PROJECT ON

INFORMATION SECURITY

ANALYSIS AND AUDIT

Vellore Institute of Technology
(Deemed to be University under section 3 of UGC Act, 1956)

J-COMPONENT PROJECT

(FINAL REPORT)

ON

IDENTIFICATION OF DUPLICATE / FAKE PRODUCT

USING BLOCKCHAIN TECHNOLOGY

UNDER THE GUIDANCE OF

Dr. THANGA MARIAPPAN L

FACULTY, VIT UNIVERSITY, VELLORE.

SUBMITTED BY

GOKULAKRISHNAN K - 20MIS0256

KAMALESH KO – 20MIS0318

KAVIN AKASH K - 20MIS0252

SEMESTER

FALL – 2023~2024

PROGRAMME

M.TECH (Integrated) SOFTWARE ENGINEERING

SCHOOL

SCHOOL OF COMPUTER SCIENCE ENGINEERING AND INFORMATION SYSTEMS (SCORE)

COURSE CODE

CSE3501

SLOT

F1

IDENTIFICATION OF DUPLICATE / FAKE PRODUCT USING BLOCK CHAIN

Kavin Akash K
20MIS0252
School of Computer Science
Engineering and Information Systems
kavinakash.k2020@vitstudent.ac.in
6374684021

Gokulakrishnan K
20MIS0256
School of Computer Science
Engineering and Information Systems
gokulakrishnan.k2020@vitstudent.ac.in
8300399838

Kamalesh KO
20MIS0318
School of Computer Science
Engineering and Information Systems
kamalesh.ko2020@vitstudent.ac.in
8825944747

Abstract*— In recent years, there has been a notable surge in interest surrounding blockchain advancements. While currency exchange is a prominent topic of discussion, its applicability extends beyond digital currency alone. This technology holds the potential to impact various industries, offering increased transparency and facilitating smoother large-scale transactions. Blockchain also serves as a tool to identify fake products, addressing a prevalent concern in today's market. The widespread presence of counterfeit goods has significant repercussions on economic development. Thus, it is crucial to provide consumers with transparent information about the authenticity of products. The escalating prevalence of unsafe and counterfeit items worldwide is a worrisome issue, and blockchain technology represents a significant stride towards eradicating it entirely. Implementing this technology not only diminishes the production of fake goods but also necessitates widespread awareness. Each legitimate item should be assigned a unique digital code during production and packaging. This code can be scanned using specialized software, enabling verification of the product's authenticity.

***Keywords*—Blockchain, Fake product, counterfeit**

I. Introduction

Counterfeiting is a widespread issue that affects nearly all industries, encompassing electronic components, automotive parts, consumer goods, pharmaceuticals, and even wine. While manufacturers, distributors, and government bodies incur significant financial losses due to counterfeit products annually, the risks to consumers can be even more severe. Faulty counterfeit items like auto parts or consumer goods can pose safety hazards, leading to overheating, fires, and, in the case of counterfeit drugs, result in more than a million fatalities each year. Despite active efforts by various stakeholders to eliminate counterfeit products from the supply chain, the identification of counterfeits remains a challenging task. In 2018, counterfeit goods cost global brands over $232 billion, with the counterfeit drug market alone responsible for over $200 billion in annual losses, equivalent to the introduction of 13 new drugs to the market every year. Counterfeit auto parts alone lead to an estimated annual loss of $2.2 billion, not accounting for safety issues and legal liability. Counterfeit consumer electronics and computer chips contribute to losses of more than $100 billion and $7.5 billion per year, respectively, along with the elimination of 11,000 jobs in the United States. Detecting counterfeit products within the supply chain is a daunting task, if not impossible. The only effective strategy to outsmart counterfeiters is to employ an infallible method for verifying product authenticity from their source to their final destination. Recently, cloud-based security technology has emerged, offering the capability to create unique, foolproof digital identifiers for products, enabling their comprehensive tracking at every stage of the supply chain.

Detecting counterfeit goods in today's advanced market poses a significant challenge for consumers, particularly in critical sectors like pharmaceuticals. Industries such as electronics, clothing, and fashion accessories also face substantial repercussions on their brand reputation due to the prevalence of fake products. E-commerce has witnessed remarkable growth, surging from $39 billion in 2017 to a projected $200 billion by 2026, driven by widespread internet and mobile phone usage. Extensive market surveys indicate a rapid rise in counterfeit products, which can have detrimental effects on overall development and economic progress. Consequently, many leading companies have received negative feedback and seen a decline in their brand rankings.

Counterfeit goods closely mimic genuine products available in the market. Established companies are tirelessly working to curb this perilous practice, which threatens individuals worldwide. Renowned brands are leveraging cutting-edge technology to distinguish fake products from authentic ones, with the IT sector providing crucial support in this endeavor. Among the various technologies in the IT domain, blockchain stands out as a promising solution to combat counterfeiting. A blockchain is a form of decentralized ledger specifically designed to thwart tampering, employing distributed consensus algorithms, smart contracts, and encrypted techniques. This technology proves instrumental in addressing the issue of product counterfeiting.

II. Literature Survey

This survey paper encompasses discussions on the architecture of cryptocurrencies, smart contracts, and various applications based on Blockchain technology. It offers an insight into how Blockchain architectures relate to cryptocurrencies, smart contracts, and other applications. Additionally, it emphasizes the progress made in consensus mechanisms, along with notable advancements and frameworks for practical implementation. Furthermore, it engages in an in-depth conversation regarding potential future research directions and unexplored areas, aiming to guide researchers in tackling the significant challenges within the field of Blockchain.

Disadvantages: Doesn't provide information on hashing and all consensus algorithms. [1]

Traditional SCM systems are well-established in the current market, while blockchain, though innovative, has yet to see widespread adoption in the industry. The longevity of current SCM systems can be attributed to their cost-effective and straightforward implementation on a large scale. Despite their extensive use, these systems have inherent shortcomings that have persisted since their inception. They exhibit opacity and are susceptible to various types of fraud and scams due to inadequate transaction record maintenance. The issue of trust among participating entities remains unresolved. Customer confidence in the system is compromised when quality assurance is not provided, a critical factor in business growth. Despite these drawbacks, major market players continue to employ these systems, leveraging their ability to manipulate product prices without much accountability.

Disadvantages: Transactions are tough when there are too many participants. [2]

In this study, the authors introduced a structure for implementing Supply Chain Quality Intelligence (SCQI) using blockchain technology. This framework establishes a conceptual foundation for the smart management of supply chain quality, leveraging the capabilities of blockchain. Additionally, it serves as a cornerstone for crafting theories regarding the management of information resources within dispersed virtual organizations, with a particular emphasis on theories pertaining to decentralized, cross-organizational management.

Disadvantages: Design of a highly inefficient sophisticated smart contract system. [3]

The paper addresses the rampant growth of counterfeit goods in both online and underground markets. The black market poses a significant challenge to the supply chain. Despite the government's efforts to enact laws and regulations against fake products, it struggles to fully control the proliferation of counterfeits. Therefore, there is a pressing need for a method to identify counterfeit products and implement security measures to notify both manufacturers and consumers within the supply chain. Manufacturers can adopt a blockchain management system to securely store pertinent information about product sales within the blockchain, accessible to all parties involved. This system ensures transparency in the total number of sales a seller can make, as well as the remaining available stock. To further bolster security, users can conduct vendor-side verification through an encryption algorithm. The sole means of decryption lies in the use of the owner's private key.

The proposed blockchain management system, outlined in this paper, empowers consumers and enterprise vendors to actively trace and verify the authenticity of products using a smartphone. Additionally, it has the capacity to identify counterfeit products and validate the legitimacy of manufacturers for both end-users and enterprise vendors.

Disadvantages: Using RFID (Radio frequency Identification) in a BCBM (Block Chain Based Management System) requires too much processing time. [4]

In this specific document, manufacturers have the capability to store pertinent details about product sales in a publicly accessible Blockchain. The total sales potential and the remaining inventory held by the seller are openly viewable. Users can utilize the provided system functions to promptly verify vendors. The system employs digital signatures for identity authentication, ensuring that the private key of the key owner cannot be decrypted unless it is accidentally disclosed by the owner. According to their system analysis, the initial contract for recording product information will only incur a cost of approximately 1.29 US dollars, while each subsequent product sale process will amount to roughly 0.17 US dollars.

Disadvantages: Although the Ethereum Blockchain, which is the finest for smart contracts, is used in the proposed system. For transactions, a digital signature is used. Every time it gets awkward to use a digital signature on every transaction. [5]

This research focuses on utilizing Blockchain technology to enhance the transparency and credibility of agricultural supply chains and operations. In recent times, there has been a notable shift in the production of food and its underlying resources. The study sought an effective means to connect the farmers who produce goods with the end consumers in the market. The approach involved implementing a Blockchain-based framework and its principles to establish reliability and openness among users and their transactions. This paper also addresses a potential limitation where farmers may not have complete knowledge about the traceability of their registered products.

Disadvantages: The only users with the ability to initiate or terminate transactions on this blockchain are farmers. The *majority of farmers are uneducated, thus their knowledge of blockchains is limited.* [6]

Blockchain technology is regarded as a means to enhance traceability within the agri-food supply chain and provide stakeholders with crucial information regarding food quality, safety, and nutrition. However, a lack of understanding in designing the user interface for traceability applications may result in usability challenges. In an effort to enhance the usability of agri-food traceability applications based on blockchain, this paper examined prior studies from a user interface standpoint.

Disadvantages: Provides a general understanding of the only user interfaces currently in use, which are confusing and inefficient for users. This system's suggested design calls for a high price tag. [7]

The supply channels in place today to tackle counterfeit goods are dependent on a single point of authority. This design has problems with storage, failure, and single point processing. Blockchain technology has come to light as a possible solution to these issues. In this work, we propose a novel decentralized supply chain, called the block-supply chain, which detects counterfeiting assaults by using Near Field Communication (NFC) and blockchain technologies. The centralized supply chain design is replaced with a new proposed consensus protocol termed block-supply chain, which finds a balance between security and efficiency. It is entirely decentralized, in contrast to current protocols. Our simulations show that the proposed protocol provides outstanding performance with a reasonable level of security when compared to the state-of-the-art consensus protocol Tendermint. [10]

This paper illustrates how crucial it is for policymakers and the governance structure to plan for the protection and security of their citizens and customers for businesses. The primary issue of counterfeit goods in the modern world is addressed in this study. In order to address the issue of counterfeiting in the Indian economy, this research highlights the needs and potential of distributed ledger technologies, such as blockchain. Following the gathering of expert opinion to better understand the problem, the research employs the SWARA (Step-wise Weight Assessment Ratio Analysis)-WASPAS (Weighted Aggregated Sum Product Assessment) technique, which leads to the prioritization of blockchain implementation in various industries. The weights of the criteria are assessed using SWARA, and the alternatives are assessed and prioritized using WASPAS. [9]

Manufacturing and marketing of fake or knockoff products and commodities puts consumers' finances, health, and safety at risk. Additionally, it harms the economic development of original manufacturers and companies through lost sales, product slander, downtime, replacement costs, forcing many brands to spend money fighting counterfeits, possibly jeopardizing the confidence of business partners, stealing sales, etc. A blockchain-based system is used in the identification of original products and also identifies duplicate products to ensure the identification of original goods in order to overcome and stop these significant effects of counterfeiting. In this project, QR (Quick Response) codes and barcodes offer a method to reduce the practise of counterfeiting due to the significant new trends in wireless technology. [8]

III. Existing System

A supply chain encompasses a coordinated network, requiring any SCM system to possess a unified structure that facilitates functionality and visibility throughout the product delivery process. This typically involves the integration of features like inventory management, warehouse management, processing of purchase orders, forecasting demand, managing supplier relationships, planning logistics, and more. Additionally, most SCM systems incorporate bookkeeping functionalities to facilitate effective ledger management and financial optimization.

In recent years, there has been a growing adoption of cloud-based SCM systems delivered as software-as-a-service (SaaS). This approach allows businesses to oversee the entire lifecycle of a project, providing detailed monitoring and comprehensive visibility at every stage. This shift addresses the limitations of traditional SCM systems, which lack the 360° management capabilities offered by cloud technology. However, it's important to note that like any technology, cloud-based systems may have potential drawbacks, such as concerns about data security, dependency on internet connectivity, and potential subscription costs. These potential disadvantages are not specifically addressed in the provided passage.

IV. Proposed System

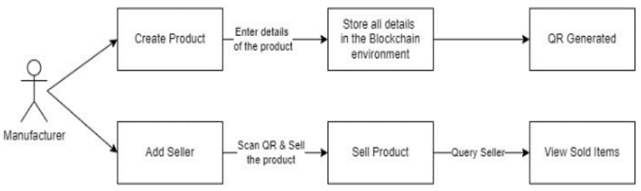
Our groundbreaking blockchain-based supply chain system revolutionizes information management for participants. It records the product details in the form of a QR code and this can be verified by the customer. This information, securely stored on the blockchain, ensures heightened traceability and minimizes losses from counterfeit activities. It also provides superior visibility and compliance in outsourced manufacturing, positioning organizations as responsible manufacturing leaders.

Blockchain's reach extends far beyond finance, with industry leaders and startups exploring its diverse applications. Provenance, a transparency startup, recently completed a successful pilot tracking tuna sourcing in Indonesia. Monegraph, established in 2014, employs blockchain to safeguard digital media usage rights, facilitating fair revenue distribution. Skuchain focuses on blockchain-based B2B trade and supply chain finance products, targeting the global trade finance market.

Blockchain-driven supply chain innovations promise significant business value. They enhance transparency, reduce risks, and optimize overall management. Here's how it operates: Manufacturers generate a unique QR code as they create a product, seamlessly integrating the seller into the system. Once sold, all pertinent details are accessible on the seller's page. When the consumer scans the QR code upon purchase, the system promptly verifies the product's authenticity. This ensures consumer confidence and trust in the supply chain process. Embrace the future of supply chain management with our cutting-edge blockchain solution.

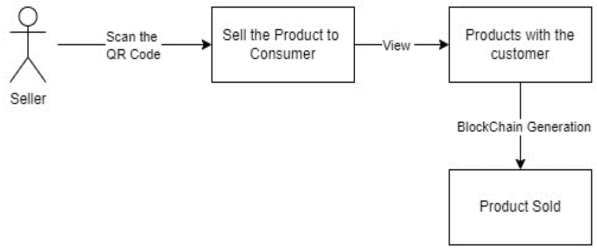
V. System Design

Manufacturer Module:


Manufacturer
Create Product
Enter details of the product
Store all details in the Blockchain environment
QR Generated
Add Seller
Scan QR & Sell the product
Sell Product
Query Seller
View Sold Items

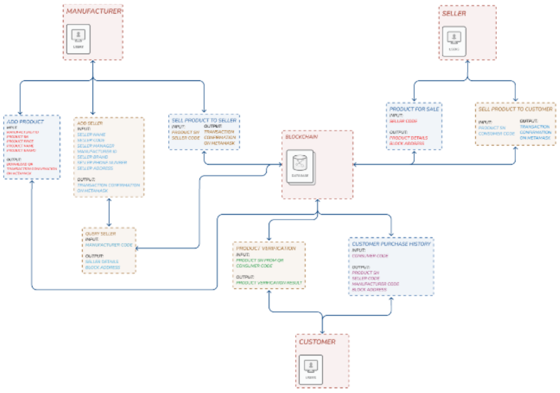
Figure(1): Manufacturer Module

Seller Module:



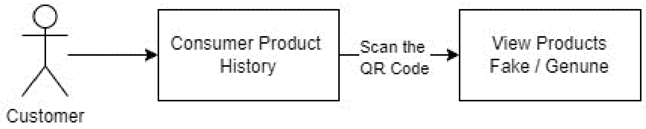
Figure(2): Distributer Module

System Architecture:



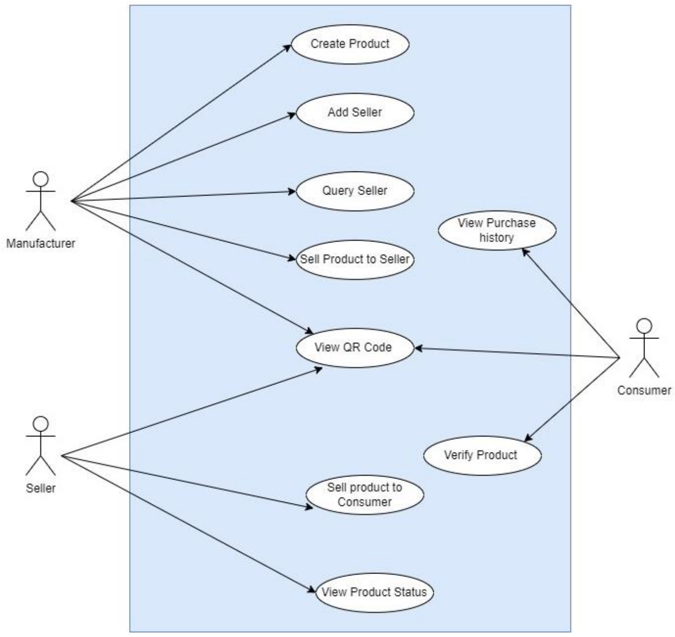
Figure(3): System Architecture

Consumer Module:



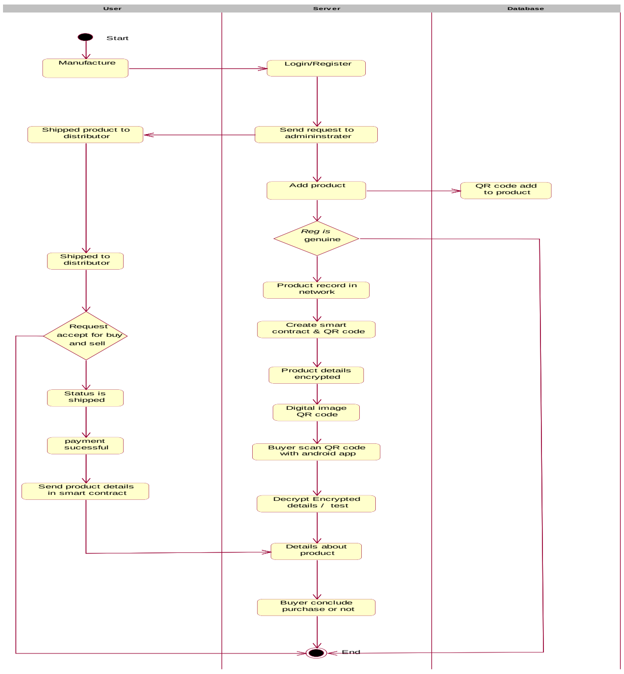
Figure(4): Consumer Module

Use Case Diagram:



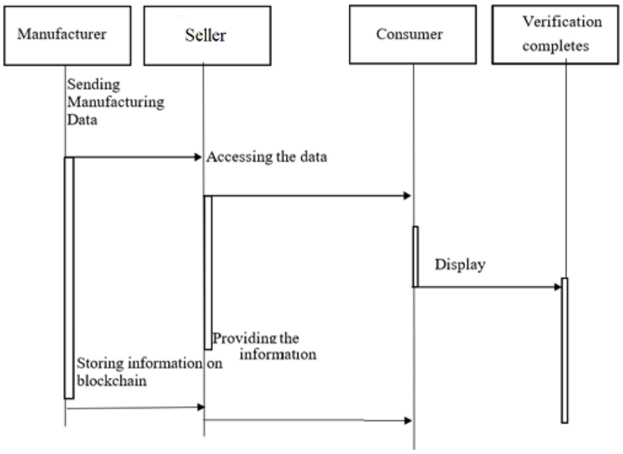
Figure(5): Use Case Diagram

Activity Diagram:


User
Server
Database
Start
Manufacture
Login/Register
Shipped product to distributor
Send request to admininstrater
Add product
QR code add to product
Reg is genuine
Shipped to distributor
Product record in network
Create smart contract & QR code
Request accept for buy and sell
Product details encrypted
Status is shipped
Digital image QR code
payment sucessful
Buyer scan QR code with android app
Send product details in smart contract
Decrypt Encrypted details / test
Details about product
Buyer conclude purchase or not
End

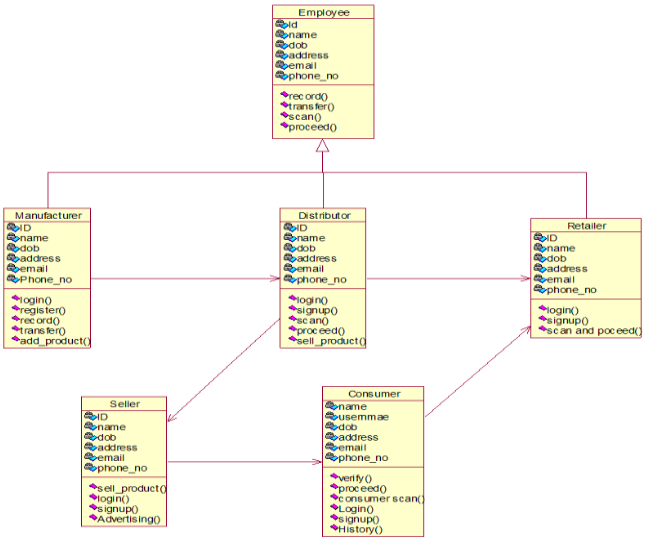
Figure(6): Activity Diagram

Sequence Diagram:


Manufacturer
Seller
Consumer
Verification completes
Sending Manufacturing Data
Accessing the data
Display
Providing the information
Storing information on blockchain

Figure(7): Sequence Diagram

Class Diagram:



Figure(8): Class Diagram

VI. Project Security Goals

Data Integrity is a crucial aspect of blockchain technology, ensuring that the product data stored within it remains unchanged and tamper-proof. This means that once information is recorded, it cannot be altered or manipulated, providing a high level of trust and reliability in the system.

Authentication plays a vital role in securing the supply chain by verifying the identities of all participants involved. This authentication process ensures that only authorized and legitimate entities are allowed access, reducing the risk of fraudulent activities or malicious actors infiltrating the system.

Confidentiality is paramount in protecting sensitive client and corporate data. The blockchain system must implement robust encryption and access control measures to prevent unauthorized parties from gaining access to private information. This safeguarding of data privacy is essential for maintaining trust and compliance with privacy regulations.

Availability is a fundamental requirement to ensure the continuous operation of the blockchain system. Despite potential threats or disruptions, the system must remain accessible and functional at all times. This resilience is crucial for maintaining the smooth flow of transactions and information within the supply chain.

Non-repudiation is a key feature of blockchain, meaning that once a party records an activity or transaction, they cannot later deny their involvement. This enforces accountability and trust among participants, as it prevents any party from disowning their actions within the system, thus ensuring transparency and integrity in the process.

VII. Security Requirements Specification

Blockchain technology, a decentralized ledger system, employs cryptographic security measures to safeguard stored data, preventing unauthorized alterations. This ensures the integrity and immutability of the information contained within. Additionally, stringent user authentication protocols are imperative to restrict system access solely to authorized personnel. This fortifies the system against potential breaches and maintains confidentiality.

Within the intricate framework of supply chains, secure communication is paramount. Employing encryption for all interactions between involved parties safeguards sensitive information, such as product details and logistics, from interception or manipulation. This guarantees the trustworthiness of the supply chain process.

To ensure uninterrupted service, regular system backups and redundancy procedures are vital. This precautionary approach mitigates the impact of potential technical failures, ensuring consistent availability of the blockchain network. Furthermore, transaction records, fundamental to the transparency and accountability of the system, must be both unchangeable and traceable to the responsible parties. This feature not only instills trust in the system but also holds individuals accountable for their actions within the blockchain environment. These combined measures serve as the foundation for a secure, reliable, and trustworthy blockchain ecosystem.

VIII. THREATS AND VULNERABLITIES

(a). Threat: Data Manipulation

Explanation: Data manipulation refers to unauthorized alterations or changes made to data, which can lead to incorrect information being used or stored.

Vulnerability: This can occur if data is not adequately protected or if there are weak controls in place to prevent unauthorized access.

Counter-Measure: Cryptographic hashing and digital signatures are used to ensure data integrity. Cryptographic hashing creates a unique fingerprint (hash) of data, and any alteration will result in a different hash. Digital signatures provide a way to verify the authenticity of the sender and the integrity of the data.

(b). Threat: Unauthorized Access

Explanation: Unauthorized access occurs when individuals gain entry to systems, applications, or data without proper authorization.

Vulnerability: Weak or misconfigured access controls, such as insufficiently strong passwords or ineffective user permissions, can lead to unauthorized access.

Counter-Measure: Multi-factor authentication adds an extra layer of security by requiring users to provide multiple forms of identification, such as a password and a one-time code sent to their phone. Additionally, proper access controls limit user privileges based on their role, ensuring they only have access to necessary resources.

(c). Threat: Network Eavesdropping

Explanation: Network eavesdropping involves unauthorized interception and monitoring of data being transmitted over a network.

Vulnerability: Insecure communication channels or protocols can expose data to eavesdropping attacks.

Counter-Measure: Transport Layer Security (TLS) encryption ensures that data transmitted between systems is encrypted, making it unreadable to anyone attempting to intercept it.

(d). Threat: Denial of Service (DoS) Attacks

Explanation: DoS attacks aim to overwhelm a system, network, or service, causing it to become slow or unavailable for legitimate users.

Vulnerability: Systems without adequate measures to handle high volumes of traffic are vulnerable to such attacks.

Counter-Measure: Load balancing distributes incoming traffic across multiple servers, preventing any single server from becoming overloaded. Redundancy ensures that if one component fails, there are backup resources available. Rate limiting sets a cap on the number of requests a system can handle, preventing it from being overwhelmed.

(e). Threat: Insider Threats

Explanation: Insider threats involve individuals with legitimate access to systems and data who misuse their privileges, intentionally or unintentionally causing harm.

Vulnerability: Insufficient controls and monitoring can lead to insider threats going undetected.

Counter-Measure: Role-based access control assigns specific permissions to users based on their role within the organization. Regular auditing of user activities allows for the detection of any unusual or suspicious behaviour.

IX. SECURITY REQUIREMENTS SPECIFICATION

QR Code Generation Module:

This module is responsible for creating unique QR codes for each product. The QR codes are generated using blockchain technology, ensuring that they cannot be easily replicated or tampered with. These QR codes serve as a digital fingerprint for each product.

Blockchain Integration Module:

This module involves the integration of blockchain technology, which consists of a series of blocks to securely store and manage data related to product authenticity. The data stored in these blocks is immutable, meaning it cannot be altered or deleted once recorded.

Product Authentication Module:

This critical module is responsible for the actual process of verifying the authenticity of products. It allows consumers to scan the QR code on the product packaging using a mobile device or dedicated scanner. The system then retrieves information from the blockchain to confirm whether the product is genuine or counterfeit.

Smart Contracts Implementation Module:

Smart contracts are self-executing contracts with predefined rules and conditions. In this module, smart contracts are created and deployed on the blockchain to facilitate interactions between different parties in the supply chain. For example, a smart contract may automatically trigger a dispatch once a product reaches a certain stage in the supply chain.

User Interface (Decentralized Application):

This module focuses on creating a user-friendly interface for consumers. It can be a web or mobile application that allows users to easily scan QR codes, view product information, and receive instant feedback on the authenticity of the product. The UI should be intuitive and easy to navigate.

Security Enhancement Module:

This module addresses security concerns related to the storage and retrieval of product data. It implements robust encryption techniques and other security measures to protect sensitive information stored on the blockchain.

X. Test Cases

(a). Manufacturer test case

Test Case	1
Name of Test	Manufacturer
Input	Takes the input from the manufacturer
Expected output	Will generate the QR code
Actual output	The QR can be downloaded, which is used to sell the product later
Result	Successful

Figure(9): Manufacturer test case

(b). Seller test case

Test Case	2
Name of Test	Seller
Input	Takes the data from the seller
Expected output	Automatic detection of Product code from the QR Code
Actual output	The Detected Manufacturer code is shown in the Product SSN
Result	Successful

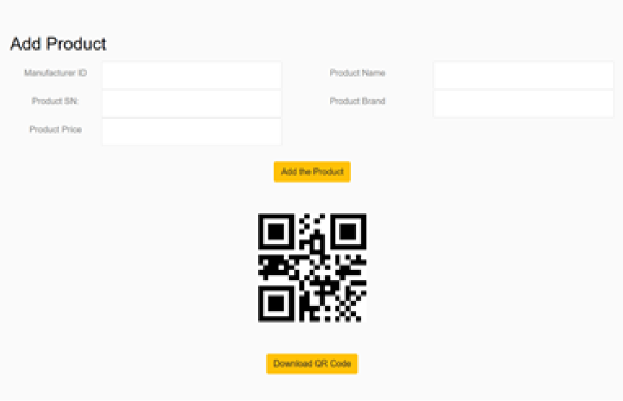
Figure(10): Seller test case

(c). Consumer test case

Test Case	3
Name of Test	Consumer
Input	Get the output from the retailer and family gives
Expected output	QR code will be checked and the desired output will be shown
Actual output	QR code is checked and the product is shown Genuine or Fake
Result	Successful

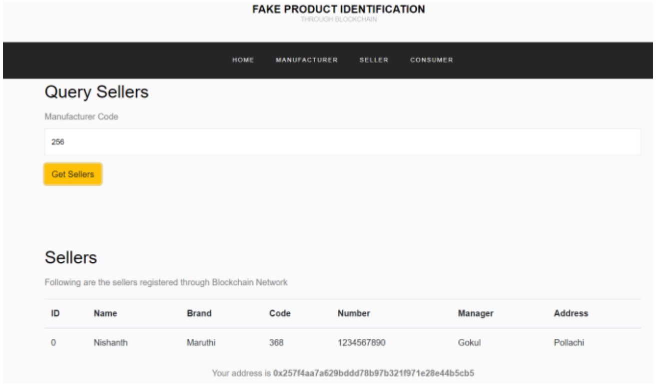
Figure(11): Consumer test case

XI. Results



Add Product

Figure(12): After adding the Product, the QR code is Generated and it can be downloaded.



FAKE PRODUCT IDENTIFICATION
THROUGH BLOCKCHAIN

Query Sellers

Manufacturer Code: 256

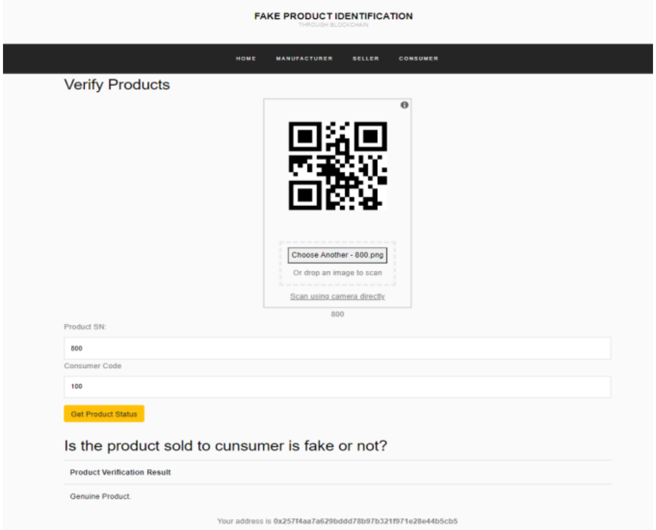
Sellers

Following are the sellers registered through Blockchain Network

ID	Name	Brand	Code	Number	Manager	Address
0	Nishanth	Maruthi	368	1234567890	Gokul	Pollachi

Your address is 0x257f4aa7a629bddd78b97b321f971e28e44b5cb5

Figure(13): On Query seller page, on entering the Manufacturer code, it gives the seller details like seller code, seller name, seller mobile number as well as the address and the corresponding seller's Manager name.



FAKE PRODUCT IDENTIFICATION
THROUGH BLOCKCHAIN

Verify Products

Product SN: 800

Consumer Code: 100

Is the product sold to cunsumer is fake or not?

Product Verification Result
Genuine Product.

Your address is 0x257f4aa7a629bddd78b97b321f971e28e44b5cb5

Figure(14): By uploading the QR, and entering the Consumer Code, the Verification is displayed, i.e., if the product is sold to that particular consumer, it shows the Product as Genuine Product else it displays as the Fake Product.

XII. Conclusion

Our innovative system harnesses the power of blockchain technology to revolutionize the battle against counterfeit products. By implementing a nominal transaction fee, users gain a robust shield against the risk of inadvertently purchasing fake goods. This breakthrough not only empowers consumers but also grants manufacturers unprecedented control and visibility into their product sales. Through blockchain, crucial details such as total sales volume and remaining inventory are made transparent, instilling confidence in both buyers and sellers.

Furthermore, our system employs digital signatures for identity verification, ensuring that private keys remain impervious to unauthorized access. This guarantees an extra layer of security for all parties involved. The meticulous cost analysis demonstrates the exceptional affordability of our approach, offering a stark contrast to traditional large-scale retail channels. This economic advantage opens up new possibilities for smaller companies with limited financial resources, allowing them to compete on a level playing field while providing consumers with the peace of mind they deserve.

XIII.Future Work

While our system marks a significant leap forward, the ever-evolving nature of blockchain technology necessitates ongoing research and development. A paramount objective is to streamline the codebase, enhancing simplicity for widespread adoption and future expansion. Introducing genuine product warranties into the platform stands as a promising avenue for further improving the customer experience and reinforcing supply chain transparency. This development would offer consumers an unprecedented level of assurance in the authenticity of their purchases.

Moreover, envisioning a cross-border product tracing framework represents an ambitious goal for the future. This framework would provide regulatory bodies worldwide with accurate and comprehensive data, facilitating more effective oversight of product authenticity. Achieving this level of data quality will require collaborative efforts, uniting regulatory support, framework development, and data-sharing initiatives. This project lays the groundwork for a more secure and transparent consumer marketplace, promising a brighter future for both manufacturers and consumers alike.

XIV.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 Blockchain", 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] Eka Dyar Wahyuni and Arif Djunaidy, "Fake Review Detection from a Product Review Using Modified Method of Iterative Computation Product", January 2016 Research Gate

[9] M. C. Jayaprasanna, V. A. Soundharya, M. Suhana and S. Sujatha, "A Block Chain based Management System for Detecting Counterfeit Product in Supply Chain," 2021 Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV), 2021, pp. 253-257

[10] Singh, Shivam & Choudhary, Gaurav & Kumar, Shishir & Sihag, Vikas & Choudhary, Arjun. (2021). Counterfeited Product Identification in a Supply Chain using Blockchain Technology. 10.22667/ReBiCTE.2021.07.15.003