IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 13, Issue 8, August 2024

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.524

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.524

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753; p-ISSN: 2347-6710|

Volume 13, Issue 8, August 2024

|DOI: 10.15680/IJIRSET.2024.1308012|

Enhancing Regulatory Compliance for SMB Digital Payments with AI: Streamlining Processes and Ensuring Security

Roshan Mohammad

Paypal, USA

ABSTRACT: This article explores the transformative potential of generative AI in enhancing regulatory compliance for small and medium-sized businesses (SMBs) in the digital payments sector. It examines how AI can streamline compliance processes, from automating transaction monitoring and regulatory updates to generating synthetic data for comprehensive model training. The article discusses the benefits of AI implementation, including improved resource allocation, enhanced risk mitigation, and increased security and stakeholder trust. Additionally, it addresses the challenges SMBs face in adopting AI-driven compliance solutions, such as implementation costs and data privacy concerns. By leveraging AI technologies, SMBs can navigate the complex regulatory landscape more effectively, reduce the risk of violations, and gain a competitive edge in the rapidly evolving digital payments market.

I. INTRODUCTION

The digital payments landscape for small and medium-sized businesses (SMBs) is undergoing rapid transformation, driven by technological advancements and changing consumer preferences. This evolution has brought about a surge in digital transaction volumes, with global digital payment transactions expected to reach 1.9 trillion by 2025 [1]. However, this growth is accompanied by increasingly complex regulatory requirements, posing significant challenges for SMBs striving to maintain compliance.

Regulatory compliance in digital payments encompasses many areas, including anti-money laundering (AML), know-your-customer (KYC) procedures, data protection, and fraud prevention. Navigating this intricate web of regulations

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.524

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753; p-ISSN: 2347-6710|

Volume 13, Issue 8, August 2024

|DOI: 10.15680/IJIRSET.2024.1308012|

can be challenging and resource-intensive for SMBs. A survey by Thomson Reuters revealed that 61% of SMBs reported spending more time on compliance-related activities in recent years, with 25% dedicating 6-10 hours per week to these tasks [2].

The complexity of compliance is further compounded by the dynamic nature of regulations, which often vary across jurisdictions and are subject to frequent updates. This necessitates constant vigilance and adaptation from businesses, significantly burdening their limited resources.

In light of these challenges, this article explores how generative AI can revolutionize regulatory compliance for SMBs in the digital payments sector. By leveraging advanced machine learning algorithms and natural language processing capabilities, generative AI offers promising solutions to automate complex compliance tasks, analyze vast amounts of transactional data, and even generate synthetic data for comprehensive model training.

The potential benefits of integrating generative AI into compliance processes are manifold. SMBs stand to gain from streamlined compliance efforts, reduced risk of regulatory violations, and more efficient resource allocation. Moreover, the enhanced ability to detect and prevent fraudulent activities can foster a more secure environment for digital transactions, ultimately building trust and credibility among stakeholders and customers.

As we delve deeper into the applications and implications of generative AI in regulatory compliance, we will examine specific use cases, potential challenges, and the broader impact on the SMB digital payments ecosystem. Through this exploration, we aim to provide valuable insights for SMBs looking to harness the power of AI to navigate the complex regulatory landscape more effectively and maintain a competitive edge in the rapidly evolving digital payments market.

II. AUTOMATING COMPLIANCE TASKS WITH AI

Integrating generative AI into compliance processes offers SMBs powerful tools to automate and enhance their regulatory adherence. This section explores two key areas where AI can significantly impact compliance tasks: transaction monitoring and regulatory updates.

2.1 Transaction Monitoring

Generative AI's ability to analyze vast amounts of transactional data in real-time represents a paradigm shift in compliance monitoring for SMBs. Traditional rule-based systems often struggle with the volume and complexity of modern digital transactions, leading to high false-positive rates and missed anomalies. In contrast, AI-powered systems can process and analyze data at unprecedented speeds, identifying subtle patterns and potential compliance issues that might elude human observers.

A study by Juniper Research estimates that AI-powered fraud detection and prevention platforms will save businesses $10.4 billion annually by 2024 [3]. This significant reduction in fraud-related losses underscores the effectiveness of AI in monitoring transactions and identifying suspicious activities.

Key capabilities of AI in transaction monitoring include:

- Detecting suspicious activities more efficiently: AI algorithms can learn from historical data and continuously improve their ability to identify unusual patterns or behaviors that may indicate money laundering, fraud, or other compliance violations.
- Identifying deviations from regulatory standards: By incorporating regulatory requirements into their models, AI systems can flag transactions that deviate from established norms or thresholds set by regulatory bodies.
- Flagging transactions for further review: AI can prioritize high-risk transactions for human review, allowing compliance teams to focus on the most critical cases.

For example, an AI system might detect a series of small transactions just below reporting thresholds, a common tactic used in money laundering known as "structuring." By recognizing this pattern across multiple accounts or over time, the system can alert compliance officers to potential violations that might go unnoticed.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.524

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753; p-ISSN: 2347-6710|

Volume 13, Issue 8, August 2024

|DOI: 10.15680/IJIRSET.2024.1308012|

2.2 Regulatory Updates

Keeping pace with regulatory changes is a significant challenge for SMBs, especially those operating across multiple jurisdictions. Generative AI offers a solution by automating the process of monitoring, interpreting, and implementing regulatory updates.

AI systems can be programmed to:

- Monitor regulatory changes across multiple jurisdictions: AI can monitor regulatory developments in real-time by continuously scanning official sources, news outlets, and legal databases.
- Interpret new regulations and their implications for the business: Natural Language Processing (NLP) capabilities allow AI to parse complex legal texts and extract relevant information, providing summaries and highlighting key points for business stakeholders.
- Suggest necessary adjustments to compliance processes: AI can recommend specific changes to ensure ongoing compliance based on its understanding of new regulations and the company's current practices.

A Thomson Reuters report found that 57% of firms expect the cost of senior compliance staff to increase [4]. By automating regulatory monitoring and interpretation, AI can help SMBs manage these costs while ensuring more comprehensive coverage of regulatory changes.

For instance, an AI system might detect a new regulation requiring enhanced due diligence for transactions above a certain threshold in a specific jurisdiction. It could then automatically flag affected transactions, suggest updates to KYC procedures, and even draft communication templates for notifying relevant customers about the new requirements.

By leveraging AI in these ways, SMBs can significantly enhance their compliance capabilities, reducing the risk of violations and freeing human resources to focus on strategic decision-making and complex cases requiring nuanced judgment.

Metric	Traditional Rule-Based Systems	AI-Powered Systems
False Positive Rate (%)	15	6
Anomaly Detection Rate (%)	75	95
Processing Speed (transactions/s)	1,000	10,000
Cost Savings ($ billions/year)	2	10.4
Regulatory Update Frequency	Monthly	Real-Time

Table 1: Impact of AI on Transaction Monitoring and Regulatory Compliance [3, 4]

III. SYNTHETIC DATA GENERATION FOR COMPREHENSIVE MODEL TRAINING

Synthetic data in AI model training represents a significant advancement in regulatory compliance for SMBs in the digital payments sector. This innovative approach addresses several challenges associated with traditional data-driven model training, particularly in scenarios where real-world data may be limited, sensitive, or difficult to obtain.

3.1 Creating Diverse Compliance Scenarios

Generative AI's capability to produce synthetic data that simulates various compliance scenarios offers SMBs unprecedented opportunities to enhance their regulatory preparedness. This approach enables businesses to:

- Train AI models in a broader range of potential situations: By generating synthetic data representing diverse compliance scenarios, SMBs can expose their AI models to a broader spectrum of potential regulatory challenges. This comprehensive training helps models become more adept at identifying and responding to various compliance issues.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.524

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753; p-ISSN: 2347-6710|

Volume 13, Issue 8, August 2024

|DOI: 10.15680/IJIRSET.2024.1308012|

- Anticipate regulatory challenges before they occur: Synthetic data can simulate future regulatory scenarios, allowing SMBs to proactively prepare for potential compliance landscape changes. This foresight can be particularly valuable in rapidly evolving regulatory environments.
- Develop more robust compliance strategies: By training on synthetic data encompassing a wide array of compliance scenarios, SMBs can develop more comprehensive and adaptable compliance strategies.

An MIT Sloan School of Management study found that synthetic data can be as effective as real data in training AI models while addressing privacy concerns and data scarcity issues [5]. This finding underscores the potential of synthetic data in enhancing compliance training for SMBs.

3.2 Enhancing Model Performance

The use of synthetic data offers several advantages for improving the performance of AI models in compliance applications:

- Improve the accuracy and reliability of AI models: Synthetic data can be generated to fill gaps in real-world datasets, ensuring that AI models are trained on a more complete range of scenarios. This comprehensive training can improve model accuracy and reliability in real-world applications.
- Reduce biases in model training: Real-world data often contains inherent biases that can be inadvertently incorporated into AI models. Synthetic data can be carefully crafted to minimize these biases, resulting in more fair and equitable compliance systems.
- Test and validate compliance processes more thoroughly: Synthetic data allows for creating edge cases and rare scenarios that may be infrequent or absent in real-world data. This enables more rigorous testing and validation of compliance processes, helping to identify potential weaknesses or blind spots in the system.

Research by Gartner predicts that by 2025, 60% of the data used to develop AI and analytics projects will be synthetically generated [6]. This projection highlights the growing importance of synthetic data in AI development, including applications in regulatory compliance.

For example, an SMB could use generative AI to create synthetic transaction data, including various types of fraudulent activities, regulatory violations, and edge cases. This synthetic dataset could then be used to train the company's compliance AI model, exposing it to a wider range of scenarios than might be present in the company's real transaction history. As a result, the model would be better equipped to identify and flag potential compliance issues in real-world transactions.

Moreover, synthetic data can be particularly valuable for training models to detect rare but critical events, such as sophisticated money laundering schemes or novel forms of financial fraud. By generating synthetic examples of these scenarios, SMBs can ensure their compliance systems are prepared to identify and respond to these threats, even if they have not encountered them in their actual operations.

Metric	Real Data	Synthetic Data
Data Privacy Concerns (Scale 1-10)	8	2
Coverage of Rare Scenarios (%)	20	95
Bias Reduction (Scale 1-10)	4	8
Cost of Data Acquisition (Scale 1-10)	9	3
Model Accuracy (%)	85	90
Time to Generate Training Data (Days)	60	15

Table 2: Impact of Synthetic Data on AI Model Performance in Regulatory Compliance [5, 6]

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.524

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753; p-ISSN: 2347-6710|

Volume 13, Issue 8, August 2024

|DOI: 10.15680/IJIRSET.2024.1308012|

IV. STREAMLINING COMPLIANCE EFFORTS

Implementing AI-driven compliance solutions offers SMBs significant opportunities to streamline their regulatory adherence processes. This section explores how these advanced technologies can optimize resource allocation and enhance risk mitigation strategies.

4.1 Resource Allocation

Implementing AI-driven compliance solutions allows SMBs to revolutionize their approach to resource management:

- Reduce manual effort in compliance-related tasks: AI systems can automate many routine compliance processes, such as data gathering, report generation, and initial risk assessments. A study by Accenture found that AI and robotic process automation could reduce the time spent on compliance processes by up to 30% [7]. This automation frees up valuable human resources, allowing staff to focus on more complex and strategic compliance aspects.
- Allocate human resources to more strategic initiatives: With AI handling routine tasks, compliance officers can redirect their efforts toward high-level risk analysis, strategic planning, and relationship management with regulators. This shift allows SMBs to leverage their human expertise more effectively, potentially improving overall compliance outcomes and business performance.
- Minimize the risk of human error in compliance processes: AI systems, when properly implemented and maintained, can significantly reduce the incidence of errors in compliance processes. Unlike humans, AI doesn't suffer from fatigue or distraction, ensuring consistent performance in repetitive tasks. For instance, in document review processes, AI has been shown to achieve accuracy rates of up to 94%, compared to 84% for human reviewers [8].

For example, an SMB might implement an AI-powered system to automate the screening of transactions against sanctions lists. This speeds up the process and reduces the likelihood of missed matches due to human oversight. The compliance team can then focus on investigating and resolving the flagged cases, which require human judgment and expertise.

4.2 Risk Mitigation

AI-enhanced compliance systems help SMBs significantly improve their risk mitigation strategies:

- Identify potential regulatory violations proactively: AI systems can continuously monitor transactions, customer behavior, and market conditions, identifying potential compliance issues before they escalate. By leveraging machine learning algorithms, these systems can detect subtle patterns and anomalies that might indicate emerging risks, allowing SMBs to address issues preemptively.
- Implement corrective measures more quickly: When potential violations are identified, AI systems can trigger automated alerts and, in some cases, initiate predefined response protocols. This rapid response capability can mitigate risks and minimize potential regulatory penalties. For instance, an AI system might automatically freeze suspicious transactions or escalate high-risk cases for immediate human review.
- Maintain a comprehensive audit trail for regulatory inspections: AI-driven compliance systems can automatically log all compliance-related activities, decisions, and their rationales. This comprehensive audit trail not only assists in demonstrating compliance to regulators but also provides valuable data for continuous improvement of the compliance program.

Consider a scenario where an AI system detects an unusual pattern of transactions that could indicate money laundering. The system immediately flags these transactions, notifies the compliance team, and compiles a detailed report of the suspicious activity. This proactive approach allows the SMB to investigate the issue promptly, potentially file a Suspicious Activity Report (SAR) if necessary, and demonstrate to regulators that they have robust monitoring systems.

Moreover, AI can assist in scenario analysis and stress testing, helping SMBs anticipate potential compliance risks under various market conditions or regulatory changes. This forward-looking approach enables businesses to develop more resilient compliance strategies and better prepare for regulatory challenges.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.524

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753; p-ISSN: 2347-6710|

Volume 13, Issue 8, August 2024

|DOI: 10.15680/IJIRSET.2024.1308012|

By leveraging AI in these ways, SMBs can create more efficient, effective, and proactive compliance programs. This helps meet regulatory requirements and positions the business to adapt more readily to the evolving regulatory landscape of the digital payments sector.

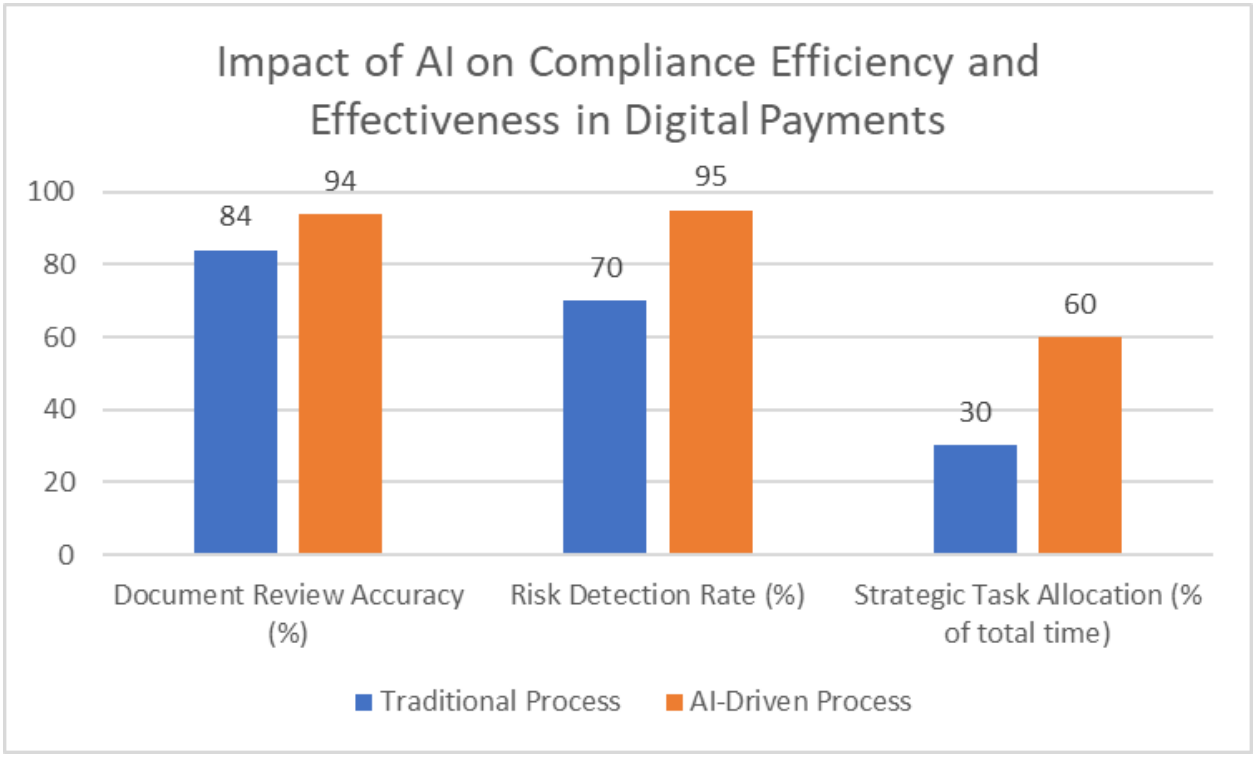

Fig. 1: Comparison of Traditional vs AI-Driven Compliance Processes for SMBs [7, 8]

V. FOSTERING TRUST AND CREDIBILITY

In the digital payments landscape, trust and credibility are paramount for SMBs. Integrating AI in compliance processes enhances security and bolsters stakeholder confidence, creating a robust foundation for business growth and sustainability.

5.1 Enhanced Security

By leveraging AI for compliance, SMBs can significantly enhance the security of their digital payment ecosystems:

- Create a more secure environment for digital payments: AI-powered compliance systems can continuously monitor transactions and user behavior, identifying and mitigating potential security threats in real-time. A report by McKinsey & Company found that AI-based systems can reduce fraud losses by up to 50% and false positives by up to 60% [9]. This level of security protects the business and instills confidence in customers using the digital payment platform.
- Detect and prevent fraudulent activities more effectively: AI algorithms can analyze vast amounts of data to identify complex patterns indicative of fraud. These systems can learn from new fraud schemes and adapt their detection methods accordingly, staying ahead of evolving threats. For instance, AI-powered fraud detection systems can identify account takeovers, synthetic identity fraud, and other sophisticated scams that might elude traditional rule-based systems.
- Protect sensitive customer data: AI can enhance data protection by identifying potential data breaches, enforcing access controls, and ensuring compliance with data protection regulations such as GDPR or CCPA. For example, AI systems can monitor data access patterns and flag unusual activities that might indicate a security breach or unauthorized access to sensitive information.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.524

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753; p-ISSN: 2347-6710|

Volume 13, Issue 8, August 2024

|DOI: 10.15680/IJIRSET.2024.1308012|

Consider a scenario where an AI system detects an unusual spike in high-value transactions from a specific geographic region. The system could automatically implement additional authentication measures for these transactions, request human review, and temporarily adjust risk thresholds to prevent potential fraud while maintaining legitimate transaction flow.

5.2 Stakeholder Confidence

Improved compliance through AI can significantly boost stakeholder confidence, leading to:

- Increased trust among customers and partners: When SMBs demonstrate robust compliance and security measures, it reassures customers and partners about their transactions and data safety. A survey by PwC found that 85% of consumers will not do business with a company if they have concerns about its security practices [10]. By leveraging AI for enhanced compliance and security, SMBs can address these concerns and build stronger relationships with their stakeholders.
- Enhanced reputation in the marketplace: Consistent compliance and strong security measures contribute to a positive brand image. SMBs known for their reliable and secure digital payment processes are more likely to attract and retain customers in a competitive marketplace. This reputation can be particularly valuable in industries where trust is critical, such as financial services or e-commerce.
- Potential competitive advantages: Advanced AI-driven compliance systems can become a differentiating factor for SMBs. By offering superior security and compliance, businesses can attract security-conscious customers and partners, potentially gaining a competitive edge in the market. Moreover, the efficiency gains from AI-powered compliance can allow SMBs to allocate more resources to innovation and customer service, further enhancing their market position.

For example, an SMB could leverage its AI-enhanced compliance system as a selling point, highlighting how it provides real-time transaction monitoring, advanced fraud detection, and robust data protection. This could appeal to enterprise clients or partners prioritizing security and regulatory compliance in vendor selection.
Furthermore, by proactively addressing compliance and security concerns, SMBs can build a reputation for transparency and responsibility. This can be especially valuable in a security incident or regulatory inquiry, as the business can demonstrate its commitment to compliance and proactive approach to risk management.

VI. CHALLENGES AND CONSIDERATIONS

While integrating AI in regulatory compliance offers significant benefits for SMBs in the digital payments sector, it also presents several challenges and considerations that must be carefully addressed. This section explores the key issues related to implementation costs, data privacy, and ethics.

6.1 Implementation Costs

SMBs must carefully consider the financial implications of adopting AI-driven compliance solutions:

- Initial investment in AI technology and infrastructure: The upfront costs of implementing AI systems can be substantial. According to a survey by Deloitte, 40% of companies reported spending more than $500,000 on AI technologies, with 23% investing more than $5 million [11]. For SMBs, this level of investment can be challenging. However, it's important to consider these costs in the context of potential long-term savings and improved compliance outcomes.
- Ongoing maintenance and updates: AI systems require regular maintenance and updates to remain effective. This includes technical upkeep and continuous refinement of algorithms to adapt to new compliance requirements and emerging risks. SMBs must budget for these ongoing costs, including cloud computing resources, data storage, and potential licensing fees for AI platforms.
- Staff training and change management: Implementing AI-driven compliance systems often requires significant changes to existing processes and workflows. Employees need to be trained to work effectively with AI systems. A study by Gartner found that 56% of organizations cite lack of skills as a top barrier to AI implementation [12]. SMBs must invest in comprehensive training programs and change management initiatives to ensure smooth adoption and maximize the benefits of AI-driven compliance solutions.

To address these cost challenges, SMBs might consider phased implementation approaches, cloud-based solutions that offer more flexible pricing models, or partnerships with AI service providers that can provide cost-effective solutions tailored to SMB needs.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.524

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753; p-ISSN: 2347-6710|

Volume 13, Issue 8, August 2024

|DOI: 10.15680/IJIRSET.2024.1308012|

6.2 Data Privacy and Ethics

As AI becomes more integral to compliance processes, businesses must address several critical ethical and privacy considerations:

- Ethical use of AI in compliance processes: SMBs must ensure that their AI systems are used ethically and not inadvertently introduce biases or unfair practices. This includes regular audits of AI decision-making processes and outcomes to identify and address unintended consequences. For instance, an AI system used for customer risk assessment should be carefully monitored to ensure it doesn't discriminate against certain demographic groups.
- Data protection and privacy concerns: AI systems often require access to large amounts of data to function effectively. SMBs must implement robust data protection measures to safeguard sensitive customer information and ensure compliance with data privacy regulations such as GDPR or CCPA. This includes implementing strong encryption, access controls, and data minimization practices.
- Transparency in AI-driven decision-making: As AI systems take on more significant roles in compliance processes, there's a growing need for transparency in how these systems make decisions. SMBs should be prepared to explain the logic behind AI-driven compliance decisions to regulators, customers, and other stakeholders. This may involve developing interpretable AI models or implementing systems that clearly explain their decisions.

For example, if an AI system flags a transaction as potentially fraudulent, the SMB should be able to explain the factors that led to this decision, both to comply with regulatory requirements and to maintain customer trust.

To address these challenges, SMBs can consider implementing AI governance frameworks that outline clear policies for the ethical use of AI, data protection, and transparency. They might also explore technologies like federated learning or differential privacy that can enhance data protection while allowing effective AI model training.

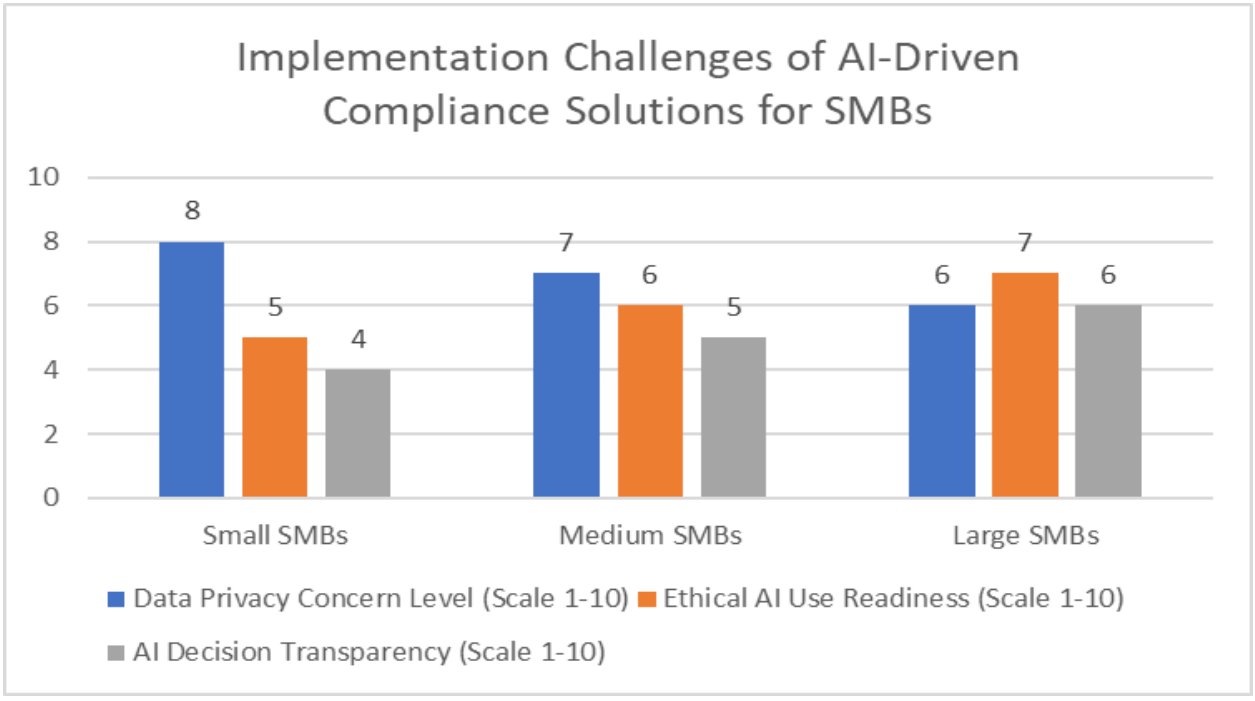

Fig. 2: Cost and Ethical Considerations in Adopting AI Compliance Systems by SMB Size [11, 12]

VII. CONCLUSION

Integrating generative AI in regulatory compliance offers SMBs in the digital payments sector a powerful tool to address the challenges of an increasingly complex regulatory environment. By automating compliance tasks, enhancing risk mitigation strategies, and fostering trust and credibility, AI-driven solutions can significantly improve the efficiency and effectiveness of compliance efforts. However, SMBs must carefully consider the implementation costs,

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.524

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753; p-ISSN: 2347-6710|

Volume 13, Issue 8, August 2024

|DOI: 10.15680/IJIRSET.2024.1308012|

data privacy issues, and ethical implications of adopting these technologies. As the digital payments landscape evolves, those SMBs that successfully leverage AI for compliance will be better positioned to thrive in a competitive market, meet regulatory requirements, and build stronger relationships with stakeholders. While challenges remain, the potential benefits of AI in regulatory compliance make it a critical consideration for SMBs looking to future-proof their operations in the digital payments ecosystem.

REFERENCES

[1] Statista, "Number of digital payments worldwide from 2020 to 2025," 2023. [Online]. Available: https://www.statista.com/statistics/1231176/digital-payments-worldwide/. [Accessed: 25-Jul-2024].
[2] Thomson Reuters, "Cost of Compliance 2021: Shaping the Future," 2021. [Online]. Available: https://legal.thomsonreuters.com/en/insights/reports/cost-of-compliance-2021. [Accessed: 25-Jul-2024].
[3] Juniper Research, "AI in Financial Services: Predictive Analytics, Fraud Detection & Claims Automation 2024-2029," 2024. [Online]. Available: https://www.juniperresearch.com/researchstore/fintech-payments/ai-in-fintech-research-report. [Accessed: 25-Jul-2024].
[4] Thomson Reuters, "Fintech, Regtech and the Role of Compliance in 2023," 2023. [Online]. Available: https://legal.thomsonreuters.com/en/insights/reports/fintech-regtech-compliance-report-2023. [Accessed: 25-Jul-2024].
[5] K. Kalyanakrishnan et al., "Synthetic Data for Machine Learning: A Practitioner's Guide," MIT Sloan Management Review, 2022. [Online]. Available: https://sloanreview.mit.edu/article/synthetic-data-for-machine-learning-a-practitioners-guide/. [Accessed: 25-Jul-2024].
[6] Gartner, "Gartner Predicts 60% of Data Used for AI and Analytics Projects Will Be Synthetically Generated," 2022. [Online]. Available: https://www.gartner.com/en/newsroom/press-releases/2022-06-22-gartner-predicts-60-percent-of-data-used-for-ai-and-analytics-projects-will-be-synthetically-generated. [Accessed: 25-Jul-2024].
[7] Accenture, "Compliance at a Crossroads: One Step Forward, Two Steps Back?" 2023. [Online]. Available: https://www.accenture.com/us-en/insights/banking/compliance-crossroads. [Accessed: 25-Jul-2024].
[8] J. Mauro et al., "AI in Law and Legal Practice - A Comprehensive View of 35 Current Applications," Emerj, 2023. [Online]. Available: https://emerj.com/ai-sector-overviews/ai-in-law-legal-practice-current-applications/. [Accessed: 25-Jul-2024].
[9] McKinsey & Company, "AI-bank of the future: Can banks meet the AI challenge?," 2023. [Online]. Available: https://www.mckinsey.com/industries/financial-services/our-insights/ai-bank-of-the-future-can-banks-meet-the-ai-challenge. [Accessed: 25-Jul-2024].
[10] PwC, "Consumer Intelligence Series: Protect.me," 2023. [Online]. Available: https://www.pwc.com/us/en/services/consulting/library/consumer-intelligence-series/cybersecurity-protect-me.html. [Accessed: 25-Jul-2024].
[11] Deloitte, "State of AI in the Enterprise, 4th Edition," 2023. [Online]. Available: https://www2.deloitte.com/us/en/insights/focus/cognitive-technologies/state-of-ai-and-intelligent-automation-in-business-survey.html. [Accessed: 25-Jul-2024].
[12] Gartner, "Gartner Survey Shows 37 Percent of Organizations Have Implemented AI in Some Form," 2023. [Online]. Available: https://www.gartner.com/en/newsroom/press-releases/2023-07-20-gartner-survey-shows-37-percent-of-organizations-have-implemented-ai. [Accessed: 25-Jul-2024].

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details