iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 12 **Issue:** III **Month of publication:** March 2024

DOI: https://doi.org/10.22214/ijraset.2024.59338

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 12 Issue III Mar 2024- Available at www.ijraset.com

Fake Product Identification System for E-Commerce Applications

Sireesha Keesara[1], Tanmayee Veerabhadra[2], Sai Sriya Tiruveedhula[3], Uma Varshitha Reddy Vajrala[4], Venkata Lakshmi Vemula[5]

[1]*Assistant Professor, Department of CSE, Vasireddy Venkatadri Institute of Technology (Autonomous), Guntur, AP*
[2, 3, 4, 5]*UG Students, Department of CSE, Vasireddy Venkatadri Institute of Technology (Autonomous), Guntur, AP*

Abstract: ***The use of blockchain technology, combined with QR codes, presents a promising solution for identifying and combating counterfeit products efficiently and securely. By integrating a blockchain-based system with QR code scanning, stakeholders can establish a reliable mechanism to verify product authenticity. This system involves storing product details and generating unique QR codes for each product as blocks in the blockchain database. When a QR code is uploaded, the system compares the code against entries in the blockchain database. If a match is found, the customer receives a notification confirming the product's authenticity; otherwise, they are alerted that the product is fake. Blockchain technology's ability to eliminate the need for trusted intermediaries, facilitate faster transactions, and provide transparency makes it particularly intriguing for addressing counterfeit issues. However, reducing counterfeits requires a comprehensive approach, including increasing awareness, legal action against counterfeiters, implementing a robust alert system, and ensuring secure packaging. These factors, combined with blockchain technology and digital signature verification, can lead to a more efficient and thorough strategy for combating counterfeiting in the marketplace.***

Keywords: Blockchain, Validation, Encryption, QR code, Digital Signature, SHA-256

I. INTRODUCTION

Counterfeiting poses an incredible risk across industries, causing significant economic loss and endangering consumer welfare. The staggering annual costs of counterfeiting in the US alone, estimated at $600 billion, and projected global impacts of $4.2 trillion by 2022 highlight the urgency of addressing this issue. The counterfeit medicine market, valued at $75 billion annually, further underscores the severity of the problem, contributing to approximately 1 million deaths each year.

In transactions, trust is essential, but intermediaries such as banks often complicate matters, increasing costs and reducing transparency. However, blockchain technology, as demonstrated by Bitcoin, offers a promising solution by enabling decentralized transactions, thus bypassing intermediaries and enhancing security. This paper investigates the potential of blockchain technology in combating counterfeiting. It proposes a decentralized inventory management system involving blockchain and its related features to detect counterfeit attacks, aiming to replace centralized supply chain models and improve security and efficiency. Subsequent sections explore traditional anti-counterfeiting methods, the design of the blockchain-based inventory management system, its performance, and concluding remarks on its potential to revolutionize efforts against counterfeiting

II. LITERATURE REVIEW

The literature review underscores the significance of combatting counterfeiting to protect financial interests, reputation, and consumer safety. It highlights key features of effective anti-counterfeiting measures, including difficulty of duplication, ease of identification, prevention of re-use, and indicators of tampering. Strategies explored encompass incorporating visible and covert elements into product design, utilizing track-and-trace technologies like RFID and barcodes, and enhancing vigilance against counterfeit suppliers.

1) Satoshi Nakamoto introduced blockchain as a core component of Bitcoin in 2008. Various blockchains serve different purposes, with Bitcoin having its own blockchain, known as the Bitcoin blockchain.

2) Christophe Zimmermann, from the World Customs Organization, notes the alarming prevalence of counterfeit drugs, stating, "We already have more fakes than genuine drugs in the market".

3) The citation "Blockchain Past Bitcoin" by S. Underwood underscores that blockchain technology, the backbone of Bitcoin, operates without reliance on a central authority, as transaction validity is determined by algorithms. This eliminates the need for third-party trust. Additionally, it highlights the broader applicability of blockchain beyond financial transactions, suggesting its potential to revolutionize the digital economy.

4) L. Li fights that extraordinary adversary of fashioning strategies should all around be not difficult to apply, yet difficult to duplicate and have four chief features: They should be trying to duplicate, it should be plausible to recognize them without uncommon stuff, it should be hard to re-use them, and it should be evident expecting they were adjusted. As indicated by a thing perspective, there are three general developments to diminish fakes -Unquestionable (Recognizable) Components expected to assist the clients with insisting the legitimacy of a pack. Such features will be essentially perceptible, and convoluted or expensive to reproduce.

5) Berman Associations need to ensure that they have the genuine confirmation and enlistments set up to be defended against fakes, this consolidates brand names, copyrights, plan licenses, etc. With this set up, it can anyway be excessive to actually fight against fakes. Especially luxury stock associations consume millions to fight fakes and work alongside confidential specialists really. Having a spending plan for circling back to fakes is thusly huge Controlling reexamine suppliers - Numerous associations use re-appropriated suppliers.

If a product is suspected to be counterfeit, immediate action should be taken, starting with visual inspection of its packaging and contents. If confirmed as fake, patients should be notified, and authorities must investigate its origin to combat counterfeiters and increase awareness. This approach aims to combat counterfeiting by enhancing vigilance and disrupting criminal networks.

III. METHODOLOGY

The research methodology involves the implementation of a blockchain-based system with four main functionalities as mentioned in the Fig 1: product registration, product retrieval, product updating, and product verification. Initially, products are registered on the blockchain, and a QR code is generated for each registered product uniquely. Users can then retrieve product information using the QR code. Furthermore, the system allows for updating product details on the blockchain. Finally, the blockchain is utilized to verify the authenticity of registered products. This methodology ensures secure and transparent tracking of product information throughout its lifecycle using blockchain technology.

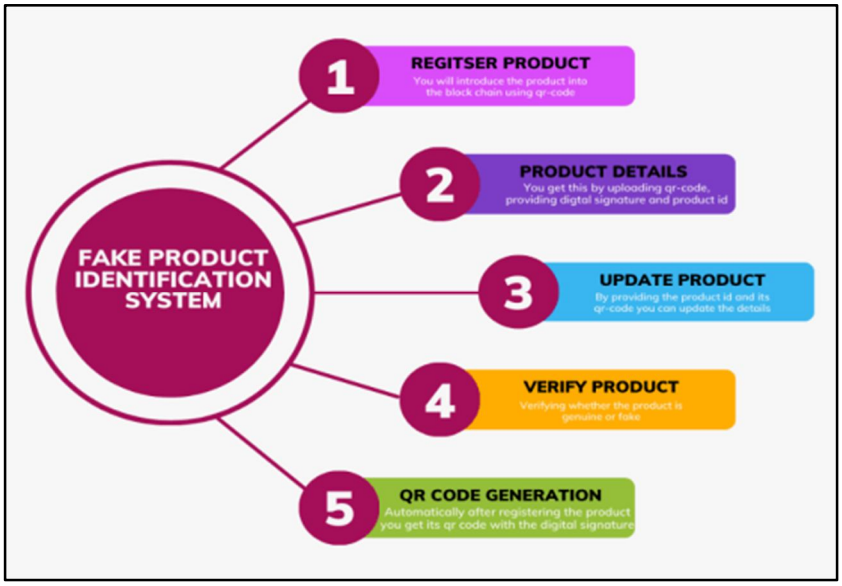


Fig.1 Work Flow of our Identification System

A. Blockchain

Essentially, blockchain is a distributed organization where the interconnected frameworks are completely open and straightforward to each other. It comprises of N number of blocks which are binded together to frame a Blockchain. Every single block comprises of the exchanges which have been endorsed by the companions. Block chain usage ensures traceability, decentralization, authentication.

Overall, blockchain technology has the capability for the detection and prevention of counterfeit products by providing an authenticated, transparent, and tamper-proof application for tracking goods throughout the supply chain. However, widespread adoption and collaboration among stakeholders will be crucial for its success in combating counterfeit products effectively.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 12 Issue III Mar 2024- Available at www.ijraset.com

B. QR Code

QR codes are commonly used in conjunction with blockchain technology for fake product detection for several reasons like there will be Easy Access to Information, Secure Verification, User understandability, uniqueness.
Overall, QR codes serve as a practical and efficient means of linking physical products to their corresponding blockchain records, enabling transparent and secure product authentication and traceability in the fight against counterfeit goods.

C. SHA-256

It is a cryptographic hash function that gives unique hash values from input data, ensuring data and its security. In digital signature, SHA-256 hashes the document, then senders data is encrypted by using a private key and a signature is created. Upon receiving the signature, the decryption is done by using the sender's public key in the receiver side and verifies the integrity by comparing the computed hash value with the decrypted hash. This process ensures secure communication and authentication of digital documents.

D. Pickle

It is a Python module, plays a crucial role in fake product detection by facilitating data preprocessing and serialization of Python objects. In the context of detecting counterfeit products, Pickle is utilized to preprocess data by cleaning, transforming, and organizing it for analysis. Moreover, Pickle enables the serialization and deserialization of Python objects representing product characteristics, facilitating efficient communication and exchange of data within the detection system. By leveraging Pickle, the system can effectively handle serialized data representations, enabling seamless processing and analysis of large datasets involved in identifying counterfeit products.

IV. IMPLEMENTATION

A. Blockchain Data

When we enter all the details of the product with the unique id and when the QR code is generated successfully we can view the product details which is stored in the blocks with the previous block hash and the current hash.
The Blockchain transactions and blocks can be visualized in a UI can be seen below.

Blockchain Previous Hash : 0099de71df68608ea88fb11fb983f3204f3447790930bcb4c935deaad2ec8459
Block No : 4
Current Hash : 008f6b3fb781a592b4c7c4332c6da438c9230ff870fd75ba89b067bf34eff1c7
Barcode Blockchain Digital Signature : 2b2308897c1d19d5df18016ac1f9f1945abd7e42766b1300f5a85f5c8b701cbf

B. Storage of Data

The data which is formed after the registration of the product is stored in the blockchain_contract.txt file in an encrypted form.
This data is not editable which ensures the trust worthiness of the product information. And no one other than having or knowing the QR code and product id cannot modify the data.

```
]��1#iphone#apple#hyderabad,7864567894#2024-03-22 19:04:21.671150#0c992c7fbba28ce8f166d4f5ec30b724e1c5d2b7c385164
]��g2#ss#sss#ss#2024-03-22 23:29:34.195221#2b2308897c1d19d5df18016ac1f9f1945abd7e42766b1300f5a85f5c8b701cbf�ah GA
]��}2#m 31 s#samsung#pune, 8975675677#2024-03-22 23:38:16.089450#2b2308897c1d19d5df18016ac1f9f1945abd7e42766b1300f5
]���3#galaxy phone#samsung#kolkata,7963467655#2024-03-22 23:38:50.360785#111e7399578a0c6361740dbbd80785eaaba313828
```

C. Generation of QR code

When all the product details are entered correctly then we will get an unique QR Code generated through an API for that product Id and that QR code is downloaded automatically in the system using that unique QR Code for a particular product we can also fetch the details of the product through that QR Code.

Fig. 2 Sample QR code Generated after the registration of the Product

D. Verification Workflow

In the proposed desktop file application, the process begins with the generation of a digital signature for the item. Upon initiating the application, the user digitally signs the item, which triggers the retrieval of relevant item data from the blockchain through the Verification Module. This data is then utilized to verify the authenticity of the item request. Upon successful verification, the application creates a new entry in the blockchain to record the transaction. The Proposed Blockchain Information Store Administration oversees the management of item data, facilitates the creation of new blocks, retrieves item information, and confirms the validity of scans based on the digital signatures.

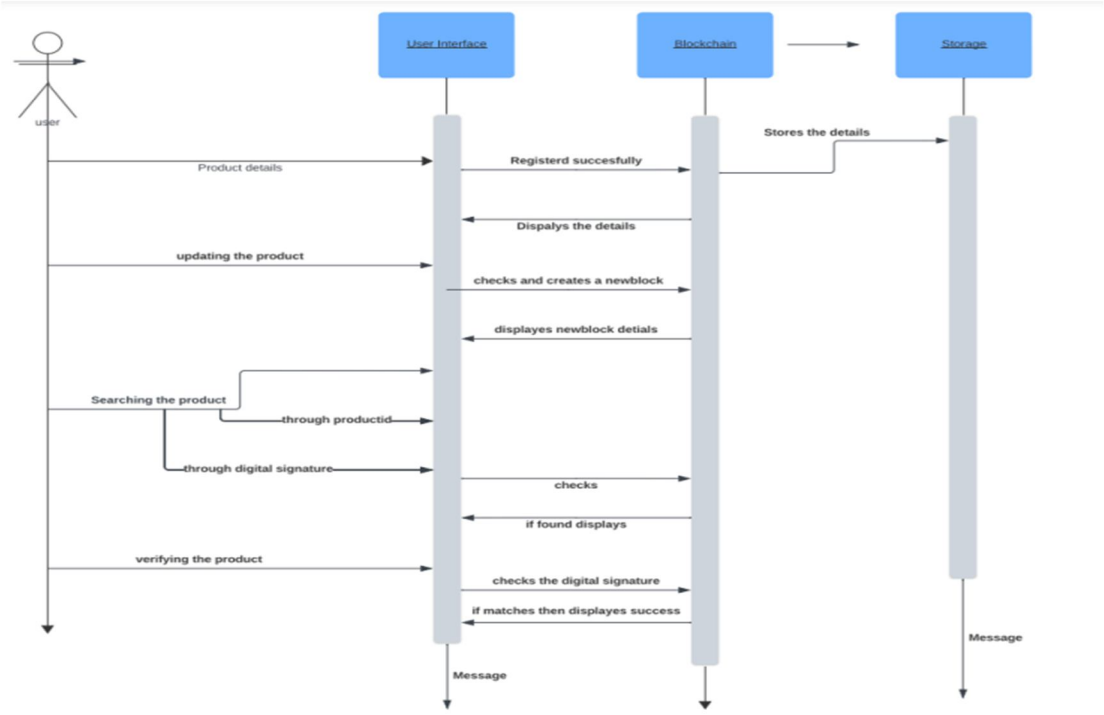


Fig. 3 Sequence Diagram for our Identification System

E. Results and discussions

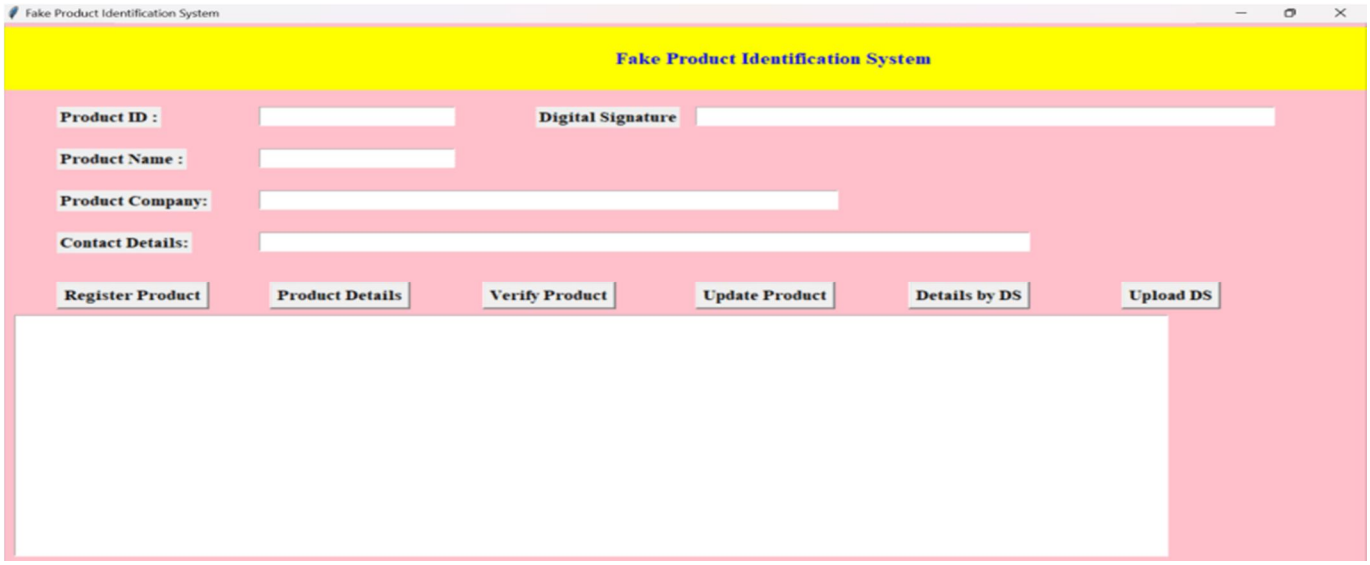


Fig. 4 Initial Screen for the User

After successfully opening the user screen you can provide all the details as mentioned in the Fig. 4

Then your screen represents as similar to that of in Fig. 5

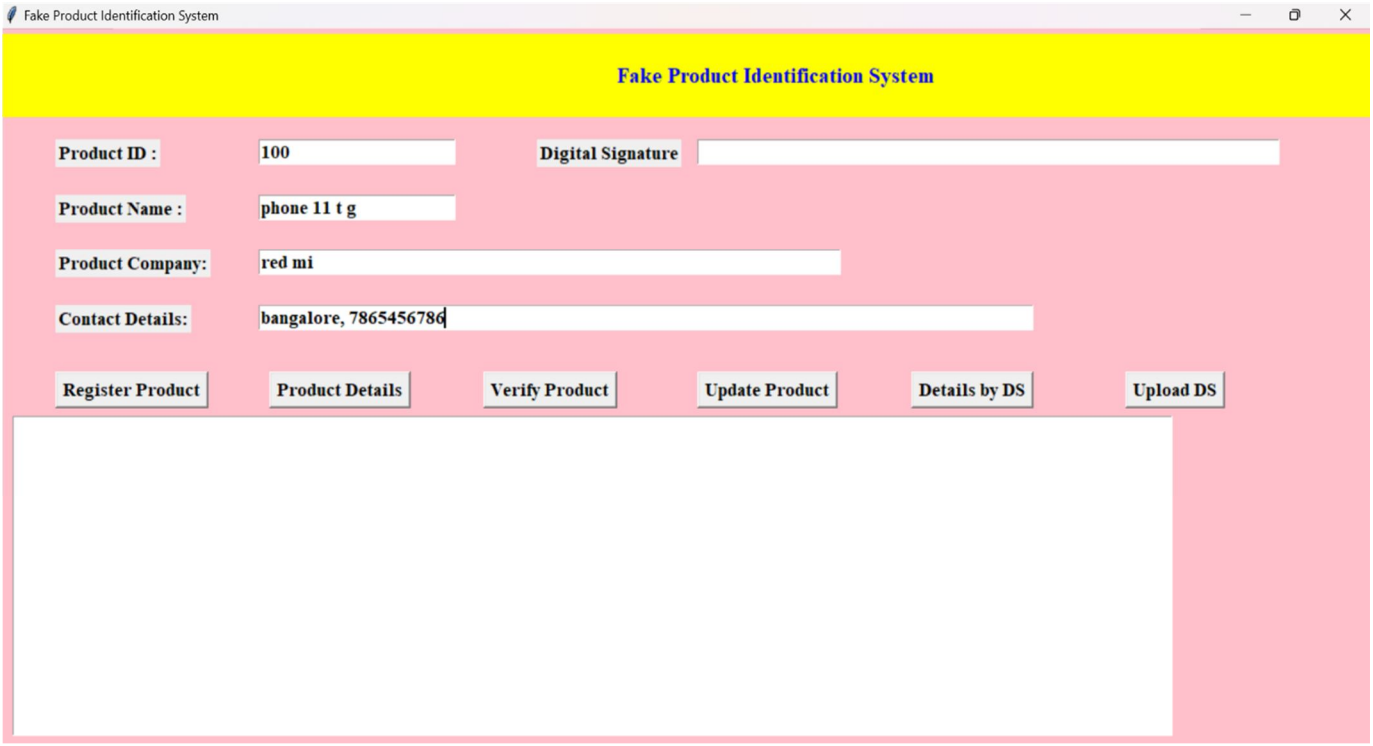


Fig.5 Providing the details for the registration of the Product

After providing all the details then it checks the conditions like whether you have all the details i
f not it is displayed as Fig. 6 and also whether Product ID already exists in your data if exist it displays as shown in Fig. 7.

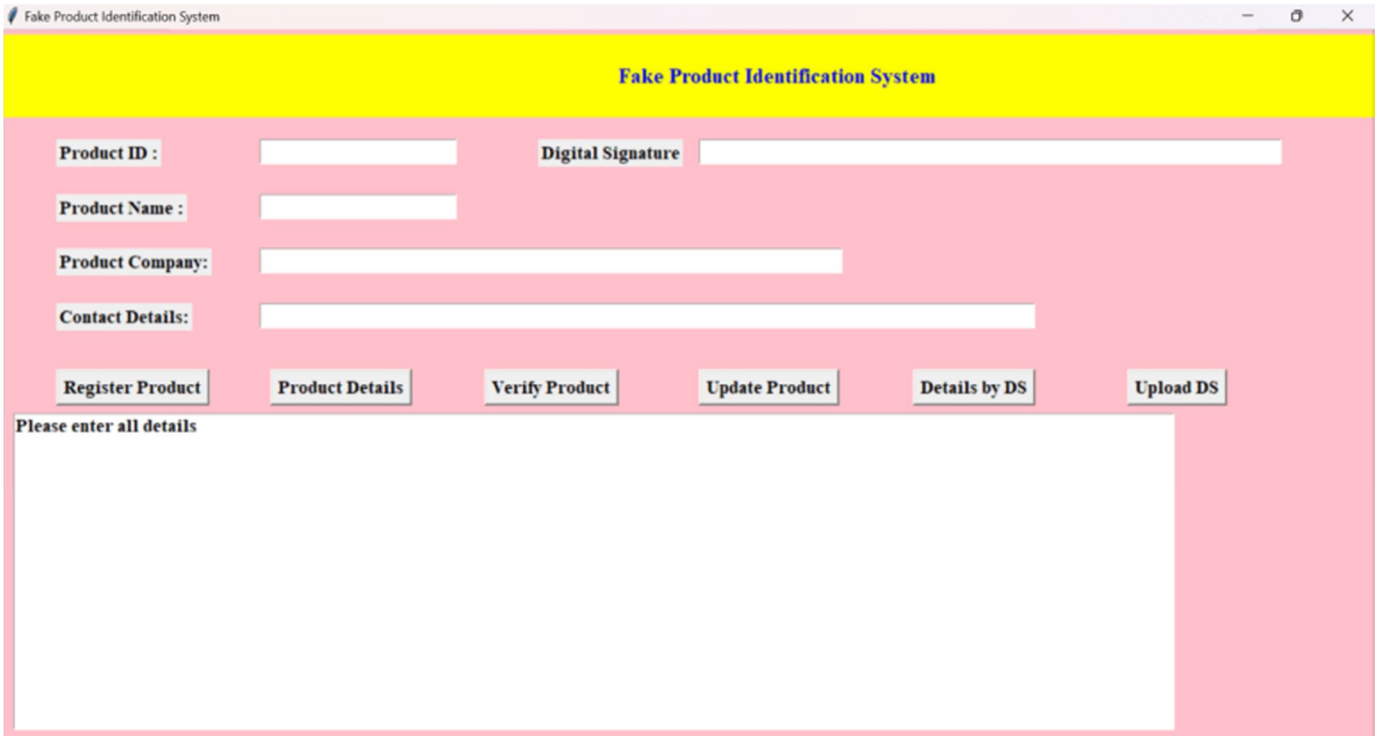


Fig. 6 Shows us to enter all the details

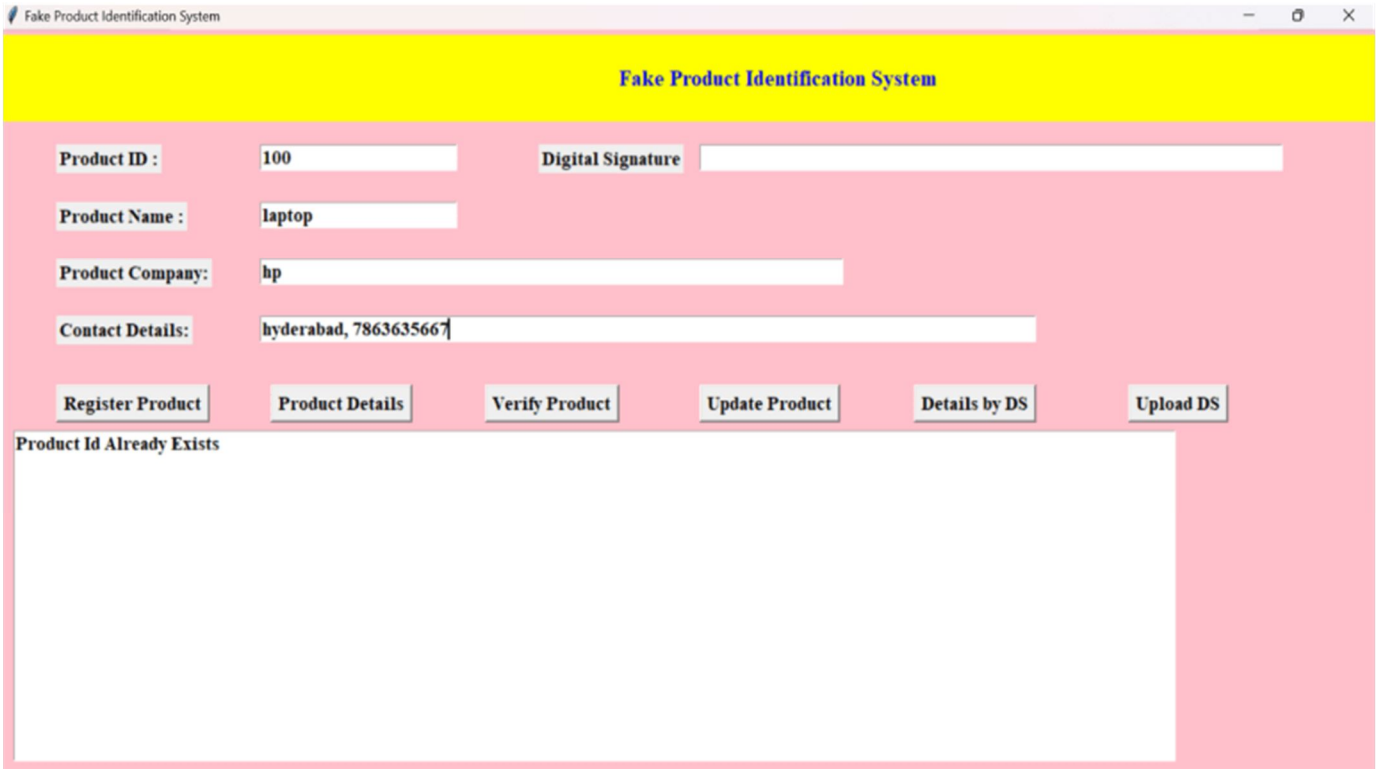


Fig. 7 If a Product with the same ID exists

After checking the above necessary conditions then the successful registration is done and displayed as in of Fig. 8

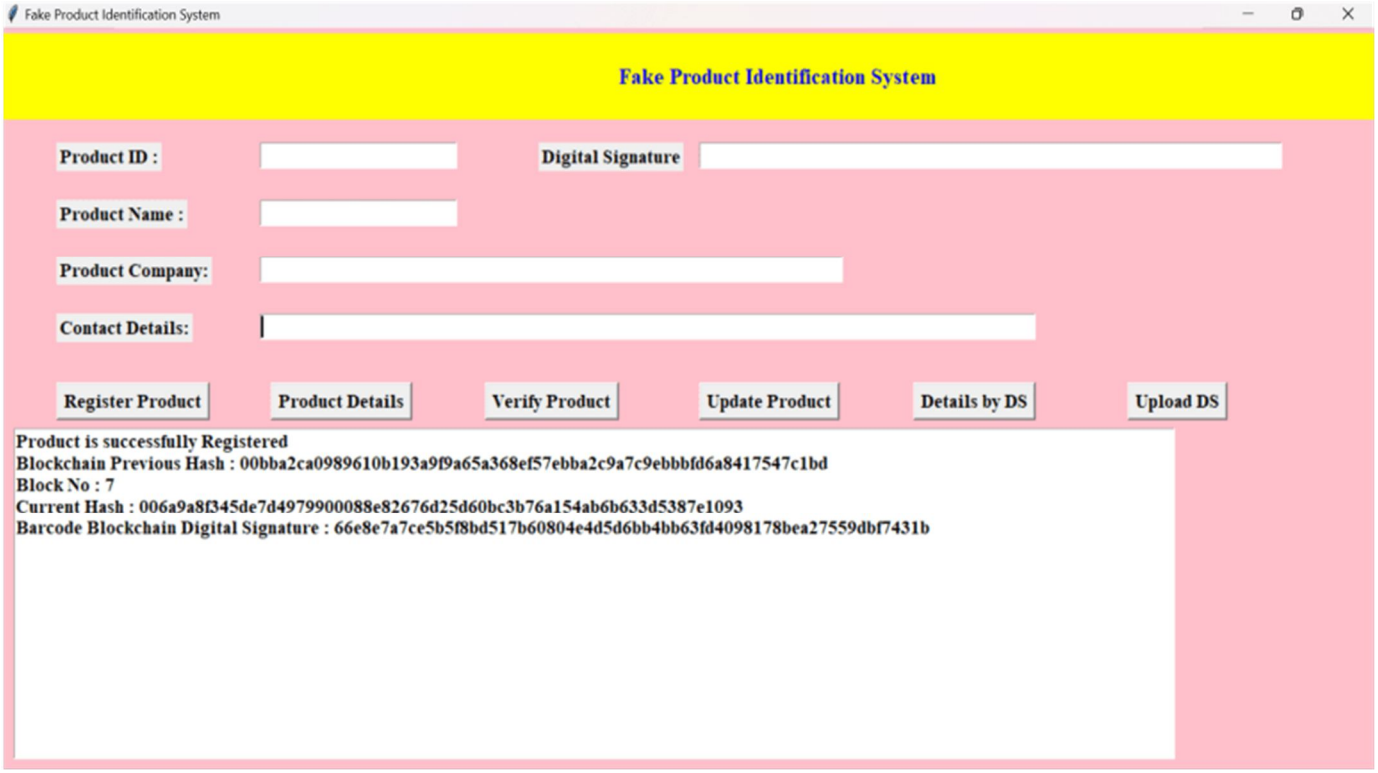


Fig.8 Successful Registration of the Product

And the Digital Signature is displayed as of in Fig. 8 and can be copied for the further use. And the related QR code is stored in the folder “barcodes” as displayed in Fig. 9

Fig. 9 All the Successfully registered products QR Codes are shown

And for getting the product details you can do that in 3 ways

1) By giving Product Id and clicking on button “Product Details” as shown in Fig. 10
2) By giving the digital signature in the text box provide above and clicking on button “Details by DS”, this is the same digital signature you get for successful registration as shown in Fig. 11
3) By clicking on button “Upload DS” a dialog box gets displayed to upload and QR code as shown in Fig. 12

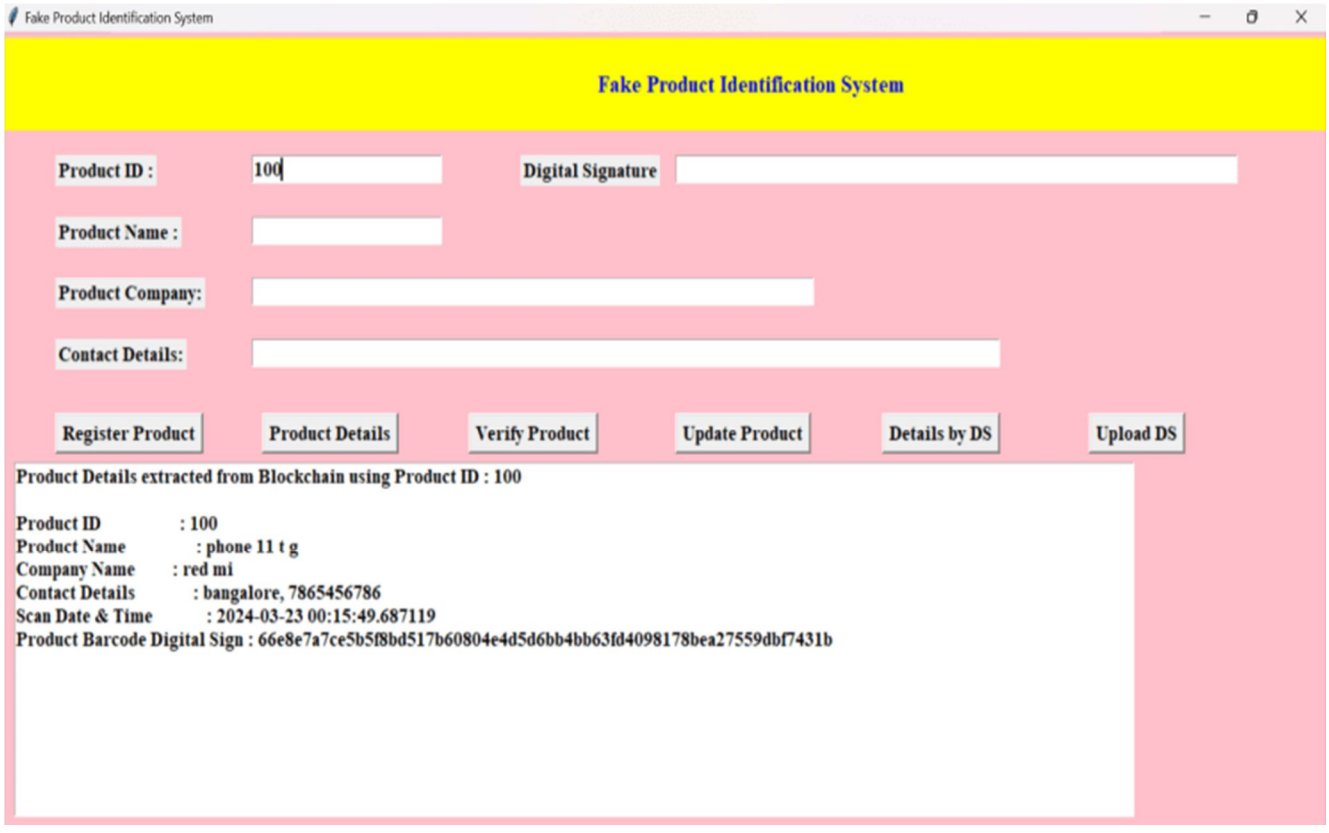


Fig. 10 Getting Product Details by Product ID

Fig. 11 Getting Product Details by Digital Signature

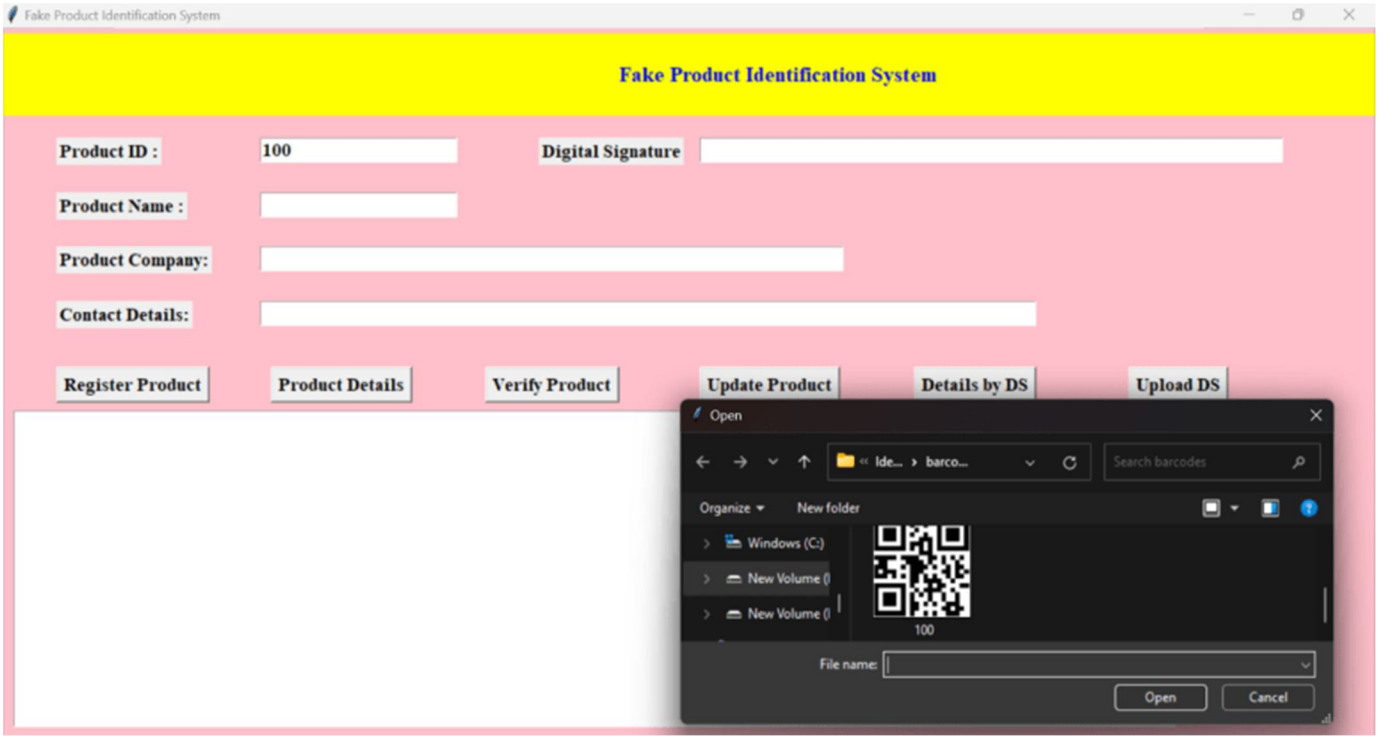


Fig. 12 Getting Details by Upload DS

You can also modify the product details by choosing Update Product. In order to do this, you need to provide the already registered Product Id from your blockchain and the related QR code then only you can update the details and that stores in the block chain.

If the details do not match displays message as of Fig. 14

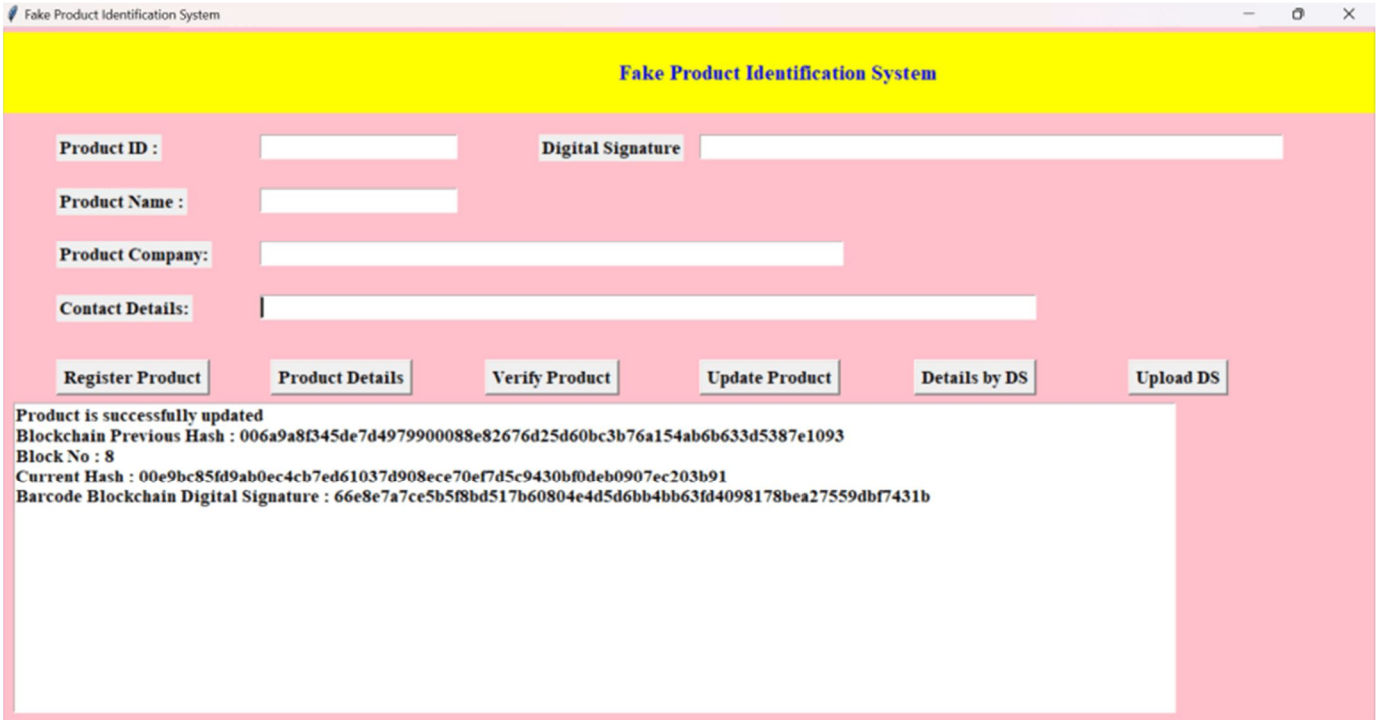


Fig. 13 Successfully Updating the Existing Data

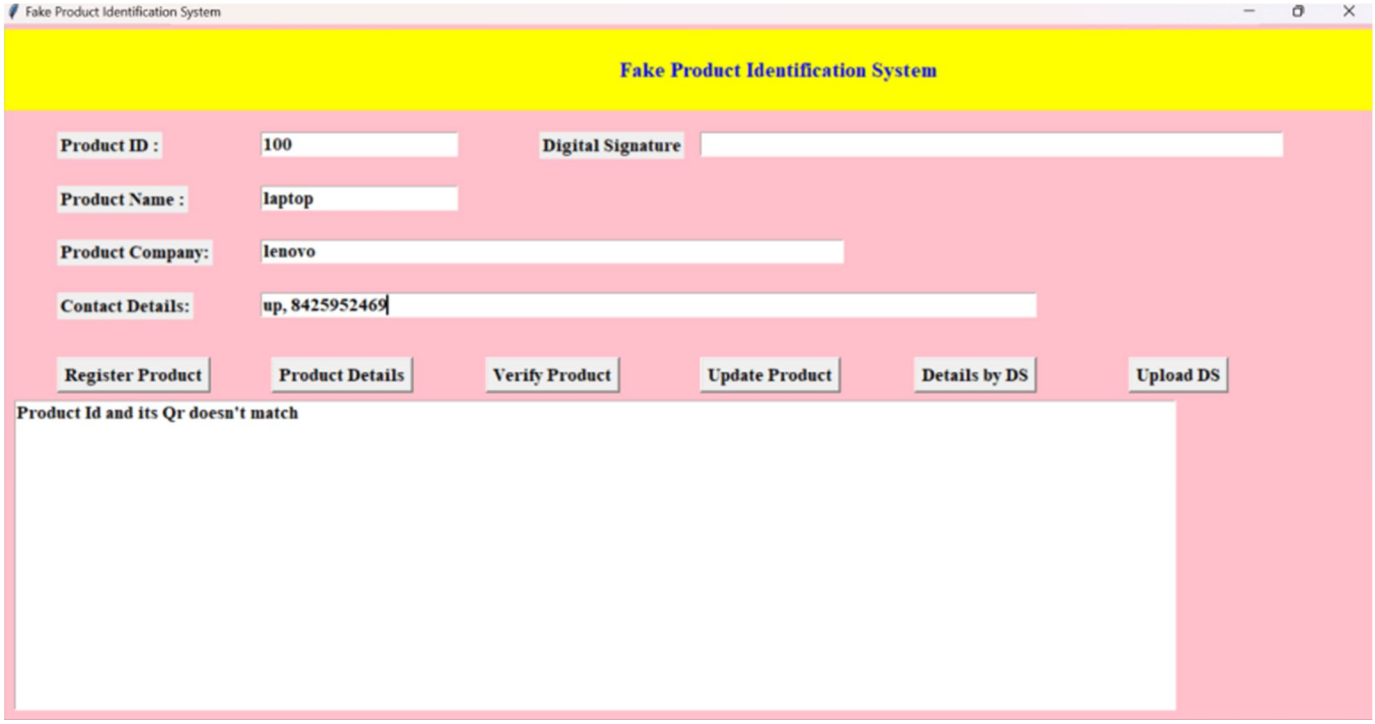


Fig. 14 If the Product Id and QR code do not match

Here comes, the final thing “The Verification of the Product”, In order to do this, you need to enter the Product ID and the QR code in which that particular details are digitally signed. Upon successful verification you get the details of the Genuine Product as shown in Fig. 15 if not then it displays as of in Fig. 16

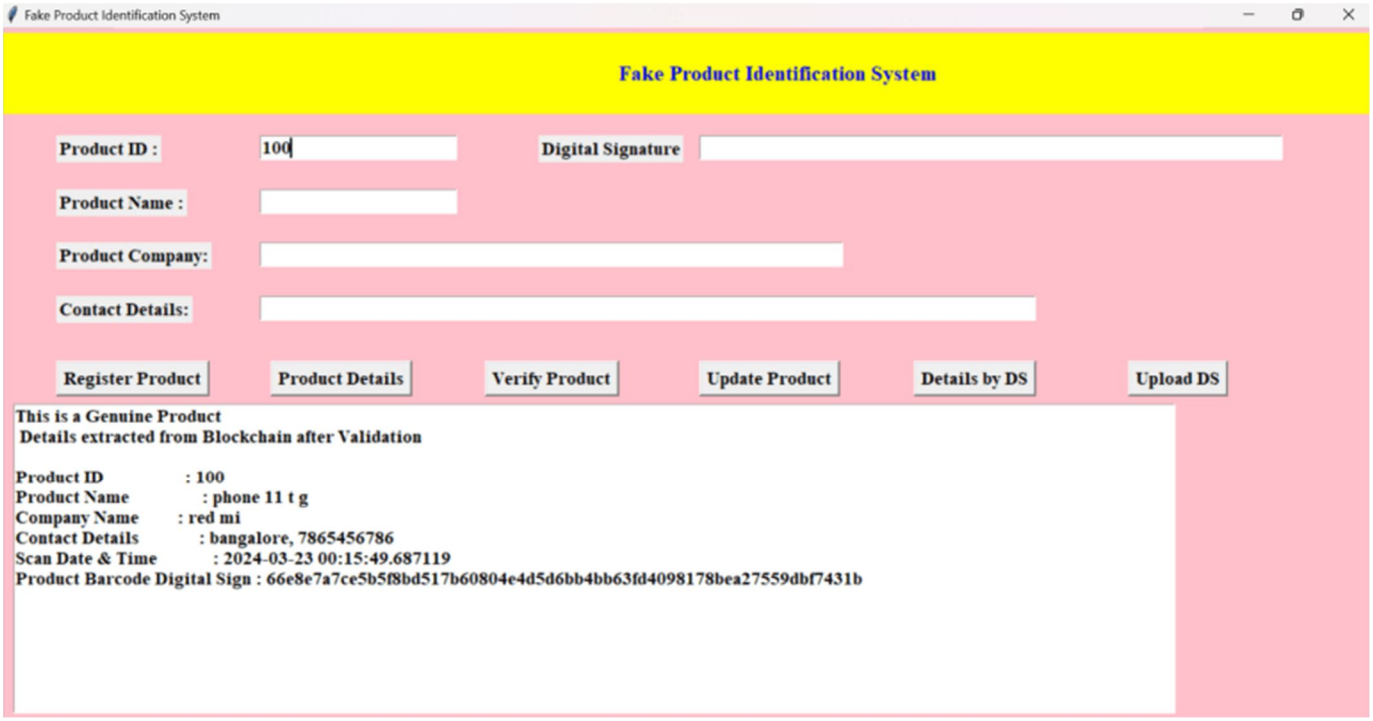


Fig. 15 The Product is Genuine

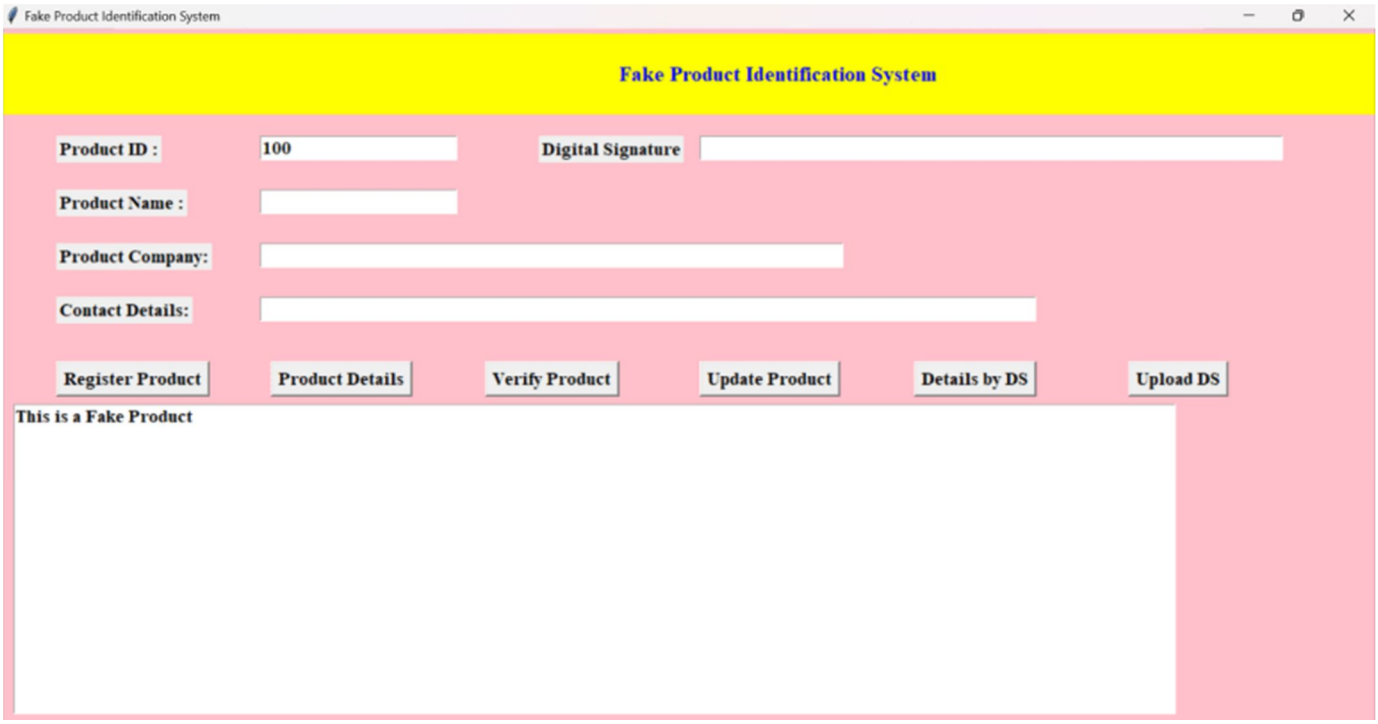


Fig. 16 The Product is Fake

V. CONCLUSIONS

In conclusion, with this the users can finally know which product is fake or real through the QR code with the help of blockchain. Through the interconnection between unique nature of the QR code assigned to every product and the details that are stored in the blockchain we can easily verify the product and its details. With the help of the blockchain we can create a trustworthy website for any fields where users can confidently verify the authentication of products.

Due to the transparency which is unparallel, immutable nature, decentralization block chain plays an important role in identifying the fake products.

VI. LIMITATIONS AND FUTURE WORK

A. *Limitations*

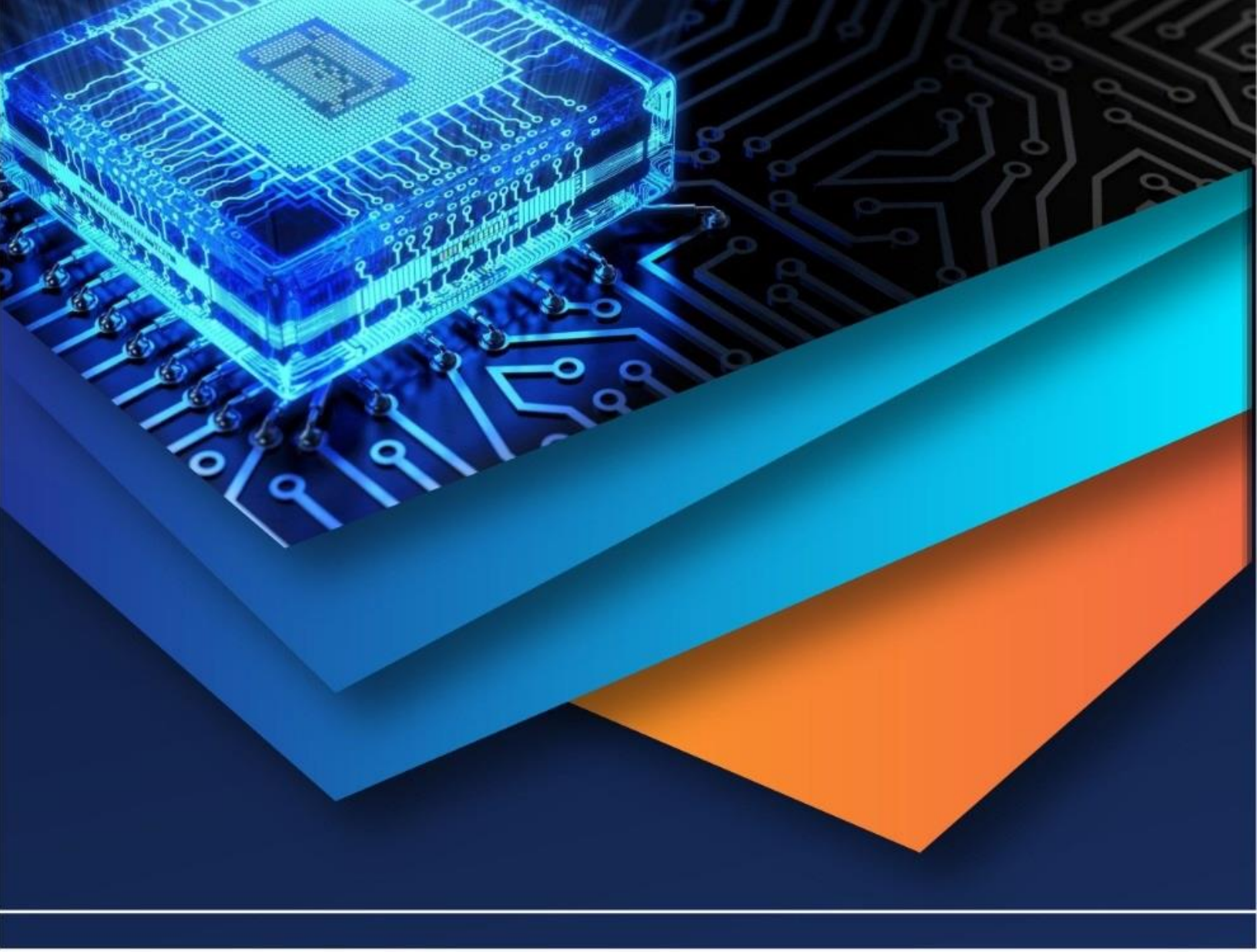
1) *Reliability on the Data:* The data that is entered into the blockchain is heavily accurate. If incorrect data is given then it can lead to the increase of propagation of the network without proper identification.
2) *Verification through Physical attributes:* It is not possible for the blockchain to detect the internal physical features of the product by the observation in order to distinguish between real and fake.
3) *Integration difficulty:* Implementation of blockchain for product verification requires integration with existing supply chain systems and technologies. This integration process can be complex and costly, and it may not be feasible for all companies, particularly smaller ones with limited resources.
4) *Scalability:* As the number of blocks and data grows sometimes it may become difficult for the blockchain to process.

B. *Future Work*

1) *Advanced Authentication:* Some of the advanced authentication mechanisms like QRCODE linked to block chain plays an important level of security and becomes more difficult for the counterfeiters to replicate the data
2) *Integration with various Technologies:* Blockchain can be integrated with various technologies like AI, ML, IOT to enhance fake product detection capabilities. AI, ML are used to detect through patterns whereas IOT provides real time data for the product.
3) *Instant Verification:* Future projects which can be developed through blockchain need not be dependent on any 3rd party apps which leads to the faster processing of verification or authentication.
4) *Optimization of Performance:* Addressing scalability and performance challenges is crucial for the widespread adoption of blockchain-based solutions for fake product detection. Future projects could focus on developing scalable blockchain platforms with improved consensus mechanisms and transaction processing speeds to support the high-volume transactions required for real-time product authentication in large-scale supply chains.

REFERENCES

[1] Satoshi Nakamoto, ―Bitcoin: A Shared Electronic Money System‖, 2008
[2] OECD (2016), Illegal Exchange: Combining Criminal Organizations, OECD Audits of Chance Administration Strategies, OECD Distributing, Paris, https://doi.org/10.1787/9789264251847-en.
[3] S. Underwood, ―Blockchain Past Bitcoin‖, in Correspondences of the ACM, vol. 59, no. 11, p. 15-17, 2016.
[4] L. Li, ―Technology intended to battle fakes in the worldwide stock chain‖, in Business Skylines, vol. 56, no. 2, p. 167-177, 2013.
[5] Berman, ―Strategies to identify and lessen duplicating activity‖, in Business Skylines, vol. 51, no. 3, p. 191-199, 2008.
[6] K. D'egardin, Y. Roggo and P. Margot. ―Understanding and battling the medication fake market‖, in Diary of Drug and Biomedical Examination, vol. 87, p. 167-175, 2013
[7] R. C. Merkle, __A computerized signature in light of a traditional encryption capability," in Proc. Conf. Hypothesis Appl. Cryptogr. Techn., 1987, pp. 369-37
[8] Fake meds. QA fake. World Wellbeing Association (WHO) 2009. Accessible from: http://www.who.int/medications/administrations/fake/faqs/QACounterfeit-october2009.pdf [last refered to on 2010 Jun 12].
[9] R.C. Merkle, "Conventions for public key cryptosystems," In Proc. 1980 Conference on Security and Protection, IEEE PC Society, pages 122-133, April 1980.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY