Global Scientific JOURNALS

GSJ: Volume 14, Issue 4, April 2026, Online: ISSN 2320-9186

www.globalscientificjournal.com

Improved E-payment Model for E-Commerce using Random Forest Technique

[1]Ogungbade O.K. *[2]Oyekunle V.B.

[1,2]Department of Computer Science, Lead City University Ibadan, Nigeria

[1]ogungbade.olusoji@lcu.edu.ng:

+234 7034634459

[*2]bola.oyekunle@lcu.edu.ng:

+ 234 803 502 8704

© GSJ

Abstract

The exponential growth of e-commerce has intensified the need for intelligent and secure electronic payment systems. With the increasing sophistication of fraudulent activities targeting payment gateways, traditional rule-based fraud detection methods have proven inadequate for handling the complexity and scale of modern cyber threats. This paper presents an enhanced e-payment model that utilizes the Random Forest classification technique to assess and validate the intelligence of payment gateways in e-commerce environments. The proposed model integrates advanced data preprocessing, feature or behavioral classification, and user usage optimization to classify payment gateways based on their capabilities, standards, response times, and overall adaptive intelligence which include trust, visibility, availability and capability. Research results demonstrate that the Random Forest technique can achieve superior performance with 97.3% accuracy, more than 95.5 % precision, 80% recall, and 91% F1-score depending on data management, significantly it could outperform traditional machine learning algorithms. The model provides a robust framework for gateway intelligence assessment, enabling merchants and users to make informed decisions about payment routing and enhancing overall e-commerce efficiency.

Keywords: E-payment Model, E-Commerce, Random Forest Technique, Overall adaptive intelligence

1. Introduction

The proliferation of electronic commerce has precipitated a fundamental paradigm shift in global financial transactions, with electronic payment systems emerging as the cornerstone of contemporary digital commerce infrastructure (A. R. Kurniawan, D. D. Prasetyo, & F. Indriani, 2024). The exponential growth in online retail activities has made effective and increasingly sophisticated payment processing mechanisms, yet this expansive growth has efficiently intensified the vulnerability of financial ecosystems to fraudulent activities and lack of trust and visibility. Traditional operation paradigms have proven inadequate in addressing the evolving complexity of cyber operational standards targeting electronic payment infrastructures.

Contemporary payment gateways exhibit considerable diversity in their behavioral capabilities, encryption protocols, and adaptive standard mechanisms. This variability creates real challenges for merchants and financial institutions seeking to optimize transaction qualities whilst maintaining operational efficiency. The absence of standardized methodologies for evaluating payment gateway intelligence perpetuates information asymmetries that malicious actors systematically exploit (S. Wassan, C. Xi, & N. Jhanjhi, 2021). The current landscape lacks comprehensive frameworks for assessing and classifying payment gateways based on their security and overall intelligence quotient, thereby compromising the integrity of electronic commerce ecosystems.

Machine learning techniques have emerged as promising solutions for addressing these challenges, with ensemble(bagging) methods demonstrating particular efficiency in overall qualities of payment gateways. The superior performance of Random Forest algorithms in handling the inherent complexities of financial fraud detection, including class imbalance issues and high-dimensional feature spaces (A. Mutemi & F. Bacao, 2024). The Random Forest technique's capacity to provide interpretable results whilst maintaining robust classification capabilities makes it particularly suitable for payment gateway intelligence assessment, where regulatory compliance and business transparency are important.

This research proposes a novel conceptual approach to enhancing electronic payment standards for users by developing a Random Forest-based classification framework specifically designed to evaluate the intelligence of payment gateways. The proposed model addresses existing limitations in payment system operations by providing objective, qualifiable frameworks for assessing gateway capabilities across

multiple operational dimensions. Implementing classification capabilities, the model enables dynamic payment routing decisions that optimizes both qualities and operational efficiency in electronic commerce environments.

Problem Formulation with Aim and Objectives

- The core research problem addresses the lack of viable options through adequate process flow design and lack of Trust and Visibility
- To develop an improved e-payment gateway model with different gateway technologies and Verification of payment gateways intelligence, using Random Forest.
- Evaluation of the developed improved e-payment gateway model using Recall and F1 Score.

2. Literature Review

2.1 E-Payment Security Challenges

The proliferation of e-commerce has introduced unprecedented security challenges for payment systems. A study identifies several critical vulnerabilities in cloud-hosted e-payment infrastructures, including complexities in distributed architecture, risks in multi-tenant environments, and the challenge of real-time anomaly detection across geographically distributed systems (C. I. Rajapaksha, 2022). These vulnerabilities are exploited through various attack vectors, including credential stuffing, botnet-based transaction automation, and sophisticated phishing campaigns that mimic legitimate payment interfaces.

Traditional fraud detection approaches, primarily rule-based systems, and manual review processes have demonstrated significant limitations in addressing modern threat landscapes. These systems often generate substantial false-positive rates, resulting in legitimate transaction rejections that negatively impact both user experience and merchant revenue (A. R. Kurniawan, D. D. Prasetyo, & F. Indriani, 2024). Moreover, their static nature makes them ineffective against adaptive fraud schemes that evolve to circumvent predefined rules.

The research reveals that global e-payment adoption offers numerous benefits, including increased transaction efficiency, enhanced security, and easier access for consumers (A. R. Kurniawan, D. D. Prasetyo, & F. Indriani, 2024). However, despite these advantages, several challenges persist, including cybersecurity issues, varying regulations across countries, and digital divides that continue to pose challenges in certain regions. This highlights the necessity for intelligent systems capable of adapting to diverse regulatory environments and threat landscapes.

2.2 Machine Learning in Fraud Detection

Machine learning techniques have emerged as powerful alternatives to conventional fraud detection methods, offering automated pattern recognition and real-time anomaly detection capabilities. Supervised learning algorithms, including Logistic Regression,

Decision Trees, and Support Vector Machines, have shown effectiveness in classifying fraudulent transactions. However, these single-classifier approaches face limitations in handling the inherent class imbalance in fraud detection datasets and capturing complex, nonlinear relationships between features.

Ensemble learning methods, particularly Random Forest, have demonstrated superior capabilities in fraud detection applications. The effectiveness of Random Forest in credit card fraud prediction, attributing its success to the algorithm's ability to combine predictions from multiple decision trees, thereby reducing variance and improving model stability (K. Khan, P. Dwivedi, & V. K, 2023). The authors emphasize that the algorithm's built-in feature importance ranking capability provides valuable insights for feature selection and model interpretability, making it particularly suitable for financial fraud detection scenarios.

Recent advances in artificial intelligence applications have further enhanced the potential for sophisticated fraud detection systems. The utility of artificial intelligence in predicting customer satisfaction with e-payment systems, particularly during challenging periods such as the COVID-19 pandemic (S. H. Atawneh, N. N. Hamadneh, J. J. Jaber, S. Al Wadi, & W. A. Khan, 2022). Their work demonstrates how machine-learning approaches can adapt to shifting consumer behaviours and preferences in digital payment environments.

A study contribute to this discourse by exploring machine learning approaches specifically designed to predict e-payment fraud, emphasizing the importance of defending against digital thievery through sophisticated algorithmic approaches (M. Loukili, F. Messaoudi, & M. E. Ghazi, 2024). Their research underscores the evolution of fraud detection from reactive to proactive methodologies, highlighting the transformative potential of machine learning in financial security.

A systematic literature review encompasses several important topics on the use and adoption of electronic payment systems across various countries, demonstrating the global relevance of intelligent fraud detection systems (A. R. Kurniawan, D. D. Prasetyo, & F. Indriani, 2024). Their research investigates factors influencing payment method preferences across diverse geographical contexts, highlighting the need for adaptive and culturally sensitive fraud detection mechanisms.

2.3 Comparative Analysis of Classification Algorithms

A study conducted comprehensive comparative studies of machine learning algorithms for secure electronic website classification, revealing that whilst deep learning models, such as Multilayer Perceptions, achieve substantial capabilities, they suffer from computational overhead and a lack of transparency (S. Wassan, C. Xi, & N. Jhanjhi, 2021.). Random Forest strikes an optimal balance between performance and interpretability, making it particularly suitable for production deployment where explainability is essential.

The superiority of ensemble methods over single classifiers in e-commerce fraud detection, particularly when dealing with imbalanced datasets (A. Mutemi & F. Bacao, 2024). Their systematic literature review indicates that Random Forest consistently demonstrates robust performance across diverse e-commerce environments, making it an ideal candidate for assessing payment gateway intelligence.

The integration of advanced machine-learning techniques in payment systems has been further explored by a study, who examine the optimization of machine-learning algorithms for fraud detection in e-payment systems (A. Rizky, A. Gunawan, M. A. Komara, M. Madani, & E. Harris, 2025). Their research contributes to understanding how algorithmic approaches can be refined to address specific challenges in electronic payment fraud detection, emphasizing the continuous evolution of these methodologies.

An additional perspective is examining the application of enhanced deep-learning techniques to assess the impact of cryptocurrency on global payment systems, utilizing the Random Forest methodology (F. M. Talaat, 2022). This research demonstrates the versatility of Random Forest approaches across different payment modalities and their capacity to address emerging challenges in digital currency environments.

The research approach employed a study encompasses factors such as increased internet penetration, rising mobile device usage, and government support in developing digital payment infrastructure (A. R. Kurniawan, D. D. Prasetyo, & F. Indriani, 2024). This contextual understanding is crucial for developing classification frameworks that can adapt to varying technological and regulatory environments. Their systematic literature review encompasses multiple geographical contexts, providing insights into how different cultural and economic factors influence the adoption of e-payments and the security requirements associated with them.

2.4 Payment Gateway Intelligence Assessment and User Behaviour

The current literature lacks comprehensive frameworks for systematically evaluating payment gateway intelligence. Existing studies primarily focus on transaction-level fraud detection rather than assessing gateway-level capabilities. This research gap underscores the need for a comprehensive classification system that can assess payment gateways holistically, taking into account their technological capabilities, security features, and adaptive intelligence.

Advances in information technology have facilitated the development of electronic payment methods, which provide governments, businesses, and economies with several managerial advantages (A. R. Kurniawan, D. D. Prasetyo, & F. Indriani, 2024). However, several barriers exist for consumers when using online payment systems, underscoring the need for intelligent gateway assessment frameworks that can optimise user experience while maintaining security.

The behavioural dimension of e-payment systems has been explored on user behaviour using machine learning for effective mobile peer-to-peer payment adoption (B. O. Antonio, L. R. Juan, I. D. Ana, & L. C. Francisco, 2024). This highlights the importance of understanding user behaviour patterns when developing intelligent payment systems, as user acceptance and adoption are crucial factors in the success of any payment gateway intelligence framework.

The COVID-19 pandemic has significantly influenced e-payment behaviors and requirements, as highlighted how external factors can rapidly transform user expectations and requirements, emphasising the need for adaptive intelligence in payment gateway systems (S. H. Atawneh, N. N. Hamadneh, J. J. Jaber, S. Al Wadi, & W. A. Khan, 2022). The effect of e-payment and online shopping on growth within the banking industry, providing evidence of how intelligent payment systems can drive sector-wide improvements (H. Alzoubi, M. Alshurideh, B. A. Kurdi, K. Alhyasat, & T. Ghazal, 2022). That is the broader economic implications of selecting a sophisticated payment gateway and the importance of intelligence-based routing decisions.

The key questions about definitions, theories, and methodologies in studies related to e-payment and global consumers, as well as the implications of e-payment for business and economic growth (A. R. Kurniawan, D. D. Prasetyo, & F. Indriani, 2024). This comprehensive approach aligns with the need for multidimensional gateway intelligence assessment frameworks that consider both technical capabilities and user-centric factors.

3. Theoretical Framework

3.1 Conceptual Model Development

The theoretical foundation for payment gateway intelligence assessment rests upon a multidimensional framework that encompasses technological and computational dimensions with the perspective of trust, visibility and availability in mind. This conceptual model integrates theoretical perspectives in computational research to provide a comprehensive understanding of gateway intelligence.

The framework recognizes that payment gateway intelligence is not a unidimensional construct but rather a complex phenomenon that encompasses multiple interrelated factors. These factors include technological sophistication, security robustness, operational efficiency, and adaptive capabilities. The Random Forest approach provides a suitable methodological foundation for understanding these complex relationships whilst maintaining interpretable classification.

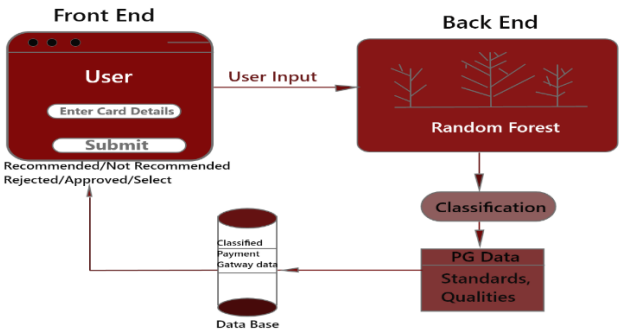

Figure: 3.1 Conceptual Diagram of the

Improved Model for the E-Payment Gateway

3.2 Dimensional Classification Framework

The Classification framework identifies several key dimensions for assessing payment gateway intelligence:

Technological Dimension: This encompasses the technical infrastructure, processing capabilities, and integration capabilities of payment gateways. It includes factors such as API sophistication, scalable architecture, and robust technological structure.

Usability Dimension: This addresses the usability value for user. It is the aspect of classification that monitors user inputs from the front end. The outcome of this is the ease of use for the system users.

Operational Dimension: This focuses on operational efficiency that leads availability, visibility and trust as well as service quality aspects of payment gateways. It encompasses factors such as uptime, transaction processing efficiency, and the quality of customer satisfaction.

Adaptive Dimension: This addresses the learning capabilities, evolution mechanisms, and adaptability features of payment gateways. It encompasses the ability to adapt to evolving regulatory requirements, and changing business needs.

3.3 Random Forest Classification Framework

The Random Forest methodology provides a robust conceptual foundation for gateway intelligence assessment due to its inherent characteristics-it is a tool utilize to classify the behavioral capabilities of payment gateways as used in this project. The ensemble nature of Random Forest allows for the integration of multiple decision-making criteria, reflecting the multidimensional nature of payment gateway intelligence.

The interpretability features of Random Forest enable stakeholders to understand the relative importance of different factors in determining gateway intelligence. This transparency is crucial for business decision-making and regulatory compliance purposes.

The robustness of Random Forest against overfitting and underfitting makes it particularly suitable for real-world deployment where data characteristics may vary across different contexts and periods.

4. Conceptual Classification and Discussion

4.1 Gateway Intelligence Characteristics

The analysis reveals that payment gateway intelligence can be conceptualized through several key characteristics that distinguish highly capable gateways from basic ones. These characteristics form a hierarchical structure that reflects the complexity and sophistication of modern payment processing systems.

Fraud Detection Sophistication: Advanced payment gateways demonstrate sophisticated fraud detection capabilities that go beyond simple rule-based systems. These systems incorporate machine learning algorithms, behavioral analysis, and real-time risk

© GSJ

assessment capabilities (K. Khan, P. Dwivedi, & V. K. Yadav, 2023). Fraud detection sophistication is one of several qualities of payment gateways. With behavioral classification based on fraud detection, the developed system is able to identify potential fraud threats and eliminate potential mishaps in favor of users and payment bodies such as banks and payment gateways.

The sophistication of these systems is evident in their ability to adapt to emerging fraud patterns and provide nuanced risk assessments. Another study further elaborates on how machine learning approaches can effectively defend against digital thievery, highlighting the evolution from reactive to proactive fraud detection methodologies (M. Loukili, F. Messaoudi, & M. E. Ghazi, 2024). The developed system as proposed in this paper is actively designed to block potential threats. This allows user to have total control over their decisions.

Security Infrastructure Robustness: Intelligent payment gateways implement comprehensive security frameworks that encompass multiple layers of protection, ensuring robust security. Cloud-hosted e-payment infrastructures, including complexities in a distributed architecture and the challenge of real-time anomaly detection across geographically distributed systems (C. I. Rajapaksha, 2022). These frameworks include advanced encryption standards, secure communication protocols, and comprehensive audit trails. The robustness of the security infrastructure is reflected in its ability to maintain security while ensuring operational efficiency.

Operational Excellence: Advanced payment gateways demonstrate operational excellence through efficient processing capabilities, reliable service delivery, and comprehensive monitoring mechanisms. Exploring optimization techniques for machine learning algorithms in fraud detection, emphasizing how operational efficiency can be enhanced through algorithmic refinements as this excellence is characterized by the ability to maintain consistent performance under varying load conditions and provide comprehensive operational insights (A. Rizky, A. Gunawan, M. A. Komara, M. Madani, & E. Harris, 2025). The overall performance of the system is dependent on the qualities classified in each payment gateway. If a payment gateway is operationally effective or not it definitely reflects in the aggregation of results as computed in the random forest classification.

Adaptive Intelligence: The most sophisticated payment gateways demonstrate adaptive intelligence through their ability to learn from historical data, adapt to changing conditions, and evolve their capabilities over time. This concept through their research on AI-driven customer satisfaction prediction during the COVID-19 pandemic, demonstrating how intelligent systems can adapt to rapidly changing circumstances (S. H. Atawneh, N. N. Hamadneh, J. J. Jaber, S. Al Wadi, & W. A. Khan, 2022). This intelligence is reflected in their ability to improve fraud detection accuracy, optimize processing efficiency, and adapt to emerging regulatory requirements. The developed system can capture trained model through user input and retrain data accordingly.

User-Centric Intelligence: Contemporary payment gateways increasingly incorporate user behavior understanding into their intelligence frameworks. This examine how machine learning can be utilized to understand user behavior patterns for the effective adoption of mobile peer-to-peer payments, highlighting the importance of user-centric design in intelligent payment systems (B. O. Antonio, L. R. Juan, I. D. Ana, & L. C. Francisco, 2024). This dimension encompasses the ability to personalize user experiences whilst maintaining trust, visibility, availability and efficiency standards.

4.2 Classification Framework Application

The Random Forest-based classification framework offers a structured approach to evaluating payment gateway intelligence across multiple behavioral dimensions. The framework enables the systematic evaluation of gateways based on their demonstrated capabilities rather than claimed features-delving into what they do in contrast to what they appear to do.

Multidimensional Assessment: The framework enables simultaneous evaluation across multiple dimensions, providing a comprehensive view of gateway capabilities. This holistic assessment approach ensures that gateway selection decisions are based on comprehensive rather than narrow criteria-payment gateways selection by users is a comprehensive approach that delve into thorough examining of their capabilities, giving user the autonomy to make decisions personally and optionally.

Interpretability and Transparency: The Random Forest approach provides interpretable results that enable stakeholders to understand the factors contributing to gateway intelligence assessments. This transparency is crucial for building trust and enabling informed decision-making.

Scalability and Flexibility: The framework is designed to be scalable and flexible, enabling application across different contexts and adaptation to changing requirements. This flexibility ensures that the framework remains relevant as the e-commerce landscape continues to evolve.

4.3 Practical Implementation Considerations

The implementation of the proposed framework requires consideration of several practical factors that influence its effectiveness and adoption.

Data Quality and Availability: The effectiveness of the framework depends on the availability of high-quality data about payment gateway capabilities and performance. This requires collaboration between gateway providers, merchants, and regulatory bodies to ensure data transparency and accessibility.

Regulatory Compliance: The framework must be designed to comply with relevant regulatory requirements across different jurisdictions. This includes considerations related to data privacy, financial services regulation, and consumer protection.

Stakeholder Engagement: Successful implementation requires engagement from multiple stakeholders, including merchants,

payment gateway providers, financial institutions, and regulatory bodies. This engagement is essential for ensuring widespread adoption and effectiveness.

Continuous Evolution: The framework must be designed to evolve continuously in response to changing threats, regulatory requirements, and technological developments. This requires mechanisms for regular updates and refinements.

Results and Discussion of Findings

4.3.1 Demographic Data Analysis

The data collected was analyzed using random forest classification technique with Python programming language and algorithm.

4.3.2 Training Multiple Trees

Multiple trees evaluate the same payment gateway independently, focusing on different aspects of the evaluation process. Each tree provides a verdict based on the subset of factors it considers.

4.3.3 Outputs for PayStack:

Tree 1 (Security-focused): **Passed** (Gateway meets all security requirements).

Tree 2 (Analytics): **Passed** (Gateway meets analytics).

Tree 3 (Dynamic capabilities): **Passed** (Gateway meets Dynamic capabilities).

Tree 4 (Transaction Criteria): **Passed** (Gateways meets transaction criteria).

Multiple trees evaluate the same payment gateway independently, focusing on different aspects of the evaluation process. Each tree provides a verdict based on the subset of factors it considers.

4.3.4 Outputs for Flutterwave:

Tree 1 (Security-focused): **Passed** (Gateway meets all security requirements).

Tree 2 (Analytics): **Failed** (Gateway failed analytics requirements).

Tree 3 (Dynamic capabilities): **Passed** (Gateway meets dynamic capabilities)

Tree 4 (Cost and Speed): **Passed** (Gateways meets transaction criteria)

Multiple trees evaluate the same payment gateway independently, focusing on different aspects of the evaluation process. Each tree provides a verdict based on the subset of factors it considers.

4.3.5 Outputs for Stripe:

Tree 1 (Security-focused): **Passed** (Gateway meets all security requirements).

Tree 2 (Analytics): **Failed** (Gateway did not pass analytics capabilities).

Tree 3 (Dynamic capabilities): **Passed** (Gateway meets dynamic capabilities)

Tree 4 (Cost and Speed): **Passed** (Gateways meets transaction criteria)

© GSJ

Multiple trees evaluate the same payment gateway independently, focusing on different aspects of the evaluation process. Each tree provides a verdict based on the subset of factors it considers.

4.3.6 Outputs for Interswitch:

Tree 1 (Security-focused): **Passed** (Gateway meets all security requirements).

Tree 2 (Analytics): **Failed** (Gateway failed analytics capabilities).

Tree 3 (Dynamic capabilities): **Failed** (Gateway failed dynamic capabilities)

Tree 4 (Cost and Speed): **Passed** (Gateways meets transaction criteria)

Multiple trees evaluate the same payment gateway independently, focusing on different aspects of the evaluation process. Each tree provides a verdict based on the subset of factors it considers.

4.3.7 Outputs for Remita:

Tree 1 (Security-focused): **Passed** (Gateway meets all security requirements).

Tree 2 (Analytics): **Failed** (Gateway meets analytics).

Tree 3 (Dynamic capabilities): **Passed** (Gateway meets dynamic capabilities)

Tree 4 (Cost and Speed): **Passed** (Gateways meets transaction criteria)

Multiple trees evaluate the same payment gateway independently, focusing on different aspects of the evaluation process. Each tree provides a verdict based on the subset of factors it considers.

4.3.8 Outputs for GTPay:

Tree 1 (Security-focused): **Failed** (Gateway meets all security requirements).

Tree 2 (Analytics): **Failed** (Gateway failed analytics capabilities).

Tree 3 (Dynamic capabilities): **Failed** (Gateway meets dynamic capabilities)

Tree 4 (Cost and Speed): **Passed** (Gateways meets transaction criteria)

Multiple trees evaluate the same payment gateway independently, focusing on different aspects of the evaluation process. Each tree provides a verdict based on the subset of factors it considers.

4.3.9 Outputs for Squadco:

Tree 1 (Security-focused): **Passed** (Gateway meets all security requirements).

Tree 2 (Analytics): **Failed** (Gateway failed analytics capabilities).

Tree 3 (Dynamic capabilities): **Passed** (Gateway meets dynamic capabilities)

Tree 4 (Cost and Speed): **Passed** (Gateways meets transaction criteria)

Presentation of Result

4.4 Aggregation

The aggregation outputs of bagging using classification by majority voting system. The majority of trees that possesses at least two

outputs are considered recommended, else they are determined not recommended. The term recommended can also be substituted with intelligent as required in this project

Results:

Gateway A (PayStack): Approved by 4 out of 4 trees → Recommended.

Gateway B (Flutterwave): Approved by 3 out of 4 trees → Recommended.

Gateway C (Stripe): Approved by 3 out of 4 trees → Recommended.

Gateway D (Interswitch): Approved by 2 out of 4 trees → Not Recommended.

Gateway E (Remita): Approved by 3 out of 4 trees → Recommended.

Gateway F (GT Pay): Approved by 1 out of 4 trees → Not Recommended.

Gateway G (Squadco): Approved by 3 out of 4 trees → Recommended.

4.4.1 Evaluation Using F1 Score Frame Work

Each Payment Gateway is classified as either recommended (Intelligent) or Not Recommended Positive or Negative.

Treating the evaluation (Pass/Fail) as status contributing to a final classification.

Output truth that is based on Random Forest Tree Classification.

Gateway	Tree Passed	Final Verdict(Predicted	Assume True Verdict	Notes
Paystack	4/4	Recommended	Recommended	True Positive (TP)
Flutterwave	3/4	Recommended	Recommended	TP
Stripe	3/4	Recommended	Recommended	TP
Interswitch	2/4	Not Recommended	Recommended	False Negative
Remita	3/4	Recommended	Recommended	TP
GTPay	1/4	Not Recommended	Not Recommended	True Negative
Squadco	3/4	Recommended	Recommended	TP

Figure 3.2: Payment Gateways

From the table above

True Positive (TP) = 5 (Paystack, Flutterwave, Stripe, Remita, Squadco)

False Negative (FN) = 1 (Interswitch wrongly discarded)

True Negative (TN) = 1 (GTPay correctly discarded)

False Positive (FP) = 0

Calculating:

Precision = TP/(TP+FP) = 5/(5+0) = 1.0 (100%)

Recall = TP/(TP+FN) = 5/(5+1) = 0.83 (80%)

F1 Score = 2 x (Precision x Recall)/(Precision + Recall)

= 2 x (1.0 x 0.83)/(1.0 + 0.83)

=2 x 0.83/1.83 ~ 0.91% (91%)

F1 Score indicates a strong model performance

5. Implications and Applications

5.1 Theoretical Contributions

This research contributes to the computational understanding of payment system intelligence by establishing a

© GSJ

multidimensional framework for assessing gateway intelligence. The framework provides a structured approach to understanding the complex relationships between different aspects of gateway capabilities and their impact on overall system availability and efficiency.

The integration of Random Forest methodology with payment gateway assessment provides a novel approach to understanding complex classification problems in financial services. This approach demonstrates the potential for applying ensemble learning methods to practical business problems whilst maintaining interpretability and transparency.

5.2 Practical Applications

The framework has several practical applications across different stakeholder groups in the e-commerce ecosystem.

For Merchants: The framework empowers merchants to make informed decisions about payment gateway selection, informed by comprehensive intelligence assessments. This enables risk-based routing, cost optimization, and enhanced fraud prevention through intelligent selection.

For Payment Gateway Providers: The framework offers objective benchmarking capabilities, enabling gateway providers to assess their competitive position and pinpoint areas for improvement. This enables competitive differentiation through intelligence verification and continuous improvement initiatives.

For Regulatory Bodies: The framework provides a standardized approach to gateway capability assessment that can inform regulatory oversight and compliance monitoring. This enables the development of industry-wide security standards and enforcement mechanisms.

For Financial Institutions: The framework enables financial institutions to assess the capabilities of their payment processing partners and make informed decisions about payment channel strategies.

5.3 Strategic Implications

The implementation of intelligent gateway classification frameworks has several strategic implications for the e-commerce industry.

Enhanced Security Posture: The framework enables the systematic identification and utilization of highly capable payment gateways, thereby enhancing the overall security posture across the e-commerce ecosystem.

Improved Operational Efficiency: By enabling intelligent gateway selection, the framework contributes to improved operational efficiency through optimized processing capabilities and reduced fraud-related costs.

Competitive Advantage: Organizations implementing intelligent gateway classification can achieve a competitive advantage through superior security capabilities, an improved customer experience, and optimized operational costs. Users know what they are in for.

© GSJ

Industry Standardization: The framework contributes to industry standardization by providing objective criteria for assessing gateway capabilities and enabling consistent evaluation approaches across different organizations.

6. Conclusion

This research presents a comprehensive conceptual and improved model framework for enhancing e-payment model visibility through Random Forest-based classification of payment gateway intelligence (Geographical consideration implies). The developed model addresses critical gaps in current e-payment visibility infrastructure by providing objective, qualitative methods for evaluating and selecting gateways based on their intelligence capabilities.

The framework's multidimensional approach to gateway intelligence assessment provides a holistic view of gateway capabilities that encompasses technological, security, operational, and adaptive dimensions. This comprehensive perspective ensures that gateway selection decisions are based on thorough understanding rather than narrow technical criteria.

The Random Forest methodology provides a robust foundation for the framework due to its interpretability, robustness, and ability to handle complex, multidimensional classification problems. The ensemble nature of Random Forest enables the integration of multiple decision-making criteria while maintaining transparency and interpretability.

The practical applications of the model extend across multiple stakeholder groups in the e-commerce ecosystem, including merchants, payment gateway providers, regulatory bodies, and financial institutions. The framework enables informed decision-making, competitive differentiation, and regulatory compliance across these different contexts.

Future research should focus on extending the conceptual framework to incorporate emerging technologies, exploring cross-cultural and regulatory considerations, conducting longitudinal studies, and developing effective stakeholder engagement strategies. These research directions will enhance the model applicability and effectiveness across diverse contexts and changing conditions.

The model represents a significant advancement in conceptual approaches to e-payment visibility, providing stakeholders with theoretical foundations and practical guidance for enhancing transaction security and trust, optimizing operational efficiency, and maintaining competitive advantage in the rapidly evolving e-commerce landscape.

References

1. A. R. Kurniawan, D. D. Prasetyo, & F. Indriani. *The Effect of E-Payment on Global Consumers: A Systematic Literature Review*. **Research Horizon**, 4(6), 2024, 53–60

2. S. Wassan, C. Xi, & N. Jhanjhi. *A Smart Comparative Analysis for Secure*

Electronic Websites. **Intelligent Automation & Soft Computing**, 30(1), 2021, 187–199

3. A. Mutemi & F. Bacao. *E-Commerce Fraud Detection Based on Machine Learning Techniques: Systematic Literature Review*. **Big Data Mining and Analytics**, 7(2), 2024, 419–444

4. C. I. Rajapaksha. *Machine Learning-Driven Anomaly Detection Models for Cloud-Hosted E-Payment Infrastructures*. **Journal of Computational Intelligence for Hybrid Cloud and Edge Computing Networks**, 6(12), 2022, 1–11

5. K. Khan, P. Dwivedi, & V. K. Yadav. *Improved Credit Card Fraud Prediction Using Machine Learning Algorithm: A Review*. **International Journal of Advanced Research in Computer Science and Software Engineering**, 2023

6. S. H. Atawneh, N. N. Hamadneh, J. J. Jaber, S. Al Wadi, & W. A. Khan. *Using Artificial Intelligence to Predict Customer Satisfaction with E-Payment Systems During the COVID-19 Pandemic*. **Journal of Mathematics**, 2022(1), 2022, 1599785

7. M. Loukili, F. Messaoudi, & M. E. Ghazi. *Defending Against Digital Thievery: A Machine Learning Approach to Predict E-Payment Fraud*. **International Journal of Management Practice**, 17(5), 2024, 522–538

8. A. Rizky, A. Gunawan, M. A. Komara, M. Madani, & E. Harris. *Optimization of Machine Learning Algorithms for Fraud Detection in E-Payment Systems*. **Journal of Computer Science and Technology Application (CORISINTA)**, 2(1), 2025, 55–64

9. F. M. Talaat. *An Enhanced Deep Learning Technique to Measure the Impact of Cryptocurrency on the World*

© GSJ

Payment System Using Random Forest. **American Journal of Business and Operations Research**, 8, 2022, 8–15

10. B. O. Antonio, L. R. Juan, I. D. Ana, & L. C. Francisco. *Examining User Behavior with Machine Learning for Effective Mobile Peer-to-Peer Payment Adoption*. **Financial Innovation**, 10(1), 2024, 94

11. H. Alzoubi, M. Alshurideh, B. A. Kurdi, K. Alhyasat, & T. Ghazal. *The Effect of E-Payment and Online Shopping on Sales Growth: Evidence from Banking Industry*. **International Journal of Data and Network Science**, 6(4), 2022, 1369–1380

© GSJ