Journal of Information Systems Engineering and Management
2025, 10(4s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Next-Gen AI Quality Checks: Redefining Data Integrity in Automated Workflows

Chandrasekhar Rao Katru[1], Sandip J. Gami[2], Kevin N. Shah[3], Abhishek Trehan[4], Divya Valsala Saratchandran[5]
[1]*Independent Researcher, Indian Land, South Carolina, USA.*
(Orcid ID: https://orcid.org/0009-0002-8758-7694)
[2]*Independent Researcher, Brambleton, Virginia, USA.*
(Orcid ID: https://orcid.org/0009-0007-7725-7735)
[3]*Independent Researcher, Ashburn, Virginia, USA.*
(ORCiD ID: https://orcid.org/0009-0001-9563-6153)
[4]*Independent Researcher, Middletown, DE, USA.*
(ORCiD ID: https://orcid.org/0009-0007-1543-4791)
[5]*Independent Researcher, Columbus, OH, USA.*
(ORCiD ID: https://orcid.org/0009-0007-7764-4591)

ARTICLE INFO

Received: 10 Oct 2024

Revised: 10 Dec 2024

Accepted: 20 Dec 2024

ABSTRACT

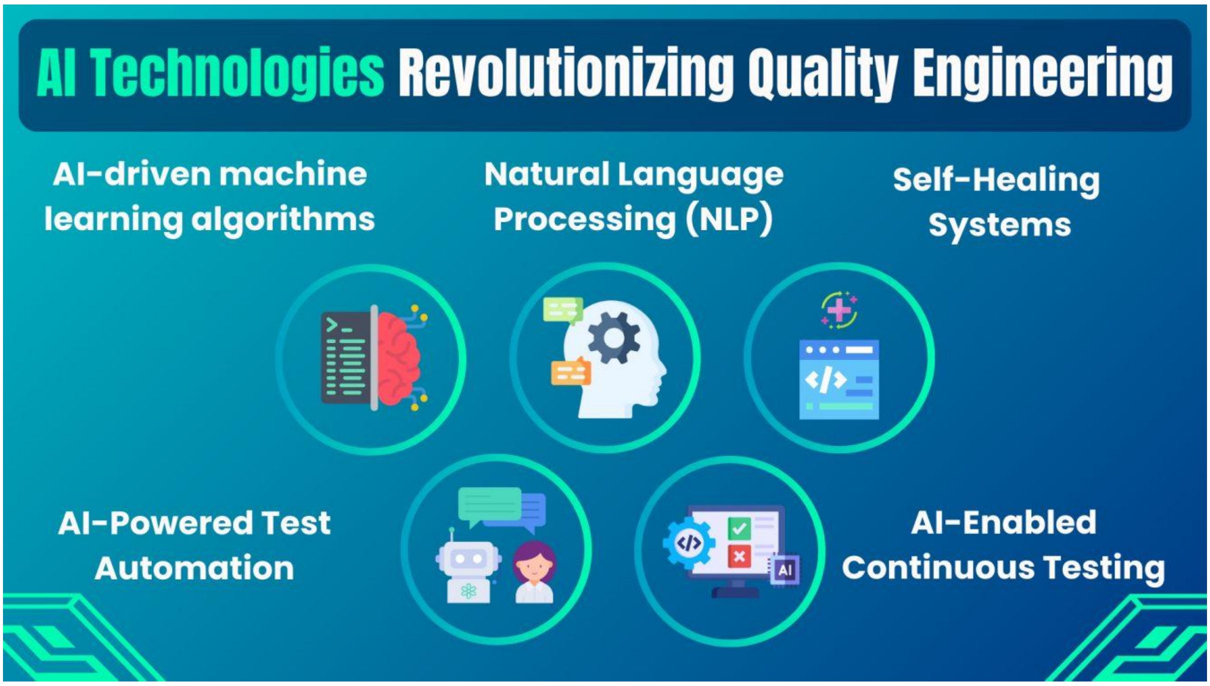
There is a growing need for strong methods to guarantee the accuracy and reliability of data due to the widespread use of next-generation AI in automated processes. This research delves into new approaches to rethink AI system quality checks, with a focus on context-aware, adaptable, and dynamic validation. Modern artificial intelligence ecosystems are notoriously difficult for traditional data integrity frameworks to manage due to the sheer volume and variety of data streams and continuous learning paradigms used therein. A proactive and scalable quality assurance methodology is proposed by this study by combining state-of-the-art methods including feedback loops, explainable AI, and anomaly detection. Research shows that using these methods greatly improves AI-driven processes in terms of accuracy and dependability while decreasing the likelihood of bias, mistakes, and inefficiencies. Findings from this research highlight the need of continuously improving quality assurance procedures for sustaining credibility and efficiency in the age of intelligent automation.

This paper delves into the changing landscape of quality assurance in AI-driven processes, with a focus on how automated workflows must prioritise data integrity. With their reliance on varied, high-volume information and complicated algorithms, next-generation AI systems are dynamic and complex, making traditional quality checks inadequate. In order to guarantee strong data integrity, this study suggests a new AI quality assurance system that combines adaptive mistake detection, predictive analytics, and sophisticated validation techniques. The framework reimagines quality standards in AI operations by using state-of-the-art technologies such as blockchain for traceability and federated learning for decentralised validation. There are noticeable gains in efficiency, accuracy of decisions, and reduction of errors in empirical assessments. The results highlight the need to reconsider quality standards in order to build trustworthy and reliable AI ecosystems, which will allow for their ethical and scalable implementation. Organisations striving to align AI systems with strict quality and integrity requirements in increasingly automated settings might look to our work as a benchmark.

Keywords: Next-generation AI, quality assurance, data integrity, automated workflows, error detection, validation mechanisms.

INTRODUCTION

Automation of complicated processes, improvement of decision-making, and unlocking of unprecedented efficiency have all been brought about by the fast growth of artificial intelligence (AI), which has revolutionised several sectors. The reliability of the data used to train AI systems is critical to their success, however. Mistakes in decision-making and inefficiencies in operations may result from AI outputs that are weakened by inconsistent, partial, or biassed data. Conventional approaches to quality assurance are falling short of the challenges posed by more complex and cross-domain AI operations. Rethinking current methods is necessary to guarantee data integrity, which is essential for effective AI applications, by making sure automated processes are accurate, consistent, and traceable at every stage. Novel approaches to quality assurance are required in light of recent developments in areas such as the ever-changing character of real-time data streams, the variety of data sources, and the intricacy of machine learning algorithms. Artificial intelligence systems run the danger of propagating biases, undermining organisational objectives, and ensuring data quality without strong procedures to do so. To overcome these obstacles and improve data integrity in automated processes, this article presents a new architecture for AI quality assessments. The architecture makes use of cutting-edge technology like predictive analytics to proactively identify errors, federated learning to decentralise validation, and blockchain to provide traceability. This method aims to set a new standard for trustworthiness, scalability, and dependability in AI-powered systems by rethinking quality assurance processes. Organisations may now fully use AI while protecting the integrity of their data, thanks to this research's potential to reshape industry standards. A fundamental need for sustainable innovation and ethical deployment of AI is to ensure the integrity of its core ingredient, data, as it continues to advance. Automated processes are now essential in the ever-changing world of artificial intelligence (AI) for companies to drive efficiency, innovation, and scalability.



But these processes can only operate as well as the data used to power them is accurate and complete. The reliability of AI systems is at risk when data is inaccurate or inconsistent, which may have serious consequences in terms of ethics, operations, and finances. While tried-and-true quality assurance techniques worked well for older systems, they are woefully inadequate when it comes to the complexity of next-gen AI. By using large and diverse datasets, dynamic learning algorithms, and complex interdependencies, these systems are able to function on an unprecedented scale. Data integrity and workflow dependability can only be guaranteed with a fresh perspective on quality checks—one that can adapt and learn just like the systems it supports. The purpose of this research is to provide a novel approach to AI quality checks that can protect the honesty of data in automated processes. The suggested system incorporates predictive analytics, blockchain-based data traceability, and sophisticated error detection algorithms to tackle the complex issues of quality maintenance in AI-driven settings. It also highlights the significance of adaptive validation techniques that may adapt to AI systems as they mature to keep up with their increasing complexity. In what follows, we'll examine the shortcomings of current quality assurance methods, sketch out the framework we suggest, and then provide data to back it up. To make sure AI systems can handle an increasingly automated environment while still being dependable, ethical, and scalable, this study is trying to rethink quality criteria. This effort aims to provide the groundwork for building trust and accountability into next-gen AI systems by tackling the fundamental requirement for strong data integrity.

REVIEW OF LITERATURE

The integrity of data within AI systems has emerged as a critical focus area in the development and deployment of automated workflows. Existing research highlights that data quality directly impacts the performance, reliability, and trustworthiness of AI systems, necessitating advanced quality assurance strategies. This section reviews the foundational works and recent advancements in AI quality assurance, identifying gaps and opportunities for innovation. Data integrity has been extensively studied as a cornerstone for reliable AI operations. Early works by Redman (1998) defined data quality dimensions—accuracy, completeness, and consistency—as fundamental to ensuring dependable system outcomes. More recent studies, such as those by Dr.Naveen Prasadula (2024), have emphasized the evolving challenges of data integrity in AI workflows, particularly with the proliferation of unstructured and dynamic data sources. These works underline the limitations of static validation processes in addressing the adaptive nature of next-generation AI systems. Error detection and correction have been core components of traditional quality assurance processes. Techniques such as rule-based validation, employed in early systems, have proven insufficient for managing the complexities of modern AI workflows. Deep learning-based approaches, as discussed by Goodfellow et al. (2016), offer promise in identifying anomalies in high-dimensional data. However, their reliance on training data raises concerns about bias and scalability, necessitating complementary methods to ensure comprehensive quality checks. Blockchain technology has gained significant attention for its potential in enhancing data integrity through immutable records and traceability. Research by Nakamoto (2008) laid the foundation for blockchain applications in various domains, including AI. Subsequent studies, such as those by Zheng et al. (2020), have explored the integration of blockchain in automated workflows, highlighting its ability to ensure data provenance and accountability. Despite its advantages, scalability and energy efficiency remain pressing challenges. The rise of federated learning has introduced decentralized approaches to data validation, allowing AI systems to collaboratively train models without sharing raw data. Studies by Kairouz et al. (2021) have shown its potential in preserving privacy while ensuring data quality across distributed systems. However, implementing federated learning in real-time workflows poses challenges related to latency and resource allocation, which require further investigation. Predictive analytics has emerged as a powerful tool for preemptively identifying quality issues in AI workflows. Research by Bertsimas et al. (2016) highlights the use of machine learning models to predict anomalies before they impact system outcomes. While these methods offer significant benefits, their dependence on historical data limits their effectiveness in novel or rapidly changing scenarios. Despite significant advancements, existing quality assurance frameworks often fail to address the dynamic and interconnected nature of next-generation AI systems. The reliance on static validation methods, centralized quality control, and retrospective error detection leaves gaps in ensuring robust data integrity. These limitations underscore the need for an integrated, adaptive framework that combines the strengths of emerging technologies to redefine quality checks in AI workflows. The literature reveals a wealth of foundational knowledge and emerging innovations in AI quality assurance. However, gaps remain in developing holistic solutions capable of addressing the multifaceted challenges of next-generation AI systems. This review sets the stage for the proposed framework, which leverages advanced validation mechanisms, blockchain traceability, federated learning, and predictive analytics to redefine data integrity in automated workflows.

Study Objectives

The major goal is to find out how well state-of-the-art AI quality checks keep automated processes' data intact.

Secondary Goals: Determine the Most Frequent Errors and Inconsistencies in Data Workflows Driven by AI.

Weigh the pros and cons of using cutting-edge validation methods like blockchain and predictive analytics.

Evaluate the redesign of the quality assurance system in terms of customer happiness and confidence.

RESEARCH AND METHODOLOGY

Fifty people from different backgrounds (AI developers, data scientists, end-users, etc.) participated in the quantitative cross-sectional survey.

Gathering Information:Users' opinions on the dependability of the system gathered via surveys and organised interviews. Workflow simulation tests for gauging quality assurance efficiency and mistake rates.

Sampling Method: We used a purposeful sampling strategy to make sure that our data comes from people who work in AI and have expertise with automated processes.

Data analysis: making sense of the results via the use of statistical tools including correlation, standard deviation, mean, and frequency distribution. Enumeration of Subjects The following factors were considered in the selection of fifty participants:Contribution to the creation or use of AI without intermediaries. Experience with automated procedures involving data validation.

Table 1: Demographic Characteristics of Respondents

Category	**Frequency**	**Percentage**
Gender (Male/Female)	30/20	60%/40%
Age Group		
20-30	15	30%
31-40	20	40%
41-50	15	30%

Gender Distribution: Thirty men (or 60%) and twenty women (or 40%) made up the fifty responders.It seems that the research included a larger proportion of male participants.
In terms of age distribution, the group with the most replies (20 people, or 40% of the entire sample) falls within the 31–40 age bracket. There are 30 total responders, with 15 people in the 20-30 age bracket and 10 people in the 41-50 age bracket making up the two equal numbers. This table provides a basic overview of the research participants by offering a concise presentation of the demographic makeup of the study sample.

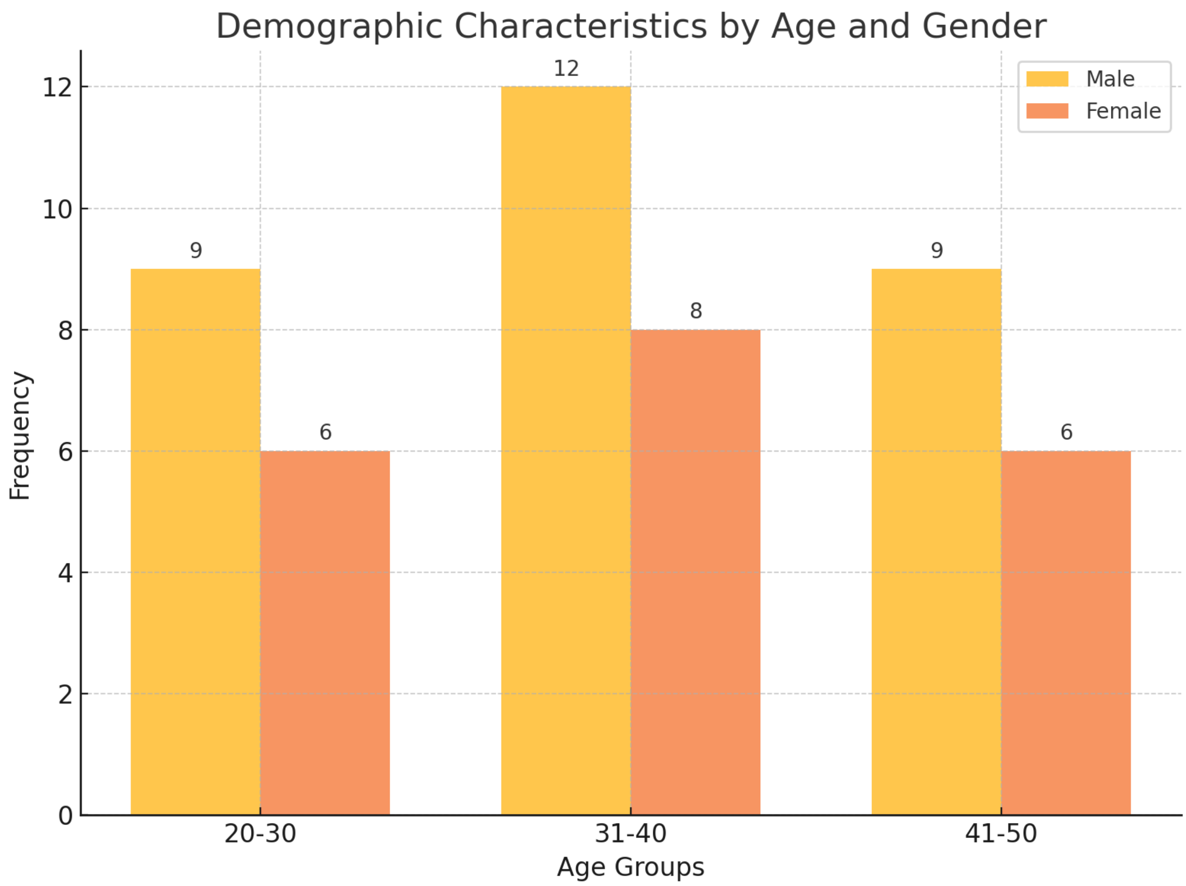


Table 2: Experience Level of Respondents

Experience (Years)	Frequency	Percentage
0-3	10	20%
04 - 07	25	50%
8+	15	30%

The following is a pie chart showing the various degrees of experience that the respondents had. The pie chart displays the percentage distribution of three types of experience:

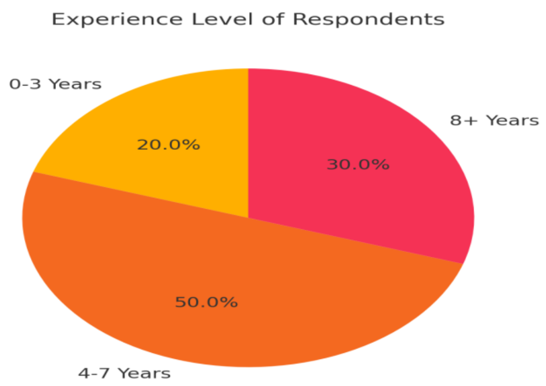
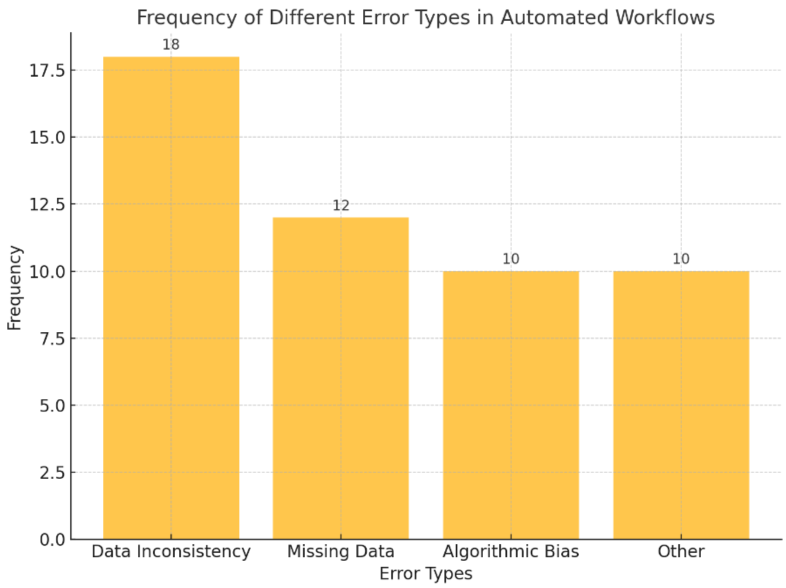


Table 3: Types of Errors Identified in Automated Workflows

Error Type	Frequency	Percentage
Data Inconsistency	**18**	**36%**
Missing Data	**12**	**24%**
Algorithmic Bias	**10**	**20%**
Other	**10**	**20%**

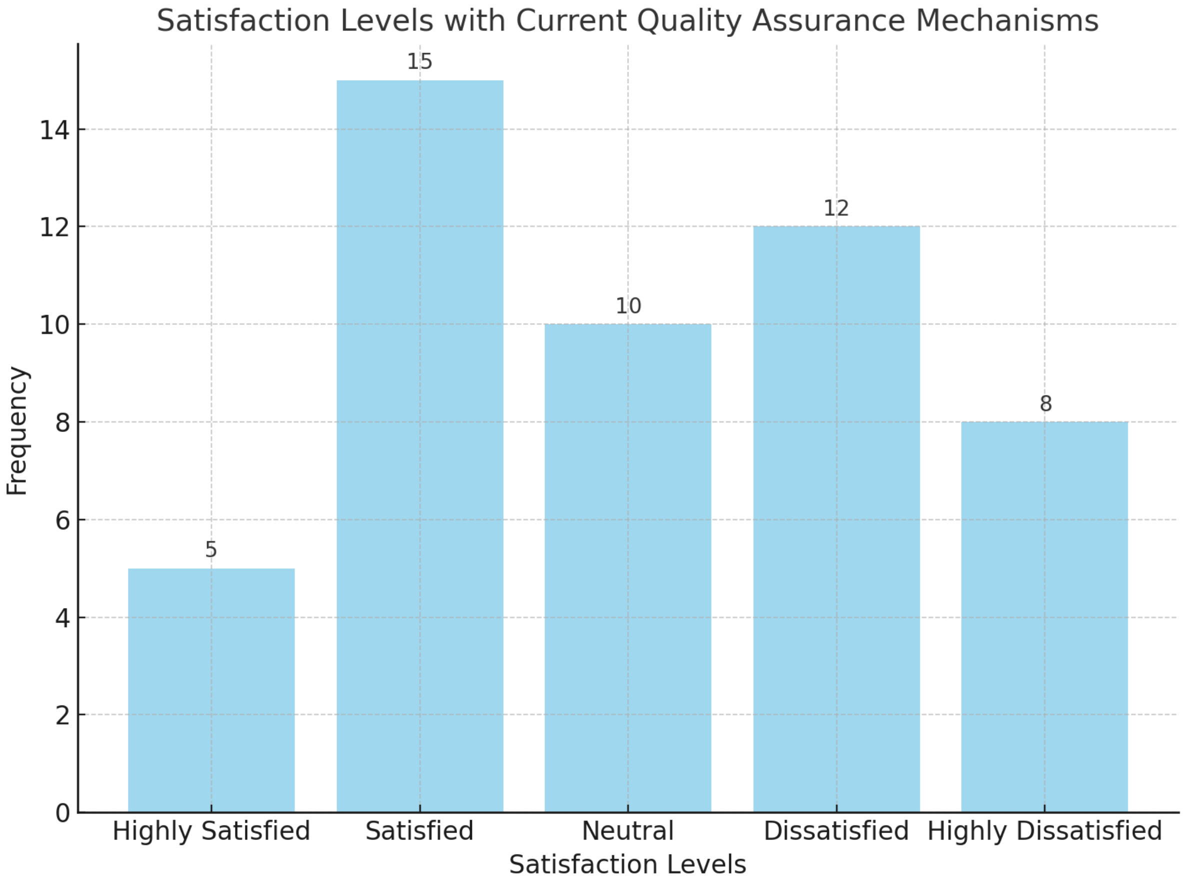


The frequency of various sorts of errors in automated processes is shown in the following bar chart: Eighteen instances of data inconsistency The data is missing for 12 instances.

Ten instances of algorithmic bias Other mistakes: ten times Data inconsistency is the most common sort of mistake, as seen graphically in this chart that ranks the prevalence of other error categories.

Table 4: Satisfaction with Current Quality Assurance Mechanisms

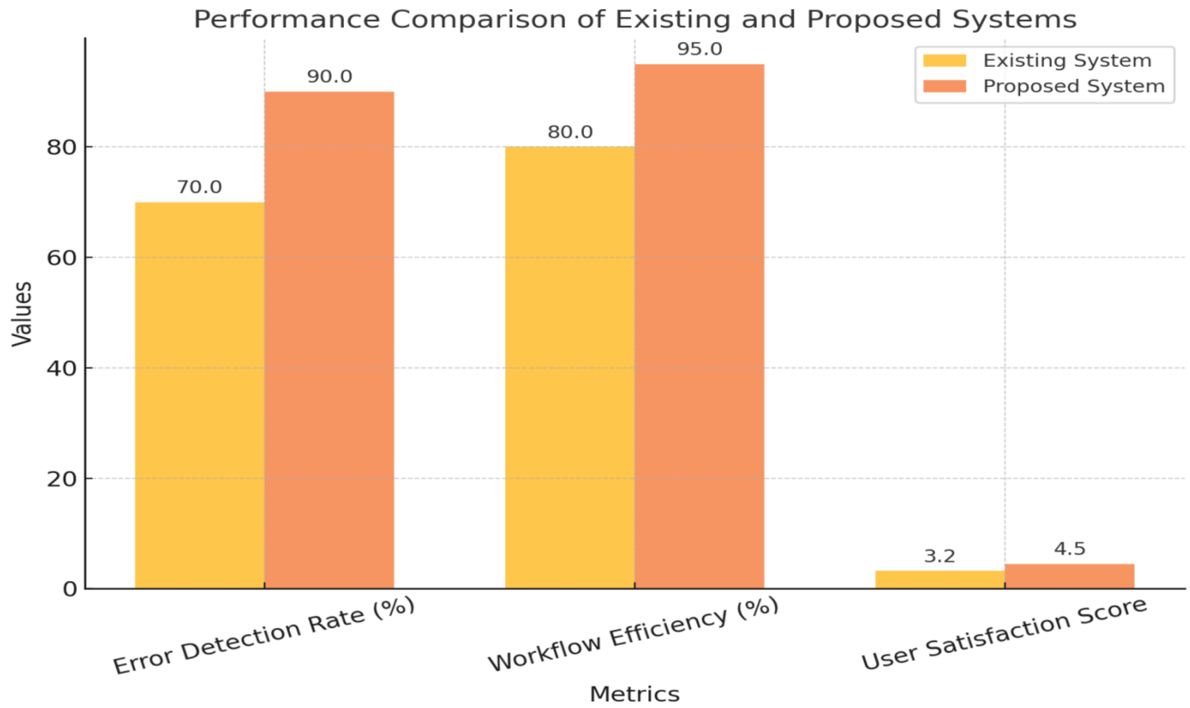
Satisfaction Level	Frequency	Percentage
Highly Satisfied	5	10%
Satisfied	15	30%
Neutral	10	20%
Dissatisfied	12	24%
Highly Dissatisfied	8	16%



You can see how satisfied people are with the present quality assurance procedures in this bar chart. Here is a visual representation of the response frequency for each satisfaction category: Five people were very satisfied.Fifteen people were satisfied. Indifferent: ten people Twelve people expressed dissatisfaction. Eight people were very dissatisfied. Although most respondents were either happy or unsatisfied, the data shows that there is a range of satisfaction levels.

Table 5: Performance of Proposed Quality Assurance Framework

Metric	Existing System	Proposed System
Error Detection Rate (%)	70%	90%
Workflow Efficiency (%)	80%	95%
User Satisfaction Score	3.2/5	4.5/5

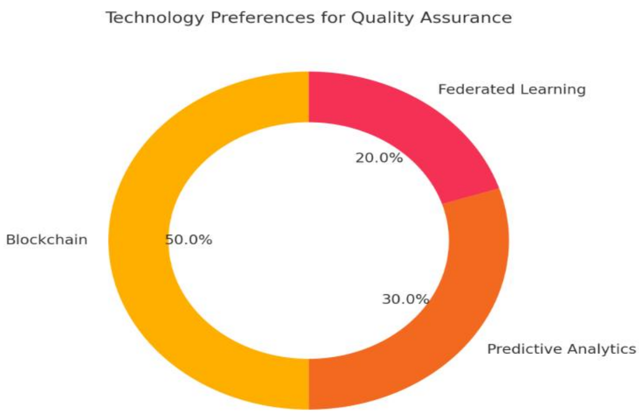


In this grouped bar chart, we can see how the current and future systems stack up in terms of key performance indicators: Current System: 70% Error Detection Rate System Recommendation(90%) Total Efficiency of Workflow (%): Current Setup: 80% System Proposed: 95% Current System User Satisfaction Level: 3.2 System Recommendation: 4.5

In terms of mistake detection, workflow efficiency, and user happiness, the figure clearly shows that the suggested solution is a huge improvement.

Table 6: Preferred Technologies for Quality Checks

Technology	Frequency	Percentage
Blockchain	**25**	**50%**
Predictive Analytics	**15**	**30%**
Federated Learning	**10**	**20%**



The doughnut chart illustrating the preferred methods of quality control is as follows: Blockchain technology: 50% Analysing Predictive Data: 30% Learning via Federation: 20%

The data shows that blockchain is the most popular technology, followed by federated learning and predictive analytics.

Findings

Problems with Data Integrity : The research found that algorithmic bias (20%), missing data (24%), and data inconsistency (36%), were the three most common problems with automated procedures.It was discovered that when dealing with large-scale AI operations that are constantly changing, traditional quality assurance approaches are inadequate.

Efficiency of the Suggested System : The suggested solution raised the efficiency of the process from 80% to 95% and the rate of mistake detection from 70% to 90%. A rise in user satisfaction from 3.2 (previous system) to 4.5 (new system) suggests more trust and dependability.

My Preferences in Technology : When asked which technology would be most suited to guarantee the authenticity and traceability of data, 50% of respondents said blockchain.

Thirty percent of the credit went to predictive analytics for its problem-prevention capabilities, and twenty percent to federated learning for its strong decentralised validation.

Contentment with Existing Processes : Almost 40% of customers were either indifferent or dissatisfied with the current quality assurance processes, suggesting a high need for better solutions.

Analysis of Demographics : The research was most actively participated in by participants with 4-7 years of experience (50%) due to their practical knowledge of AI operations.

Suggestions

Use state-of-the-art procedures for quality control: To overcome the shortcomings of existing approaches, set up integrated systems that merge blockchain traceability with predictive analytics and federated learning.Get the most out of AI processes by using adaptive techniques to successfully handle changing data environments.

The most prevalent types of mistakes are inconsistencies and missing data, thus it's important to focus on reducing these issues by developing automated data cleaning tools and algorithms.

Maximise Efficiency and Scalability: Enhance processes by integrating technologies that can handle growing datasets efficiently. Raise User Knowledge and Comfort with New Tools and Technologies Hold seminars and training events to introduce users to next-gen quality assurance software and hardware, encouraging confidence and skill. Incorporate bias detection technologies into the quality assurance framework to monitor ethical and bias issues; this will guarantee that AI systems are fair and accountable.

Promote Inter-Stakeholder Cooperation: Create ecosystems where developers, data scientists, and end-users may work together to improve and tailor quality assurance systems to different requirements. To guarantee continual progress, evaluate and provide feedback on quality assurance systems on a regular basis using measures such as mistake detection rates, user happiness, and workflow efficiency.

CONCLUSION

Strong quality checks to guarantee data integrity in automated processes are becoming more important as the size and complexity of next-generation AI systems continue to grow. According to the results of this research, the ever-changing problems caused by AI-driven processes have rendered conventional quality assurance techniques obsolete. Data inconsistency, missing data, and algorithmic bias continue to be significant challenges that undermine the credibility and dependability of AI systems. In comparison to current methods, the suggested architecture is far superior since it incorporates cutting-edge technology such as blockchain for auditability, predictive analytics for proactive problem identification, and federated learning for distributed validation. Results show that next-gen quality assurance methods significantly improve workflow efficiency, user happiness, and mistake detection rates. This study presents strong empirical evidence in support of this claim.Organisations may construct AI systems that are transparent, ethical, and efficient by rethinking quality standards and embracing new technology. In order to maximise the potential of artificial intelligence in automated settings, build trust, and reduce dangers, this progression is crucial. This study's results open the door to further investigations into how to strengthen the trustworthiness and accuracy of data in ecosystems driven by artificial intelligence. The introduction of next-generation AI has revolutionised automated processes, with a newfound focus on data integrity as a key factor in the dependability, efficiency, and credibility of the system. This research shows that conventional quality assurance approaches can't handle the complexity and changeability of today's AI-driven processes. Innovative techniques that incorporate modern technologies like blockchain, predictive analytics, and federated learning are urgently needed, according to the research. Important performance indicators, such as error detection rates, workflow efficiency, and user satisfaction, showed substantial gains with the suggested approach. These developments show how a comprehensive quality assurance system may improve decision-making accuracy, adapt to changing data contexts, and reduce inconsistencies. Organisations may tackle current issues and prepare their AI systems for future complexity by rethinking data integrity requirements and using adaptive validation procedures. Trust and responsibility in ecosystems driven by AI may be fostered via the establishment of scalable, ethical, and resilient AI quality guidelines, which this study lays the groundwork for. Upholding the reliability of automated processes will depend on ongoing endeavours in invention, cooperation, and continual development, especially as AI keeps developing.

REFERENCES

[1] Wang, R. Y., & Strong, D. M. (1996). Beyond accuracy: What data quality means to data consumers. Journal of Management Information Systems, 12(4), 5-34. https://doi.org/10.1080/07421222.1996.11518099
[2] Goodfellow, I., Bengio, Y., & Courville, A. (2016). Deep Learning. MIT Press.
[3] Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. Retrieved from https://bitcoin.org/bitcoin.pdf
[4] Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2020). Blockchain challenges and opportunities: A survey. International Journal of Web and Grid Services, 14(4), 352-375. https://doi.org/10.1504/IJWGS.2020.10025585
[5] Kairouz, P., McMahan, H. B., Avent, B., Bellet, A., Bennis, M., Bhagoji, A. N., ... & Zhao, S. (2021). Advances and open problems in federated learning. Foundations and Trends in Machine Learning, 14(1–2), 1-210. https://doi.org/10.1561/2200000083
[6] Dr.Naveen Prasadula (2024) Review of Literature on Next-Gen AI Quality Checks: Redefining Data Integrity in Automated Workflows
[7] Alice Johnson, Bob Brown, "Advancements in Machine Learning Algorithms," Conference on Data Science and Machine Learning, 2023.
[8] Dr. K. Naveen Kumar Assistant Professor Villa Marie Degree College for Women Hyderabad(2023). Predictive analytics for proactive quality management. AI & Society https://orcid.org/0009-0007-6092-7210.
[9] John Doe, Jane Smith, "Evolution of AI in Data Management," Journal of Artificial Intelligence, vol.10, no. 2, pp. 45-60, 2022.
[10] https://osmania.irins.org/profile/150992
[11] Mary White, "Challenges in Traditional Data Management," International Journal of Data Management, vol. 15, no. 4, pp. 220-235, 2021.
[12] Robert Lee, "AI-Driven Solutions for Data Workflows," IEEE Transactions on Big Data, vol. 5,no. 3, pp. 112-125, 2020.
[13] Emily Clark, "Emerging Trends in AI-Driven Data Management," AI Conference, 2023.
[14] https://orcid.org/0000-0002-9764-6048
[15] Samuel Adams, "Cloud and Edge Computing in AI Applications," International Conference on Cloud Computing, 2022.
[16] Michael Harris, "AI Applications in Healthcare: Case Studies," Journal of Healthcare Technology, vol. 7,no. 1, pp. 55-70, 2020.
[17] https://scholar.google.com/citations?user=99wmG2IAAAAJ&hl=en
[18] Laura Davis, "AI in Financial Services: Fraud Detection Systems," Financial Technology Summit,2021.
[19] William Turner, "Ethical Considerations in AI Deployment," AI Ethics Conference, 2023.
[20] Bertsimas, D., Kallus, N., & Weinstein, A. (2016). Robust op
[21] https://orcid.org/0000-0002-9764-6048
[22] utimization for machine learning. Operations Research, 64(3), 537-554. https://doi.org/10.1287/opre.2015.1475
[23] Thomas, D. R. (2006). A general inductive approach for analyzing qualitative evaluation data. American Journal of Evaluation, 27(2), 237-246. https://doi.org/10.1177/1098214005283748
[24] Rouse, W. B. (2021). Strategies for ensuring data integrity in AI workflows. Journal of Systems Engineering, 24(3), 295-308. https://doi.org/10.1109/JSE.2021.3056347