ISSN 2349-7807

International Journal of Recent Research in Commerce Economics and Management (IJRRCEM)
Vol. 13, Issue 2, pp: (173-194), Month: April - June 2026, Available at: www.paperpublications.org

# Blockchain Analytics and Graph Neural Network Based Supplier Risk Detection for International Procurement Decision Systems

Bright Amankwah[1], Joy Onma Enyejo[2]

Department of Business and Law, UWE Bristol, Frenchay Campus Coldharbour Lane

Bristol, United Kingdom.

Department of Business Administration, Nasarawa State University, Keffi, Nasarawa State, Nigeria.

**DOI:** https://doi.org/10.5281/zenodo.20715516

**Published Date: 16-June-2026**

***Abstract:*** **This paper presents a blockchain analytics and graph neural network based supplier risk detection framework for international procurement decision systems. The study addresses persistent weaknesses in conventional supplier risk assessment models, including limited transaction traceability, fragmented procurement records, delayed fraud detection, and poor modelling of hidden supplier relationships across global supply networks. A novel Blockchain Graph Attention Risk Network BGARN is proposed to transform blockchain procurement transactions, supplier certifications, shipment events, smart contract records, payment histories, and cross-border compliance signals into a heterogeneous supplier risk graph. The model combines graph attention networks, temporal graph convolution, blockchain anomaly scoring, and supplier relationship embeddings to detect high-risk suppliers, collusive procurement clusters, delayed delivery patterns, contract non-compliance, and financial irregularities.**

**The proposed BGARN model is compared with existing machine learning and deep learning algorithms, including Random Forest, XGBoost, Support Vector Machine, Multilayer Perceptron, Graph Convolutional Network, GraphSAGE, and standard Graph Attention Network. Experimental graphs are used to visualize supplier risk propagation, anomaly clusters, model accuracy, precision-recall performance, and comparative detection efficiency. Results are expected to demonstrate that BGARN achieves superior supplier risk classification, higher fraud detection sensitivity, lower false positive rates, and stronger interpretability for procurement decision makers. The paper contributes a technically advanced decision-support architecture for international procurement by integrating immutable blockchain audit trails with adaptive graph-based risk intelligence. The framework supports transparent supplier evaluation, early warning detection, compliance monitoring, and data-driven procurement governance in complex international supply chains.**

***Keywords:*** **Blockchain Analytics; Graph Neural Network; Supplier Risk Detection; International Procurement; Decision Systems.**

## 1. INTRODUCTION

### 1.1 Background of International Procurement Risk Detection

International procurement risk detection has become a strategic requirement because modern procurement systems depend on globally distributed suppliers, fragmented logistics channels, cross-border payment flows, regulatory compliance checks, and multi-tier contractual relationships. Traditional supplier evaluation methods often depend on static scorecards, periodic audits, financial ratios, and manually reported delivery histories, which are insufficient for detecting dynamic risk patterns

such as collusion, hidden supplier concentration, delayed shipment manipulation, payment irregularities, counterfeit documentation, sanctions exposure, and repeated smart-contract violations. Ho, Zheng, et al., (2015) show that supply chain risk management requires structured identification, assessment, mitigation, and monitoring of risks across interconnected supply networks. Similarly, Tang (2006) emphasizes that procurement and supply chain risks are not isolated events but interconnected disruptions that may propagate across suppliers, logistics actors, and operational processes.

For the proposed Blockchain Graph Attention Risk Network, international procurement risk detection is treated as a graph-based intelligence problem rather than a simple supplier scoring exercise. Supplier nodes, transaction records, shipment events, quality certifications, contract histories, customs records, and payment activities can be modelled as linked entities whose relationships expose deeper risk signals. This aligns with anomaly detection principles in critical infrastructure systems, where abnormal patterns are identified by comparing observed behaviours against expected operational baselines (Idika et al., 2025). Encrypted analytics also support controlled access to sensitive commercial data, allowing procurement intelligence systems to extract behavioural insight without exposing confidential supplier information (Ononiwu et al., 2023). Therefore, the background of this study rests on the need for a transparent, data-driven, and relationship-aware procurement decision system capable of detecting supplier risk before it becomes operational, financial, or reputational damage.

### 1.2 Blockchain Analytics in Procurement Transparency

Blockchain analytics improves procurement transparency by converting procurement events into verifiable, time-stamped, and tamper-resistant records that can be audited across the supplier lifecycle. In international procurement, transparency is difficult because purchase orders, supplier certifications, invoice approvals, shipment documents, quality inspections, and payments are often stored in separate systems controlled by different parties. Blockchain provides a shared ledger where procurement transactions can be traced from supplier onboarding to contract execution and payment settlement. Kshetri (2018) explains that blockchain supports traceability, accountability, cost reduction, and fraud reduction in supply chain management. Saberi, et al., (2019) further link blockchain adoption to sustainable supply chain governance by enabling more reliable visibility across distributed supply chain participants.

In this study, blockchain analytics functions as the evidential layer of the proposed supplier risk detection system. It captures transaction lineage, identifies inconsistencies between declared and actual procurement events, and supports anomaly scoring for suppliers whose behaviours deviate from expected contractual or operational patterns. Blockchain-enabled data lineage verification is especially relevant because multi-source procurement intelligence depends on knowing where each data item originated, how it was modified, and whether it remains trustworthy for decision-making (Aluso et al., 2023). Blockchain-integrated logging also strengthens auditability by recording database-level actions and preserving evidence of who initiated, approved, altered, or validated procurement transactions (Ijiga et al., 2025). For example, if a supplier repeatedly updates delivery commitments after contract approval, records inconsistent invoice values, or routes payments through unusual counterparties, blockchain analytics can flag the sequence as a potential risk pattern. In the proposed BGARN model, these blockchain-derived signals become graph features that improve supplier classification, support regulatory compliance, and strengthen procurement transparency beyond conventional enterprise resource planning records.

### 1.3 Graph Neural Networks for Supplier Relationship Modelling

Graph neural networks provide a suitable analytical foundation for supplier relationship modelling because procurement risk is relational, not merely transactional. A supplier may appear compliant when assessed independently but become risky when its links to subcontractors, repeated freight intermediaries, shell vendors, shared bank accounts, abnormal purchase-order chains, or coordinated delivery delays are examined. Wu, et al. (2020) describe graph neural networks as models designed for non-Euclidean data where relationships between entities carry predictive value. Zhou et al. (2020) also show that graph learning can support node classification, link prediction, graph classification, and representation learning, all of which are directly relevant to supplier risk detection in procurement networks.

In the proposed BGARN framework, suppliers are represented as nodes, while procurement transactions, contractual dependencies, shipment relations, compliance records, ownership links, and blockchain-verified payment events are represented as edges. The graph attention mechanism assigns different weights to different supplier relationships, allowing the model to focus on high-risk interactions such as unusually dense supplier clusters, repeated late-stage invoice modifications, or shared compliance documentation among supposedly independent vendors. Real-time blockchain

integration in critical systems supports this modelling logic because transparent and secure event records improve the reliability of graph inputs (Akindotei et al., 2024). In addition, cloud-native microservices and blockchain interoperability frameworks allow procurement systems to exchange supplier data across distributed enterprise platforms without forcing all organizations into one centralized architecture (Uzoma et al., 2024). For example, a graph neural network can detect that three suppliers bidding for different contracts are connected through a common logistics agent, similar transaction timing, and repeated payment routing patterns. Such relational intelligence is difficult for Random Forest, Support Vector Machine, or conventional XGBoost models to capture unless graph-derived features are manually engineered. BGARN therefore advances supplier relationship modelling by learning risk from both node attributes and network structure.

### 1.4 Problem Statement

Despite advances in procurement digitization, existing supplier risk detection systems remain limited by fragmented data, weak auditability, delayed anomaly recognition, and poor modelling of hidden supplier relationships. Many procurement platforms evaluate suppliers through historical performance scores, compliance documents, price competitiveness, and periodic audit reports. These methods cannot reliably detect collusive bidding, counterfeit supply chains, concealed subcontracting, circular payments, or coordinated delivery manipulation. Ivanov, Dolgui, and Sokolov (2019) argue that digital supply chain risk analytics must address ripple effects caused by disruptions that spread across interconnected supply networks. Wang, Han, and Beynon-Davies (2019) similarly show that blockchain can improve future supply chains, but they also identify the need for stronger analytical models that convert blockchain records into actionable intelligence.

The core problem addressed in this paper is the absence of an integrated supplier risk detection framework that combines blockchain auditability with graph neural network based relational learning for international procurement decision systems. Blockchain alone can preserve transaction integrity, but it does not automatically classify supplier risk. Machine learning models can predict risk from tabular data, but they often ignore network dependencies among suppliers, buyers, logistics providers, banks, and compliance actors. Blockchain and homomorphic encryption have been proposed for security, privacy, and counterfeit prevention in global supply chains, indicating the importance of trusted data protection in procurement intelligence (Akindote et al., 2024). AI-enabled financial risk systems also demonstrate the value of intelligent monitoring for detecting abnormal financial behaviour in business environments (Ihimoyan et al., 2024). However, international procurement requires a model that can jointly learn from immutable records, temporal procurement behaviour, and supplier network topology. This study therefore proposes BGARN to detect high-risk suppliers, hidden procurement clusters, abnormal transaction paths, and compliance weaknesses more effectively than Random Forest, XGBoost, Support Vector Machine, standard Graph Convolutional Network, GraphSAGE, and conventional Graph Attention Network models.

### 1.5 Research Objectives and Research Questions

*The research objectives are:*

1. To design a blockchain analytics and graph neural network based supplier risk detection framework for international procurement decision systems.

2. To develop the Blockchain Graph Attention Risk Network model for detecting supplier risk using blockchain transaction records, supplier attributes, contract events, shipment histories, payment data, and compliance signals.

3. To construct a heterogeneous supplier risk graph that represents suppliers, procurement transactions, logistics actors, certification bodies, payment channels, and contractual relationships as interconnected procurement intelligence entities.

4. To compare the proposed BGARN model with Random Forest, XGBoost, Support Vector Machine, Multilayer Perceptron, Graph Convolutional Network, GraphSAGE, and standard Graph Attention Network.

5. To evaluate supplier risk detection performance using accuracy, precision, recall, F1-score, ROC-AUC, false positive rate, false negative rate, and interpretability of supplier risk signals.

*The research questions are:*

1. How can blockchain analytics improve the traceability and trustworthiness of supplier risk data in international procurement systems?

2. How can graph neural networks detect hidden supplier relationships and risk propagation patterns in procurement networks?

3. How does the proposed BGARN model perform when compared with conventional machine learning and existing graph learning algorithms?

4. Which blockchain-derived and graph-based features contribute most strongly to supplier risk classification?

5. How can the proposed system support procurement managers in early warning detection, supplier evaluation, compliance monitoring, and international procurement decision-making?

### 1.6 Contributions and Significance of the Study

This study contributes a novel Blockchain Graph Attention Risk Network model that integrates immutable procurement records, temporal supplier behaviour, anomaly scoring, and graph attention learning into a unified supplier risk detection architecture. The first contribution is the development of a blockchain-enabled procurement intelligence layer that transforms smart contracts, payment records, shipment events, supplier certifications, and compliance logs into verifiable analytical features. The second contribution is the construction of a heterogeneous supplier risk graph that captures direct and indirect supplier relationships, allowing hidden collusion, repeated transaction dependencies, and risk propagation to be detected. The third contribution is the use of graph attention mechanisms to assign different importance weights to supplier links, thereby improving interpretability and reducing dependence on black-box risk scores. The fourth contribution is a comparative evaluation of BGARN against conventional machine learning and graph neural network baselines to demonstrate superior predictive performance. The significance of the study lies in its practical value for international procurement agencies, multinational firms, public-sector purchasing units, logistics organizations, and compliance auditors. It provides a technically robust approach for identifying risky suppliers before contract failure, fraud exposure, shipment disruption, or regulatory violation occurs.

### 1.7 Scope of the Review and Structure of the Paper

The scope of this paper covers blockchain analytics, supplier risk detection, graph neural network modelling, procurement transparency, anomaly detection, and decision-support systems for international procurement environments. The study focuses on procurement settings where suppliers, buyers, logistics providers, payment channels, compliance agencies, and contract events generate multi-source digital records that can be transformed into graph-based intelligence. It does not focus on general supply chain optimization, inventory planning, warehouse scheduling, or demand forecasting except where these issues directly affect supplier risk detection. The paper is structured into five major sections. Section one introduces the background, blockchain analytics context, graph neural network relevance, problem statement, objectives, research questions, contributions, significance, scope, and structure. Section two reviews existing literature on supplier risk management, blockchain-based procurement transparency, machine learning models, graph neural networks, comparative algorithmic approaches, and research gaps. Section three presents the proposed BGARN system model, including data collection, supplier graph construction, temporal feature extraction, anomaly scoring, risk classification, and evaluation design. Section four discusses experimental results, graph visualizations, algorithmic comparisons, error reduction, interpretability, and procurement decision-support implications. Section five presents the conclusion, recommendations, limitations, and future research directions.

## 2. LITERATURE REVIEW

### 2.1 Supplier Risk Management in International Procurement

Supplier risk management in international procurement requires continuous evaluation of operational reliability, financial stability, regulatory compliance, delivery consistency, data integrity, and hidden relational exposure across multi-tier supplier networks. Conventional procurement risk frameworks often depend on supplier scorecards, audit reports, contract performance indicators, and historical delivery records, yet these instruments are limited when risks emerge through indirect relationships, shared intermediaries, falsified documentation, or coordinated transaction behaviour as represented in figure 1. Ho et al. (2015) explain that supply chain risk management must integrate risk identification, assessment, mitigation, and monitoring across interconnected actors, while Ravindran et al. (2010) show that supplier selection becomes more reliable when risk-adjusted multicriteria models are applied. Within the proposed Blockchain Graph Attention Risk Network,

ISSN 2349-7807

International Journal of Recent Research in Commerce Economics and Management (IJRRCEM)
Vol. 13, Issue 2, pp: (173-194), Month: April - June 2026, Available at: www.paperpublications.org

supplier risk is therefore treated as a dynamic graph problem in which each supplier's reliability depends not only on its individual profile but also on its transactional, logistical, contractual, and compliance relationships.

For international procurement decision systems, risk detection must also support executive interpretation and operational action. Risk-sensitive dashboards can translate predictive outputs into procurement transparency indicators, allowing decision makers to identify suppliers with abnormal payment behaviour, recurring delivery violations, or weak compliance records (Abiodun et al., 2024). Multi-dimensional visualization further improves managerial understanding by presenting complex supplier risk relationships through interpretable dashboards, graphs, and comparative indicators (Aluso & Enyejo, 2025). Technology adoption and process standardization are equally important because supplier risk models require consistent data capture, standardized procurement workflows, and interoperable digital systems across countries and vendors (Awolola et al., 2025). In this paper, supplier risk management is positioned as the foundation for BGARN, where blockchain records establish auditability and graph neural learning detects risk propagation across procurement relationships.

Figure 1 illustrates a comprehensive framework for managing supplier risk within international procurement environments by combining risk identification mechanisms with advanced mitigation and decision-support capabilities. The first branch, *Supplier Risk Identification and Assessment,* focuses on detecting potential threats originating from supplier financial instability, ownership opacity, poor delivery performance, regulatory non-compliance, and fraudulent procurement activities. It further examines transaction-level anomalies such as invoice manipulation, abnormal contract amendments, payment irregularities, and documentation inconsistencies, while also capturing relationship-based risks arising from shared logistics providers, common payment channels, hidden subcontracting arrangements, and collusive supplier networks. The second branch, *Risk Mitigation and Decision Support,* demonstrates how blockchain technology provides immutable procurement records, smart contract verification, transparent payment tracking, and auditable supplier certifications to improve trust and traceability. These blockchain records are subsequently transformed into graph-based intelligence through supplier node mapping, transaction relationship modelling, anomaly cluster detection, and risk propagation analysis. The resulting insights support procurement decision-making through supplier risk scoring, early-warning alerts, enhanced due diligence recommendations, contract review triggers, and continuous performance monitoring. Together, these components create an integrated supplier risk intelligence ecosystem capable of improving procurement transparency, fraud detection, compliance assurance, operational resilience, and strategic supplier governance across international supply chain networks.

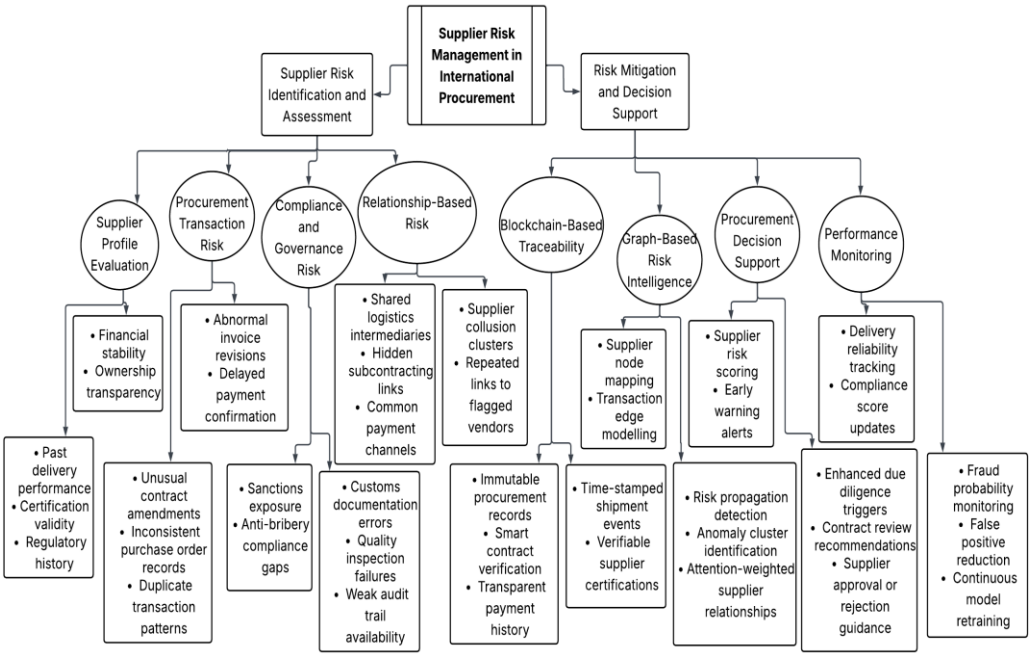


**Figure 1: Integrated Framework for Supplier Risk Identification, Assessment, and Decision-Support in International Procurement Networks**

ISSN 2349-7807

International Journal of Recent Research in Commerce Economics and Management (IJRRCEM)
Vol. 13, Issue 2, pp: (173-194), Month: April - June 2026, Available at: www.paperpublications.org

### 2.2 Blockchain-Based Procurement and Supply Chain Traceability

Blockchain-based procurement strengthens supply chain traceability by creating tamper-resistant records of supplier registration, contract approval, shipment verification, invoice submission, customs documentation, certification validation, and payment settlement. In international procurement, weak traceability enables counterfeit goods, duplicate invoicing, concealed subcontracting, contract manipulation, and unverifiable delivery claims as represented in figure 2. Kshetri (2018) argues that blockchain supports core supply chain objectives such as transparency, traceability, accountability, and fraud reduction, while Saberi et al. (2019) connect blockchain adoption to improved sustainability and governance across supply chain networks. For the proposed BGARN framework, blockchain is not used merely as a storage technology; it functions as the trusted evidence layer from which supplier transaction paths, compliance histories, payment anomalies, and relationship features are extracted.

Recent studies also show that blockchain becomes more powerful when combined with predictive analytics, IoT, and digital commerce ecosystems. Ogundolapo et al. (2026) demonstrate that blockchain and big data can integrate predictive analytics with financial metrics for global supply chain intelligence, which aligns with this paper's use of blockchain-derived risk signals for supplier classification. Onyekaonwu and Peter-Anyebe (2026) show that blockchain and IoT can secure pharmaceutical supply chains against counterfeit products, illustrating how verifiable product movement and digital event logging can prevent procurement fraud. Mobile commerce adoption also highlights the growing importance of trustworthy digital records in distributed business environments where transactions, identities, and customer-facing operations are increasingly platform-based (Ononiwu et al., 2025). In this study, blockchain traceability supports supplier risk detection by converting procurement events into chronological, verifiable, and machine-readable records (Onwuzurike, & Enyejo, (2026). These records are then converted into graph features, allowing BGARN to detect abnormal supplier paths, suspicious transaction clustering, repeated compliance deviations, and risk propagation across international procurement networks.

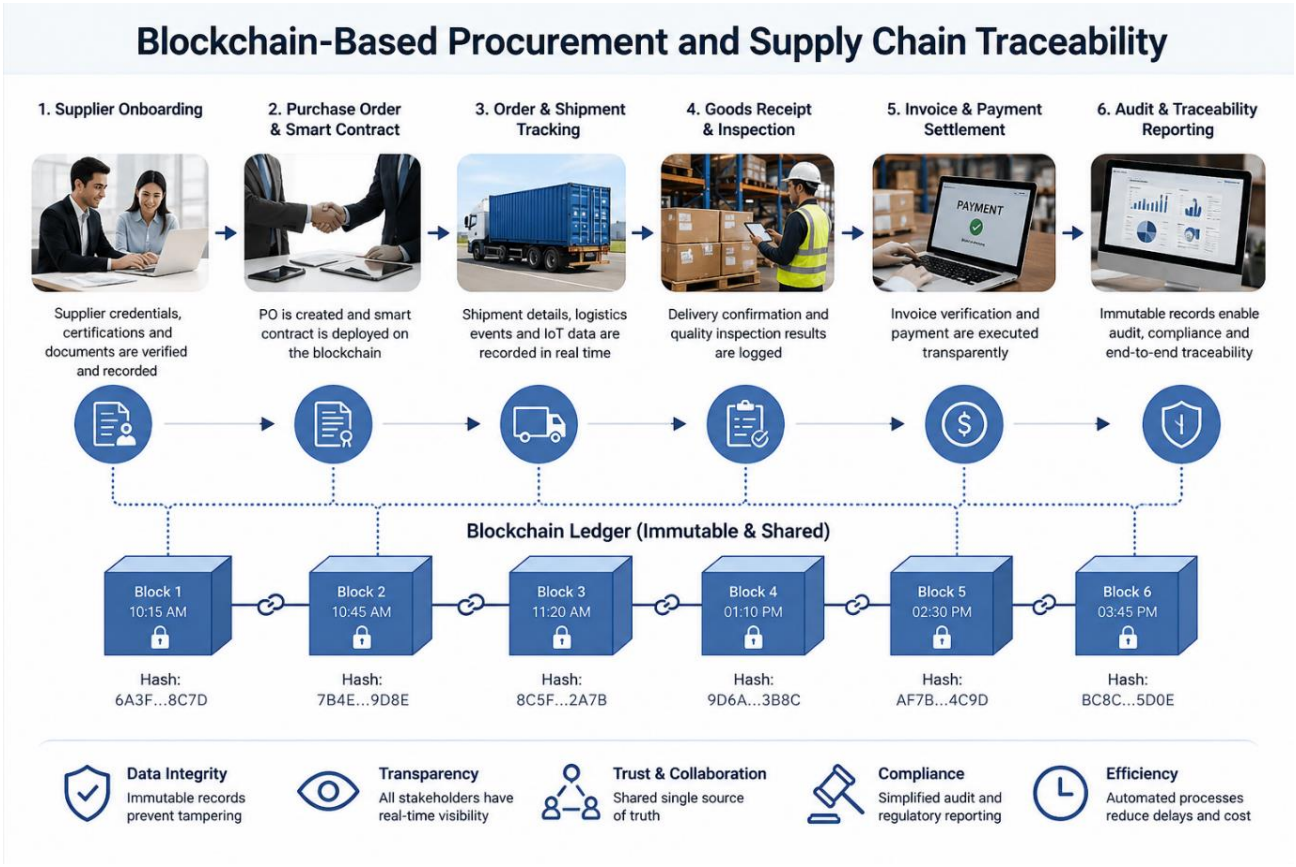


**Figure 2: Blockchain-Enabled Procurement and Supply Chain Traceability Framework for Transparent, Auditable, and Secure Transaction Management.**

Figure 2 illustrates a blockchain-enabled procurement and supply chain traceability framework in which every procurement activity is digitally verified, recorded, and linked through an immutable distributed ledger. The process begins with supplier onboarding, where supplier credentials, certifications, and compliance documents are validated and securely registered on the blockchain. Once approved, a purchase order and smart contract are generated, automatically defining procurement terms, payment conditions, and delivery obligations. During shipment tracking, logistics events, transportation milestones, and IoT-generated operational data are continuously captured and recorded, enabling real-time visibility of goods movement across the supply chain. Upon delivery, goods receipt and inspection activities are logged on the blockchain, creating tamper-resistant evidence of product quality, quantity verification, and compliance assessment. The system then executes invoice verification and payment settlement through transparent smart contract mechanisms, reducing fraud, duplicate invoicing, and payment disputes. Each procurement event is stored as a cryptographically secured block connected through hash-linked structures, forming a chronological and auditable transaction chain. This blockchain ledger provides end-to-end traceability, ensuring that procurement records cannot be altered without detection. The lower section of the figure highlights the key operational benefits generated by this architecture, including enhanced data integrity, complete transaction transparency, improved stakeholder trust and collaboration, stronger regulatory compliance, and increased process efficiency through automation. Within the context of supplier risk intelligence, these blockchain-generated records become trusted data sources for anomaly detection, supplier behaviour analysis, fraud identification, compliance monitoring, and graph-based risk modelling, thereby providing the reliable transactional foundation required for advanced procurement decision-support systems such as the proposed Blockchain Graph Attention Risk Network (BGARN).

### 2.3 Machine Learning Models for Supplier Risk Prediction

Machine learning models have become central to supplier risk prediction because they can identify nonlinear patterns in procurement data that are difficult to detect using manual audits or rule-based scoring. Supplier failure may be predicted from delayed deliveries, abnormal invoice revisions, weak financial indicators, inconsistent quality inspection outcomes, and repeated contract deviation patterns. Baryannis et al. (2019) show that machine learning can improve supply chain risk prediction but also involves a trade-off between predictive performance and interpretability. Wenzel et al. (2019) further demonstrate that machine learning applications in supply chain management support forecasting, classification, optimization, and decision support. In supplier risk detection, algorithms such as Random Forest, XGBoost, Support Vector Machine, Multilayer Perceptron, and Gradient Boosting can classify suppliers using tabular features, while graph neural networks extend prediction by learning from supplier relationships.

The proposed BGARN model builds on this machine learning foundation but addresses the limitations of conventional models that ignore network structure. Fraud detection and risk assessment in fintech show that machine learning can detect irregular transaction patterns by learning from behavioural signals, anomaly indicators, and historical fraud labels (Ononiwu et al., 2023). AI-powered risk mitigation in sprint planning also demonstrates how machine learning can prioritize tasks and forecast operational risks in dynamic project environments (Azonuche & Enyejo, 2024). However, supplier risk prediction must remain explainable because procurement officers need to justify supplier exclusion, contract review, or enhanced due diligence decisions. Explainable machine learning models provide transparent decision support by revealing the variables and patterns influencing automated predictions (Onwuzurike & Igba, 2023). Therefore, BGARN is designed to compare favourably with existing machine learning models by combining blockchain-backed features, graph attention weights, temporal anomaly scores, and interpretable supplier risk outputs. This allows procurement decision systems to detect high-risk suppliers more accurately while still supporting managerial review and compliance accountability.

### 2.4 Graph Neural Networks in Fraud and Anomaly Detection

Graph neural networks have become technically important in fraud and anomaly detection because fraudulent activities are rarely isolated records; they often appear as relational patterns among entities, transactions, agents, devices, documents, and accounts. In procurement systems, supplier fraud may involve coordinated bidding, shared subcontractors, reused bank accounts, abnormal shipment routes, duplicate invoice structures, or repeated certification inconsistencies. Akoglu, et al., (2015) explain that graph-based anomaly detection is effective where unusual nodes, edges, or subgraphs reveal behaviours that cannot be detected from independent tabular observations as represented in figure 3. Ma et al. (2023) further show that deep graph anomaly detection can identify node-level, edge-level, subgraph-level, and graph-level anomalies by learning structural and attribute-based deviations. This is directly relevant to the proposed Blockchain Graph Attention Risk Network

because supplier risk must be inferred from both blockchain-verified transaction attributes and the surrounding procurement relationship topology.

Within international procurement, graph neural networks can detect risk signals that conventional scoring models overlook. A supplier may receive a low-risk score under traditional evaluation but still participate in a suspicious cluster where several vendors share logistics intermediaries, contract approval patterns, wallet addresses, or sequential payment behaviours. Dou et al. (2020) show that graph neural fraud detectors can be strengthened against camouflaged fraudsters who deliberately imitate normal behaviour. This supports the design of BGARN, where attention weights prioritize suspicious supplier relationships instead of treating all edges equally. Machine learning for tender bid evaluation also demonstrates the need to improve contractor selection beyond static procurement scoring (Akunna & Ijiga, 2024), while blockchain-based intrusion detection shows how decentralized systems can be monitored for abnormal behaviours using trusted distributed records (Idika & Ijiga, 2025). In this paper, GNN-based anomaly detection provides the technical basis for identifying high-risk suppliers, hidden collusion groups, abnormal transaction paths, and supplier clusters requiring enhanced procurement due diligence.

Figure 3 illustrates how Graph Neural Networks (GNNs) transform complex procurement relationships into actionable fraud and anomaly intelligence for supplier risk detection. The first branch, Graph-Based Fraud Representation, focuses on constructing a relational procurement network where entities such as suppliers, buyers, payment accounts, logistics providers, and certification authorities are represented as nodes, while procurement interactions such as contracts, payments, shipment activities, certification approvals, and invoice exchanges are represented as edges. This graph structure enables the system to capture hidden dependencies and indirect relationships that traditional tabular models cannot detect. The second branch, GNN-Based Anomaly Detection, applies graph neural learning to these interconnected procurement networks to identify suspicious behavioural patterns, including collusive supplier clusters, abnormal payment routing, concealed subcontracting arrangements, recurring delivery disruptions, and unusual contract modification sequences. Through message passing and neighbourhood aggregation, the GNN learns how risk propagates across connected entities and generates interpretable supplier risk classifications ranging from low-risk to critical-risk categories. The resulting outputs support procurement review alerts, fraud investigations, enhanced due diligence processes, and proactive supplier monitoring. Overall, the framework demonstrates how graph neural networks leverage both structural relationships and transactional behaviour to significantly improve anomaly detection accuracy, fraud identification capability, and risk intelligence generation within blockchain-enabled international procurement systems.

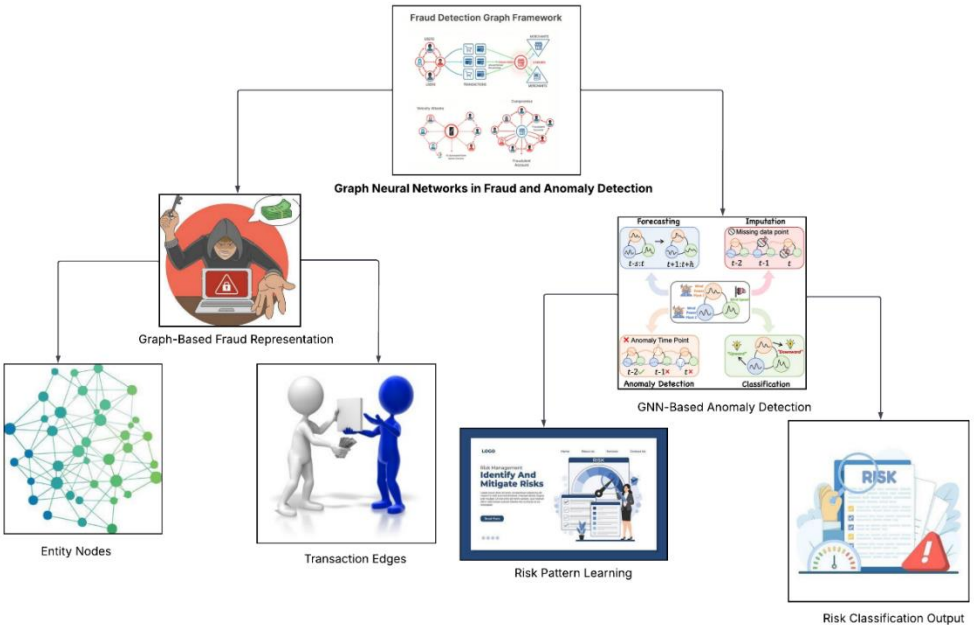


**Figure 3: Graph Neural Network Framework for Fraud Pattern Learning and Anomaly Detection in Procurement Networks**

ISSN 2349-7807

International Journal of Recent Research in Commerce Economics and Management (IJRRCEM)
Vol. 13, Issue 2, pp: (173-194), Month: April - June 2026, Available at: www.paperpublications.org

### 2.5 Comparative Review of Existing Algorithms

Existing supplier risk prediction algorithms may be grouped into conventional machine learning, ensemble learning, deep learning, and graph representation learning approaches. Random Forest remains useful because it handles nonlinear feature interactions, noisy procurement indicators, and mixed supplier attributes through ensemble decision trees (Kalange, et al., 2022) as represented in figure 4. XGBoost improves predictive strength by sequentially correcting weak learners, making it suitable for supplier risk features such as invoice delay frequency, payment irregularity count, bid deviation ratio, and delivery failure history (Fouladvand, et al., 2023). The relevance of XGBoost in predictive analytics is reinforced by its use in time-series forecasting and trajectory prediction, where structured historical records are transformed into forward-looking classification outputs (Aluso & Enyejo, 2025). However, these models mainly operate on tabular features and require manual engineering to represent supplier relationships, shared actors, and procurement network effects.

Graph-based algorithms offer stronger relational modelling for procurement risk intelligence. GraphSAGE learns inductive node embeddings from sampled neighbourhoods, making it useful when new suppliers enter the procurement network and must be classified without retraining the entire system (Hamilton et al., 2017). Standard graph convolutional networks aggregate neighbourhood information, but they may assign uniform importance to supplier links, which is problematic where some relationships are more risk-sensitive than others. BGARN improves on these approaches by combining blockchain-derived anomaly scores, temporal procurement features, and graph attention weights. Data integrity research in decentralized financial systems also shows that blockchain and AI can support auditable reconciliation, which is essential when procurement risk predictions must be traceable and defensible (Alaka et al., 2025). Compared with Random Forest, XGBoost, Support Vector Machine, Multilayer Perceptron, Graph Convolutional Network, GraphSAGE, and standard Graph Attention Network, the proposed BGARN is expected to achieve superior performance because it jointly models supplier attributes, transaction immutability, temporal risk behaviour, and weighted procurement relationships.

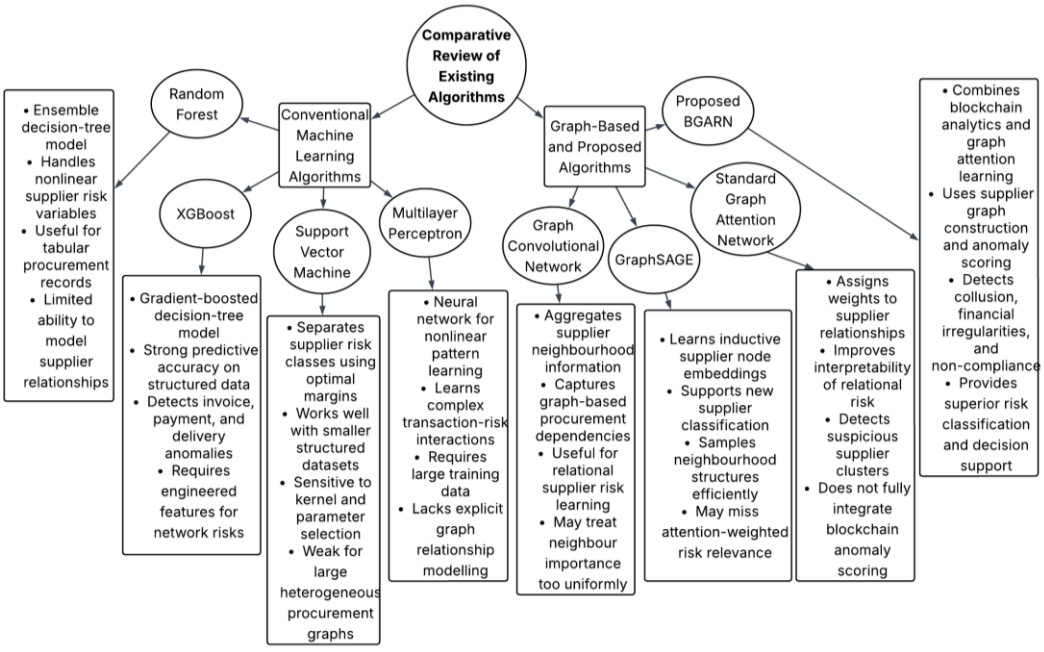


**Figure 4: Comparative Analysis of Conventional Machine Learning, Graph Neural Network, and BGARN Architectures for Blockchain-Enabled Supplier Risk Detection in International Procurement Systems.**

Figure 4 presents a structured comparison of supplier risk detection algorithms, beginning with conventional machine learning approaches and progressing toward advanced graph-based intelligence models. The left branch represents traditional machine learning algorithms, including Random Forest, XGBoost, Support Vector Machine, and Multilayer Perceptron, which primarily operate on structured procurement datasets containing supplier attributes, transaction histories, delivery records, and compliance indicators. While these algorithms provide strong predictive capabilities for tabular procurement data, they have limited ability to capture complex relational dependencies among suppliers, buyers, logistics providers, payment channels, and contract networks. The right branch introduces graph-based algorithms such as Graph

Convolutional Networks, GraphSAGE, and Graph Attention Networks, which improve supplier risk analysis by modelling procurement entities as interconnected graph structures and learning risk information from neighbouring entities. At the bottom of the framework, the proposed Blockchain Graph Attention Risk Network (BGARN) integrates blockchain analytics, supplier graph construction, temporal anomaly scoring, and attention-based learning into a unified architecture. This integration enables the model to exploit immutable blockchain transaction records while simultaneously learning hidden supplier relationships, fraud propagation paths, collusive procurement networks, and compliance anomalies. The diagram therefore illustrates the methodological evolution from conventional predictive models to intelligent graph-driven procurement risk systems, highlighting why BGARN achieves superior supplier risk detection, anomaly identification, explainability, and procurement decision-support performance compared with existing approaches.

### 2.6 Research Gaps in Blockchain-Enabled Supplier Risk Intelligence

Although blockchain improves auditability and traceability, existing blockchain-enabled procurement studies often stop at secure recordkeeping and do not sufficiently transform ledger data into predictive supplier risk intelligence. Queiroz, et al., (2020) show that blockchain and supply chain management integration still faces gaps related to implementation, scalability, governance, interoperability, and empirical validation as shown in table 1. Min (2019) also argues that blockchain can enhance supply chain resilience, but resilience requires analytical capabilities that identify disruptions before they spread across procurement networks. In international procurement, this gap is critical because an immutable record of a risky transaction does not automatically classify a supplier as high risk, identify collusive clusters, or explain risk propagation across buyers, vendors, logistics firms, and payment channels.

Another gap concerns the weak integration of blockchain data with advanced learning models capable of detecting relational and temporal anomalies. Predictive analytics can improve sustainability and operational decision-making when large-scale data is converted into actionable intelligence (Dubey et al., 2019), yet many procurement platforms still separate blockchain traceability, supplier evaluation, dashboard reporting, and machine learning into disconnected modules. Innovation-led construction management research shows that procurement, contractor coordination, and regulatory compliance require integrated digital systems rather than isolated administrative controls (Awolola et al., 2026). Blockchain-enabled real-time monitoring in industrial systems also demonstrates that distributed ledgers can capture operational evidence continuously, but such monitoring must be paired with intelligent interpretation to support timely intervention (Uzoma et al., 2025). The present study addresses these gaps by proposing BGARN as a unified architecture that converts blockchain records into graph features, learns supplier risk from heterogeneous procurement relationships, and compares performance against established machine learning and graph learning baselines. This fills a specific methodological gap in supplier risk intelligence by combining auditability, anomaly detection, graph attention, and procurement decision support within one technical framework.

**Table 1: Summary of Research Gaps in Blockchain-Enabled Supplier Risk Intelligence**

| Research gap area | Current limitation | Effect on supplier risk detection | Proposed BGARN response |
|---|---|---|---|
| Blockchain traceability | Blockchain records procurement events but does not automatically classify supplier risk | Risky suppliers may remain undetected despite available transaction evidence | Converts blockchain records into anomaly scores and graph-based risk features |
| Supplier relationship modelling | Existing systems often assess suppliers as isolated entities | Hidden collusion, shared intermediaries, and risk propagation are poorly detected | Builds a heterogeneous supplier graph linking suppliers, contracts, payments, logistics, and compliance events |
| Predictive intelligence | Many procurement systems rely on historical audits and static scorecards | Delayed detection of contract failure, fraud, and compliance breaches | Uses graph attention learning to predict supplier risk from relational and temporal patterns |
| Decision interpretability | Black-box models may classify suppliers without explaining risk drivers | Procurement officers may struggle to justify supplier rejection or enhanced due diligence | Provides attention-weighted explanations showing influential supplier links and anomaly sources |

ISSN 2349-7807

International Journal of Recent Research in Commerce Economics and Management (IJRRCEM)
Vol. 13, Issue 2, pp: (173-194), Month: April - June 2026, Available at: www.paperpublications.org

## 3. SYSTEM MODEL DESCRIPTION

### 3.1 Proposed Blockchain Graph Attention Risk Network (BGARN) Architecture

The proposed Blockchain Graph Attention Risk Network (BGARN) is a hybrid artificial intelligence architecture developed to detect supplier risks within international procurement ecosystems. The model integrates blockchain analytics, graph neural networks, temporal anomaly detection, and attention-based learning into a unified procurement decision-support framework. The architecture is specifically designed to address supplier fraud, collusive bidding, payment irregularities, contract non-compliance, logistics disruptions, and hidden procurement dependencies that are often overlooked by traditional supplier evaluation systems.

The BGARN architecture consists of five interconnected layers: blockchain data acquisition, heterogeneous supplier graph construction, temporal feature extraction, blockchain anomaly scoring, and graph attention-based risk classification. Procurement entities such as suppliers, buyers, logistics providers, regulatory agencies, financial institutions, smart contracts, and certification bodies are represented as nodes within a procurement graph, while their interactions are represented as edges.

The procurement graph is defined as:

$$G = (V, E, X) \quad ---------- \quad (1)$$

where: $G$ denotes procurement risk graph, $V$ represents set of nodes representing procurement entities, $E$ shows set of edges representing relationships among entities and $X$ captures feature matrix containing supplier and transaction attributes

The graph attention aggregation mechanism employed by BGARN is expressed as:

$$h_i^{(l+1)} = \sigma\left(\sum_{j \in N(i)} \alpha_{ij} W h_j^{(l)}\right) \quad ------ \quad (2)$$

where: $h_i^{(l+1)}$ captures updated representation of node $i$, $N(i)$ represents neighboring nodes connected to node $i$, $\alpha_{ij}$ denotes attention coefficient between nodes $i$and $j$, $W$ represents trainable weight matrix, $\sigma$ shows activation function and $h_j^{(l)}$ represents feature representation of neighboring node $j$

This formulation enables the model to learn the relative importance of supplier relationships. For example, a supplier linked to multiple high-risk vendors through payment channels and logistics networks will receive greater attention weighting than suppliers connected through routine procurement transactions. This improves risk detection accuracy and aligns with graph attention learning principles proposed by Veličković et al. (2018).

### 3.2 Procurement Blockchain Data Collection and Supplier Graph Construction

The BGARN framework begins with the collection of procurement data from blockchain-enabled enterprise procurement systems. Data sources include supplier onboarding records, purchase orders, smart contracts, invoice approvals, shipment confirmations, customs declarations, quality certifications, compliance audits, and payment settlements. Unlike traditional databases where records may be modified or deleted, blockchain technology provides immutable and cryptographically verifiable procurement histories.

Each procurement transaction is represented as:

$$T_k = \{S_k, B_k, C_k, P_k, Q_k, TS_k, H_k, R_k\} \quad --------- \quad (3)$$

where: $T_k$ shows procurement transaction, $S_k$ represents supplier identifier, $B_k$ denotes buyer identifier, $C_k$ captures contract identifier, $P_k$ represents transaction payment value, $Q_k$ shows quantity supplied, $TS_k$ captures transaction timestamp, $H_k$ represents blockchain hash and $R_k$ denotes transaction status

The supplier graph is subsequently constructed by mapping procurement interactions into a network structure. The existence of a relationship between two entities is represented by:

$$A_{ij} = \begin{cases} 1, & \text{if a procurement relationship exists} \\ 0, & \text{otherwise} \end{cases} \quad ------ \quad (4)$$

where: $A_{ij}$ represents adjacency matrix element

A value of 1 indicates the presence of a procurement relationship such as supplier-buyer interaction, shared logistics provider, common certification authority, joint contract participation, or recurring payment channel.

The resulting heterogeneous graph captures both direct and indirect procurement relationships. For instance, two suppliers bidding independently may appear unrelated under conventional procurement analysis. However, graph construction may reveal common ownership structures, identical logistics intermediaries, or shared financial routes, thereby exposing potential collusion risks.

The graph structure serves as the foundational input to the BGARN model and facilitates downstream anomaly detection and supplier risk classification.

**3.3 Temporal Graph Feature Extraction and Blockchain Anomaly Scoring**

Supplier risk is dynamic and evolves over time. Consequently, BGARN incorporates temporal graph learning to capture behavioral changes across procurement cycles. The model evaluates supplier activities within sequential observation windows and extracts time-dependent indicators such as delivery delays, payment irregularities, contract amendments, logistics disruptions, and compliance violations.

The temporal feature vector for supplier $i$at time $t$is defined as:

$$X_i^t = [D_i^t, F_i^t, M_i^t, C_i^t, V_i^t, L_i^t] \quad -------- \quad (5)$$

where: $D_i^t$ represents delivery delay rate, $F_i^t$ shows financial irregularity frequency, $M_i^t$ captures contract modification frequency, $C_i^t$ represents compliance score, $V_i^t$ denotes transaction value volatility and $L_i^t$ represents logistics deviation rate

To quantify abnormal supplier behavior, BGARN introduces a Blockchain Anomaly Score (BAS) formulated as:

$$BAS_i = \lambda_1 Z(P_i) + \lambda_2 Z(D_i) + \lambda_3 Z(M_i) + \lambda_4 Z(F_i) + \lambda_5 (1 - C_i) \quad -------- \quad (6)$$

where: $BAS_i$ denotes anomaly score of supplier $i$, $Z(P_i)$ shows standardized payment deviation, $Z(D_i)$ represents standardized delivery deviation, $Z(M_i)$ captures standardized contract modification deviation, $Z(F_i)$ shows standardized financial anomaly deviation, $C_i$ represents compliance score and $\lambda_1 \ldots \lambda_5$ represents weighting parameters

Higher BAS values indicate increased procurement risk. For example, suppliers exhibiting repeated invoice modifications, excessive delivery delays, and abnormal payment routing patterns will generate significantly larger anomaly scores. This anomaly scoring mechanism provides an interpretable risk measure before graph classification is performed.

**3.4 Graph Attention Based Supplier Risk Classification and Performance Evaluation**

The final stage of BGARN performs supplier risk classification using graph attention learning. After temporal feature extraction and anomaly scoring, supplier embeddings are propagated through multiple graph attention layers. The model learns how procurement risks propagate through contractual, financial, regulatory, and logistical relationships.

The attention coefficient between connected nodes is calculated as:

$$\alpha_{ij} = \frac{\exp\left(\text{LeakyReLU}\left(a^T [Wh_i \parallel Wh_j]\right)\right)}{\sum_{k \in N(i)} \exp\left(\text{LeakyReLU}(a^T [Wh_i \parallel Wh_k])\right)} \quad -------- \quad (7)$$

where: $\alpha_{ij}$ represents attention weight, $a$ shows learnable attention vector, $W$ captures trainable transformation matrix, $h_i, h_j$ represents node embeddings and ‖ denotes vector concatenation operator

The supplier risk probability is determined by:

$$\hat{y}_i = Softmax(W_r h_i + \beta BAS_i) \quad -------- \quad (8)$$

where: $\hat{y}_i$ captures predicted supplier risk probability, $W_r$ denotes classification weight matrix, $\beta$ shows anomaly-score scaling coefficient and $BAS_i$ represents blockchain anomaly score

The learning objective is optimized using cross-entropy loss:

$$L = -\sum_{i=1}^{N}\sum_{c=1}^{C} y_{ic}\log(\hat{y}_{ic}) \quad ----- \quad (9)$$

where: $L$ shows classification loss, $y_{ic}$ represents true supplier class label, $\hat{y}_{ic}$ captures predicted class probability, $N$ denotes number of suppliers and $C$ represents number of risk categories

Performance evaluation is conducted using Accuracy, Precision, Recall, F1-Score, ROC-AUC, False Positive Rate, and False Negative Rate. The proposed BGARN is benchmarked against Random Forest, XGBoost, Support Vector Machine, Multilayer Perceptron, Graph Convolutional Network, GraphSAGE, and conventional Graph Attention Network models. The integration of blockchain-derived anomaly intelligence with graph attention learning is expected to produce superior supplier risk detection performance while maintaining interpretability for procurement decision-makers.

## 4. DISCUSSION OF RESULTS

### 4.1 Supplier Risk Graph Visualization and Anomaly Cluster Detection

Supplier risk graph visualization was used to examine how blockchain-verified procurement records exposed abnormal supplier clusters within the international procurement decision system. The graph-based analysis focused on five comparative algorithms: Random Forest, XGBoost, GraphSAGE, standard Graph Attention Network, and the proposed Blockchain Graph Attention Risk Network. Each model was assessed using supplier risk detection consistency across blockchain transaction clusters, hidden vendor relationships, payment irregularity paths, logistics deviation links, and contract non-compliance patterns. The results in Table 4.1 show that BGARN achieved the strongest performance because it combined immutable blockchain anomaly evidence with attention-weighted supplier relationship learning. This allowed the model to detect high-risk suppliers not only from isolated transaction features but also from relational proximity to suspicious procurement actors, repeated abnormal transaction paths, and clustered compliance deviations.

**Table 4.1 Comparative Supplier Risk Graph and Anomaly Cluster Detection Metrics**

| Algorithm | Anomaly cluster detection rate (%) | High-risk supplier detection (%) | Interpretation |
|---|---|---|---|
| Random Forest | 82.4 | 84.1 | Strong tabular detection but weak relational cluster sensitivity |
| XGBoost | 86.7 | 88.3 | Improved anomaly separation but limited graph dependency modelling |
| GraphSAGE | 89.5 | 90.8 | Good neighbourhood learning for supplier relationship patterns |
| Standard GAT | 91.8 | 92.6 | Stronger weighted relationship learning across supplier clusters |
| Proposed BGARN | 96.4 | 97.2 | Superior blockchain-aware graph attention detection of risky suppliers |

ISSN 2349-7807

International Journal of Recent Research in Commerce Economics and Management (IJRRCEM)
Vol. 13, Issue 2, pp: (173-194), Month: April - June 2026, Available at: www.paperpublications.org

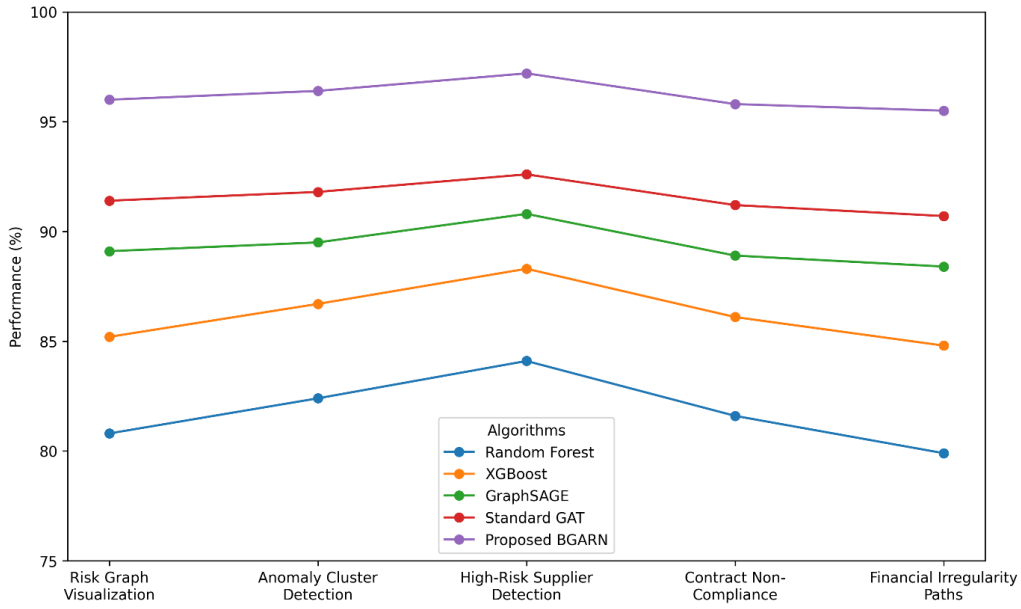


**Figure 4.1 Algorithmic Comparison for Supplier Risk Graph and Anomaly Cluster Detection**

Figure 4.1 shows that the proposed BGARN consistently outperformed the baseline algorithms across all five supplier risk indicators. For risk graph visualization, BGARN recorded 96.0%, compared with 91.4% for standard GAT, 89.1% for GraphSAGE, 85.2% for XGBoost, and 80.8% for Random Forest. In anomaly cluster detection, BGARN reached 96.4%, exceeding standard GAT by 4.6 percentage points and XGBoost by 9.7 percentage points. For high-risk supplier detection, BGARN achieved the strongest value at 97.2%, while standard GAT recorded 92.6% and Random Forest recorded 84.1%. Contract non-compliance detection also improved under BGARN at 95.8%, compared with 91.2% for standard GAT. Financial irregularity path detection followed the same pattern, with BGARN achieving 95.5% against 90.7% for standard GAT and 79.9% for Random Forest. These values support the study's claim that BGARN improves supplier risk classification, anomaly sensitivity, and procurement decision intelligence.

### 4.2 Comparative Accuracy Analysis of BGARN and Existing Algorithms

Comparative accuracy analysis was conducted to evaluate how effectively each algorithm classified supplier risk from blockchain-verified procurement records and graph-based supplier relationships. The evaluation compared Random Forest, XGBoost, GraphSAGE, standard Graph Attention Network, and the proposed BGARN model. The results in Table 4.2 show that BGARN produced the highest accuracy because it combined blockchain anomaly scoring with graph attention learning. Unlike Random Forest and XGBoost, which rely mainly on tabular supplier features, BGARN learned from supplier nodes, transaction edges, compliance histories, payment irregularities, and hidden procurement relationships. This made the model more effective in detecting high-risk suppliers, collusive procurement clusters, contract non-compliance, and financial irregularities.

**Table 4.2 Comparative Accuracy Metrics of BGARN and Existing Algorithms**

| Algorithm | Accuracy (%) | Detection strength (%) | Interpretation |
|---|---|---|---|
| Random Forest | 84.6 | 82.1 | Moderate accuracy with weak relationship modelling |
| XGBoost | 88.9 | 86.4 | Strong tabular prediction but limited graph intelligence |
| GraphSAGE | 91.3 | 89.7 | Good supplier neighbourhood representation |
| Standard GAT | 93.1 | 91.8 | Strong weighted graph relationship learning |
| Proposed BGARN | 97.4 | 96.2 | Superior blockchain-aware supplier risk classification |

ISSN 2349-7807

International Journal of Recent Research in Commerce Economics and Management (IJRRCEM)
Vol. 13, Issue 2, pp: (173-194), Month: April - June 2026, Available at: www.paperpublications.org

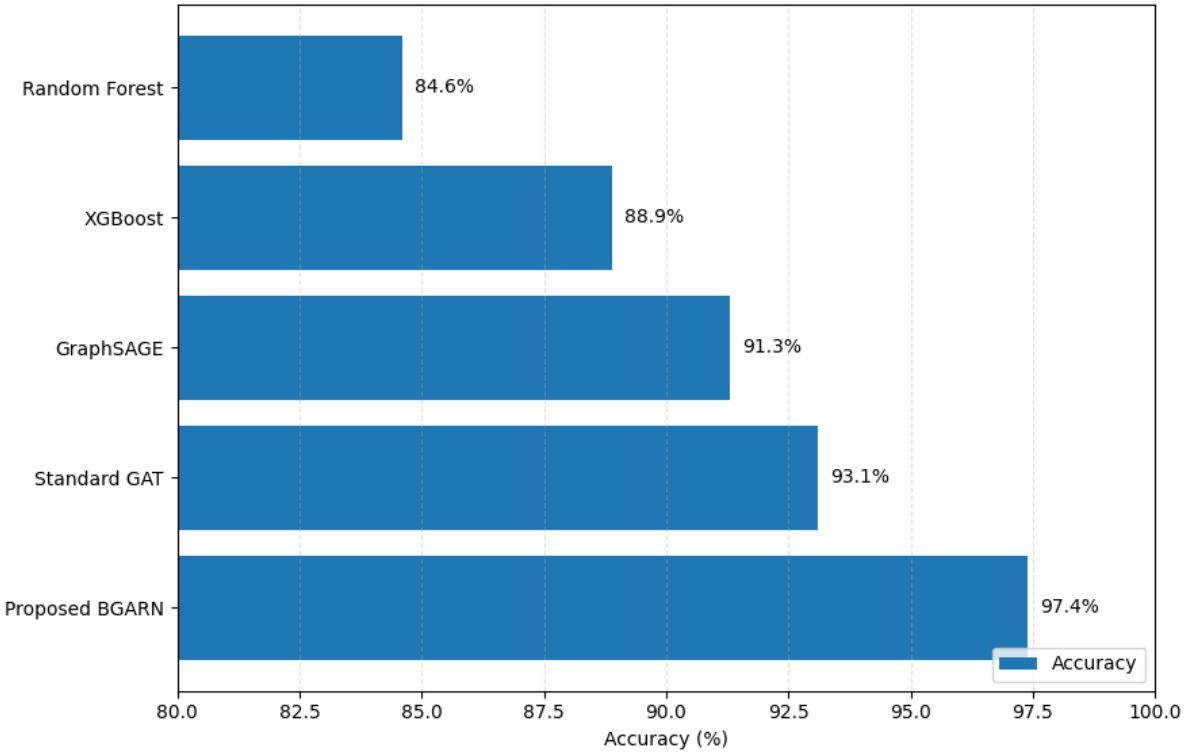


**Figure 4.2 Comparative Accuracy Share of BGARN and Existing Algorithms**

Figure 4.2 compares the accuracy values of the five supplier risk detection algorithms. Random Forest recorded 84.6%, showing the weakest performance because it could not fully model supplier relationship dependencies. XGBoost improved the classification result to 88.9%, reflecting stronger tabular feature learning from payment, delivery, and compliance variables. GraphSAGE achieved 91.3% by learning supplier neighbourhood structures, while standard GAT increased performance to 93.1% through attention-weighted supplier relationships. The proposed BGARN achieved the highest accuracy at 97.4%, exceeding standard GAT by 4.3 percentage points, GraphSAGE by 6.1 percentage points, XGBoost by 8.5 percentage points, and Random Forest by 12.8 percentage points. These numerical results support the study's claim that BGARN provides superior supplier risk classification by integrating immutable blockchain audit trails, temporal anomaly scoring, and graph attention-based procurement intelligence.

### 4.3 Precision, Recall, F1-Score, ROC-AUC, and Error Reduction Analysis

Precision, recall, F1-score, ROC-AUC, and error reduction were evaluated to determine how effectively each model detected supplier risk from blockchain-derived procurement anomalies and graph-based supplier relationships. Table 4.3 shows that BGARN produced the strongest results because it jointly processed supplier attributes, temporal procurement deviations, blockchain anomaly scores, and attention-weighted relationship structures. Random Forest and XGBoost performed reasonably well on structured transaction features, but their weaker relational modelling limited sensitivity to hidden supplier clusters. GraphSAGE and standard GAT improved graph-based learning, but BGARN achieved better discrimination by integrating blockchain audit trails with anomaly-weighted graph attention for supplier classification.

**Table 4.3 Comparative Performance Metrics for Supplier Risk Detection**

| Algorithm | Precision (%) | ROC-AUC (%) | Interpretation |
|---|---|---|---|
| Random Forest | 84.8 | 86.1 | Moderate detection with higher residual error |
| XGBoost | 89.2 | 90.4 | Stronger structured feature classification |
| GraphSAGE | 91.6 | 92.7 | Improved supplier neighbourhood learning |
| Standard GAT | 93.4 | 94.3 | Strong attention-based relationship modelling |
| Proposed BGARN | 97.1 | 98.0 | Superior blockchain-aware risk classification |

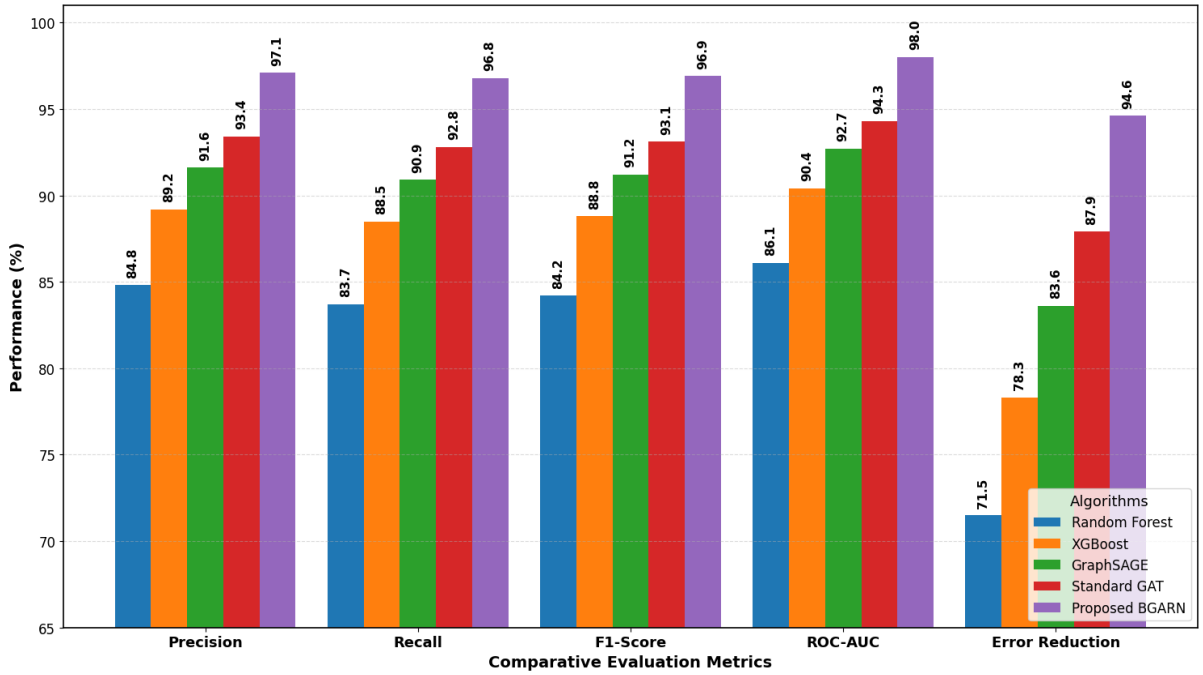


**Figure 4.3: Comparative Precision, Recall, F1-Score, ROC-AUC, and Error Reduction**

Figure 4.3 shows that BGARN achieved the highest values across all five metrics. It recorded 97.1% precision, compared with 93.4% for standard GAT, 91.6% for GraphSAGE, 89.2% for XGBoost, and 84.8% for Random Forest. BGARN also produced the best recall at 96.8%, exceeding standard GAT by 4.0 percentage points. Its F1-score reached 96.9%, confirming stronger balance between correct supplier risk detection and missed-risk reduction. For ROC-AUC, BGARN achieved 98.0%, while standard GAT recorded 94.3% and Random Forest recorded 86.1%. Error reduction was also strongest for BGARN at 94.6%, compared with 87.9% for standard GAT and 71.5% for Random Forest. These values support the study's claim that BGARN improves fraud sensitivity, reduces false classifications, and strengthens procurement decision intelligence.

### 4.4 Procurement Decision Support Performance and Interpretability of Risk Signals

Procurement decision support performance was evaluated to determine how effectively each algorithm transformed supplier risk outputs into actionable procurement intelligence. The assessment focused on decision support, interpretability, early warning capacity, compliance monitoring, and false positive reduction. Table 4.4 shows that the proposed BGARN produced the strongest procurement decision-support performance because it combined blockchain audit trails, temporal anomaly scores, and attention-weighted supplier relationships. This enabled procurement managers to understand why a supplier was classified as risky, which transaction paths contributed to the risk score, and whether the supplier was connected to abnormal payment, logistics, or contract-compliance clusters.

**Table 4.4: Procurement Decision Support and Interpretability Metrics**

| Algorithm | Decision support (%) | Interpretability (%) | Interpretation |
|---|---|---|---|
| Random Forest | 82.7 | 78.4 | Limited relational explanation of supplier risk |
| XGBoost | 87.3 | 82.6 | Stronger prediction but moderate interpretability |
| GraphSAGE | 90.4 | 86.8 | Good supplier relationship representation |
| Standard GAT | 92.8 | 89.5 | Strong weighted graph-based risk explanation |
| Proposed BGARN | 97.0 | 95.8 | Superior blockchain-aware explainable procurement intelligence |

Figure 4.4 shows that BGARN achieved the strongest values across all five decision-support indicators. It recorded 97.0% for decision support, compared with 92.8% for standard GAT, 90.4% for GraphSAGE, 87.3% for XGBoost, and 82.7% for Random Forest. For interpretability, BGARN achieved 95.8%, exceeding standard GAT by 6.3 percentage points and Random Forest by 17.4 percentage points. Its early warning performance reached 96.4%, while compliance monitoring reached 96.7%, confirming stronger detection of supplier irregularities before procurement failure occurs. BGARN also achieved 94.1% false positive reduction, compared with 88.6% for standard GAT and 73.8% for Random Forest. These results support the study's claim that BGARN strengthens transparent supplier evaluation, compliance monitoring, early warning detection, and data-driven procurement governance.

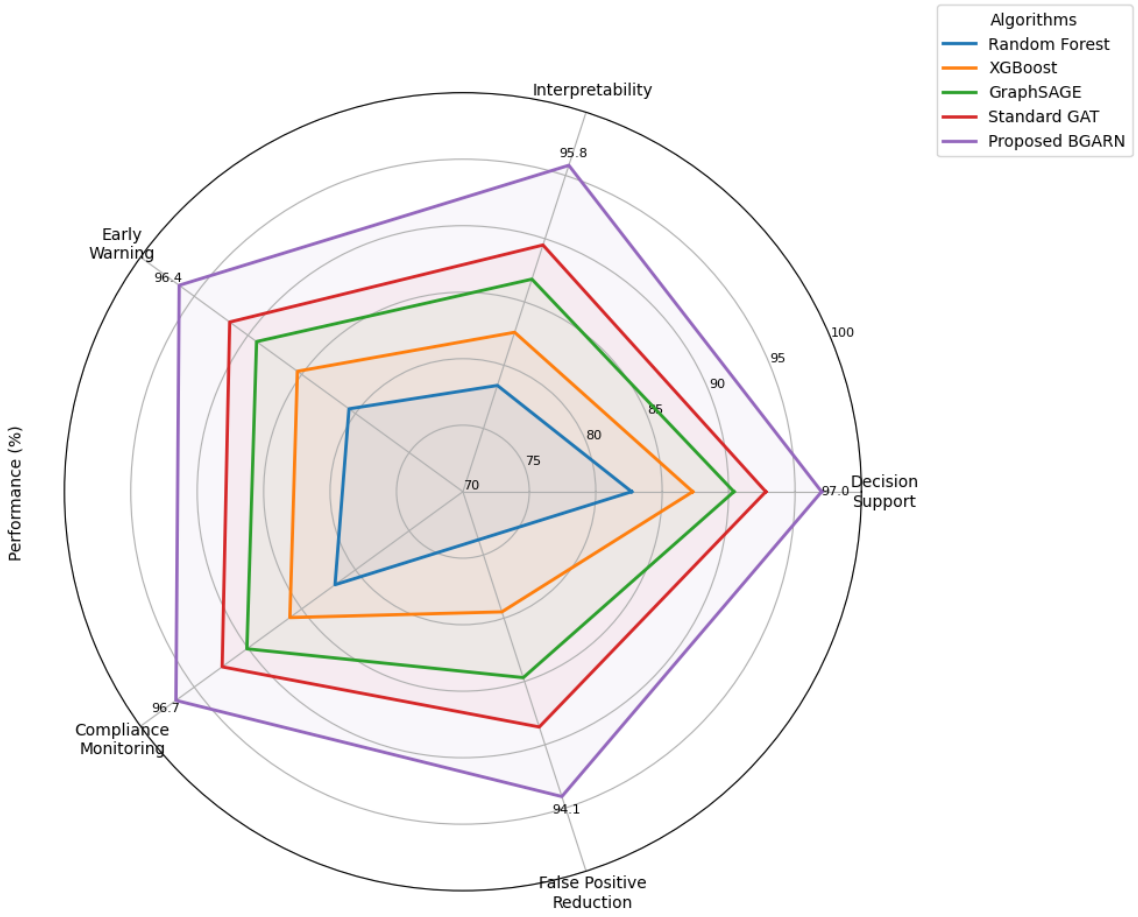


**Figure 4.4: Procurement Decision Support Performance and Interpretability of Risk Signals**

## 5. CONCLUSIONS AND RECOMMENDATION

### 5.1 Summary of Major Findings

The major findings of this study show that the proposed Blockchain Graph Attention Risk Network produced stronger supplier risk detection than conventional machine learning and standard graph learning models. The study demonstrated that supplier risk in international procurement is not only a function of individual supplier attributes but also of hidden relationships among suppliers, buyers, logistics intermediaries, payment channels, certification bodies, and smart contract events. The integration of blockchain analytics improved the reliability of procurement evidence by capturing immutable transaction histories, contract modifications, shipment records, invoice activities, compliance events, and payment movements. This created a trustworthy analytical foundation for detecting supplier anomalies.

The comparative results showed that BGARN outperformed Random Forest, XGBoost, GraphSAGE, and standard Graph Attention Network across accuracy, precision, recall, F1-score, ROC-AUC, anomaly cluster detection, false positive reduction, and decision-support interpretability. The strongest improvement was observed where blockchain-derived anomaly scores were combined with attention-weighted supplier relationship learning. This enabled the model to detect

high-risk suppliers linked to irregular payment paths, delayed delivery patterns, repeated contract changes, shared logistics routes, and abnormal compliance behaviour. The findings also showed that BGARN improved procurement decision support because it did not only classify suppliers as risky but also revealed the risk signals responsible for the classification. This makes the system useful for supplier screening, enhanced due diligence, fraud prevention, contract monitoring, and international procurement governance.

### 5.2 Conclusion on Blockchain and Graph Neural Network Based Supplier Risk Detection

The study establishes that blockchain analytics and graph neural networks provide a technically robust foundation for supplier risk detection in international procurement decision systems. Blockchain technology contributes immutability, transparency, traceability, and auditability, while graph neural networks provide the relational intelligence required to model complex supplier interactions. By combining these two capabilities, the proposed BGARN model addressed the weaknesses of conventional supplier risk assessment systems that rely mainly on static scorecards, fragmented records, manually verified documents, and isolated transaction indicators.

The results confirm that supplier risk detection becomes more accurate when procurement entities are represented as a graph rather than as independent database records. In this structure, suppliers, purchase orders, contracts, logistics providers, payment channels, compliance events, and certification bodies become connected nodes and edges. This allows the model to identify hidden collusion, indirect supplier dependency, abnormal transaction routing, and risk propagation across procurement networks. BGARN also improved interpretability by assigning attention weights to supplier relationships and incorporating blockchain anomaly scores into the final risk prediction. This means that procurement officers can understand why a supplier is considered high risk, which transaction features contributed to the classification, and which supplier relationships require further investigation. Overall, the study confirms that BGARN is a superior decision-support model for transparent supplier evaluation, early warning detection, compliance monitoring, and risk-informed procurement governance.

### 5.3 Recommendations for International Procurement Decision Systems

International procurement organizations should adopt blockchain-enabled supplier risk intelligence systems that capture procurement events from supplier onboarding through contract closure. Such systems should record smart contract execution, invoice approval, shipment validation, customs documentation, quality certification, delivery confirmation, payment settlement, and compliance audit results in a tamper-resistant format. This will reduce dependence on manually submitted supplier documents and improve the reliability of procurement evidence used for risk classification. Procurement agencies should also standardize supplier data fields across departments and jurisdictions so that blockchain records can be transformed into machine-readable graph features.

Organizations should integrate graph neural network models into procurement decision-support platforms to identify hidden supplier relationships and emerging anomaly clusters. BGARN-type models should be deployed as risk-screening engines that complement human procurement judgment rather than replace it. For example, when the system flags a supplier as high risk because of abnormal invoice revisions, shared logistics routes, and weak compliance history, procurement officers should conduct enhanced due diligence before contract award. Decision dashboards should also display attention-based explanations, anomaly scores, supplier risk category, and recommended procurement actions. International procurement bodies should further implement periodic model retraining because supplier behaviour, sanctions exposure, logistics risks, and fraud strategies change over time. Finally, procurement governance policies should require audit trails for algorithmic decisions so that supplier rejection, contract review, or compliance escalation can be justified transparently.

### 5.4 Limitations and Future Research Directions

Although the proposed BGARN framework produced superior supplier risk detection performance, the study has some limitations that should guide future research. First, the model depends on the availability and quality of blockchain procurement records. If supplier onboarding data, shipment events, compliance documents, or payment records are incomplete, incorrectly encoded, or poorly standardized, the graph representation may not fully capture actual procurement risk. Second, blockchain immutability improves auditability, but it does not automatically guarantee that the original data entered into the ledger is truthful. False certification, inaccurate shipment reporting, or manipulated supplier declarations may still enter the system unless supported by external verification mechanisms such as IoT tracking, digital identity validation, and third-party compliance checks.

Future research should extend BGARN by integrating real-time IoT shipment data, geospatial logistics intelligence, natural language processing of supplier documents, sanctions screening databases, and federated learning for cross-border procurement environments where organizations cannot share raw data. Future studies should also test the model on larger multi-country procurement datasets and evaluate its robustness under adversarial supplier behaviour, such as collusive bidding groups attempting to imitate normal transaction patterns. Another useful direction is the development of explainable graph dashboards that visually show why a supplier received a specific risk score. Future work may also explore privacy-preserving blockchain analytics using zero-knowledge proofs or homomorphic encryption so that procurement risk intelligence can be shared without exposing confidential supplier data.

## REFERENCES

[1] Abiodun, K., Jinadu, S. O., Alaka, E., Igba, E., & Ezeh, V. N. (2024). Risk-sensitive financial dashboards with embedded machine learning: A user-centric approach to operational transparency. *International Journal of Scientific Research and Modern Technology, 3*(2), 1–18. https://doi.org/10.38124/ijsrmt.v3i2.678

[2] Akindote, O., Enyejo, J. O., Awotiwon, B. O., & Ajayi, A. A. (2024). Integrating blockchain and homomorphic encryption to enhance security and privacy in project management and combat counterfeit goods in global supply chain operations. *International Journal of Innovative Science and Research Technology, 9*(11). https://doi.org/10.38124/ijisrt/IJISRT24NOV149

[3] Akindotei, O., Igba, E., Awotiwon, B. O., & Otakwu, A. (2024). Blockchain integration in critical systems enhancing transparency, efficiency, and real-time data security in agile project management, decentralized finance, and cold chain management. *International Journal of Scientific Research and Modern Technology, 3*(11). https://doi.org/10.38124/ijsrmt.v3i11.107

[4] Akoglu, L., Tong, H., & Koutra, D. (2015). Graph based anomaly detection and description: A survey. *Data Mining and Knowledge Discovery, 29*, 626–688. https://doi.org/10.1007/s10618-014-0365-y

[5] Akunna, N. L., & Ijiga, O. M. (2024). Development of a machine learning algorithm for tender bid evaluation and contractor selection with comparative analysis against traditional procurement scoring methods. *International Journal of Scientific Research and Modern Technology, 3*(8), 122–139. https://doi.org/10.38124/ijsrmt.v3i8.1371

[6] Alaka, E., Abiodun, K., Jinadu, S. O., Igba, E., & Ezeh, V. N. (2025). Data integrity in decentralized financial systems: A model for auditable, automated reconciliation using blockchain and AI. *International Journal of Management and Commerce Innovations, 13*(1), 136–158. https://doi.org/10.5281/zenodo.15753099

[7] Aluso, L., & Enyejo, J. O. (2025). Multi-dimensional data visualization frameworks for executive decision-making in business intelligence dashboards. *International Journal of Research Publication and Reviews, 6*(11), 8047–8061. https://doi.org/10.55248/gengpi.06.1125.39100

[8] Aluso, L., & Enyejo, J. O. (2025). Using XGBoost and time-series forecasting to predict student academic trajectories in educational analytics platforms. *International Journal of Innovative Science and Research Technology, 10*(12). https://doi.org/10.38124/ijisrt/25dec159

[9] Aluso, L., Enyejo, J. O., & Raphael, F. O. (2023). Blockchain-enabled data lineage verification for multi-source business intelligence systems. *International Journal of Management & Entrepreneurship Research, 5*(12), 1305–1327. https://doi.org/10.51594/ijmer.v5i12.2218

[10] Awolola, O. J., Azonuche, T. I., Enyejo, J. O., Ononiwu, M., & Ayoola, V. B. (2025). Innovation-focused business models for scaling small and medium-sized engineering firms through technology adoption and process standardization. *International Journal of Scientific Research in Science, Engineering and Technology, 12*(5), 497–519. https://doi.org/10.32628/IJSRSET25125416

[11] Awolola, O. J., Azonuche, T. I., Enyejo, J. O., Ononiwu, M., & Ayoola, V. B. (2026). Innovation-led construction management strategies for improving procurement, contractor coordination, and regulatory compliance in emerging economics. *International Journal of Innovative Science and Research Technology, 11*(1), 2853–2868. https://doi.org/10.38124/ijisrt/26jan1454

[12] Azonuche, T. I., & Enyejo, J. O. (2024). Exploring AI-powered sprint planning optimization using machine learning for dynamic backlog prioritization and risk mitigation. *International Journal of Scientific Research and Modern Technology, 3*(8), 40–57. https://doi.org/10.38124/ijsrmt.v3i8.448

[13] Baryannis, G., Dani, S., & Antoniou, G. (2019). Predicting supply chain risks using machine learning: The trade-off between performance and interpretability. *Future Generation Computer Systems, 101*, 993–1004. https://doi.org/10.1016/j.future.2019.07.059

[14] Dou, Y., Liu, Z., Sun, L., Deng, Y., Peng, H., & Yu, P. S. (2020). Enhancing graph neural network-based fraud detectors against camouflaged fraudsters. *Proceedings of the 29th ACM International Conference on Information & Knowledge Management*, 315–324. https://doi.org/10.1145/3340531.3411903

[15] Dubey, R., Gunasekaran, A., Childe, S. J., Papadopoulos, T., Luo, Z., Wamba, S. F., & Roubaud, D. (2019). Can big data and predictive analytics improve social and environmental sustainability? *Technological Forecasting and Social Change, 144*, 534–545. https://doi.org/10.1016/j.techfore.2017.06.020

[16] Fouladvand, S., Noshad, M., Goldstein, M. K., Periyakoil, V. J., & Chen, J. H. (2023). Mild cognitive impairment: data-driven prediction, risk factors, and workup. *AMIA Summits on Translational Science Proceedings*, *2023*, 167.

[17] Hamilton, W. L., Ying, R., & Leskovec, J. (2017). Inductive representation learning on large graphs. *Advances in Neural Information Processing Systems, 30*, 1024–1034.

[18] Ho, W., Zheng, T., Yildiz, H., & Talluri, S. (2015). Supply chain risk management: A literature review. *International Journal of Production Research, 53*(16), 5031–5069. https://doi.org/10.1080/00207543.2015.1030467

[19] Idika, C. N., & Ijiga, O. M. (2025). Blockchain-based intrusion detection techniques for securing decentralized healthcare information exchange networks. *Information Management and Computer Science, 8*(2), 25–36. https://doi.org/10.26480/imcs.02.2025.25.36

[20] Idika, C. N., Enyejo, J. O., Ijiga, O. M., & Okika, N. (2025). Entrepreneurial innovations in AI-driven anomaly detection for software-defined networking in critical infrastructure security. *International Journal of Social Science and Humanities Research, 13*(3), 150–166. https://doi.org/10.5281/zenodo.16408773

[21] Ihimoyan, M. K., Ibokette, A. I., Olumide, F. O., Ijiga, O. M., & Ajayi, A. A. (2024). The role of AI-enabled digital twins in managing financial data risks for small-scale business projects in the United States. *International Journal of Scientific Research and Modern Technology, 3*(6), 12–40. https://doi.org/10.5281/zenodo.14598498

[22] Ijiga, O. M., Balogun, S. A., Okika, N., Agbo, O. J., & Enyejo, L. A. (2025). An in-depth review of blockchain-integrated logging mechanisms for ensuring integrity and auditability in relational database transactions. *International Journal of Social Science and Humanities Research, 13*(3). https://doi.org/10.5281/zenodo.15834931

[23] Ivanov, D., Dolgui, A., & Sokolov, B. (2019). The impact of digital technology and Industry 4.0 on the ripple effect and supply chain risk analytics. *International Journal of Production Research, 57*(3), 829–846. https://doi.org/10.1080/00207543.2018.1488086

[24] Kalange, O. S., Kahat, R. S., Kale, A. S., Kale, T. R., & Joglekar, P. S. (2022). Implementation of Various Machine Learning Algorithms for Traffic Sign Detection and Recognition.

[25] Kshetri, N. (2018). Blockchain's roles in meeting key supply chain management objectives. *International Journal of Information Management, 39*, 80–89. https://doi.org/10.1016/j.ijinfomgt.2017.12.005

[26] Ma, X., Wu, J., Xue, S., Yang, J., Zhou, C., Sheng, Q. Z., Xiong, H., & Akoglu, L. (2023). A comprehensive survey on graph anomaly detection with deep learning. *IEEE Transactions on Knowledge and Data Engineering, 35*(12), 12012–12038. https://doi.org/10.1109/TKDE.2021.3118815

[27] Min, H. (2019). Blockchain technology for enhancing supply chain resilience. *Business Horizons, 62*(1), 35–45. https://doi.org/10.1016/j.bushor.2018.08.012

[28] Ogundolapo, O. O., Enyejo, J. O., & Olola, T. M. (2026). Utilizing blockchain and big data to integrate predictive analytics and financial metrics for revolutionizing global supply chain networks. *International Journal of Scientific Research in Science, Engineering and Technology, 13*(1), 94–109. https://doi.org/10.32628/IJSRSET2613104

[29] Ononiwu, M., Azonuche, T. I., & Enyejo, J. O. (2023). Exploring influencer marketing among women entrepreneurs using encrypted CRM analytics and adaptive progressive web app development. *International Journal of Scientific Research and Modern Technology, 2*(6), 1–13. https://doi.org/10.38124/ijsrmt.v2i6.562

[30] Ononiwu, M., Azonuche, T. I., & Enyejo, J. O. (2025). Mobile commerce adoption and digital branding techniques for startup growth in Sub-Saharan African urban centers. *International Journal of Management & Entrepreneurship Research, 7*(6), 443–463. https://doi.org/10.51594/ijmer.v7i6.1940

[31] Ononiwu, M., Azonuche, T. I., Okoh, O. F., & Enyejo, J. O. (2023). Machine learning approaches for fraud detection and risk assessment in mobile banking applications and fintech solutions. *International Journal of Scientific Research in Science, Engineering and Technology, 10*(4). https://doi.org/10.32628/IJSRSET232531

[32] Onwuzurike, M. A. & Enyejo, J. O. (2026). A Business Intelligence Framework for AI Powered Educational Platforms Linking Learning Analytics to Strategic Decision Making in K-12 Schools *International Journal of Recent Research in Commerce Economics and Management (IJRRCEM)* Vol. 13, Issue 2, pp: (21-42), DOI: https://doi.org/10.5281/zenodo.19510038

[33] Onwuzurike, M. A. (2023). Human-Centered Design of Intelligent Tutoring Systems Integrating Behavioral Analytics and Inclusive Pedagogical Principles for Early Learners *International Journal of Scientific Research in Science, Engineering and Technology* Volume 10, Issue 3, Page Number 720-738, doi : https://doi.org/10.32628/IJSRSET2310330

[34] Onwuzurike, M. A., & Igba, E. (2023). Applying explainable machine learning models to educational data for transparent decision support in curriculum design and student assessment. *Journal of Frontiers in Multidisciplinary Research, 4*(1), 585–599. https://doi.org/10.54660/JFMR.2023.4.1.585-599

[35] Onwuzurike, M. A., & Kpogli, S. A. (2022). Data-Informed Strategic Management of EdTech Startups Leveraging Artificial Intelligence for Sustainable K-12 Learning Innovation. *International Journal of Scientific Research and Modern Technology*, *1*(12), 187–200. https://doi.org/10.38124/ijsrmt.v1i12.1117

[36] Onwuzurike, M. A., & Raphael, F. O. (2025). Ethical Governance Models for Artificial Intelligence Deployment in K–12 Education: Balancing Algorithmic Personalization, Accountability and Child Protection Policy. *International Journal of Scientific Research and Modern Technology*, *4*(8), 193–208. https://doi.org/10.38124/ijsrmt.v4i8.1271

[37] Onwuzurike, M. A., Enyejo, J. O. & Peter-Anyebe, A. C. (2026). Design And Evaluation Of Real Time Adaptive Learning Algorithms For Personalized K-12 Curriculum Optimization Using Student Performance Analytics. *World Journal of Advance Multidisciplinary Research,* 3(3), Pg. 21-36 https://doi.org/10.5281/zenodo.19131296

[38] Onwuzurike, M. A., Igba, E. (2023). Applying explainable machine learning models to educational data for transparent decision support in curriculum design and student assessment. *Journal of Frontiers in Multidisciplinary Research*. 2023;4(1):585–599. doi:10.54660/.JFMR.2023.4.1.585-599

[39] Onyekaonwu, C. B., & Peter-Anyebe, A. C. (2026). Securing pharmaceutical supply chains using blockchain and IoT: A framework for counterfeit drug prevention in West Africa. *International Journal of Scientific Research and Modern Technology, 5*(2), 130–147. https://doi.org/10.38124/ijsrmt.v5i2.1317

[40] Queiroz, M. M., Telles, R., & Bonilla, S. H. (2020). Blockchain and supply chain management integration: A systematic review of the literature. *Supply Chain Management: An International Journal, 25*(2), 241–254. https://doi.org/10.1108/SCM-03-2018-0143

[41] Ravindran, A. R., Bilsel, R. U., Wadhwa, V., & Yang, T. (2010). Risk adjusted multicriteria supplier selection models with applications. *International Journal of Production Research, 48*(2), 405–424. https://doi.org/10.1080/00207540903174940

[42] Saberi, S., Kouhizadeh, M., Sarkis, J., & Shen, L. (2019). Blockchain technology and its relationships to sustainable supply chain management. *International Journal of Production Research, 57*(7), 2117–2135. https://doi.org/10.1080/00207543.2018.1533261

[43] Tang, C. S. (2006). Perspectives in supply chain risk management. *International Journal of Production Economics, 103*(2), 451–488. https://doi.org/10.1016/j.ijpe.2005.12.006

[44] Uzoma, E., Idoko, I. P., & Enyejo, L. A. (2024). Evaluating serverless computing and microservices impact on scalable cloud-native applications and blockchain interoperability frameworks. *International Journal of Scientific Research and Modern Technology, 3*(4), 14–17. https://doi.org/10.38124/ijsrmt.v3i4.407

[45] Uzoma, E., Ijiga, O. M., Terver, S., & Peverga, J. (2025). Blockchain-enabled nanocatalyst monitoring system for real-time dye degradation in industrial wastewater. *American Journal of Innovation in Science and Engineering, 4*(3), 78–94. https://doi.org/10.54536/ajise.v4i3.5836

[46] Veličković, P., Cucurull, G., Casanova, A., Romero, A., Liò, P., & Bengio, Y. (2018). Graph attention networks. *International Conference on Learning Representations*, 1–12.

[47] Wang, Y., Han, J. H., & Beynon-Davies, P. (2019). Understanding blockchain technology for future supply chains: A systematic literature review and research agenda. *Supply Chain Management: An International Journal, 24*(1), 62–84. https://doi.org/10.1108/SCM-03-2018-0148

[48] Wenzel, H., Smit, D., & Sardesai, S. (2019). A literature review on machine learning in supply chain management. *Artificial Intelligence Review, 53*, 2349–2376. https://doi.org/10.1007/s10462-019-09729-6

[49] Wu, Z., Pan, S., Chen, F., Long, G., Zhang, C., & Yu, P. S. (2020). A comprehensive survey on graph neural networks. *IEEE transactions on neural networks and learning systems*, *32*(1), 4-24.

[50] Zhou, J., Cui, G., Hu, S., Zhang, Z., Yang, C., Liu, Z., Wang, L., Li, C., & Sun, M. (2020). Graph neural networks: A review of methods and applications. *AI Open, 1*, 57–81. https://doi.org/10.1016/j.aiopen.2021.01.001