Fake Product Identification Scanner Using Blockchain

[1]HARINI.M, [2]ANKITHA.I, [3]LAVANYA.M, [4]SARAVANAN ELUMALAI
[5]DR. V. SAI SHANMUGARAJA, [6]DR. G. GUNASEKARAN
[1,2,3,] IV Year B.Tech CSE Students, [4,] Assistant Professor, [5,6,]professor
Dept of Computer Science and Engineering,
Dr. MGR Educational and Research Institute,
Maduravoyal, Chennai-95, Tamil Nadu, India
[1]muraliharini2003@gmail.com, [5]saishanmugaraja.cse@drmgrduac.in, [6]gunasekaran.cse@drmgrdu.ac.in

***Abstract*— Safeguarding a company's products from counterfeiting is crucial for sustainable business development, which can detrimentally impact brand image and pose potential health risks due to inferior product quality. Counterfeiters exploit lower-quality materials and production methods for financial gain. Identifying counterfeit products is challenging for consumers, often requiring examination by a trained professional, incurring time and cost. In this paper, we propose a method for counterfeit detection through a simple scan of the product's quick response code, which is generated by unique algorithms. These QR codes, being both unique and resistant to replication, offer enhanced security against forgery. Additionally, implementing an encrypted peer-to-peer database system further fortifies the defense against tampering by attackers. This innovative approach aims to reduce manufacturing and material costs associated with traditional counterfeiting methods like Radio-Frequency Identification and holographic techniques.**

***Keywords*—Blockchain, counterfeit, QR code**

1. INTRODUCTION

The global advancement of a product or technology inherently carries risks such as counterfeiting and duplication, which can adversely impact a company's reputation, revenue, and customer satisfaction. The proliferation of counterfeit products in trade and marketing is escalating rapidly. To address the identification of fraudulent goods and combat this issue, a fully operational blockchain system is suggested. Companies would only need to invest minimal effort, alleviating concerns about counterfeit products. The prevalence of counterfeit items poses significant challenges for manufacturers, resulting in substantial damage to the company's reputation and brand value. A potential solution to this predicament involves the adoption of a blockchain-based system. Blockchain, a distributed and decentralized technology, stores data in blocks within a connected chain in the database. When new data is introduced, it seamlessly integrates with existing data, forming a continuous chain. Notably, blockchain prevents users from modifying or deleting existing data, ensuring the security and integrity of information. This capability positions blockchain as a valuable tool in mitigating the problem of counterfeit products.

2. RELATED WORK

In this article “Fake Product Monitoring System using Artificial Intelligence”[1] by Roy, Reema and Patil, Sunita, uses a mobile application for logo detection, utilizing an Artificial Intelligence algorithm to distinguish between counterfeit and genuine products based on diverse features such as shapes, text, font, and color. The system operates through two distinct phases. The initial phase involves logo detection through spelling and color recognition, while the subsequent phase entails training the Machine Learning model and subsequently identifying fake or authentic logos through the Feature Extraction method.

This article “A Novel RFID-Based Anti-Counterfeiting Scheme for Retail Environments”[2] by G. Khalil, R. Doss and M. Chowdhury uses an innovative and secure method for anti-counterfeiting through the utilization of RFID technology. It is designed to be lightweight, making it well-suited for implementation in extensive retail settings with the use of affordable passive tags. Additionally, we conduct an examination of a recent proposal by Tran and Hong to pinpoint certain vulnerabilities in their scheme. A comprehensive security analysis of the suggested system demonstrates its adherence to formal security requirements, ensuring correctness and resilience against security attacks.

The article "IMPROVING FAKE PRODUCT DETECTION USING AI- BASED TECHNOLOGY"[3] by Daoud, Eduard & Vu Nguyen Hai, Dang & Nguyen, Hung & Gaedke, Martin, primarily focuses on the architecture of an AI application, comprising three key components: the dataset, detection models, and the trained model. It is designed as a machine learning-based solution for anti-counterfeiting, specifically aiming to identify counterfeit products. The process involves two crucial steps: training the models and detecting logos. The Faster R-CNN method is employed for its ability to achieve high accuracy with a reduced training time. In the realm of AI and machine learning applications, Convolutional Neural Networks (CNN) tend to be time and memory-intensive, necessitating both training and testing phases before practical implementation. Notably, this artificial intelligence system may fall short in detecting tag reapplication attacks, where a counterfeiter removes a legitimate tag from an authentic product and affixes it to a counterfeit or expired item.

The article "Lightweight Authentication Protocol for NFC Based Anti-Counterfeiting System in IoT Infrastructure"[4] by B. A. Alzahrani, K. Mahmood and S. Kumari presents an innovative authentication protocol designed for anti-counterfeiting drug systems, leveraging the Internet of Things (IoT) to verify the legitimacy of individual drug unit dosages. The protocol utilizes near-field communication (NFC) for its suitability in mobile environments. Additionally, our approach includes a dependable update phase specifically tailored for NFC. Moreover, the system is accompanied by a performance assessment and employs the random oracle model for a formal security analysis.

In this article "Preventing Counterfeit Products Using Cryptography, QR Code and Webservice"[5] by Shaik, Cheman, it shows the incorporation of QR codes containing both public and private keys for products. The scanning application employed must possess cryptographic capabilities to decipher the QR code. Additionally, the manufacturer is required to operate a server for processing requests, verifying the buyer's name, and matching it with the item code. The scanning application should also feature cryptographic functionality to decrypt the cipher text embedded in the QR code, corresponding to the item code. Existing systems face limitations as brands utilize QR codes on products to authenticate their validity; however, these QR codes are susceptible to duplication and may be exploited to label counterfeit products.

This article "Application for Counterfeit Detection in Supply Chain using Blockchain Technology" [6] by A. Thakkar, N. Rane, A. Meher and S. Pawar uses decentralized technology such as blockchain in the supply chain guarantees the traceability of goods through an unalterable transaction history, preventing the infiltration of counterfeit products. This fosters transparency and collaboration among manufacturers, suppliers, and distributors, as all pertinent information is recorded and easily accessible, reducing the risk of tampering with records. Hence, they intend to deliver an efficient and economical implementation that ensures the security, decentralization, and verifiability of a supply chain. This solution addresses shortcomings in authentic product supply, streamlining the identification of faulty areas and reducing associated costs.

3. EXISTING SYSTEM

The system effectively combats product counterfeiting in the retail market, benefiting manufacturers and consumers. However, it encounters a flaw when a genuine product's QR code is transferred to a fake one, leading the initially sold item to be perceived as authentic, irrespective of its actual authenticity. Additionally, the extensive storage of supply chain details for each product demands a substantial memory capacity, contributing to the system's overall costliness.

4. PROPOSED SYSTEM

Counterfeit has spread worldwide and has huge effects on organizations, manufacturers, and consumers. It affects the influence of the organization and the wellbeing of the consumers. The proposed system uses a copy-resistant QR code, so the counterfeiters can't copy the original products QR code. The system scans the product's QR code to detect whether the product is original or fake. If the product is detected as fake, then a notification is sent to the concern manufacturer that their company's product is detected as fake. So the manufacturer is aware that their company's product is counterfeited. This system helps both the manufacturers and consumers.

5. METHODOLOGY

In this system, the Manufacturer and consumer are the primary components. Upon the manufacturer's login, they input product details such as product ID, name, and company name. This information is then securely stored in blocks, with the SHA-256 algorithm generating a unique hash code for the data. Subsequently, this hash code is transformed into a copy resistant QR code using secure QR code technology. This QR code is printed on the product. When a consumer purchases the product, they scan the QR code using either a webcam or a QR-code scanner.

Verification occurs by comparing the hash code within the blockchain to the one generated after scanning. A match confirms the product's authenticity; otherwise, it is flagged as counterfeit. Then it sends a notification to the concern manufacturer that one of their company product is detected as fake. This helps the manufacturer to know that their product is forged.

Implementation of this project involves angular17, HTML,CSS, javascript, node JS ,springboot, a MySQL database for efficient data storage, and apache, tomcat a web server to support seamless communication between modules.

We have deployed a blockchain by following the outlined steps:
The data will be stored in JSON format, known for its simplicity in both implementation and readability. Each block houses multiple copies of the data, and new blocks are added every minute. Fingerprinting is utilized to distinguish between these blocks.

Hashing, specifically the SHA256 method, is employed to ensure data integrity. Each block possesses a unique hash, incorporating the hash of the preceding block, preventing data manipulation. The current block's hash becomes the previous hash for the next block, creating an interconnected chain of blocks.

To enhance security, a proof-of-work method is implemented, increasing the difficulty of creating and adding new blocks to the chain. This design ensures that anyone attempting to edit a previous block must redo the work associated not only with that block but also with all subsequent blocks. Further restrictions can be imposed by elevating the difficulty level for creating new blocks.

6. CONCLUSION

The rise of counterfeit products is surging, necessitating robust measures for detection. The proposed system offers a promising solution to the limitations of conventional anti-counterfeiting methods. It enables the identification of genuine or fake products through the integration of QR codes and blockchain technology. This approach eliminates the dependency on third-party confirmation for product safety, ensuring a more reliable and accurate authentication process.

7. FUTURE WORK

A future enhancement may explore additional security measures, scalability, and integration with e-commerce platforms.

REFERENCE

[1] Roy, Reema and Patil, Sunita, Fake Product Monitoring System using Artificial Intelligence (May 7, 2021). Proceedings of the 4th International Conference on Advances in Science & Technology (ICAST2021), Available at SSRN: https://ssrn.com/abstract=3867602 or http://dx.doi.org/10.2139/ssrn.3867602

[2] G. Khalil, R. Doss and M. Chowdhury, "A Novel RFID-Based Anti-Counterfeiting Scheme for Retail Environments," in IEEE Access, vol. 8, pp. 47952-47962, 2020, doi: 10.1109/ACCESS.2020.2979264.

[3] Daoud, Eduard & Vu Nguyen Hai, Dang & Nguyen, Hung & Gaedke, Martin. (2020). IMPROVING FAKE PRODUCT DETECTION USING AI- BASED TECHNOLOGY. 10.33965/es2020_202005L015.

[4] B. A. Alzahrani, K. Mahmood and S. Kumari, "Lightweight Authentication Protocol for NFC Based Anti-Counterfeiting System in IoT Infrastructure," in *IEEE Access*, vol. 8, pp. 76357-76367, 2020, doi: 10.1109/ACCESS.2020.2989305.

[5] Shaik, Cheman, Preventing Counterfeit Products Using Cryptography, QR Code and Webservice (February 18, 2021). Computer Science & Engineering: An International Journal (CSEIJ), Vol 11, No 1, February 2021, Available at SSRN: https://ssrn.com/abstract=3787844

[6] A. Thakkar, N. Rane, A. Meher and S. Pawar, "Application for Counterfeit Detection in Supply Chain using Blockchain Technology," *2021 International Conference on Advances in Computing, Communication, and Control (ICAC3)*, Mumbai, India, 2021, pp. 1-6, doi: 10.1109/ICAC353642.2021.9697187.

[7] P. S, H. K, T. N and P. B. Babu, "Counterfeit Product Detection In Supply Chain Management With Blockchain," *2022 1st International Conference on Computational Science and Technology (ICCST)*, CHENNAI, India, 2022, pp. 841-844, doi: 10.1109/ICCST55948.2022.10040383.

[8] N. M. Chinni, S. Sri Burramsetty, S. D. Achnata, R. Kotturu, A. A. Sai and N. Neelima, "Counterfeit Drug Detection System with Multi-Layered Check and SCM using Blockchain," *2022 6th International Conference on Computing Methodologies and Communication (ICCMC)*, Erode, India, 2022, pp. 61-65, doi: 10.1109/ICCMC53470.2022.9753778

[9] M. M. Hassan Sohan, M. M. Khan, I. Nanda and R. Dey, "Fake Product Review Detection Using Machine Learning," *2022 IEEE World AI IoT Congress (AIIoT)*, Seattle, WA, USA, 2022, pp. 527-532, doi: 10.1109/AIIoT54504.2022.9817271.