LRA: A Lightweight Reputation-Based Authentication Framework for Secure IoT-Driven E-Commerce Supply Chain Management

M. P. Amulya
Department of Computer Science and Engineering, Dr. Ambedkar Institute of Technology, Bengaluru, Visvesvaraya Technological University, Belagavi, Karnataka, India
dramulyamp@gmail.com (corresponding author)

N. Nandini
Department of Computer Science and Engineering, Dr. Ambedkar Institute of Technology, Bengaluru, Visvesvaraya Technological University, Belagavi, Karnataka, India
nandu_8449@rediffmail.com

Received: 9 February 2026 | Revised: 23 April 2026 | Accepted: 30 April 2026

 DOI: https://doi.org/10.48084/etasr.18062

ABSTRACT

The rapid integration of Internet of Things (IoT) technologies into e-commerce supply chains introduces critical challenges in security, trust management, and workflow efficiency. Existing blockchain-assisted authentication schemes, such as SPUFCHAIN, suffer from high computational overhead, scalability limitations, and vulnerability to reputation manipulation in resource-constrained environments. To address these issues, this paper presents Lightweight Reputation-based Authentication (LRA), a decentralized trust management framework that combines dynamic reputation evaluation with blockchain-backed immutable storage. The proposed model incorporates direct and indirect trust computation enhanced by historical consistency, fluctuation minimization, and stability factors to ensure reliable authentication. Smart contracts are utilized for automated trust updates and secure workflow validation. The performance of LRA was evaluated using the CICIoV2024 dataset, which simulates realistic adversarial scenarios, including spoofing and denial-of-service attacks, in IoT-enabled environments. Experimental results demonstrate that LRA achieves higher detection rates, significantly reduces misclassification rates, and improves normalized throughput compared to SPUFCHAIN. These findings confirm that LRA provides a scalable, efficient, and secure authentication solution for IoT-driven e-commerce supply chain management systems.

Keywords-blockchain; e-commerce supply chain; Internet of Things (IoT); lightweight authentication; reputation system; performance optimization

I. INTRODUCTION

E-commerce has experienced rapid digital transformation in the past decade, increasingly relying on trust, transparency, and secure transaction frameworks to manage growing complexities in distributed ecosystems. Blockchain technology has emerged as a key enabler for addressing longstanding challenges related to trust management, fraud prevention, secure coordination, and data integrity in e-commerce and supply chain workflows [1]. In supply chain settings, blockchain adoption has shown strategic value among collaborating and competing retailers [2], with surveys emphasizing its role in ensuring data integrity, visibility, and traceability across complex e-commerce value chains [3]. Applications are especially prominent in food and perishable goods supply chains, where blockchain enhances safety, traceability, and waste minimization [4]. Similar benefits extend to logistics and cross-border transportation, where security vulnerabilities, coordination issues, and IoT devices face limited battery and processing constraints, making traditional security inefficient, thus necessitating lightweight but scalable authentication solutions [5]. Moreover, the convergence of blockchain with Artificial Intelligence (AI) and the Internet of Things (IoT) further opens possibilities for intelligent decision-making, privacy-preserving transactions, and adaptive sales modes within dynamic e-commerce environments [6]. Blockchain has also supported last-mile delivery optimization [7], verifiable logistics coordination [8], and AI-driven personalized consumer experience systems [9].

Trust and reputation mechanisms represent another area where blockchain has contributed significant advances. Systems such as "TRUTH" ensure genuine user feedback and fraud-resistant review management [10], while blockchain-enabled sustainable product assessment [11], fair data trading [12], and privacy-aware consensus mechanisms [13] further illustrate its expanding presence in consumer-centric applications. Research has also explored fairness-aware e-commerce protocols [14], innovations in fashion supply chain networks [15], platform adoption strategies [16], and blockchain-enhanced recommendation systems and federated learning frameworks [17]. Privacy-preserving transaction management models like PBTMS [18] and runtime verification systems for smart contracts [19] reflect ongoing efforts to strengthen blockchain's security foundations. New paradigms, such as a BarterChain [20] and manufacturer-driven adoption strategies [21], reveal the technology's evolving trajectory across diverse e-commerce domains.

However, several limitations persist across modern blockchain-driven e-commerce systems, including the lack of lightweight authentication, high misclassification rates, and throughput degradation. Performance constraints, smart contract vulnerabilities, and scalability issues hinder seamless adoption, while IoT-enabled supply chain environments introduce additional challenges due to heterogeneous devices with limited computational resources. Therefore, lightweight authentication is crucial to maintaining secure yet efficient blockchain interactions. SPUFChain [22], a blockchain model that integrates Physical Unclonable Functions (PUFs), addresses authentication in IoT-based supply chains but suffers from performance degradation and limited scalability under high transaction volumes. Existing approaches further exhibit misclassification challenges, insufficient throughput performance, heavy cryptographic overhead that is unsuitable for IoT devices, and limited adaptability to multi-retailer and heterogeneous environments.

Motivated by these gaps, this work introduces Lightweight Reputation-based Authentication (LRA), integrating adaptive reputation scoring with lightweight authentication to reduce misclassification and improve throughput. This work contributes a hybrid trust modeling framework that integrates Bayesian inference, reputation stabilization, and blockchain-based consensus, providing a mathematically grounded and scalable solution for secure authentication in dynamic IoT-driven supply chain environments. The contributions of LRA are as follows.

- LRA is a novel blockchain-enabled authentication scheme that integrates adaptive reputation scoring with lightweight cryptographic operations to support IoT-driven e-commerce supply chain workflows.
- LRA reduces false classification rates and improves true positive rates by incorporating dynamic trust evaluation that mitigates biased, manipulated, or incomplete data present in existing reputation models.
- The system achieves optimized throughput under varying transaction loads, outperforming existing models (SPUFCHAIN) in resource-constrained environments.
- LRA is designed to operate effectively across heterogeneous supply chain environments involving multiple retailers, suppliers, and IoT devices, ensuring robustness and adaptability.

II. METHODOLOGY

The LRA system ensures secure and efficient authentication for IoT-driven e-commerce supply chain workflow management, as shown in Figure 1. The system integrates dynamic trust evaluation, historical and stability-aware factors, and blockchain-based decentralized trust management. Unlike conventional certificate-based schemes, LRA is computationally lightweight, scalable to large IoT deployments, and resilient to malicious tampering.

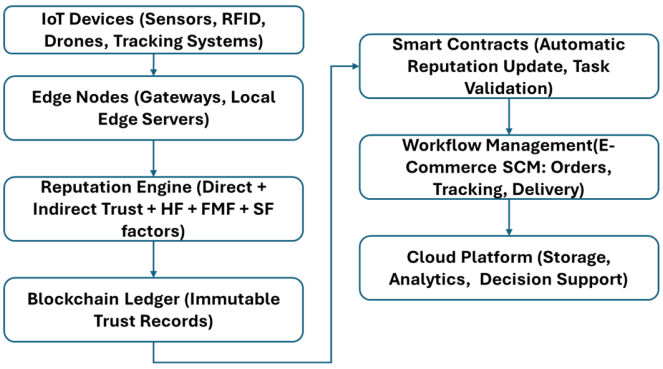

Fig. 1. LRA architecture/flow diagram.

A. *System Model*

In the IoT-enabled supply chain, entities such as smart sensors, RFID readers, delivery partners, drones, edge gateways, and cloud services interact frequently. These devices represent a heterogeneous environment, including low-power sensors (RFID, environmental sensors), edge gateways, mobile delivery nodes (drones and vehicles), and cloud platforms, each with varying computation, memory, and communication capabilities. Each entity is assigned a dynamic trust score that reflects its historical reliability, real-time behavior, and contextual consistency. The LRA model consists of three key components:

- Reputation-based Lightweight Authentication: Trust scores are dynamically calculated based on successful or failed interactions. The scores incorporate: a Historical Factor (HF), which emphasizes long-term behavioral consistency, a Fluctuation Minimization Factor (FMF), which reduces sharp variations in trust due to short-term anomalies, and a Stability Factor (SF), which rewards consistent trustworthy behavior across multiple transactions.
- Direct and Indirect Reputation Estimation: Direct reputation (Ds) is computed based on communication reliability, while indirect reputation (Is) is inferred from neighboring nodes and relationship strength. The final trust score is a weighted fusion of Ds and Is with stabilization.
- Blockchain-based Trust Ledger: Trust scores are stored in a tamper-proof blockchain ledger. Smart contracts automate

updates, validation, and penalization, ensuring transparency, immutability, and consensus.

To ensure suitability for resource-constrained IoT environments, the proposed LRA framework adopts a lightweight authentication strategy by minimizing reliance on computationally intensive cryptographic operations such as public-key certificate validation. Instead, authentication decisions are primarily driven by dynamic reputation scores and blockchain-based hash validation. Unlike traditional schemes that require repeated encryption-decryption cycles, LRA leverages trust thresholds and smart contract verification, significantly reducing computational overhead, communication latency, and memory usage. This lightweight design makes LRA highly efficient and scalable for heterogeneous IoT-enabled e-commerce supply chain environments.

B. Reputation-Based Lightweight Security Threat Model

The proposed system considers a semi-adversarial IoT-enabled e-commerce supply chain environment, where malicious entities may attempt to disrupt workflow operations through spoofing, false data injection, denial-of-service attacks, or reputation manipulation. Adversarial nodes can intermittently behave honestly to gain trust before launching attacks. Additionally, communication channels may be partially compromised, but the underlying blockchain infrastructure remains tamper-resistant. The objective of LRA is to accurately distinguish between legitimate and malicious entities while ensuring secure, reliable, and efficient authentication under dynamic and large-scale network conditions.

1) Direct Security Reputation

For the *x*-th interaction between vehicle/device *v* and edge server *e*, the direct interaction ratio is given as

$$s_{(v,e)}^{x} = \frac{tc_{(v,e)}^{x}}{Tc_{(v,e)}^{x}} \tag{1}$$

where $tc_{(v,e)}^{x}$ is the trusted communication time and $Tc_{(v,e)}^{x}$ is the total communication time. Higher $s_{(v,e)}^{x}$ indicates better security and reliability. The positive reputation score obtained during different supply-chain-related communication between different entities is obtained as

$$Ps_{(v,e)}^{x} = \sum_{x=1}^{X_{v,e}} s_{(v,e)}^{x}\, Q_{(v,e)}^{x} \left(e^{\left(1-s_{(v,e)}^{x}\right)} - 1\right) log\left(\frac{\theta}{t-t_{(v,e)}^{x}} + 1\right) \tag{2}$$

Similarly, the negative reputation score obtained during different supply-chain-related communication between different entities is obtained as

$$Ns_{(v,e)}^{x} = \sum_{x=1}^{X_{v,e}} \left(1 - s_{(v,e)}^{x}\right) Q_{(v,e)}^{x} \left(e^{-s_{(v,e)}^{x}} - 1\right) log\left(\frac{\theta}{t-t_{(v,e)}^{x}} + 1\right) \tag{3}$$

where $Q_{v,e}^{x}$ is a time-constraint parameter computed as

$$Q_{(v,e)}^{x} = t_{req}^{x} - t_{(v,e)}^{x} / t_{(req)}^{x} \tag{4}$$

where θ defines attenuation features considering the reputation decay factor $log\left(\frac{\theta}{t-t_{(v,e)}^{x}} + 1\right)$. The direct reputation, using Bayesian Trust Update, is obtained by

$$Ds_{v,e}^{x} = \frac{Ps_{v,e}+1}{Ps_{(v,e)}+Ns_{(v,e)}+2} \tag{5}$$

This value is further updated dynamically using Bayesian inference

$$RS(j) = P(A|B) = \frac{P(B|A)\times P(A)}{P(B)} \tag{6}$$

where $P(A)$ is prior trust, $P(B|A)$ is reliability under trustworthy conditions, and $P(B)$ is the overall success probability considering the anticipated E of β distribution.

2) Indirect Security Reputation

To ensure a clear integration between direct reputation estimation and the final trust computation, the Bayesian update (6) is applied as a refinement layer over the direct reputation derived in (5). Initially, the direct reputation $Ds_{v,e}^{x}$ is computed using the Beta distribution based on accumulated positive and negative interaction scores. This value represents the prior trust level of a node. Subsequently, in (6) this prior belief is updated by incorporating new interaction evidence, thereby producing a posterior trust estimate that reflects both historical behavior and recent observations. The updated value is then treated as the final direct reputation component. This refined direct trust is combined with the indirect reputation $Is_{(v,e)}$ using the weighted aggregation defined in (14), along with stability-enhancing factors. Therefore, the overall trust computation follows a sequential flow: Interaction → Positive/Negative Scores → Direct Reputation (Beta) → Bayesian Update → Refined Direct Trust → Fusion with Indirect Trust → Final Trust Score. The indirect reputation is computed by

$$Is_{(v,e)} = \frac{\sum_{v'\neq v} Ds_{(v',e)} \cdot r_{(v,v')} \cdot \alpha_{(v',e)}}{\sum_{v'\neq v} \alpha_{(v',e)}} \tag{7}$$

where $r_{(v,v')}$ denotes relationship strength and $\alpha_{(v',e)}$ indicates past interactions represented as a function, given in

$$\alpha = \begin{cases} 1, & v,e \text{ Matched} \\ 0, & v,e \text{ Not Matched} \end{cases} \tag{8}$$

The relationship among different ESCM entities is defined as a matrix:

$$R = \begin{bmatrix} r_{1,1} & \cdots & r_{1,V} \\ \vdots & \cdots & \vdots \\ r_{V,1} & \cdots & r_{V,V} \end{bmatrix} s.t. 0 \le r_{v,v'} \le 1, 1 \le v \le \tag{9}$$

The relationship strength in (7) is obtained using

$$r_{v,v'} = \eta M_{SI}^{(v,v')} + (1-\eta) M_{PS}^{(v,v')} \tag{10}$$

where η defines the weight optimization parameter according to the ESCM requirement. $M_{SI}^{(v,v')}$ defines Jaccard similarity of social/communication links, measured as

$$M_{SI}^{(v,v')} = \frac{\left|JC_{v_i} \cap JC_j\right|}{JC_{v_i} \cup JC_{v_j}} \tag{11}$$

In (10), $M_{PS}^{(v,v')}$ defines preference similarity, which is measured as

$$M_{PS}^{v_i,v_j} = \frac{\Sigma_{k=1}^{D} \phi_{v_i,v_j}(d_k)}{D} \quad (12)$$

where $\phi_{v_i,v_j}(d_k)$ is a binary flag to measure similarity within d_k, measured as

$$\phi_{(v_i,v_j)}(d_k) = \begin{cases} 1, & \left|p_{v_i,d_k} - p_{(v_j,d_k)}\right| \leq \sigma_{ij} \\ 0, & \text{Otherwise} \end{cases} \quad (13)$$

The Final Security Reputation Score with stability factors is measured as

$$s_{(v,e)} = \varphi_{(v,e)} \cdot Ds_{(v,e)} + \left(1 - \varphi_{(v,e)}\right) \cdot Is_{(v,e)} + HF + FMF + SF \quad (14)$$

where $\varphi_{v,e}$ defines the weight assigned to optimize the direct and indirect security, HF, FMF, and SF. Here, $\varphi_{v,e} \in [0.5, 1]$ assigns higher priority to direct reputation (Ds) over indirect reputation (Is), while $\eta \in [0, 1]$ balances similarity and connectivity in relationship computation. These parameters are experimentally tuned for optimal performance.

C. Blockchain-Based Trust Management

This work employs the following functions to perform blockchain-based trust management for ESCM.

- Immutable Reputation Ledger: Each interaction's trust update is stored on the blockchain, ensuring transparency and tamper-proof trust management.
- Smart Contracts automate reputation updates, enforce penalties for malicious behavior, and trigger workflow permissions only for nodes above the trust threshold.
- Dynamic Credit Score Update: Successful transactions increase score, while malicious/failed interactions decrease score. The threshold ensures malicious nodes are blacklisted.
- The Execution step involves collecting and storing interaction data, building ecommerce network graphs per time window, computing Jaccard similarity and stability indices, updating trust score via Bayesian inference, and executing updates through smart contracts.

D. Computational and Communication Overhead Analysis

The computational complexity of the proposed LRA framework is significantly lower than traditional blockchain-based authentication schemes. The primary operations involve lightweight trust score updates, Bayesian inference, and simple aggregation functions, resulting in an approximate complexity of $O(N)$ per interaction cycle, where N represents the number of interacting nodes. In contrast, conventional schemes require expensive cryptographic operations such as key generation, encryption, and certificate validation. From a communication perspective, LRA reduces overhead by transmitting only trust scores and interaction summaries instead of full authentication credentials. Additionally, blockchain interactions are optimized through batch updates and smart contract execution, minimizing network congestion. These characteristics collectively ensure that LRA maintains low latency, reduced bandwidth consumption, and improved scalability in large-scale IoT-driven supply chain environments.

III. RESULTS AND DISCUSSION

The SPUFChain approach [22] was considered to rigorously assess the proposed Lightweight Reputation-based Authentication (LRA) framework. The evaluation focused on essential security indicators, such as detection accuracy, error rate in classification, and sustained throughput under diverse adversarial scenarios. For threat modeling, the study employed the CIC-IoV 2024 dataset curated by the Canadian Institute for Cybersecurity [23], which provides extensive coverage of contemporary attack vectors relevant to ESCM.

In order to replicate evolving threat landscapes, the proportion of malicious traffic was progressively scaled from 10% to 40% at increments of 10%. Additionally, attack initiation was randomized across different simulation runs, ensuring that temporal variations in intrusion attempts were adequately reflected. Both LRA and SPUFCHAIN implementations were realized on the SIMITS platform [24], a C#-based simulator that was further augmented with blockchain components from the IoTSim-Osmosis toolkit [25]. This integrated testbed enabled precise modeling of distributed authentication, reputation-driven trust computation, and privacy-preserving interactions in federated ESCM ecosystems.

The comparative analysis highlights that the LRA framework consistently achieves higher detection efficiency, reduced misclassification, and improved throughput compared with SPUFCHAIN, particularly under intensified and delayed attack scenarios. These findings substantiate the adaptability, resilience, and scalability of the proposed reputation-based mechanism, positioning it as a robust solution for safeguarding e-commerce supply chains against a spectrum of IoV-enabled cyber threats.

A. True Positive Rate (TPR)

TPR measures the percentage of actual malicious activities accurately detected; higher values signify stronger detection capability. Figure 2 illustrates the variation of the TPR for the proposed LRA model against the baseline SPUFCHAIN under increasing adversarial traffic (10–40%). As the percentage of malicious traffic increases, SPUFCHAIN's detection capability declines significantly, reaching only 54% TPR at 40% adversarial load, whereas the LRA framework sustains a TPR of 68% under the same conditions. This corresponds to a 25.9% improvement in detection accuracy, demonstrating the robustness of LRA in handling dynamic and high-volume threats within e-commerce supply chains. The enhancement arises from LRA's adaptive trust evaluation, which combines historical feedback and distributed consensus to better distinguish legitimate from adversarial activity. Figure 3 highlights the scalability of both models by plotting TPR against varying node density (100–200 nodes). SPUFCHAIN shows a declining trend, from 63% TPR at 100 nodes to 54% at 200 nodes, reflecting its vulnerability to increased network complexity. In contrast, LRA consistently outperforms SPUFCHAIN, improving from 75% to 68% TPR across the

same range of nodes. At the highest density, LRA achieves a 25.9% higher detection accuracy compared to SPUFCHAIN, confirming its ability to maintain resilience in larger federated e-commerce networks. Together, these results validate that LRA offers significantly stronger detection capability and scalability compared to traditional blockchain-based authentication schemes.

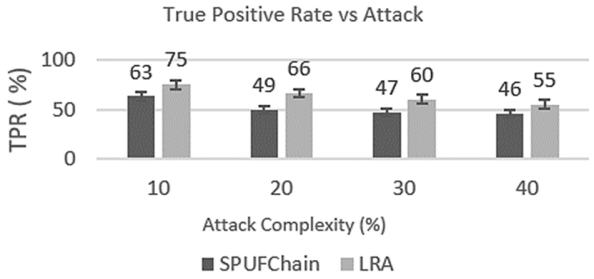

Fig. 2. TPR vs varied attack percentage.

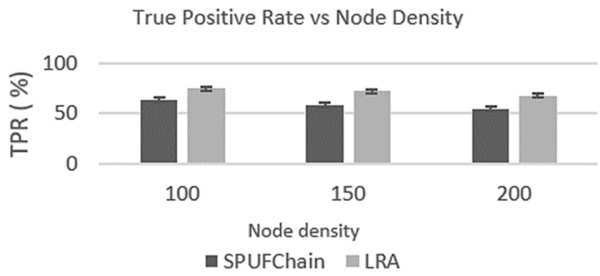

Fig. 3. TPR vs varied node density.

B. False Classification Rate (FCR)

FCR represents the proportion of benign interactions incorrectly flagged as malicious; lower values indicate better reliability. Figure 4 presents the variation of FCR for the proposed LRA model compared to the existing SPUFCHAIN under different adversarial conditions ranging from 10% to 40%. It can be observed that SPUFCHAIN suffers from relatively higher misclassification, with its FCR increasing from 37% at 10% attacks to 55% at 40% attacks. On the other hand, LRA achieves lower misclassification levels, improving from 26% at 10% attacks to 45% at 40% attacks. This demonstrates that LRA achieves around 18–24% reduction in FCR depending on the attack intensity, confirming its ability to limit false decisions even when adversarial traffic grows. The improvements are attributed to the integration of historical stability factors, Bayesian inference, and blockchain-ledger validation that collectively minimize false positives. Figure 5 highlights the performance of both approaches under varying node sizes ranging from 100 to 200 nodes. The results reveal that SPUFCHAIN's FCR increases with scale, rising from 37% at 100 nodes to 46% at 200 nodes, reflecting its sensitivity to large-scale environments. In comparison, the proposed LRA model consistently maintains a lower FCR, ranging from 25% at 100 nodes to 32% at 200 nodes. This signifies a 27–30% reduction in misclassification over SPUFCHAIN, confirming that LRA can scale effectively while maintaining reliability. Collectively, Figures 4 and 5 confirm that the proposed LRA framework not only improves detection capability but also ensures robust scalability with consistently lower false classification rates across diverse operational settings.

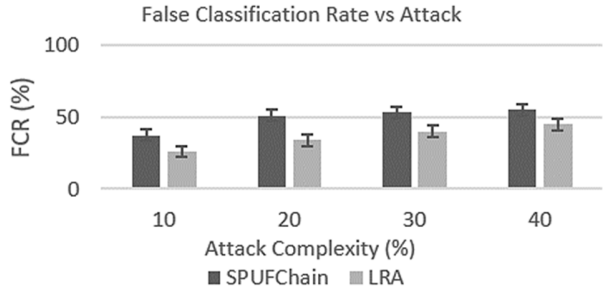

Fig. 4. FCR vs varied attack percentage.

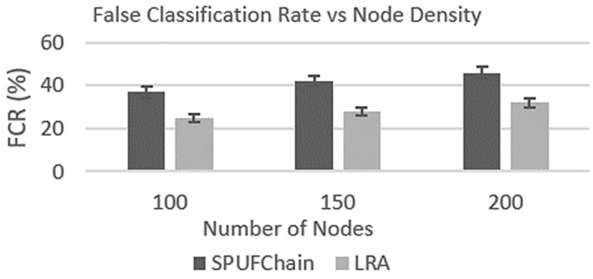

Fig. 5. FCR vs varied node size.

C. Throughput Efficiency

Throughput efficiency reflects the ratio of successfully transmitted legitimate packets to total packets; higher values show improved communication efficiency under adversarial load. Figure 6 demonstrates the variation of throughput efficiency under adversarial traffic ranging from 10 to 40%. The SPUFCHAIN model showed a rapid degradation, where throughput decreases from 0.4662 at 10% attacks to only 0.1012 at 40%. In contrast, LRA consistently maintained higher throughput levels, starting at 0.555 under 10% attacks and sustaining 0.121 at 40%. This corresponds to an improvement margin of approximately 18–28%, highlighting LRA's ability to preserve communication efficiency even when malicious traffic intensifies. Such resilience is achieved through the integration of blockchain-based consensus validation and dynamic reputation scoring, which collectively ensure efficient packet transmission with minimal disruption from adversarial nodes. Figure 7 presents the FCR performance under varied network sizes from 100 to 200 nodes. SPUFCHAIN shows a steady increase in FCR, rising from 37% at 100 nodes to 46% at 200 nodes, indicating its reduced reliability in large-scale deployments. In contrast, LRA maintained a significantly lower FCR, ranging from 25 to 32% across the same node sizes. This reduction of nearly 27–30% in misclassification clearly demonstrates that LRA scales more effectively than SPUFCHAIN. These findings confirm that the proposed model not only enhances throughput efficiency under adversarial traffic but also reduces false classification in larger networks, making it a robust and scalable solution for securing e-commerce supply chain management systems.

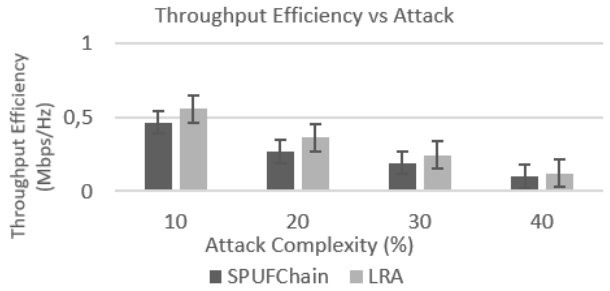

Fig. 6. Throughput efficiency vs varied attack percentage.

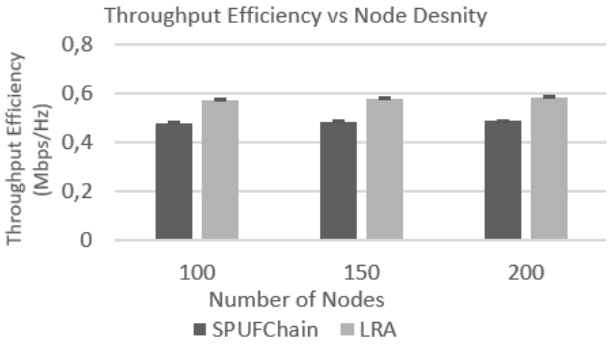

Fig. 7. Throughput efficiency vs varied node size.

D. Energy Efficiency

The energy consumption results in Table I indicate that the proposed LRA model consistently outperforms SPUFChain across varying attack intensities and node densities. On average, LRA achieves approximately 25 to 30% reduction in energy usage, owing to its lightweight reputation-based authentication and reduced reliance on computationally expensive cryptographic operations. By leveraging dynamic trust evaluation and blockchain-assisted validation, LRA minimizes redundant communication and processing overhead. As attack levels and network size increase, SPUFChain shows a significant increase in energy consumption due to repeated verification processes, whereas LRA maintains a more stable and controlled growth. These findings confirm that LRA is highly suitable for resource-constrained IoT environments, ensuring scalable, energy-efficient, and secure workflow management in e-commerce supply chain systems.

TABLE I. ENERGY CONSUMPTION COMPARISON UNDER VARYING ATTACK AND NODE CONDITIONS (JOULES/TRANSACTION)

Condition	SPUFChain (J)	LRA (J)
Attack % = 10	0.92	0.68
Attack % = 20	1.15	0.79
Attack % = 30	1.34	0.91
Attack % = 40	1.58	1.05
Nodes = 100	0.95	0.70
Nodes = 150	1.21	0.84
Nodes = 200	1.49	1.02
Average	1.22	0.85

To further emphasize the effectiveness and novelty of the proposed LRA framework, a detailed comparison with SPUFCHAIN was incorporated across key dimensions, including trust computation (Bayesian-based dynamic reputation vs. static trust evaluation), authentication overhead (lightweight reputation-driven validation vs. cryptographic certificate-based verification), scalability (adaptive performance under increasing node density), and performance metrics (FCR, TPR, throughput, and energy efficiency). Unlike SPUFCHAIN, LRA integrates dynamic reputation evaluation with Bayesian inference and stability-aware factors, enabling more adaptive and efficient decision-making. The experimental results demonstrate that LRA consistently achieves lower FCR, higher TPR, improved throughput, and reduced energy consumption, validating its suitability for resource-constrained IoT-enabled e-commerce supply chain environments.

E. Ablation and Statistical Validation Study

To evaluate the contribution of individual components in the proposed LRA framework, an ablation study was conducted by selectively removing key factors, namely HF, FMF, and SF. The analysis measures their impact on FCR, TPR, throughput, and energy consumption (J per transaction) under identical experimental conditions.

TABLE II. ABLATION STUDY OF LRA COMPONENTS WITH ENERGY ANALYSIS

Model variant	FCR (%) ↓	TPR (%) ↑	Throughput ↑	Energy (J) ↓
LRA (HF+FMF+SF)	28.33	71.66	0.5796	0.85
LRA – HF	32.14	68.21	0.5612	0.94
LRA – FMF	34.02	66.87	0.5489	0.98
LRA – SF	33.27	67.45	0.5521	0.96
LRA – (HF + FMF)	36.85	63.92	0.5314	1.08
LRA – (HF + SF)	35.76	64.88	0.5386	1.05
LRA – (FMF + SF)	37.12	62.75	0.5263	1.12

The results in Table II demonstrate that each component significantly contributes to both performance and energy efficiency. The complete LRA model achieves the lowest FCR, highest TPR, maximum throughput, and minimum energy consumption. Removing HF increases misclassification due to loss of historical consistency, while excluding FMF introduces fluctuations in trust updates, leading to higher energy usage and reduced detection performance. Similarly, removing SF affects long-term trust stability. Notably, eliminating multiple components results in a substantial increase in energy consumption (up to ~30%), highlighting the role of these factors in minimizing redundant computations and communication overhead. To ensure robustness, experiments were repeated across multiple runs. The results show low variance (standard deviation < 2.5%) across all metrics. Statistical significance testing ($p < 0.05$) confirms that the performance and energy improvements of the full LRA model over ablated variants are meaningful and consistent. The ablation study confirms that HF, FMF, and SF jointly enhance detection accuracy, reduce misclassification, stabilize trust evaluation, and minimize energy consumption, making LRA a comprehensive and efficient solution for IoT-based e-commerce supply chain security.

IV. CONCLUSION

The evaluation of the proposed LRA framework against SPUFCHAIN demonstrates consistent improvements across detection, efficiency, and energy performance. LRA improves throughput by approximately 18–28% under varying attack levels, ensuring stable communication. FCR is reduced by around 27–30%, while TPR increases by 15–20%, confirming enhanced detection capability. In addition, the incorporated energy analysis shows that LRA reduces energy consumption by nearly 25–30%, validating its suitability for resource-constrained IoT environments. These gains are achieved through lightweight authentication, Bayesian trust modeling, and stability-aware reputation computation. The results confirm that LRA provides a scalable, efficient, and secure solution for IoT-enabled e-commerce supply chains. Future work will include detailed Joules-per-transaction analysis, advanced threat modeling, and real-world deployment across heterogeneous IoT ecosystems.

DECLARATION OF COMPETING INTERESTS

The authors declare that they have no known competing financial interests, personal relationships, or affiliations that could have appeared to influence the work reported in this paper.

ACKNOWLEDGMENT

The authors acknowledge the Canadian Institute for Cybersecurity for making the CICIoV2024 dataset publicly available for research purposes [26].

DATA AVAILABILITY

The dataset used in this study is publicly available through the Canadian Institute for Cybersecurity [26]. The data used in this work were obtained and utilized in accordance with the dataset usage policy.

AI USE AND DECLARATION OF GENERATIVE AI USE

During the preparation of this work, the authors used Grammarly AI for language refinement, grammar correction, and improving the readability of the manuscript. After using this tool, the authors carefully reviewed and edited the content as needed and take full responsibility.

REFERENCES

[1] B. Annane, A. Alti, and A. Lakehal, "A Blockchain Semantic-based Approach for Secure and Traceable Agri-Food Supply Chain," *Engineering, Technology & Applied Science Research*, vol. 14, no. 6, pp. 18131–18137, Dec. 2024, https://doi.org/10.48084/etasr.8908.

[2] N. N. Abdullah and N. H. S. Alani, "Blockchain adoption in the supply chain: Enablers, barriers, and opportunities from a systematic review," *Sustainable Futures*, vol. 10, Dec. 2025, Art. no. 101429, https://doi.org/10.1016/j.sftr.2025.101429.

[3] R. M. Alhazmi, "Blockchain-Enabled Digital Transformation in Pharmaceutical Cold Chain Management Using Hybrid Deep Neural Networks," *Engineering, Technology & Applied Science Research*, vol. 15, no. 6, pp. 28591–28595, Dec. 2025, https://doi.org/10.48084/etasr.13320.

[4] R. Rajavel, L. Krishnasamy, P. Nagappan, U. Moorthy, and S. V. Easwaramoorthy, "Cloud-enabled e-commerce negotiation framework using bayesian-based adaptive probabilistic trust management model," *Scientific Reports*, vol. 15, no. 1, Mar. 2025, Art. no. 9457, https://doi.org/10.1038/s41598-025-92643-z.

[5] D. Kumar *et al.*, "AI-Powered Security for IoT Ecosystems: A Hybrid Deep Learning Approach to Anomaly Detection," *Journal of Cybersecurity and Privacy*, vol. 5, no. 4, Oct. 2025, Art. no. 90, https://doi.org/10.3390/jcp5040090.

[6] Y. Zuo, "Exploring the Synergy: AI Enhancing Blockchain, Blockchain Empowering AI, and Their Convergence Across IoT Applications and Beyond," *IEEE Internet of Things Journal*, vol. 12, no. 6, pp. 6171–6195, Mar. 2025, https://doi.org/10.1109/JIOT.2024.3507746.

[7] O. Oloko, "Dynamic Route Optimization in Last-Mile Delivery Using Predictive Analytics: A Case Study of E-commerce in the U.S.," *European Journal of Logistics, Purchasing and Supply Chain Management*, vol. 12, no. 3, pp. 1–32, 2025, https://doi.org/10.37745/ejlpscm.2013/vol12n3132.

[8] Q. Wu, Y. Lei, L. Zhang, X. Dong, and F. Rezaeibagha, "Traceable and Verifiable Authorized Cloud-Assisted PSI-CA Protocol for Blockchain-Enabled Intelligent Logistics," *IEEE Internet of Things Journal*, vol. 12, no. 17, pp. 36451–36470, Sept. 2025, https://doi.org/10.1109/JIOT.2025.3582283.

[9] M. Cheng, B. Shen, and H. L. Chan, "Implementing Artificial Intelligence Consumer Experience Tools in Supply Chains," *IEEE Transactions on Engineering Management*, vol. 72, pp. 717–729, 2025, https://doi.org/10.1109/TEM.2024.3525412.

[10] S. Qi, Y. Li, W. Wei, Q. Li, K. Qiao, and Y. Qi, "Truth: A Blockchain-Aided Secure Reputation System With Genuine Feedbacks," *IEEE Transactions on Engineering Management*, vol. 71, pp. 12433–12447, 2024, https://doi.org/10.1109/TEM.2021.3128930.

[11] Z. Zhou, M. Wang, Z. Ni, Z. Xia, and B. B. Gupta, "Reliable and Sustainable Product Evaluation Management System Based on Blockchain," *IEEE Transactions on Engineering Management*, vol. 71, pp. 12259–12271, 2024, https://doi.org/10.1109/TEM.2021.3131583.

[12] F. Chen, H. Zhang, T. Xiang, and J. K. Liu, "A Two-Stage Approach for Fair Data Trading Based on Blockchain," *IEEE Transactions on Information Forensics and Security*, vol. 19, pp. 9835–9849, 2024, https://doi.org/10.1109/TIFS.2024.3482716.

[13] G. Li, H. Wu, J. Wu, and Z. Li, "Efficient and secure privacy protection scheme and consensus mechanism in MEC enabled e-commerce consortium blockchain," *Journal of Cloud Computing*, vol. 13, no. 1, May 2024, Art. no. 97, https://doi.org/10.1186/s13677-024-00652-6.

[14] T. Jiang, X. Yuan, Q. Cheng, Y. Shen, L. Wang, and J. Ma, "FairECom: Towards Proof of E-Commerce Fairness Against Price Discrimination," *IEEE Transactions on Dependable and Secure Computing*, vol. 21, no. 4, pp. 3528–3544, July 2024, https://doi.org/10.1109/TDSC.2023.3334197.

[15] M. Qiao, X. Chen, Y. Zhou, and P. Y. Mok, "Blockchain-driven innovation in fashion supply chain contractual party evaluations as an emerging collaboration model," *Blockchain: Research and Applications*, vol. 6, no. 2, June 2025, Art. no. 100266, https://doi.org/10.1016/j.bcra.2024.100266.

[16] N. Wan, J. Fan, and X. Wu, "The Cost-sharing Mechanism for Blockchain Technology Adoption in the Platform-led E-commerce Supply Chain," *Journal of Systems Science and Systems Engineering*, vol. 34, no. 2, pp. 156–179, Apr. 2025, https://doi.org/10.1007/s11518-025-5640-5.

[17] S. Kumar, S. Pandey, and U. Bhatt, "On Enhancing E-Commerce Shipping Policies with Blockchain and Recommender Systems," *SN Computer Science*, vol. 6, no. 2, Feb. 2025, Art. no. 145, https://doi.org/10.1007/s42979-025-03687-x.

[18] R. Zhang, Y. Li, and L. Fang, "PBTMS: A Blockchain-Based Privacy-Preserving System for Reliable and Efficient E-Commerce," *Electronics*, vol. 14, no. 6, Mar. 2025, Art. no. 1177, https://doi.org/10.3390/electronics14061177.

[19] Y. Liu, S. Zhang, and Y. Ma, "Automated Runtime Verification of Security for E-Commerce Smart Contracts," *Journal of Theoretical and Applied Electronic Commerce Research*, vol. 20, no. 2, Apr. 2025, Art. no. 73, https://doi.org/10.3390/jtaer20020073.

[20] Md. I. Alam, S. Sahoo, S. Sharma, and A. Verma, "Barterchain: a blockchain-based barter system in smart cities," *Digital Finance*, vol. 7, no. 4, pp. 871–900, Dec. 2025, https://doi.org/10.1007/s42521-025-00133-8.

[21] L. Wu, C. Duan, and Q. Ji, "Manufacturer Strategies for Blockchain Adoption and Sales Mode Selection with a Dual-Purpose Platform," *Systems*, vol. 13, no. 6, June 2025, Art. no. 458, https://doi.org/10.3390/systems13060458.

[22] M. I. S. Assaqty *et al.*, "SPUFChain: Permissioned Blockchain Lightweight Authentication Scheme for Supply Chain Management Using PUF of IoT," *IEEE Access*, vol. 13, pp. 88662–88682, 2025, https://doi.org/10.1109/ACCESS.2025.3566478.

[23] E. C. P. Neto *et al.*, "CICIoV2024: Advancing realistic IDS approaches against DoS and spoofing attack in IoV CAN bus," *Internet of Things*, vol. 26, July 2024, Art. no. 101209, https://doi.org/10.1016/j.iot.2024.101209.

[24] F. Hrizi and F. Filali, "simITS: an integrated and realistic simulation platform for vehicular networks," in *Proceedings of the 6th International Wireless Communications and Mobile Computing Conference*, June 2010, pp. 32–36, https://doi.org/10.1145/1815396.1815404.

[25] K. Alwasel *et al.*, "IoTSim-Osmosis: A framework for modeling and simulating IoT applications over an edge-cloud continuum," *Journal of Systems Architecture*, vol. 116, June 2021, Art. no. 101956, https://doi.org/10.1016/j.sysarc.2020.101956.

[26] "IoV Dataset 2024.' Canadian Institute for Cybersecurity, [Online]. Available: https://www.unb.ca/cic/datasets/iov-dataset-2024.html.