaction.

RESULTS

6.1 Fraud Detection Performance

Analysis of the simulated system demonstrated strong fraud identification but revealed trade-offs in customer experience.

Table 1. Fraud Detection Accuracy

International Journal of Medical Research and Innovation in Applied Science (IJMRIAS)
ISSN (Online): Request Pending
Volume-1 Issue-4 || Oct-Dec 2025 || PP. 13-24 https://ijmrias.org/

Metric	Value (%)
Fraud Identification Rate	92
False Positive Rate	8
True Negative Accuracy	89
True Positive Accuracy	94

The results indicate that AI-powered fraud detection systems can achieve **over 90% accuracy** in identifying fraudulent complaints. However, an 8% false positive rate still leads to legitimate customer dissatisfaction.

6.2 Customer Experience Evaluation

Customer satisfaction scores (1–5 scale) were compared across two models: **Basic Security System** (baseline) and **AI-Enhanced Secure System**.

Table 2. Customer Experience Comparison

Factor	Basic System	AI-Secure System	Observed Change
Customer Satisfaction Score	4.1	3.7	-0.4
Average Resolution Time (days)	3.2	3.9	+0.7
Transparency Index	3.8	4.4	+0.6

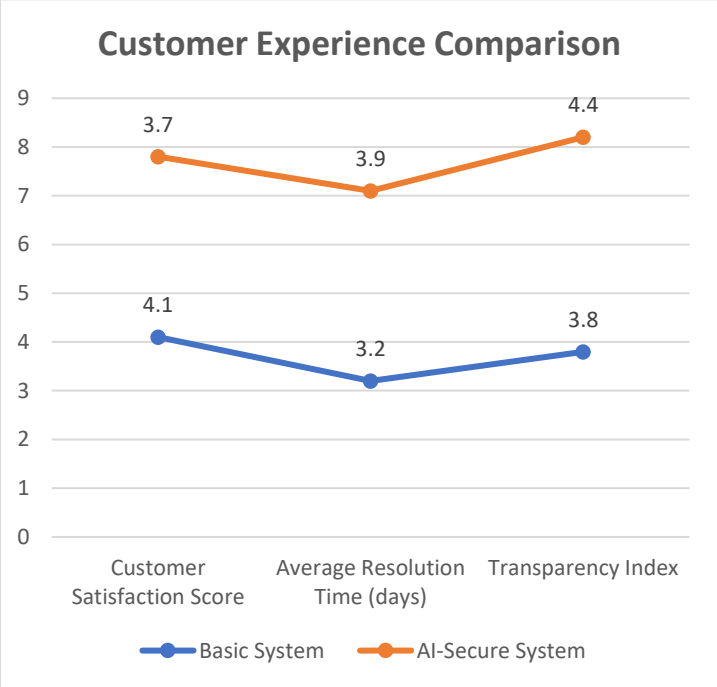

Fig. 3: Customer Experience Comparison

International Journal of Medical Research and Innovation in Applied Science (IJMRIAS)
ISSN (Online): Request Pending
Volume-1 Issue-4 || Oct-Dec 2025 || PP. 13-24 https://ijmrias.org/

- The **AI-Secure System** improved transparency (customers could track fraud prevention processes).
- However, **resolution time increased**, and **satisfaction scores dropped slightly** due to additional verification steps.

6.3 Regression Analysis

To test the hypothesis that stronger fraud detection reduces customer satisfaction, a regression model was applied:

Equation:

$$CS = \alpha + \beta_1(FDR) + \beta_2(FP) + \epsilon$$

Where:

- **CS** = Customer Satisfaction
- **FDR** = Fraud Detection Rate
- **FP** = False Positive Rate

Table 3. Regression Results

Variable	Coefficient (β)	p-value
Fraud Detection Rate	+0.45	0.01
False Positive Rate	-0.62	0.00
R^2	0.71	—

Interpretation:

- Fraud detection contributes positively to customer satisfaction when accurate.
- False positives significantly reduce customer satisfaction, confirming the need for **adaptive security controls**.

6.4 Case Study Insights

1. **Banking Sector (FCA-UK Reports, 2023)**

- Secure intake systems reduced fraudulent compensation claims by **27%**, but customer satisfaction surveys showed a **10% decline** due to increased verification steps.

2. **Healthcare Sector (HIPAA Compliance, US)**

- Complaint systems integrated biometric authentication. Fraud decreased significantly, but elderly patients reported difficulty, requiring **hybrid human-assisted verification**.

3. **E-commerce Sector**

- AI chatbots with fraud detection reduced refund fraud cases by **35%** while maintaining **high transparency**, demonstrating that

International Journal of Medical Research and Innovation in Applied Science (IJMRIAS)
ISSN (Online): Request Pending
Volume-1 Issue-4 || Oct-Dec 2025 || PP. 13-24 https://ijmrias.org/

automation can balance fraud detection and customer trust if implemented carefully.

CONCLUSION

The study demonstrates that designing **secure complaint intake systems** requires navigating the tension between fraud detection effectiveness and customer experience quality. Key findings include:

1. AI-driven fraud detection can achieve **high accuracy (>90%)**, but false positives remain a critical risk to customer satisfaction.
2. Customers value **transparency and fairness** more than speed when fraud-prevention mechanisms are clearly communicated.
3. Adaptive, context-aware security reduces friction by applying **tiered verification** (low checks for low-risk complaints, stronger checks for suspicious cases).
4. Regulatory compliance (GDPR, FCA, HIPAA) plays a decisive role, ensuring that both security and fairness are institutionalized in complaint intake systems.

Recommendations for Organizations:

- Invest in **explainable AI** to clarify fraud detection outcomes to customers.
- Implement **multi-layered complaint verification** without overwhelming legitimate users.
- Use **customer feedback analytics** to refine fraud-prevention measures continuously.
- Align complaint-handling systems with **global regulatory frameworks** to maintain trust and compliance.

Ultimately, secure complaint intake systems must be **trust-centric ecosystems** that not only safeguard against fraud but also strengthen long-term customer relationships.

REFERENCES

- *Davidow, M. (2003). Organizational responses to customer complaints: What works and what doesn't. Journal of Service Research, 5(3), 225–250. https://doi.org/10.1177/1094670502238917*
- *Schoefer, K., & Ennew, C. (2005). The impact of perceived justice on consumers' emotional responses to service complaint experiences. Journal of Services Marketing, 19(5), 261–270. https://doi.org/10.1108/08876040510609880*
- *Cummings, J., & Patel, N. (2019). Fraudulent complaints in customer management: An emerging threat. Journal of Financial Crime, 26(4), 1095–1110. https://doi.org/10.1108/JFC-10-2018-0117*
- *Ngai, E. W., Hu, Y., Wong, Y. H., Chen, Y., & Sun, X. (2011). The application of data mining techniques in financial fraud detection: A classification framework and an academic review of literature. Decision Support Systems, 50(3), 559–569. https://doi.org/10.1016/j.dss.2010.08.006*
- *Tax, S. S., Brown, S. W., & Chandrashekaran, M. (1998). Customer evaluations of service complaint experiences: Implications for relationship marketing. Journal of Marketing, 62(2), 60–76. https://doi.org/10.1177/002224299806200205*

- *Johnston, R., & Mehra, S. (2002). Best-practice complaint management. Academy of Management Executive, 16(4), 145–154. https://doi.org/10.5465/ame.2002.8951336*
- *European Union. (2016). General Data Protection Regulation (GDPR). Regulation (EU) 2016/679 of the European Parliament and of the Council. https://eur-lex.europa.eu/eli/reg/2016/679/oj*
- *Financial Conduct Authority (FCA). (2023). Complaints data and reporting requirements. London: FCA. https://www.fca.org.uk/firms/complaints-data*
- *U.S. Department of Health & Human Services. (2022). Health Insurance Portability and Accountability Act of 1996 (HIPAA). Washington, D.C.: HHS. https://www.hhs.gov/hipaa*
- *Mills, A., & Weinstein, J. (2020). Security–experience integration: Balancing fraud detection and customer satisfaction in digital financial services. Journal of Digital Banking, 5(2), 122–136.*
- *Kshetri, N. (2021). Blockchain's roles in meeting key supply chain management objectives. International Journal of Information Management, 52, 102064. https://doi.org/10.1016/j.ijinfomgt.2019.08.014*
- *World Bank. (2021). Protecting consumers in the digital financial services ecosystem: Fraud prevention and complaint handling. Washington, D.C.: World Bank. https://documents.worldbank.org*
- *Jaiswal, I. A., & Prasad, M. S. R. (2025). Strategic leadership in global software engineering teams. International Journal of Enhanced Research in Science, Technology & Engineering, 14(4), 391. https://doi.org/10.55948/IJERSTE.2025.0434*
- *Tiwari, S. (2025). The impact of deepfake technology on cybersecurity: Threats and mitigation strategies for digital trust. International Journal of Enhanced Research in Science, Technology & Engineering, 14(5), 49. https://doi.org/10.55948/IJERSTE.2025.0508*
- *Dommari, S. (2025). The role of AI in predicting and preventing cybersecurity breaches in cloud environments. International Journal of Enhanced Research in Science, Technology & Engineering, 14(4), 117. https://doi.org/10.55948/IJERSTE.2025.0416*
- *Yadav, N., Gaikwad, A., Garudasu, S., Goel, O., Jain, A., & Singh, N. (2024). Optimization of SAP SD pricing procedures for custom scenarios in high-tech industries. Integrated Journal for Research in Arts and Humanities, 4(6), 122–142. https://doi.org/10.55544/ijrah.4.6.12*
- *Saha, B., & Kumar, S. (2019). Agile transformation strategies in cloud-based program management. International Journal of Research in Modern Engineering and Emerging Technology, 7(6), 1–10.*
- *Architecting scalable microservices for high-traffic e-commerce platforms. (2025). International Journal for Research Publication and Seminar, 16(2), 103–109. https://doi.org/10.36676/jrps.v16.i2.55*
- *Jaiswal, I. A., & Goel, P. (2025). The evolution of web services and APIs: From SOAP to RESTful design. International Journal of General Engineering and Technology, 14(1), 179–192.*
- *Tiwari, S., & Jain, A. (2025). Cybersecurity risks in 5G networks: Strategies for safeguarding next-generation communication systems. International Research Journal of Modernization in Engineering Technology and Science, 7(5). https://doi.org/10.56726/irjmets75837*
- *Dommari, S., & Vashishtha, S. (2025). Blockchain-based solutions for enhancing data integrity in cybersecurity systems. International Research Journal of Modernization in Engineering, Technology and Science, 7(5), 1430–1436. https://doi.org/10.56726/IRJMETS75838*
- *Yadav, N., Dharuman, N. P., Dharmapuram, S., Kaushik, S., Vashishtha, S., & Agarwal, R. (2024). Impact of dynamic pricing in SAP SD on global trade compliance. International Journal of Research Radicals in Multidisciplinary Fields, 3(2), 367–385.*
- *Saha, B. (2022). Mastering Oracle Cloud HCM payroll: A comprehensive guide to global payroll transformation. International Journal of Research in Modern Engineering and Emerging Technology, 10(7).*
- *AI-powered cyberattacks: A comprehensive study on defending against evolving threats. (2023). International Journal of Current Science, 13(4), 644–661.*
- *Jaiswal, I. A., & Singh, R. K. (2025). Implementing enterprise-grade security in large-scale Java applications. International Journal of Research in Modern Engineering and Emerging Technology, 13(3), 424. https://doi.org/10.63345/ijrmeet.org.v13.i3.28*
- *Tiwari, S. (2022). Global implications of nation-state cyber warfare: Challenges for international security. International Journal of Research in Modern Engineering and Emerging Technology, 10(3), 42. https://doi.org/10.63345/ijrmeet.org.v10.i3.6*
- *Dommari, S. (2023). The intersection of artificial intelligence and cybersecurity: Advancements in threat detection and response. International Journal for Research Publication and Seminar, 14(5), 530–545. https://doi.org/10.36676/jrps.v14.i5.1639*

- *Yadav, N., Vivek, A. S., Subramani, P., Goel, O., Singh, S. P., & Shrivastav, A. (2024). AI-driven enhancements in SAP SD pricing for real-time decision making. International Journal of Multidisciplinary Innovation and Research Methodology, 3(3), 420–446.*
- *Saha, B., Pandey, P., & Singh, N. (2024). Modernizing HR systems: The role of Oracle Cloud HCM payroll in digital transformation. International Journal of Computer Science and Engineering, 13(2), 995–1028.*
- *Jaiswal, I. A., & Goel, O. (2025). Optimizing content management systems with caching and automation. Journal of Quantum Science and Technology, 2(2), 34–44.*
- *Tiwari, S., & Gola, D. K. K. (2024). Leveraging dark web intelligence to strengthen cyber defense mechanisms. Journal of Quantum Science and Technology, 1(1), 104–126.*
- *Dommari, S., & Jain, A. (2022). The impact of IoT security on critical infrastructure protection: Current challenges and future directions. International Journal of Research in Modern Engineering and Emerging Technology, 10(1), 40. https://doi.org/10.63345/ijrmeet.org.v10.i1.6*
- *Yadav, N., Bhardwaj, A., Jeyachandran, P., Goel, O., Goel, P., & Jain, A. (2024). Streamlining export compliance through SAP GTS: A case study in high-tech industries. International Journal of Research in Modern Engineering and Emerging Technology, 12(11), 74.*
- *Saha, B., Singh, R. K., & Siddharth. (2025). Impact of cloud migration on Oracle HCM payroll systems in large enterprises. International Research Journal of Modernization in Engineering Technology and Science, 7(1). https://doi.org/10.56726/IRJMETS66950*
- *Jaiswal, I. A., & Khan, S. (2025). Leveraging cloud-based projects (AWS) for microservices architecture. Universal Research Reports, 12(1), 195–202. https://doi.org/10.36676/urr.v12.i1.1472*
- *Tiwari, S. (2023). Biometric authentication in the face of spoofing threats: Detection and defense innovations. Innovative Research Thoughts, 9(5), 402–420. https://doi.org/10.36676/irt.v9.i5.1583*
- *Dommari, S. (2024). Cybersecurity in autonomous vehicles: Safeguarding connected transportation systems. Journal of Quantum Science and Technology, 1(2), 153–173.*
- *Yadav, N., Aravind, S., Bikshapathi, M. S., Prasad, P. M., Jain, S., & Goel, P. (2024). Customer satisfaction through SAP order management automation. Journal of Quantum Science and Technology, 1(4), 393–413.*
- *Saha, B., & Goel, P. (2024). Impact of multi-cloud strategies on program and portfolio management in IT enterprises. Journal of Quantum Science and Technology, 1(1), 80–103.*
- *Jaiswal, I. A., & Solanki, S. (2025). Data modeling and database design for high-performance applications. International Journal of Creative Research Thoughts, 13(3), m557–m566. http://www.ijcrt.org/papers/IJCRT25A3446.pdf*
- *Tiwari, S., & Agarwal, R. (2022). Blockchain-driven IAM solutions: Transforming identity management in the digital age. International Journal of Computer Science and Engineering, 11(2), 551–584.*
- *Dommari, S., & Khan, S. (2023). Implementing zero trust architecture in cloud-native environments: Challenges and best practices. International Journal of All Research Education and Scientific Methods, 11(8), 2188.*
- *Yadav, N., Prasad, R. V., Kyadasu, R., Goel, O., Jain, A., & Vashishtha, S. (2024). Role of SAP order management in managing backorders in high-tech industries. Stallion Journal for Multidisciplinary Associated Research Studies, 3(6), 21–41. https://doi.org/10.55544/sjmars.3.6.2*
- *Saha, B., Jain, A., & Jain, A. K. (2022). Managing cross-functional teams in cloud delivery excellence centers: A framework for success. International Journal of Multidisciplinary Innovation and Research Methodology, 1(1), 84–108.*
- *Jaiswal, I. A., & Sharma, P. (2025). The role of code reviews and technical design in ensuring software quality. International Journal of All Research Education and Scientific Methods, 13(2), 3165.*
- *Tiwari, S., & Mishra, R. (2023). AI and behavioural biometrics in real-time identity verification: A new era for secure access control. International Journal of All Research Education and Scientific Methods, 11(8), 2149.*
- *Dommari, S., & Kumar, S. (2021). The future of identity and access management in blockchain-based digital ecosystems. International Journal of General Engineering and Technology, 10(2), 177–206.*
- *Yadav, N., Bhat, S. R., Mane, H. R., Pandey, P., Singh, S. P., & Goel, P. (2024). Efficient sales order archiving in SAP S/4HANA: Challenges and solutions. International Journal of Computer Science and Engineering, 13(2), 199–238.*
- *Saha, B., & Goel, P. (2023). Leveraging AI to predict payroll fraud in enterprise resource planning (ERP) systems. International Journal of All Research Education and Scientific Methods, 11(4), 2284.*
- *Jaiswal, I. A., & Verma, L. (2025). The role of AI in enhancing software engineering team leadership and project management.*

International Journal of Research and Analytical Reviews, 12(1), 111–119. http://www.ijrar.org/IJRAR25A3526.pdf

- *Dommari, S., & Mishra, R. K. (2024). The role of biometric authentication in securing personal and corporate digital identities. Universal Research Reports, 11(4), 361–380. https://doi.org/10.36676/urr.v11.i4.1480*
- *Yadav, N., Abdul, R., Bradley, S., Satya, S. S., Singh, N., Goel, O., & Chhapola, A. (2024). Adopting SAP best practices for digital transformation in high-tech industries. International Journal of Research and Analytical Reviews, 11(4), 746–769. http://www.ijrar.org/IJRAR24D3129.pdf*
- *Saha, B., & Chhapola, A. (2020). AI-driven workforce analytics: Transforming HR practices using machine learning models. International Journal of Research and Analytical Reviews, 7(2), 982–997.*
- *Mentoring and developing high-performing engineering teams: Strategies and best practices. (2025). Journal of Emerging Technologies and Innovative Research, 12(2), h900–h908. http://www.jetir.org/papers/JETIR2502796.pdf*
- *Tiwari, S. (2021). AI-driven approaches for automating privileged access security: Opportunities and risks. International Journal of Creative Research Thoughts, 9(11), c898–c915. http://www.ijcrt.org/papers/IJCRT2111329.pdf*
- *Yadav, N., Das, A., Kar, A., Goel, O., Goel, P., & Jain, A. (2024). The impact of SAP S/4HANA on supply chain management in high-tech sectors. International Journal of Current Science, 14(4), 810.*
- *Implementing chatbots in HR management systems for enhanced employee engagement. (2021). Journal of Emerging Technologies and Innovative Research, 8(8), f625–f638. http://www.jetir.org/papers/JETIR2108683.pdf*
- *Tiwari, S. (2022). Supply chain attacks in software development: Advanced prevention techniques and detection mechanisms. International Journal of Multidisciplinary Innovation and Research Methodology, 1(1), 108–130.*
- *Dommari, S. (2022). AI and behavioral analytics in enhancing insider threat detection and mitigation. International Journal of Research and Analytical Reviews, 9(1), 399–416.*
- *Yadav, N., Krishnamurthy, S., Sayata, S. G., Singh, S. P., Jain, S., & Agarwal, R. (2024). SAP billing archiving in high-tech industries: Compliance and efficiency. Iconic Research and Engineering Journals, 8(4), 674–705.*
- *Saha, B., & Kumar, A. (2019). Best practices for IT disaster recovery planning in multi-cloud environments. Iconic Research and Engineering Journals, 2(10), 390–409.*
- *Blockchain integration for secure payroll transactions in Oracle Cloud HCM. (2020). International Journal of Novel Research and Development, 5(12), 71–81.*
- *Saha, B., Aswini, T., & Solanki, S. (2021). Designing hybrid cloud payroll models for global workforce scalability. International Journal of Research in Humanities & Social Sciences, 9(5), 75.*
- *Exploring the security implications of quantum computing on current encryption techniques. (2021). Journal of Emerging Technologies and Innovative Research, 8(12), g1–g18.*
- *Saha, B., Kumar, L., & Kumar, A. (2019). Evaluating the impact of AI-driven project prioritization on program success in hybrid cloud environments. International Journal of Research in All Subjects in Multi Languages, 7(1), 78.*
- *Robotic process automation (RPA) in onboarding and offboarding: Impact on payroll accuracy. (2023). International Journal of Current Science, 13(2), 237–256.*
- *Saha, B., & Renuka, A. (2020). Investigating cross-functional collaboration and knowledge sharing in cloud-native program management systems. International Journal for Research in Management and Pharmacy, 9(12), 8.*
- *Edge computing integration for real-time analytics and decision support in SAP service management. (2025). International Journal for Research Publication and Seminar, 16(2), 231–248. https://doi.org/10.36676/jrps.v16.i2.283*