IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 12, May 2026
Impact Factor: 8.2

Preventing Data Tampering in Block chain: Leveraging Hybrid Forensics and Multiparty Computation in Supply Chain

Supriya Mane[1], Rajaram Ambole[2]
Comp (AI & DS), Vidya Pratishthan's Kamalnayan Bajaj Institute of Engineering and Technology, Pune, India[12]
manesupriya1305@gmail.com1 rajaram.ambole@vpkbiet.org2

Abstract: *Supply chains involve many companies and people working together to move products from manufacturers to customers. Keeping the data in these supply chains accurate and safe from tampering is a big challenge today. Blockchain technology works like a shared digital notebook that many people can see but no one can secretly change thus making it a popular tool for tracking products. However, even blockchain systems can be attacked or manipulated, especially when data is first entered into the system or when insiders try to cheat. In this paper, we review two powerful techniques that can make blockchain supply chains much more secure. The first is hybrid forensics which is a method that combines different investigation tools to detect when something goes wrong and collect digital evidence, just like a detective investigating a crime scene. The second is Multi-Party Computation (MPC) such as a technique that allows multiple companies to share and verify information with each other without actually revealing their private business data, similar to solving a puzzle together without showing your own puzzle pieces.*

Keywords: Blockchain, Supply Chain Security, Data Tampering Prevention, Hybrid Blockchain Architecture, Multi- Party Computation (MPC), Digital Forensics, Privacy-Preserving Verification, Cross-Chain Forensics, Tamper Detection.

I. INTRODUCTION

Supply chain consists of various parties involved from supplier, manufacturer, distributor, and retailer and so on, until the product reaches the customer. They all have to work together efficiently in order to deliver quality product on time. In a distributed system as this, reliability and veracity of data become critical issue to run the system profitably. Loss due to tampering or incorrect data entry can cause significant financial losses to company, impact on product quality, damage customer loyalty and non-compliance to various regulations [1], [2]. Globalized supply chain with huge involvement of digital technologies, has become an attractive target for cyber criminals, counterfeits, data manipulators and so on.

The Blockchain technology can be used to build reliable information systems. Information can be stored in a transparent, traceable and honest way to manage goods in flow. From a technical point of view information is stored on decentralized digital ledgers which cannot be tampered with. Records of transactions are protected by hashing and verified by nodes of a decentralized network. Beside the benefits for the traceability of products in flow and the dissuasion from counterfeiting, there are some specific limitations to the practical application of this technology. Most importantly there is no full end-to-end data security. The major weakness of the blockchain technology is its dependence on off-chain data sources. However, the data captured from the sources like Internet of Things (IoT), Radio Frequency Identification (RFID) and human interventions may be compromised before it is actually written into the blockchain.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 12, May 2026 Impact Factor: 8.2

This article focuses on the immutability feature of blockchain technology, as well as its limitations related to real-time tamper detection and forensic analysis to track data breaches. Moreover, we discuss the violations of data origin authenticity, timing, and integrity. When it comes to implementing a blockchain-based supply chain, another key issue is privacy. Companies are often hesitant to reveal sensitive details of business operations such as pricing, current inventory levels or even the finer details of their proprietary processes, due to competitive or regulatory reasons [8]. While permissioned blockchain models can be set up with access control to some extent, there are still many issues with data privacy during verification and auditing processes. With the growing trend of supply chain ecosystems that are made up of hybrid and cross-chain structures, there are even more opportunities for data breaches, as well as interoperability and verification inconsistencies.

To overcome these challenges, recent research has focused on integrating blockchain with complementary technologies such as digital forensics and secure Multi-Party Computation (MPC). Digital forensics enables systematic monitoring, tamper detection, and evidence preservation by analyzing both on-chain and off-chain data [9]. MPC, on the other hand, allows multiple stakeholders to collaboratively verify computations on sensitive data without revealing their private inputs, thereby ensuring confidentiality while maintaining trust [10].

II. METHODOLOGY

To tackle data tampering in blockchain-based supply chains, we present a novel methodology for preventing and detecting data frauds using hybrid digital forensics and Multi-Party Computation (MPC). The methodology leverages techniques to guarantee data integrity and privacy and to track changes along the different stages of the supply chain lifecycle.

A. Overall Methodological Framework

This paper presents a methodology that consists of five stages, namely, data acquisition, privacy-preserving verification, blockchain recording, hybrid forensic monitoring, and audit analysis. These stages tackle the vulnerabilities that exist in traditional supply chain management methods, particularly, off-chain data tampering, privacy leakage, and lack of forensic capability. The framework adopts a **hybrid blockchain architecture**, combining permissioned and public blockchain. Sensitive transactional and operational data are handled within a permissioned blockchain to maintain confidentiality, while cryptographic proofs and verification hashes are anchored to a public blockchain to ensure transparency and auditability.

B. Privacy-Preserving Verification Using Multi-Party Computation

To address privacy in a scenario involving mutually untrusted parties, our methodology utilizes secure Multi-Party Computation (MPC). Pricing, inventory and other proprietary operational data are never shared between parties and are never stored in plaintext on the blockchain. MPC is not used here to hide user input but rather to privately compute over user input. Input is first split among computation nodes. Joint computation (e.g., transaction validation, compliance check, summing) is then performed on those shares without ever revealing the input. Only the final verified outcome or cryptographic proof is shared and recorded, ensuring both correctness and confidentiality.

III. LITERATURE REVIEW

A. Blockchain in Supply Chain Management

With growing adoption in supply chain management, blockchain promises decentralized, immutable, and transparent data management. Crosby et al. (2016) in particular demonstrated how blockchain uses cryptographic hashing and distributed consensus mechanisms to guarantee integrity of stored data. Saberi et al. (2017) also noted the importance of blockchain-driven transparency to build trust among stakeholders in supply chains. However, these studies primarily focus on transparency and fail to address **data correctness at the source**, making blockchain vulnerable to tampering before data is recorded.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 12, May 2026
Impact Factor: 8.2

B. IoT-Integrated Blockchain Systems

While there are some existing researches on integrating blockchain into IoT to support real-time monitoring, most of them have not fully addressed the potential issues of using IoT sensors in monitoring settings. For example, Dorri et al. [4] Proposed a blockchain framework for IoT security and sharing data among authorized parties, enhancing data transparency and exchange efficiency. However, they assumed that sensor reading is always reliable and trustworthy.

C. Insider Attacks and Smart Contract Vulnerabilities

Insider threats remain a significant challenge in permissioned blockchain. Conti et al. [6] demonstrated that authorized users can manipulate blockchain transactions without detection. Additionally, Atzei et al. [7] analyzed vulnerabilities in smart contracts, such as logic flaws and reentrancy attacks, which may result in unauthorized data manipulation. Existing blockchain systems lack **forensic auditing tools** to analyze such incidents.

D. Privacy-Preserving Techniques Using MPC

There is a growing interest in ensuring privacy in supply chains. From a technical perspective, one approach to achieve privacy is based on Multi-Party Computation (MPC). MPC was first studied by Goldreich and later other studies followed. It is based on allowing several parties to jointly compute a function of their private data without divulging their input. Since the last two years, researchers have started to combine MPC with blockchain, exploring the combination to further strengthen privacy.

TABLE I: Literature Review

Sr.No	Paper Name and Year	Techniques Used	Advantages	Gaps
1.	Blockchain-Based Anti-Counterfeiting in Supply Chains (2019)	Blockchain with Physically Unclonable Functions (PUFs)	Ensures product authenticity and reduces counterfeiting	Lacks digital forensics and privacy-preserving verification
2.	Secure IoT Data Collection Using Blockchain (2021)	Trusted Execution Environment (TEE) with blockchain	Protects sensor Data before blockchain entry	No forensic analysis or cross-stakeholder Verification.
3.	Privacy-Preserving Blockchain Transactions (2021)	Multi-Party Computation (MPC)	Strong confidentiality of sensitive data	High computational overhead; no real-time tamper detection
4.	Multi-Tier Blockchain Architecture for Supply Chains (2020)	Multi-tier blockchain framework	Improves transparency and coordination	No tamper detection or forensic mechanisms
5.	Blockchain-Based Digital Forensics: A Review (2024)	Systematic review of forensic techniques	Identifies challenges and research directions	Limited focus on supply chain privacy and MPC
6.	Forensic Cross: Cross-Chain Blockchain Forensics (2024)	Cross-chain forensic framework	Enables evidence collection across blockchains	No MPC integration; limited real-time detection.
7.	Blockchain-Based Product Verification System (2024)	Barcode-based blockchain tracking	Improves product verification accuracy	Lacks forensic support and privacy mechanisms.
8.	Privacy and Security Enhancement in Blockchain Systems (2021)	MPC and homomorphy encryption	Provides high data confidentiality	Not tailored for supply chain tamper detection

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 12, May 2026 Impact Factor: 8.2

9.	Blockchain-Based Food Safety and Traceability (2020)	Hyperledger Fabric with IoT sensors	Improves transparency and food safety	No tamper detection or privacy-preserving verification
10.	IoT-Enabled Blockchain for Food Supply Chains (2025)	IoT-integrated blockchain	Enhances traceability and real-time monitoring	Assumes trusted sensor data; no forensic validation
11.	Zhou et al. (2021): "Privacy-Preserving Blockchain via Multi-Party Computation"	Multi-Party Computation (MPC)	Strong privacy preservation for sensitive blockchain data	High computational overhead; no real-time tamper detection
12.	Atlam et al. (2024): "Digital Forensics in Blockchain-based Systems"	Blockchain-based digital forensic review	Identified challenges and future research directions	Limited focus on privacy-preserving supply chain forensics
13.	Chen et al. (2021): "Smart Contract-based Traceability in Blockchain Supply Chains"	Smart contract-based traceability	Automated verification and reduced human errors	Vulnerable to contract bugs; no tamper alerts
14	Salvankar et al. (2024): "Barcode-based Blockchain for Product Tracking"	Barcode-based blockchain tracking	Improved product verification	Lacks forensic mechanisms and privacy support
15	Singh et al. (2022): "AI-based Anomaly Detection on Blockchain IoT Networks"	Blockchain with AI-based anomaly detection	Detects suspicious activity in real-time	High computational cost; limited IoT integration

IV. Discussion and Findings

A. Effectiveness of Blockchain for Data Integrity

Research clearly shows that blockchain is a reliable tool for keeping supply chain data accurate and traceable. It uses cryptographic hashing and distributed consensus mechanisms to ensure that once data is recorded, it cannot be secretly changed and can always be audited [1], [2]. However, several studies point out an important weakness blockchain cannot guarantee that the data entered into it is correct in the first place, especially when it comes from IoT devices or is manually entered by authorized users [3]. This means that while blockchain protects data after it is recorded, it cannot fully stop tampering or errors at the point where data is originally created or entered.

B. Limitations in Tamper Detection Mechanisms

Even the most prevalent blockchain-based supply chain applications have a major vulnerability, real-time tamper detection. Although information stored in a blockchain is tamper-proof, this doesn't mean that incorrect or bad information can't be submitted and entered into the system in the first place. As earlier security-related research has discovered, supply chain systems may be vulnerable to insider threats as well as tampering from IoT devices. As a result, there is a clear need for monitoring and a means of conducting forensic analysis that goes beyond traditional blockchain functions.

C. Role of Hybrid Digital Forensics

Hybrid digital forensics, which combines **on-chain transaction analysis with off-chain log and metadata analysis**, has been identified as an effective approach for detecting anomalies and unauthorized activities [10]. Forensic readiness improves accountability by enabling evidence collection and post-incident investigation. However, existing

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 12, May 2026
Impact Factor: 8.2

forensic frameworks are mostly reactive and **do not incorporate privacy-preserving verification**, limiting their applicability in sensitive supply chain environments [11].

D. Need for Integrated Forensics and MPC

A major finding of this review is that existing solutions address **forensics and privacy independently**, but not in an integrated manner. Blockchain forensic frameworks focus on traceability and evidence collection [10], [11], while MPC-based approaches focus primarily on confidentiality [8], [9]. The absence of a unified approach results in systems that are either transparent but privacy-weak, or private but forensic-weak. This gap strongly motivates the integration of **hybrid forensics with MPC**.

E. Proposed System

The proposed system addresses the limitations of the existing approach by introducing an immutable, decentralized reference (the blockchain) alongside the operational database. Every product record is bound to a cryptographic hash at the time of registration; that hash is stored both in the database and on the blockchain. Later, anyone can verify whether the current record matches the original by recomputing the hash and comparing it to the on-chain value. No single party controls the verification outcome, and the blockchain provides an audit trail that cannot be altered by the database administrator.

A. System Overview

The proposed system is a web-based prototype that registers supply chain products and stores a SHA-256 hash of each record in a SQLite database and on an Ethereum-compatible blockchain via a Solidity smart contract (HashStorage.sol). Users can add products (name, origin, and destination), view all products, edit or delete products from the View Products page, and verify tampering by product ID. The verification module fetches the product from the database, recomputes the hash from the current fields (name, origin, destination, timestamp), retrieves the hash stored on the blockchain for that product ID via getHash(id), and compares the both result Valid or Tampered. Thus, the system leverages hybrid forensics (database + blockchain). An MPC demo allows users to split a secret into three additive shares and reconstruct it, demonstrating that no single share reveals the value. The backend is implemented in Python (Flask, hashlib, Web3.py), the frontend in HTML/CSS/Bootstrap with pages for Home, Add Product, View Products, Verify Tampering, MPC Demo, and About, and the blockchain component in Solidity deployed on Ganache. The flow for demonstrating tampering is: add a product and verify (Valid); then edit the same product on View Products and verify again (Tampered).

B. System Architecture

The system follows a **three-tier architecture**, which separates concerns into presentation, business logic, and data layers. The **presentation tier** is the web frontend: HTML defines structure, CSS (and Bootstrap) defines layout and styling, and JavaScript (**Fetch API**, and **ethers.js** when a wallet is used) sends HTTP requests to the backend and updates the DOM with responses. **Cryptographic hashing of product payloads remains on the server** (deterministic SHA-256 in Flask); the browser wallet is used to **sign and broadcast** storeHash transactions and optionally to read getHash, while read-only verification can still use server-side Web3.py for convenience. The **business logic tier** is the Flask backend: it receives HTTP requests, validates input, orchestrates hashing (via Python's hashlib), database operations (via SQLite3), and blockchain interaction (via Web3.py **and** JSON endpoints that support browser clients, e.g. /wallet_config), and returns HTTP responses with JSON bodies. This tier contains the core algorithms (hash computation, tamper verification, secret sharing).

1) **SQLite**, a file-based relational database that stores the products table (id, name, origin, destination, timestamp, data_hash) and supports SQL queries (INSERT, SELECT, UPDATE, DELETE);

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 12, May 2026
Impact Factor: 8.2

2) The **Ethereum-compatible blockchain** (Ganache), which hosts the HashStorage smart contract whose storage is a mapping from product ID to hash string.

Fig.1. System Architecture

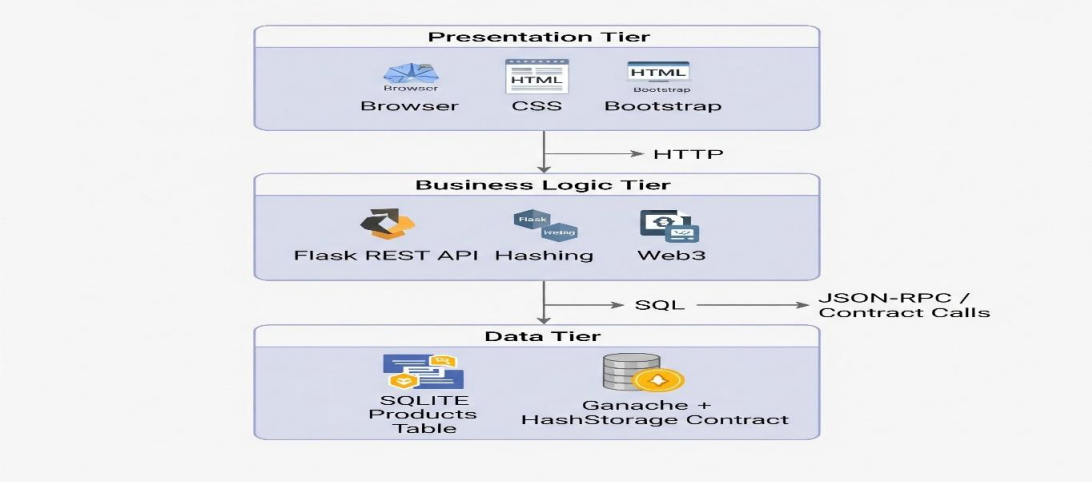
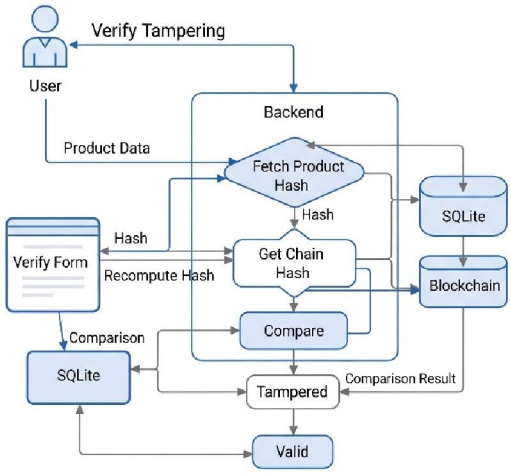


Fig.2. Data Flow Diagram



IV. FUTURE DIRECTIONS

Although the proposed system effectively addresses data tampering and privacy challenges in blockchain-enabled supply chains, several future enhancements can improve its scalability, intelligence, and real-world applicability.

A. AI-Driven Anomaly Detection

In the future, the system could incorporate artificial intelligence and machine learning technologies in order to make the system "smarter" and able to detect unusual or suspicious activity in real time. This is more powerful than typical rule-based systems which rely on a human to define and anticipate a full spectrum of threats. AI/Machine Learning based systems are able to recognize complex patterns of threats including insider threats and even predict potential threats before they occur. Cross-Chain and Interoperable Forensics. As supply chains increasingly operate across multiple blockchain platforms, future research should focus on cross-chain forensic frameworks. Interoperable forensic

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 12, May 2026 Impact Factor: 8.2

mechanisms can enable evidence collection, correlation, and verification across heterogeneous blockchains, improving investigation capabilities in multi-network environments.

B. Optimization of MPC Protocols

Supply chains are increasingly leveraging multiple blockchain platforms. Thus, future work needs to focus on designing forensic tools to collect evidence (and prove its authenticity) that are interoperable with various blockchain systems at the same time, in order to support investigations more effectively. Automated Forensic Response and Smart Contracts.

C. Regulatory Compliance and Standardization

Although existing MPC systems, such as MPCs for private data processing, are robust at privacy protection, they suffer from insufficient computational efficiency including large processing time and power consumption. In order to realize practical MPC for large-scale supply chain management, improving the system to be faster and more efficient is necessary.

D. Automated Forensic Response and Smart Contracts

Smart Contracts for Automatic Investigation But there are even more interesting possibilities. Automation of threat response using smart contracts can be another promising future direction. Smart contracts can automatically send an alert, freeze assets, or even begin an investigation without human intervention. Automation can greatly reduce the time needed to respond to an incident, thereby minimizing potential damage.

V. CONCLUSION

To address the challenge of data tampering in blockchain-based supply chains, in this paper, we propose a comprehensive solution that incorporates hybrid digital forensics with Multi-Party Computation (MPC). The hybrid digital forensics module incorporates in-depth analysis to monitor the blockchain and identify anomalies, detect any unwanted modification, and discover potential adversarial behavior. Meanwhile, MPC protocols are used to enable multiple stakeholders to verify highly sensitive data in a secure manner, without disclosing their private input. In this work, we develop a holistic solution that combats data tampering by addressing current lacunas in blockchain-based supply chains by utilizing a novel combination of on-chain verification, off-chain-logs, and collaborative MPC-based verifications. Our framework therefore also provides end-to-end tamper detection, traceability, and privacy preserving capability, to strengthen data security, enhance transparency, and foster trust between supply chain actors.

To a greater extent the framework can be expanded and scaled up to larger and more complex systems and to different industry types, like healthcare and food (including agriculture), and to logistics providers where chain of custody and traceability is of utmost importance. Potential future research directions include the integration of AI to support predictive analytics and cross-chain data transfer as well as the ability to automatically resolve anomalies detected along the chain to further support tamper prevention, better performance and decision-making.

REFERENCES

1. Atlam, H. F., Ekuri, N., Azad, M. A., and Lallie, H. S., “Blockchain Forensics: A Systematic Literature Review of Techniques, Applications, Challenges, and Future Directions”, Electronics, 2024.
2. AMusa, T. H., and Bouras, A., “Anomaly Detection in Blockchain-Enabled Supply Chain: An Ontological Approach”, IFIP (International Federation for Information Processing), 2022.
3. Aniello, L., Halak, B., Chai, P., Dhall, R., Mihalea, M., And Wilczynski, A., “Towards a Supply Chain Management System for Counterfeit Mitigation using Blockchain and PUF”, arXiv pre-print, 2019.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 12, May 2026
Impact Factor: 8.2

4. Singh, A.,And Pandey, R., "Blockchain in Supply Chain and Procurement", International Journal of Engineering Research and Technology (IJERT), 2019.
5. Nanaji, U., C.P.V.N.J Mohan Rao, And Vara Prasad, K., "Secure Supply Chain Management using Blockchain and Anomaly Detection System using Python, AI and ML", EPRA International Journal of Research and Development (IJRD), 2025.
6. Marangone, E., Di.Ciccio, C., And Weber, I., "Fine-grained Data Access Control for Collaborative Process Execution on Blockchain", arXiv pre-print, 2022.
7. Chandrakala, M., Saggithya, R.P., Sumithra, B., And Indumaathi, R., "Securing Forensic Data Using Blockchain", IJRASET Journal for Research in Applied Science and Engineering Technology, 2024.
8. Malik, S., Dedeoglu, V., Kanhere, S., And Jurdak, R., "PrivChain: Provenance and Privacy Preservation in Blockchain enabled Supply Chains", arXiv pre-print, 2021.
9. Ren, Q., Wu, Y., Liu, H., Li, Y., Victor, A., Lei, H., Wang, L., And Chen, B., "SMPTC³: Secure Multi- Party Protocol Based Trusted Cross-chain Contracts", Mathematics, 2024.
10. "Using Secure Multi-Party Computation to Protect Privacy on a Permissioned Blockchain", Sensors, 2021.
11. "Security of Blockchain-Based Supply Chain Management Systems: Challenges and Opportunities", Applied Sciences, 2021.
12. Singh, [fill authors] "Counterfeit Detection and Prevention Using Block-Chain Algorithms", Revista Electr´onica de Veterinaria, 2023.
13. Musa, T. H., and Bouras, A., "Anomaly Detection in Blockchain-Enabled Supply Chain: An Ontological Approach", IFIP (International Federation for Information Processing), 2022.
14. Taher, S.Sh., Ameen, S.Y., And Ahmed, J.A., "Advanced Fraud Detection in Blockchain Transactions: An Ensemble Learning and Explainable AI Approach", Engineering, Technology and Applied Science Research, Vol.14.Issue.1, 2024.
15. T. H. Noor, Q. Z. Sheng, A. Alfazi, and J. Yu, "Trust management of services in cloud environments: Obstacles and solutions," ACM Computing Surveys, vol. 46, no. 1, pp. 1–30, 2013.
16. A. Reyna, C. Martín, J. Chen, E. Soler, and M. Díaz, "On Blockchain and Its Integration with IoT: Challenges and Opportunities," Future Generation Computer Systems, vol. 88, pp. 173–190, 2018.
17. M. Casino, T. K. Dasaklis, and C. Patsakis, "A Systematic Literature Review of Blockchain-Based Applications," Telematics and Informatics, vol. 36, pp. 55–81, 2019.
18. H. Wang, Z. Zheng, S. Xie, H. Dai, and X. Chen, "Blockchain Challenges and Opportunities: A Survey," International Journal of Web and Grid Services, vol. 14, no. 4, pp. 352–375, 2018.
19. J. Jodeiri, A. Ghaemi-Bafghi, and R. Azmi, "Forensic Analysis of Blockchain-Based Systems: A Survey," IEEE Access, vol. 10, pp. 11245– 11265, 2022.
20. A. Atlam, R. Walters, and G. Wills, "Blockchain and Digital Forensics: Challenges and Future Directions," Journal of Digital Forensics, Security and Law, vol. 15, no. 2, pp. 1–18, 2024.
21. S. Manupati et al., "Blockchain-Based Approach for Sustainable Supply Chain Management," IEEE Transactions on Engineering Management, vol. 67, no. 3, pp. 1–14, 2022.
22. J. Jodeiri, A. Ghaemi-Bafghi, and R. Azmi, "Forensic Analysis of Blockchain-Based Systems: A Survey," IEEE Access, vol. 10, pp. 11245– 11265, 2022.
23. A.Atlam, R. Walters, and G. Wills, "Blockchain and Digital Forensics: Challenges and Future Directions," Journal of Digital Forensics, Security and Law, vol. 15, no. 2, pp. 1–18, 2024

DOI: 10.48175/IJARSCT-35929