Counterfeit Detection And Prevention Using Block-Chain Algorithms

Antony Vigil M S[1], Sairam Kantheti[2], Ganesh Balaji[3], Galla Prasith[4]

[1,2,3,4] Department of Computer Science and Engineering, SRM Institute of Science and technology, Ramapuram, Chennai, India

Abstract— The prevalence of counterfeit products in today's supply chains makes it requires to implement a application that allows end users to verify the authenticity of the products they purchase. This proposed system manages product ownership using the Inter Planetary File System (IPFS), which operates on a distributed web. By leveraging IPFS, the system ensures efficient distribution of large volumes of data, avoiding duplication. Like blockchain, IPFS can securely manage data by allowing users to address vast amounts of data and store immutable, permanent within a block chain transaction. This process timestamps and secures content without any intrusions with help of solidity and hash algorithms security of applications will be conducted with decentralized network no entity will be in control of data centers with highly sophisticated sha -256 algorithm 16 characters unique code will be generated for blocks each block hash code will contained in the next block to access independent block is impossible This proposed system utilizes the Inter Planetary File System (IPFS) to manage product ownership on a distributed web. By leveraging IPFS, it ensures efficient distribution of large data volumes, preventing duplication. Similar to blockchain, IPFS securely manages data by enabling users to address and store vast amounts of data immutably and permanently within a blockchain transaction.

Keywords: Inter Planetary File System (IPFS), Blockchain, Counterfeit Products, Supply Chains, Authenticity Verification, Graphical User Interface (GUI), Product Ownership, Ownership Tracking

I. INTRODUCTION

Introducing the "COUNTERFEIT DETECTION" – Businesses across various sectors are increasingly worried about the rise of counterfeit goods. These fake products not only lead to significant revenue losses and brand damage but also pose serious risks to public health. To address this issue and create a more transparent and secure supply chain, many companies are looking towards blockchain technology as a potential solution. One proposed approach involves using blockchain to allow customers to easily verify the authenticity of products by scanning a unique QR code on each item. Blockchain technology offers a secure and permanent record of transaction data, making it difficult for counterfeiters to operate. In the medical industry, where counterfeit drugs pose a serious threat to public health, blockchain provides a solution by creating an immutable ledger that tracks every step in the supply chain down to the individual drug level. A key feature of this approach is the use of unique QR codes or digital identifiers for each product. Customers can scan these codes using a smartphone or other device to access detailed information about the product, including its origin, manufacturing details, and the entire chain of custody from production to the point of sale. This not only empowers consumers to verify the authenticity of the products they purchase but also builds trust in the brand.In addition to enhancing consumer confidence, blockchain technology also helps manufacturers and retailers detect and prevent the distribution of counterfeit goods. Since every transaction and movement within the supply chain is recorded on the blockchain, any attempt to introduce counterfeit products can be quickly identified and traced back to the source. This makes it extremely difficult for counterfeiters to infiltrate the supply chain.

The medical industry stands to benefit significantly from block chain-based solutions. Counterfeit drugs are a major concern worldwide, posing serious risks to patient safety and leading to potentially life-threatening consequences. By implementing block chain technology, pharmaceutical companies can create an immutable and transparent ledger that tracks each drug from its creation through every stage of the supply chain. This ensures that only genuine, approved products reach patients, reducing the risk of counterfeit drugs entering the market.

Moreover, blockchain can enhance regulatory compliance by providing an trail of all transactions, helping companies meet stringent regulatory requirements. It also facilitates better collaboration between manufacturers, distributors, and regulators, ensuring that all stakeholders have access to accurate, real-time information.

II. RELATED WORKS

"Detection of Fake Products using Blockchain" published in 2022 authored by Swati Y, investigates the application of Fake product detection in, Blockchain The review addresses the unique challenges associated with implementing and detecting, particularly the complexities of shared responsibility models and the intricacies of security configurations.A detailed analysis, the paper sheds light on the critical role of detection in ensuring secure and efficient Blockchain operations. The author elaborates on the mechanisms for integrating detection in blockchain infrastructures and discusses strategies to mitigate security risks, thus providing a comprehensive guide for organizations aiming to enhance their blockchain

[1] The paper titled "Fake Product Detection," published in 2020 by Northeast Electric Power University Jilin city China and authored by Jing Dong Wang , provides a analysis of the Fake Product Detection and benefits of implementing Blockchain Algorithms This survey evaluates the cost-effectiveness of examining several key financial advantages, including the reduction of incident costs, the avoidance of regulatory issues, and the enhancement of brand reputation. The author delves into the direct and indirect cost savings associated with Blockchain, such as decreased expenditure on security breaches and compliance management. Additionally, the paper highlights how Blockchain can lead to improved operational efficiency and user experience, thereby contributing to a stronger competitive position in the market. By presenting a detailed cost-benefit framework.

[2] The paper titled "Fake Product Detection," published in 2021 by the Easwari Engineering college and authored by PM Lavanya, examines the ethical considerations involved in using Blockchain service systems. This addresses important concerns related to user privacy and data security, emphasizing the need for responsible implementation practices. The author discusses the potential risks associated with data sharing among organizations and the importance of establishing robust privacy controls to safeguard user information.

Additionally, it highlights the ethical responsibilities that organizations have when deploying Blockchain Algorithms, aiming to ensure that user rights are protected throughout the process.[3] The paper published in 2021, titled "Block chain Supply chain Management," authored by Sanjai Krishna. It focuses on the role of Block chain in monitoring database and ensuring the security of essential applications. It examines how traditional approaches can be adapted to better serve modern database environments, highlighting the need for robust monitoring solutions to protect sensitive data. Additionally, the paper discusses the challenges organizations face in implementing effective Blockchain strategies and offers insights into best practices for enhancing application security. By addressing these key areas, the study provides valuable guidance for organizations aiming to strengthen their database security measures.

[4] It is published in 2023, titled "Counterfeit Detection Using Semi-Conductor process," authored by Matthias Ludwig from the College of Munich, explores the role Detection in securing emerging technologies such as block chain, artificial intelligence (AI), and the Internet of Things. It discusses various adaptation methods for implementing Fake product detection in these complex environments and identifies the unique challenges organizations face. By examining the interplay between algorithms and these technologies, the paper highlights the importance of maintaining data integrity and security in a rapidly evolving digital landscape. Additionally, the study provides insights into best practices for effectively integrating Blockchain solutions to protect critical infrastructure and data.

[5] It published in 2017, titled "Hardware Based Anti-Counterfeit Techniques," authored by MD Tanvir from University of Maryland, examines the significant advantages of combining Monitoring and maintain with threat intelligence to enhance cybersecurity. The survey details how this integration boosts security by enabling proactive risk detection, allowing organizations to identify potential threats before they escalate. It emphasizes the importance of prioritizing critical alerts, ensuring that security teams can focus on the most pressing issues without being overwhelmed by less urgent notifications. Further, the paper discusses how leveraging threat intelligence can detect response strategies, enabling organizations to develop more effective response plans to emerging threats.

By analyzing real-world case studies and best practices, the author provides insights into how organizations can use these strategies effectively. The study ultimately underscores of adopting a comprehensive security create a resilient security posture capable of adapting to evolving cyber threats.

[6] It is published in 2021 , titled “Diagnosis of pulpitis from dental panoramic radio graph using histogram of gradients with discreet wavelet transform and multilevel neural network techniques”.

[7]I is published 2020 by Ghaith Khalil, Robin Doss, Morshed Chowdhury, ” A Novel RFID-Based Anti-Counterfeiting Scheme for Retail Environments” which is an contemporary analysis

[8] Published by Si Chen, Rui Shi, Zhuangyu Ren , Jiaqi Yan , Yani shi , Jinyu Zhang,“ A Blockchainbased Supply Chain Quality Management Framework”, 2017 IEEE 14th International Conference on e-Business Engineering (ICEBE). Shown an significant analysis on qr code generation

[9] Which is authored by Jinhua Ma , Shih-Ya Lin , Xin Chen , Hung-Min Sun,A Blockchain-Based Application System for Product Anti-Counterfeiting” International Journal Of Scientific & Technology Research Volume 8, Issue 12, December 2019. highlights the ethical responsibilities that organizations have when deploying Blockchain Algorithms, aiming

[10] Wu, C., & Wu, M. (2021). "An Integrated Approach for Anti-Counterfeiting in the Pharmaceutical Supply Chain using Blockchain and IoT." Journal of Manufacturing Systems, explores the role Detection in securing emerging technologies such as block chain, artificial intelligence

III. PROPOSED WORK

In today's digital world, safeguarding the integrity of files, directories, and communications is utmost priority for ensuring data security and maintaining trust. However, users often face a fragmented array of integrity-checking tools, A supply chain operates as an interconnected network, so any Supply Chain Management (SCM) system must be designed with a cohesive structure that ensures both functionality and visibility throughout the product delivery journey. Typically, an SCM system includes features like inventory management, warehouse management, purchase order processing, demand forecasting, supplier relationship management, and logistics planning, among others.

Many SCM systems are integrated with bookkeeping tools, allowing businesses to manage their ledgers and optimize their financial operations efficiently. In recent years, there has been a significant shift towards adopting cloud-based SCM systems offered as Software-as-a-Service. Managing the supply chain through cloud technology enables businesses to track the entire life cycle of a project, offering enhanced monitoring and detecting counterfeit products at every stage.

These modern approaches and addresses the shortcomings of traditional SCM systems, which set backs in the comprehensive management capabilities provided by cloud technology. In conclusion , cloud-based SCM systems offer greater scalability and efficiency, making them an increasingly popular choice for businesses looking to improve their supply chain processes and of illicit products.

In the existing methods, Time complexity was very high in identifying and displaying of product information is one of the major drawbacks. After scanning the product the chain of commands is taking more time to process and many instances were found regarding security of the data which was provided by the manufacturer at initial stage.

The database was setup in a traditional model where vulnerabilities were very high constant inspection of manufacturing the products by a particular person results in a negative approach .Modern approaches address the shortcomings of traditional supply chain management (SCM) systems, particularly their limitations in providing comprehensive management capabilities. Cloud-based SCM systems, in contrast, offer enhanced scalability and efficiency, making them an increasingly popular choice for businesses aiming to improve their supply chain processes and mitigate the risk of illicit products.

Maintaining the integrity of files, directories, and communications is critical for ensuring data security and trust. However, users frequently deal with a disjointed array of integrity-checking tools. Because a supply chain operates as an interconnected network, any Supply Chain Management (SCM) system needs to be designed with a unified structure that ensures both functionality and visibility throughout the entire product delivery process. Typically, an SCM system includes features such as inventory management, warehouse management, purchase order processing, demand forecasting, supplier relationship management, and logistics planning, among others.

Blockchain technology has shown significant promise in combating the sale of counterfeit products. As a decentralized digital ledger, blockchain enables secure and transparent record-keeping. Addressing this issue is crucial for the future of the global market.

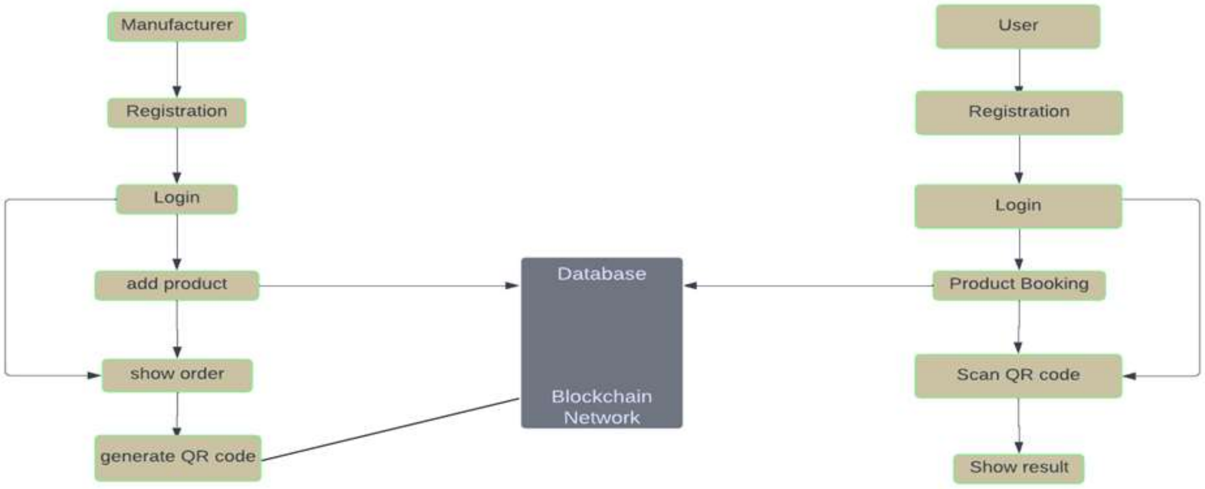

Figure 1: Architectural diagram for the block chain database

The product details will be registered in the data base created by using the blockchain technology and the registered product will be entered in the blockchain network. The above process undergoes only for the registered products the manufacturer provides all the required details of the product at the time of registration to prove the products authenticity. The essential information such as product bar code, ID, Price will be stored in the data base. By searching the above details of the product via bar code a robust unique QR code will be generated by accessing QR code the nature of the product will be detected and details will be displayed. This process assures prominent supply chain management. The attached architectural representation will ensure the product authenticity in an accurate method.

This process applies exclusively to registered products, where the manufacturer provides all necessary details at the time of registration to verify the product's authenticity. Essential information such as the product's barcode, ID, and price will be stored in the database. By searching for these details via the barcode, a unique and secure QR code will be generated. Scanning this QR code will reveal the product's nature and display its details, ensuring robust supply chain management. The accompanying architectural representation ensures the product's authenticity with precision.

The database is equipped with blockchain technology where it is technically impossible to penetrate and tamper the data with the help of solidity smart contracts were written where it makes completely decentralized no entity will be able to control it. The information of products as well as statements were stored in blocks where it is highly secured with hash algorithms which is an indistinguishable and ambiguity.

This makes it virtually impossible to penetrate or tamper with the data. Solidity smart contracts are employed to ensure complete decentralization, preventing any single entity from gaining control. Product information and related statements are stored in blocks, which are highly secured by hash algorithms that produce a unique 16-character alphanumeric code, ensuring both security and clarity. aims to provide a comprehensive suite of features that effectively address the critical challenges of data integrity and unlawful detection. It includes a secure file upload and storage module, enabling users to confidently submit their digital content for integrity verification while supporting various file formats. Furthermore, the counterfeit scanning module utilizes advanced algorithms, such as the Random Forest model, to perform thorough scans on individual files, accurately searching whether they are legit or illicit. The project also incorporates a robust training phase that focuses on data acquisition, encompassing extensive datasets of both counterfeit and legit data files. This phase emphasizes required the preprocessing techniques, including blockchain algorithms. The blockchain model is built using this pre-processed data, enabling it to differentiate between fake and real files effectively. In the classification phase, incoming files undergo similar preprocessing, allowing the trained model to deliver reliable predictions by aggregating the results from multiple decision algorithms, ensuring a high level of accuracy in detecting fake products.

The address key issues related to data independency and the detection of counterfeit items. It includes a secure file upload and storage module, allowing users to submit their digital content for integrity verification with confidence, while supporting various file formats. Additionally, the counterfeit scanning module employs advanced algorithms, such as the Random Forest model, to thoroughly examine files and determine their authenticity. The project features a robust training phase focused on data acquisition, utilizing extensive datasets of both counterfeit and legitimate files. This phase includes necessary preprocessing techniques and blockchain algorithms. The blockchain model, built on this preprocessed data, effectively distinguishes between genuine and counterfeit files. During the classification phase, incoming files undergo similar preprocessing, enabling the trained model to provide accurate predictions by aggregating results from multiple decision algorithms, ensuring high precision in detecting counterfeit products.

3.1 File Upload and Storage

The file upload module allows users and manufactures to securely upload their digital content for integrity verification. It includes features for handling various file formats and ensuring secure storage. Additionally, the QR scanning module leverages the blockchain to conduct thorough QR code scans on individual files, identifying and reporting whether a product is legit or fake. With the help of decentralized network there is no data servers are placed in a single location they are situated in various locations which makes more sophisticated for intruders to access sensitive information solidity is used for uploading and accessing the files.

3.2 Training Phase

The training phase begins with data acquisition, which involves collecting a complex dataset of product information. The blockchain dataset should encompass various types, including QR code, product information the dataset should represent legitimate software that users might encounter. Next, data preprocessing is necessary to clean and transform the raw data to make it suitable for the model. selection techniques are used to choose the most reliable product information. During training, the application learns the patterns that differentiate between original and fake files. Hyperparameter tuning might be required to optimize the model's performance, involving adjusting parameters.

3.3 Encompassing Phase

In the encompassing phase, incoming data (files to be analysed) undergoes similar preprocessing steps as in the training phase, including feature extraction and normalization. The pre-processed incoming data is then fed into the trained blockchain model. Each chain in the blockchain relentlessly analyses the data and makes a prediction (legit or illicit) based on its learned decision norms. The final classification for the incoming data is determined by aggregating the predictions of all chains in the blockchain.

similar to those in the training phase, including feature extraction and normalization. The pre-processed data is then input into the trained blockchain model. Each chain within the blockchain rigorously analyses the data and makes a prediction (legitimate or illicit) based on its learned decision criteria. The final classification for the incoming data is determined by aggregating the predictions

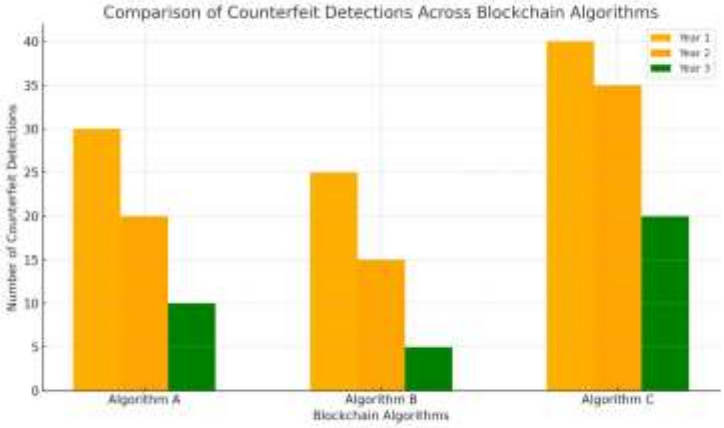

Figure 2: Comparison of data sets

VI. RESULT AND DISCUSSION

The Proposed System for the "Counterfeit Product Detection" project emphasizes prominent processing speed, optimal resource utilization, scalability, and high accuracy. It aims to strike a balance between security and performance while providing a user-friendly interface for smooth interactions. The application integrates smoothly with external applications, prominent maintenance, and incorporates user feedback to ensure ongoing enhancement.

Upon comparing the existing and proposed "Counterfeit product detection" system, substantial advancements are evident in efficiency, scalability, accuracy, security, user-friendliness, and integration capabilities in the proposed system. These enhancements effectively mitigate identified weaknesses in the current system, underscoring the benefits and ultimatum of the new system.

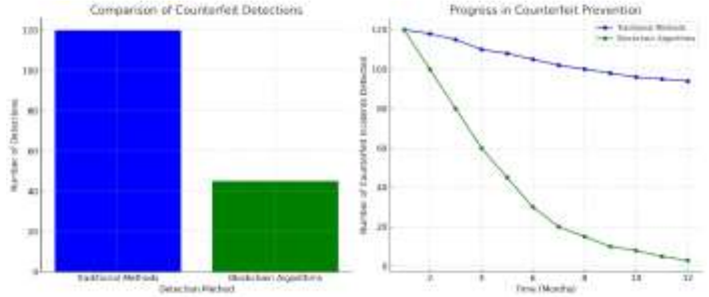

Figure 3: Implementation of the counterfeit product detection

VII. CONCLUSION

The Counterfeit Product Detection is designed for users seeking assurance about the integrity and authenticity of their digital files. Developed using Block chain. The initiative is committed to evolving into a more robust and indispensable tool in the field of digital security by emphasizing key fields such as real-time updates, comprehensive reporting, user account management, and thorough documentation. Looking ahead, the project aims to enhance its capabilities by integrating real-time updates that ensure users are frequently informed about the latest threats and system performance. Comprehensive reporting features will provide users with detailed insights into malware detection results and file integrity checks, helping them make informed decisions. Furthermore, implementing user account management will provide personalized experiences and improve security by allowing users to manage their profiles and access levels effectively. Extensive documentation will further support users by providing clear guidelines and resources for maximizing the tool's effectiveness. Through these enhancements, fake product detection aspires to become an prominent asset in maintaining digital security.

Using blockchain technology, this initiative is dedicated to evolving into a more robust and essential tool in digital security. It focuses on key areas such as real-time updates, comprehensive reporting, user account management, and thorough documentation. Looking ahead, the project plans to enhance its features by integrating real-time updates to keep users informed about the latest threats and system performance. Comprehensive reporting will offer detailed insights into malware detection results and file integrity checks, aiding users in making informed decisions. Additionally, user account management will enable personalized experiences and improve security by allowing users to effectively manage their profiles and access levels. Extensive documentation will provide clear guidelines and resources to help users maximize the tool's

VIII. REFERENCES

1. Muhammad Nasir Mumtaz Bhutta, Amir A. Khwaja, Adnan Nadeem, Hafiz Farooq Ahmad, Muhammad Khurram Khan, Moataz A. Hanif, Houbing Song, Majed Alshamari, and Yue Cao , "A Survey on Blockchain Technology: Evolution, Architecture and Security", IEEE special section on intelligent big data analytics for internet of things, services and people,2021, pp. 61048 – 61073.
2. Rishabh Sushil Bhatnagar, Sneha Manoj Jha, Shrey Surendra Singh, Rajkumar Shende "Product Traceability using Block chain", 2020 2nd International Conference on Advances in Computing, Communication Control and Networking (ICACCCN).
3. Si Chen, Rui Shi, Zhuangyu Ren , Jiaqi Yan , Yani shi , Jinyu Zhang," A Blockchainbased Supply Chain Quality Management Framework", 2017 IEEE 14th International Conference on e-Business Engineering (ICEBE).
4. M.C.Jayaprasanna, .V.A.Soundharya , M.Suhana, S.Sujatha," A Block Chain based Management System for Detecting Counterfeit Product in Supply Chain" ,IEEE 2021 Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV).
5. Jinhua Ma , Shih-Ya Lin , Xin Chen , Hung-Min Sun**,**A Blockchain-Based Application System for Product Anti-Counterfeiting" International Journal Of Scientific & Technology Research Volume 8, Issue 12, December 2019 issn 2277-8616.
6. B. M. A. L. Basnayake, C. Rajapakse," A Blockchain-based decentralized system to ensure the transparency of organic food supply chain" ,IEEE 2019 International Research Conference on Smart Computing and Systems Engineering (SCSE)
7. Atima Tharatipyakul and Suporn Pongnumkul, "User Interface of Blockchain-Based Agri-Food Traceability Applications", IEEE vol 9, 2019,pp.82909-82929.
8. Si Chen, Rui Shi, Zhuangyu Ren, Jiaqi Yan,Yani Shi, Jinyu Zhang, "A Blockchain-based Supply Chain Quality Management Framework",14th, IEEE International Conference on e-Business Engineering, 2017.
9. Mitsuaki Nakasumi, "Information Sharing for Supply Chain Management based on Block Chain Technology", 19th Conference on Business Informatic, IEEE, 2017.Daniel Tse, Bowen Zhang, Yuchen Yang, Chenli Cheng, Haoran Mu, "Blockchain. Application in Food Supply Information Security", 2017 IEEE International Conference on Industrial Engineering and Engineering Management (IEEM).
10. Zhang, Y., Wang, L., Zhang, Y., & Zhang, Y. (2022). "Enhancing Product Authentication via Blockchain and IoT Integration." In Proceedings of the International Conference on Advanced Information Systems Engineering (CAISE), pp. 125-139.
11. Chen, Y., Li, W., & Wang, H. (2022). "Blockchain-Enabled Product Traceability: A Case Study in the Food Industry." Sustainability, 14(2), 596.
12. Kulkarni, S., & Manjunath, B. S. (2021). "A Blockchain-Based Framework for Secure Anti-Counterfeiting in Pharmaceutical Supply Chains." Journal of Pharmaceutical Innovation, 16(4), 459-470.
13. Garg, R., & Tyagi, V. (2021). "Blockchain-Based Supply Chain Management for Anti-Counterfeiting: A Case Study in the Fashion Industry." Journal of Enterprise Information Management, 35(6), 13891414.
14. Wang, Z., Cheng, C., & Zheng, K. (2022). "Blockchain-Based AntiCounterfeiting and Traceability System for High-Value Agricultural Products." IEEE Transactions on Industrial Informatics, 18, 1-1.
15. Xu, J., Cheng, R., & Yang, H. (2022). "A Novel Blockchain-Based AntiCounterfeiting System for Electronics Industry." Journal of Manufacturing Systems, 64, 51-61.
16. Wu, C., & Wu, M. (2021). "An Integrated Approach for Anti-Counterfeiting in the Pharmaceutical Supply Chain using Blockchain and IoT." Journal of Manufacturing Systems, 59, 178-188.
17. Li, X., Liu, D., & Liu, J. (2022). "Blockchain and IoT Integrated System for Ensuring the Authenticity of Luxury Goods." IEEE Transactions on Engineering Management.
18. M.S. Antony Vigil, Prakash Pathak, Shubham Upadhyay, Deepankar Singh, Vaibhav Garg,2022, Detection of cloud shadows using deep CNN utilising spatial and spectral features of landsat imagery,IEEE
19. Guo, Y., Wang, S., & Zeng, Z. (2021). "A Blockchain-Based AntiCounterfeiting System for Fast-Moving Consumer Goods." IEEE Transactions on Industrial Informatics, 17(6), 4292-4300.
20. Jin, J., Lin, Q., & Zhang, X. (2022). "A Blockchain-Based AntiCounterfeiting System for Automotive Parts." IEEE Transactions on Intelligent Transportation Systems.
21. Chen, R., Zhang, Z., & Liu, J. (2021). "Combating Counterfeiting in Aerospace Industry: A Blockchain Approach." Journal of Manufacturing Science and Engineering. IEEE
22. M.C. Jayaprasanna, V.A. Soundharya, M. Suhana, S. Sujatha, " A Block Chain based Management System for Detecting Counterfeit Product in Supply Chain"(2021),IEEE

23. Ghaith Khalil, Robin Doss, Morshed Chowdhury, ” A Novel RFID-Based Anti-Counterfeiting Scheme for RetailEnvironments”(2020),IEEE
24. JINHUA MA, SHIH-YA LIN, XIN CHEN, HUNG-MIN SUN, YEH-CHENG CHEN, ” A Blockchain-Based Application System for Product Anti-Counterfeiting”(2020)
25. PENG ZHU, JIAN HU, YUE ZHANG AND XIAOTONG A Blockchain Based Solution for Medication Anti-Counterfeiting and Traceability”(2020)
26. Randhir Kumar, Rakesh Tripathi, ” Traceability of counterfeit medicine supply chain through Blockchain”(2019)
27. M.S. Antony Vigil,, Karan Bhavsar, Sanjay Kimbahune, Dr Sundeep Khandelwal, Avik Ghose and Dr Arpan Pal, ” Detection of Counterfeit Medicines Using Hyperspectral Sensing”(2020)
28. M.S. Antony Vigil ,Harrish P, Selva J,2022, Time Series Modelling and Domain specific predicting air passenger flow traffic using Neural Network
29. M.S. Antony Vigil ,2018, A review on rc home automation using Id and IR sensors
30. Sunil Ghora Bhatnagar, Surendra Singh, Rajkumar Shende “Product detection using Block chain”, 2020 2nd International Conference on Advances in Computing, Communication Control and Networking (ICACCCN).
31. Zhe Yang, Tao Wang. Application of data storage management system in Blockchain-based technology[J]. Techniques of Automation and Applications, 2022,IEEE
32. Zhiwei Gao, Hongbo Fan, Jinjiang Liu. Blockchain-based solution for secure storage and sharing of shipping data[J]. China Water Transport, 2022(10):57-58.,IEEE
33. Yong Li, Lin Tang, Xubo Wen. Research on Blockchain-based equipment data storage and sharing technology[J]. Computer Era,IEEE, 2022(10):41-44+50.
34. Kai Yan, Yue Du, Lei Guo, Jie Wang, Changbao Wu. Blockchainbased encryption method for trusted data storage of metering assets[J]. International Electronic Elements, 2022,30(17):41-44+49.
35. Yaping Zhang, Shaoying Yang. Research on the implementation method of Blockchain-based data storage scheme[J]. XINXI JILU CAILIAO, 2022,23(09):234-236