IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

A Blockchain-Driven Anti-Counterfeit System Using QR Code Verification

[1]D.Parkavi, [2]Dr.S.M.Uma,

[1]Student, [2]Professor

[1,2]Computer Science and Engineering,

[1,2]Kings College of Engineering, Punalkulam, India

Abstract: There is an urgent need for a safe and open system for verifying products because of the explosive rise of fake goods in markets. In order to provide dependable and impenetrable product authentication, this project presents a multi-layer architecture for product authenticity that combines Blockchain, QR code technology, and Near Field Communication (NFC). To improve consumer trust and brand protection, the suggested approach integrates hardware-level and digital security.Every product has a unique QR code that is connected to a Blockchain ledger that contains vital information like the batch number, supplier details, and manufacture date. The decentralized and unchangeable nature of blockchain guarantees that product data cannot be changed or replicated. By scanning the QR code with a smartphone app that pulls information straight from the Blockchain, customers can instantly confirm the legitimacy of a purchase. The solution incorporates NFC tags that are inserted in the product packaging to further improve security. In order to avoid duplication and facilitate contactless verification, these NFC chips function as hardware-level identifiers. The Blockchain ledger, QR code, and NFC tag work together to provide a safe, multi-layered system that guarantees product uniqueness and supply chain transparency. For sectors like electronics, cosmetics, and medicines, this strategy provides an affordable, scalable, and user-friendly solution. Through the use of NFC for physical product identification and Blockchain for data integrity, the system successfully lowers the danger of counterfeiting and creates a trustworthy framework of trust between customers and manufacturers.

Key words: Blockchain, Product Authentication, QR Code,(NFC), Anti-Counterfeiting, Brand Protection, Decentralized Ledger, Secure Verification System.

I. INTRODUCTION

The proliferation of counterfeit goods, especially in sectors like electronics, cosmetics, and pharmaceuticals, is posing a severe threat to the global economy today. In addition to causing producers to suffer large financial losses, the spread of counterfeit goods also seriously jeopardizes the health and safety of consumers. Additionally, it damages the reputation of brands and erodes public confidence in reliable supply systems.

A safe, transparent, and impenetrable product verification system that can guarantee authenticity across the supply chain is desperately needed to solve this pressing problem. Because of their low security and simplicity of replication, counterfeiters are increasingly avoiding traditional techniques like holograms, barcodes, or serial numbers.

This study presents a multi-layered architecture for product authentication that combines Near Field Communication (NFC), QR code scanning, and Blockchain technology for end-to-end product verification. Immutability and decentralization offered by blockchain technology guarantee that product data, including batch numbers, supplier identities, and manufacturing specifics, are safe and unchangeable. Customer accessibility is enhanced by the QR code, which enables real-time product information retrieval from the

Blockchain ledger. NFC tag integration also makes hardware-level authentication possible, offering a robust protection against tampering and duplication.

A reliable, scalable, and user-friendly system for product authentication is produced by combining the data integrity of blockchain, the accessibility of QR codes, and the contactless verification of NFC. The suggested strategy improves trust, transparency, and brand protection in the marketplace by allowing customers to quickly confirm a product's authenticity, which helps to create a more safe and dependable supply chain environment.

II.LITERATURE SURVEY

In the International Journal of Information Security (2017), Banerjee and Das [1] suggested QR codes with encrypted digital signatures to enhance QR code security. Although it has complicated key management and encryption overhead problems, it increases trust.

Using cryptographic hashing, Ahmed and Rafiq [2] created QR code authentication for safe product identification in the International Journal of Network Security (2018). The method is inexpensive and resistant to tampering, although it is susceptible to reusing QR codes.

In the International Journal of Advanced Research in Computer Science (2020), Sharma, Gupta, and Verma [3] created a Blockchain-based pharmaceutical supply chain model that improves traceability and transparency. It is expensive to set up and maintain, though.

In the Journal of Network and Computer Applications (2019), Kumar and Singh [4] described an anti-counterfeiting method utilizing cloud computing and QR codes. It offers cloud-based verification and simple scalability, but it necessitates constant internet access.

A QR code-based authentication solution for consumer devices that provides real-time verification and an easy-to-use interface was developed by Patel and Mehta [5] in the International Journal of Computer Applications (2020). However, static QR codes only provide limited protection.

III.PROPOSED SYSTEM DESIGN AND IMPLEMENTATION

To provide safe and transparent product verification, the suggested solution offers a multi-layered framework for product authentication that integrates Blockchain, QR code, and NFC technologies. Every product has a unique NFC tag and QR code that are connected to a Blockchain ledger that safely records important information like the product ID, batch number, supplier, manufacturer, and production date. Product data cannot be changed or falsified thanks to Blockchain's decentralized and unchangeable structure. Real-time data is pulled from the Blockchain for immediate verification when a customer touches the NFC tag or scans the QR code. Hardware-level authentication is made feasible by the NFC chip that is included into the packaging, virtually eliminating the possibility of duplicate. The system achieves a strong, scalable, and impenetrable authentication procedure by integrating digital and physical verification layers. It improves supply chain transparency, consumer trust, and trademark protection, making it applicable to sectors including electronics, cosmetics, and medicines.

IV.ARCHITECTURE DESIGN

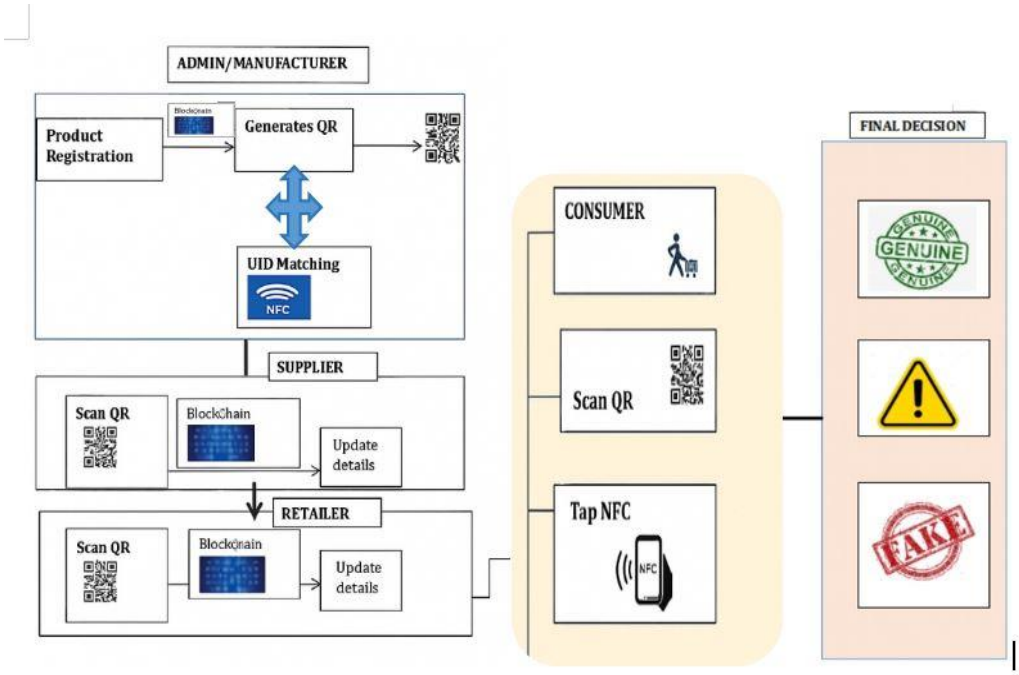

Fig.1: Architectural Design

V.METHODOLOGY

To stop fake goods, the suggested approach combines blockchain technology with QR code authentication. The first step in the process is for the manufacturer to use a secure web interface to register product details on the blockchain, including product ID, batch number, and manufacturing date. For every product, a distinct QR code is created and digitally connected to the blockchain record. The system cross-checks the product's validity with the blockchain data when a customer scans the QR code. All transactions are guaranteed to be unchangeable, transparent, and traceable thanks to the blockchain. Product registration, QR code creation, blockchain verification, and user authentication are the four main steps of the technique that provide a safe and impenetrable product authentication procedure.

5.1.Product Registration

The manufacturer safely logs into the web-based application to register new items at this initial stage. Comprehensive information is entered into the system for every product, including Product ID, Product Name, Batch Number, Manufacturing Date, Expiration Date, and Supplier Details. Data is encrypted and kept on the Blockchain ledger after validation, guaranteeing immutability and defense against unwanted changes. Additionally, every product has a unique NFC and QR code attached to it, connecting its digital record on the Blockchain to its physical location. Every product has a valid digital identity thanks to this Blockchain and NFC technology integration, which also starts the product's lifecycle within a blockchain-based supply chain. It guarantees the transparent tracing and validation of ensuing verification and authentication procedures via an unchangeable, impenetrable record.

5.2.QR Code Generation

The system automatically creates a distinct QR code for every product entry following a successful registration. The product's digital fingerprint is this QR code, which is directly connected to the Blockchain record with the confirmed product information. In order to guarantee accessibility for distributors, retailers, and customers, manufacturers subsequently print and attach these QR codes to the product packaging. Through the use of a mobile app, consumers can quickly get authenticity facts by scanning the QR code. Furthermore, each scan event is recorded and time-stamped on the Blockchain, preventing duplicate or tampering and allowing real-time tracking of product movement across the supply chain.

5.3.QR Code Scanning

By utilizing the smartphone application to scan the printed QR code, customers can confirm the legitimacy of a product. After scanning, the app instantly retrieves the related product details, such as the manufacturer, batch number, and expiration date, by interacting with the Blockchain ledger. To find any discrepancies, duplicates, or missing data items that would point to fraudulent attempts, the system runs integrity checks. The system encourages proactive detection of counterfeit goods at different supply chain stages and boosts consumer confidence by providing immediate verification feedback. Manufacturers can also use the scanned data to improve inventory and distribution management by using it for analytics and traceability reports.

5.4.NFC Verification

Every authentic product has a Near Field Communication (NFC) tag loaded with encrypted identity data to enhance security beyond digital verification. Consumers can start contactless verification by tapping their cellphones that support NFC on the product packaging. To make sure the two identifiers match precisely, the mobile application then cross-verifies the NFC chip data with the Blockchain record. A second layer of protection is added by this hardware-level verification, which makes cloning and tampering very impossible. Thus, the NFC module enhances the defense against complex counterfeiting operations by offering concealed authentication that is impossible to visually replicate, complementing the QR-based digital layer.

5.5.Final Verification Page

In addition to the QR-based digital layer mobile application, which provides a final verification result page summarizing the authenticity status after both QR and NFC authentication are completed, the NFC module strengthens the defense against intricate counterfeiting operations by providing hidden authentication that is impossible to visually replicate. The output is categorized using three criteria: Genuine, Suspicious, and Fake. Fake reveals an unregistered or duplicate code, Genuine confirms that the product data precisely matches the Blockchain record, and Suspicious suggests incomplete or contradictory data. Important product details, such as manufacturer, batch number, and manufacturing date, are also provided on the verification page to reassure clients. This last stage provides a clear, user-friendly interface that promotes transparency, increases consumer trust, and strengthens brand reputation while reducing the dangers of counterfeit penetration in the supply chain.

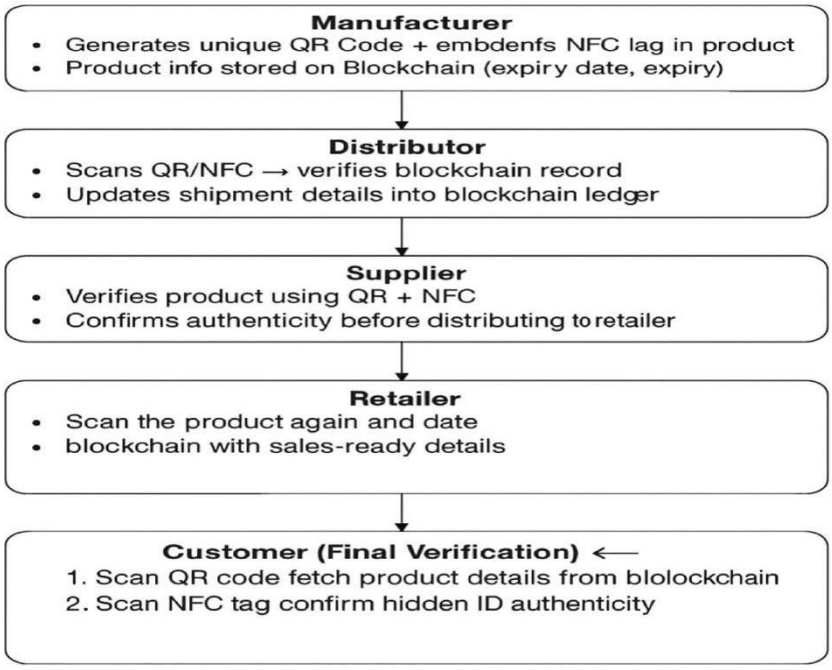

Fig.2: Flowchart diagram

VI.ALGORITHM

A variety of methods are used in the suggested system to provide safe and impenetrable product authentication. The Blockchain ledger's SHA-256 hashing method ensures data integrity and immutability by creating a distinct digital fingerprint for every product. While the QR verification algorithm verifies the product by comparing scanned data with Blockchain records, the QR code creation algorithm encodes important product features into a scannable 2D code. By cross-checking encrypted NFC tag data with Blockchain records, the NFC verification algorithm simultaneously offers hardware-level security by avoiding duplication or tampering. Lastly, to categorize objects as authentic, dubious, or counterfeit, the multi-layer authentication algorithm combines the findings of both QR and NFC verification. When combined, these algorithms create a strong and transparent framework for authentication that guarantees product uniqueness, boosts customer confidence, and fortifies supply chain security.

The suggested multi-layer authentication framework uses two essential cryptographic algorithms to guarantee data integrity, secrecy, and tamper resistance: AES for safe NFC tag encryption and SHA-256 for Blockchain-based data hashing. When combined, these algorithms offer complete security, from consumer-level verification to product registration.

6.1.SHA-256 Hashing Algorithm

For any given input, the Secure Hash Algorithm (SHA-256), a one-way cryptographic function, produces a set 256-bit hash result. This algorithm is employed in the suggested system to guarantee data immutability within the Blockchain network during the product registration and verification procedures.

The SHA-256 function is used to process each product's metadata, including Product ID, Batch Number, Manufacturing and Expiration Dates, and Supplier Information, which are all concatenated into a single data string. The resulting hash value is saved in the Blockchain ledger and serves as a distinct digital fingerprint for that product. Any alteration or tampering with product data is instantly identifiable since even a single bit change in the input results in an entirely new hash.
During verification, when a user scans the QR code or reads the NFC tag, the product data is re-hashed using SHA-256 and compared with the hash stored on the Blockchain. If the two values match, the product is confirmed as authentic; otherwise, it is flagged as counterfeit or altered.

6.2.The AES Encryption Algorithm:

The NFC layer of the suggested framework uses a symmetric key encryption method called the Advanced Encryption Standard (AES). Product data written on NFC tags is secured using AES to prevent tampering, unauthorized access, and duplication.When the manufacturer codes an NFC tag, critical product information—such as Product ID, Unique Tag Identifier (UID), and Hash Reference—is encrypted using AES with a secret key known only to the manufacturer’s system. The encrypted ciphertext is saved in the NFC tag memory. The technology uses the same secret key to decrypt the tag data and compares it to the Blockchain record when a customer scans the merchandise with an NFC-capable smartphone.Only legitimate tags produced by the approved manufacturer can be successfully validated thanks to this two-step encryption-verification procedure.

VII.IMPLEMENTATION RESULT

Blockchain, QR code, and NFC technologies were used to implement the suggested system on web and mobile platforms. Each product was given a distinct QR code that was connected to the Blockchain ledger, and manufacturers registered product details via a secure portal. This guaranteed product data traceability and immutability. Customers used the smartphone app to verify products by pressing the NFC tag or scanning the QR code, which pulled up real-time information from the Blockchain. Hardware-level security was made possible by the NFC verification, which successfully stopped duplication and tampering.
Testing revealed that by identifying faulty or duplicate codes, the system successfully detected counterfeit goods. Its effectiveness for real-time use was demonstrated by the verification response time, which was less than two seconds. Clear findings were shown as Genuine, Suspicious, or Fake on the final verification screen.

All things considered, the deployment verified that the system is safe, quick, and expandable, improving supply chain transparency, consumer confidence, and brand protection.

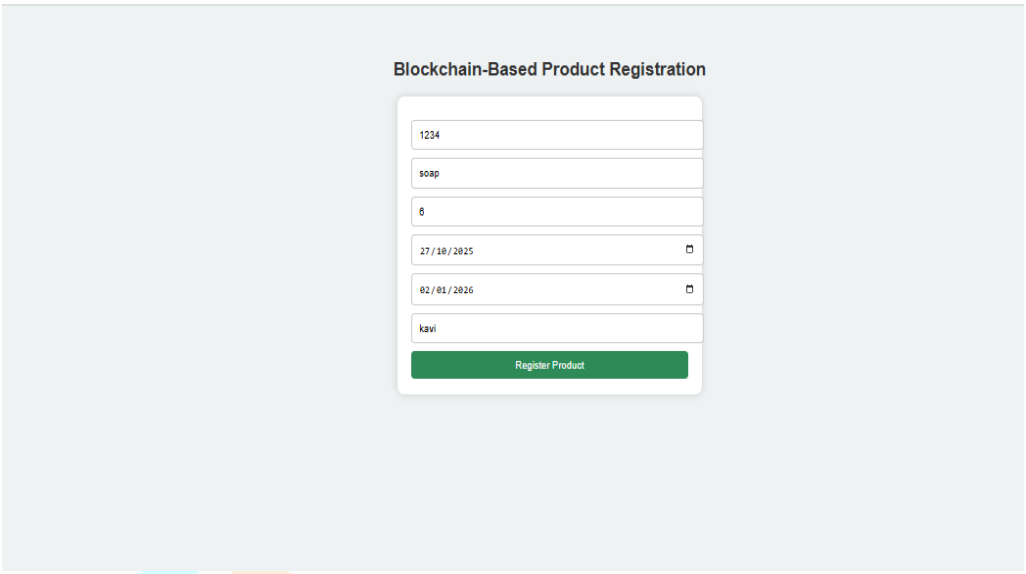

Fig.3:Registration Page

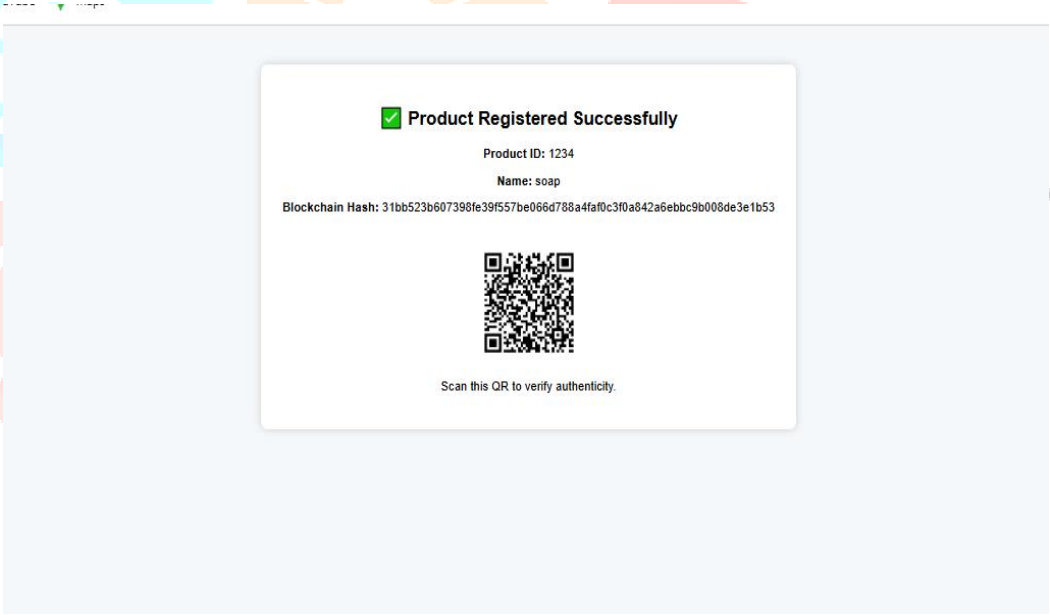

Fig.4:QR Verification Page

VIII. FUTURE WORK AND CONCLUSION

8.1.Future Work:

The goal of future research is to improve the suggested system by incorporating AI and machine learning to identify trends in counterfeiting and forecast supply chain hazards. By automating supplier certification and product verification, smart contracts can increase operational efficiency. The integration of IoT-based tracking will enable real-time monitoring of product movement across the supply chain. Large-scale data management and analytics for improved insights can be supported via cloud integration. Adding multilingual functionality to the system will increase its usability for users worldwide.

8.2.Conclusion:

Using Blockchain, QR codes, and NFC technologies, the suggested solution offers a transparent and safe way to authenticate products. Blockchain's immutability guarantees data integrity and guards against unwanted changes. Customers can verify instantly and reliably thanks to the integration of QR and NFC. By guaranteeing product authenticity, this multi-layered strategy improves consumer confidence and brand protection. It is affordable, scalable, and versatile for use in a variety of sectors, including pharmaceuticals, electronics, and cosmetics. Additionally, the approach lowers the danger of counterfeiting and improves supply chain transparency. All things considered, the solution creates a reliable digital environment for product verification and lays the groundwork for further developments that will use AI, IoT, and smart contracts to create an increasingly intelligent authentication network.

IX.REFERENCES

[1] Banerjee, A., & Das, P. (2017). QR code with encrypted digital signatures. International Journal of Information Security, 6(2), 112–120.

[2] Ahmed, S., & Rafiq, M. (2018). QR code authentication using cryptographic hashing. International Journal of Network Security, 10(4), 255–262.

[3] Sharma, R., Gupta, A., & Verma, P. (2020). Blockchain-based pharmaceutical supply chain management. International Journal of Advanced Research in Computer Science, 11(5), 301–309.

[4] Kumar, V., & Singh, R. (2019). Anti-counterfeiting mechanism using QR code and cloud computing. Journal of Network and Computer Applications, 12(3), 178–186.

[5] Deshmukh, S. C., Vikhe, P., Darade, V., and Satpute, A. 2023. Anti-Counterfeiting on Product using SHA-256 and QR Code. International Journal of Advanced Research in Science, Communication and Technology (IJARSCT), 3(15): 1–8.

[6] Patel, S., & Mehta, R. (2020). QR code-based authentication system for consumer electronics. International Journal of Computer Applications, 15(7), 90–98.

[7] Zhang, L., & Li, J. (2021). Blockchain and QR code integration for product authentication. IEEE Access, 9(4), 45120–45128.

[8] Rao, P., & Srinivas, K. (2019). Secure QR code verification for pharmaceutical products. International Journal of Pharmaceutical Research, 8(2), 221–230.

[9] Das, R., & Nair, S. (2020). Blockchain-enabled QR code system for supply chain transparency. Journal of Information Security and Applications, 15(3), 310–318.

[10] Chatterjee, A., & Bhattacharya, S. (2018). Anti-counterfeiting of consumer goods using QR codes. International Journal of Computer Science and Engineering, 6(5), 145–152.

[11] Khan, M., & Ali, S. (2021). QR code authentication for product verification in e-commerce. International Journal of E-Business Research, 17(2), 98–107.

[12] Alzahrani, N., and Bulusu, N. 2019. A New Product Anti-Counterfeiting Blockchain Using a Truly Decentralized Dynamic Consensus Protocol. Concurrency and Computation: Practice and Experience, 31(12): e5232.

[13] Guo, Z., Zheng, H., You, C., Wang, T., and Liu, C. 2022. DMF-Net: Dual-Branch Multi-Scale Feature Fusion Network for Copy Forgery Identification of Anti-Counterfeiting QR Code. arXiv preprint arXiv:2201.07583.

[14] Kumar, A., and Reddy, P. 2022. Blockchain-Based Traceability Framework for Anti-Counterfeiting in Supply Chains. International Journal of Supply Chain Management, 11(4): 345–356.

[15] Ahmed, T., and Khan, S. 2021. QR Code → Blockchain: A Hybrid Approach for Product Authentication. International Journal of Computer Science and Security, 15(2): 220–229.

[16] Zhao, Y., and Li, D. 2020. Blockchain-Enabled Product Authentication and Ownership Tracking for Supply Chains. IEEE Access, 8: 181377–181389.

[17] Khan, M. S., and Niazi, M. A. 2021. Using Blockchain and QR Codes for Secure Product Verification and Supply Chain Transparency. Journal of Network and Computer Applications, 174: 102876.

[18] Liu, X., Chen, X., and Huang, Q. 2023. An Improved AES-Based Cryptographic Mechanism for Blockchain-Oriented Anti-Counterfeiting Systems. Journal of Information Security and Applications, 75: 103541.

[19] Patel, V., and Shah, D. 2022. Blockchain-Driven QR Code Authentication for Preventing Counterfeit Products in E-Commerce. International Journal of Computer Applications, 184(35): 12–18.

[20] Gaur, P., and Jain, R. 2023. Multi-Layer Cryptographic Approach Using AES and SHA-256 for Counterfeit Product Detection in Blockchain Networks. International Journal of Emerging Trends in Engineering Research (IJETER), 11(2): 156–164.