JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Combating Counterfeit Goods: A Blockchain-Enabled QR Code Authentication System

[1] Karndeo Aditya, [2] Himanshu Gautam, [3] Dr. Akash Saxena
[1]M.Tech Scholar, [2] Assistant Professor, [3] Professor
[1]Department of Computer Science and Engineering,
[1] Compucom Institute Of Technology And Management

Abstract: The proliferation of counterfeit goods in digital commerce threatens brand reputation and consumer trust. This research proposes a solution by integrating QR codes with blockchain technology to authenticate products. Each product is assigned a unique QR code during manufacturing, which is stored in a blockchain database. Consumers can verify product authenticity by scanning the QR code, which checks the blockchain for matches, confirming the product's genuineness. This method ensures privacy and offers a robust defense against counterfeiting.

***Index Terms* -** Counterfeit goods, QR codes, blockchain, product authentication, brand protection, digital commerce.

I. Introduction

The exponential growth of digital commerce has transformed the global marketplace, offering consumers unparalleled convenience and access to a vast array of products. However, this surge in online transactions has also paved the way for an increase in counterfeit goods, posing serious threats to businesses and consumers alike. Counterfeit products not only undermine the trust that consumers place in reputable brands but also lead to significant financial losses for companies. The widespread availability of fake items, often sold at tempting prices, makes it increasingly difficult for consumers to distinguish between genuine and counterfeit products. This issue has become a pressing concern for businesses that are expanding into physical retail spaces, where the presence of counterfeit goods can further erode brand value and customer loyalty [1].

To address this growing challenge, there is a critical need for innovative solutions that can effectively combat the proliferation of counterfeit goods. One promising approach lies in the integration of Quick Response (QR) codes into the manufacturing process. QR codes, when paired with the secure and transparent architecture of blockchain technology, offer a robust mechanism for authenticating products and protecting consumers from fraudulent practices. By assigning a unique QR code to each product during its production, businesses can create a digital footprint that is securely stored in a blockchain database. This database contains comprehensive information about each product, ensuring that the data is both accurate and immutable [1].

The use of blockchain technology in this context is particularly advantageous due to its decentralized nature, which ensures that no single entity has control over the stored data. This feature enhances the reliability of the information and prevents unauthorized modifications, thereby maintaining the integrity of the authentication process. When consumers scan the QR code using their smartphones, the system performs a real-time search within the blockchain database to verify the product's authenticity. A matching result confirms that the product is genuine, while any discrepancy alerts the consumer to the possibility of a counterfeit item. This method not only empowers consumers to make informed purchasing decisions but also reinforces the credibility of the brand [2].

Furthermore, the proposed system prioritizes privacy, as all product-related data is confined within the blockchain, eliminating the need for external information storage. This approach not only protects consumer data but also enhances the overall security of the authentication process. As businesses continue to grapple with the challenges posed by counterfeit goods, the adoption of blockchain-enabled QR code systems represents a significant step forward in safeguarding brand integrity and ensuring consumer trust in the increasingly complex global marketplace [2].

II. LITRARTURE REVIEW

Asmat and Qasim (2019) [5] explored the use of graphical authentication as a widely adopted method in the modern mobile computing environment. This technique was developed to enhance security measures by addressing the shortcomings of traditional text-based passwords, PINs, and other easily guessable password strategies, which are often difficult to remember and vulnerable to external attacks. The proposed method allows users to divide an image into distinct segments, and unlocking the device requires correctly selecting these defined segments, granting access. This technique effectively counters shoulder-surfing and smudge attacks, while also providing strong resistance against password guessing and dictionary attacks. The approach significantly improves the security of graphical password systems without causing additional operational delays.

Khan and Chefranov (2020) [6] focused on enhancing authentication security to comprehensively protect users' personal information. Their study introduced a graphical password model that balances security with user convenience, combining recognition-based strategies with recalled and flagged review-based approaches, ultimately providing superior security compared to existing schemes.

Mu and Yao (2019) [7] emphasized the widespread use of graphical passwords in modern contexts, including two-factor authentication, facial recognition, and fingerprint authentication. They introduced a new form of graphical password, called Hanzi-gpw, which is stored using an arithmetic grid on a computer. This research differentiates text-based passwords (TB-paws) from Hanzi-gpws and proposes various methods for generating TB-paws from Hanzi-gpws, incorporating topological designs and graphical coloring/labeling. The use of Chinese characters in password design specifically targets the Chinese population, and the study also introduces a novel graph labeling technique alongside related mathematical concepts.

Bilgi and Tugrul (2018) [8] discussed graphical passwords, or Graphical User Authentication (GAU), as a viable alternative to traditional text-based password methods, owing to their ease of use and reliability. The foundation of graphical authentication lies in the principle that individuals recall visual objects more readily than text. Given the tendency for people to use authentication mechanisms in public spaces, such as public transportation, restaurants, and classrooms, the risk of shoulder-surfing attacks has increased. Hybrid images are created by combining elements from two images, where one individual sees one image while others perceive a different image. This study developed a graphical authentication system resistant to shoulder-surfing by using hybrid images. The proposed system was compared to other graphical and text-based strategies regarding security and convenience.

Gupta et al. (2017) [9] noted the presence of various risks in online, organizational, and secure environments. Often, due to a lack of awareness and information, general users select simple and similar password combinations that are easy to remember. This paper highlighted the use of graphical password protection within a virtual environment, allowing users to choose their graphical representations from objects presented in a virtual environment, thereby creating unique passwords.

Jaffar and Zeki (2020) [10] emphasized the importance of user authentication in security. While alphanumeric usernames and passwords are commonly used, the vulnerabilities associated with this approach led to the introduction of graphical passwords as an alternative. Recognizing that humans can recall images more effectively over time, this study thoroughly examined graphical password schemes, evaluating them based on resistance to attacks and usability. It also explored whether graphical passwords offer superior security compared to alphanumeric passwords.

Yang et al. (2019) [11] introduced two models within a ring network framework based on the concept of odd-easy labelings, contributing to the creation of topologically realistic passwords (Topsnut-gpws). These passwords can be encoded by correlating Topsnut-grid and text-based passwords, enhancing data transmission security and reliability.

Shen et al. (2017) [12] discussed the crucial role of smart mobile devices in today's world. While users often input related words or simple graphics on touch screens to unlock screensavers, this method, though convenient, poses data leakage risks under strict security conditions. The physical proximity of others may provide opportunities for information retrieval, potentially compromising device security and the user's personal data.

Irfan et al. (2018) [13] acknowledged that despite the effectiveness of graphical password schemes, they remain susceptible to shoulder-surfing and are less efficient due to a large password space. This paper proposed a solution based on text-based graphical password techniques, combining the Déjà vu and Moveable Frame approaches. The study demonstrated that text-based images can more effectively replace the Déjà vu component. The goal was to eliminate shoulder-surfing and reduce the login time required for pass images. The proposed graphical password system, utilizing a combination of alphabetical characters, showed superior usability compared to image-based systems.

III. PROPOSED CONCEPT

The research methodology for this study involves a comprehensive approach that integrates blockchain technology with QR code-based product authentication to address the problem of counterfeit goods in the eCommerce industry. The methodology is structured into several key phases: problem identification, system design, algorithm selection, implementation, and validation.

1. Problem Identification: The first phase of the research focuses on identifying and understanding the widespread issue of counterfeit products in the eCommerce sector. Through a detailed analysis of current challenges faced by consumers and businesses, the study highlights the negative impact of counterfeit goods on customer trust, brand reputation, and financial losses. This phase establishes the need for a robust solution that can ensure product authenticity and prevent the circulation of fake products in the market.

2. System Design: The next phase involves the conceptualization and design of a blockchain-based system that integrates QR codes into the manufacturing process. The design outlines the integration of QR codes with blockchain technology, where each product is assigned a unique digital identity. This identity includes essential information such as the product ID, batch number, and manufacturing location, all of which are stored as blocks within the blockchain. The system design ensures that every product's information is securely and immutably recorded in the blockchain, enabling reliable verification of authenticity.

3. Algorithm Selection – BLAKE2b-512: To ensure the security and efficiency of the proposed system, the BLAKE2b-512 hashing algorithm is selected. This phase involves an in-depth analysis of the BLAKE2b-512 algorithm, known for its high-speed performance and cryptographic security. The algorithm generates a 512-bit digest, which is used to hash the product information stored in the blockchain. The choice of BLAKE2b-512 is motivated by its optimization for 64-bit computing platforms and its ability to produce varying digest lengths, making it suitable for the diverse requirements of the proposed system.

4. Implementation: The implementation phase involves the practical application of the designed system and the selected hashing algorithm. During the manufacturing process, each product is embedded with a QR code that links to its corresponding blockchain entry. The BLAKE2b-512 algorithm is employed to hash the product data, ensuring its integrity and security within the blockchain. The QR codes serve as digital fingerprints for the products, allowing consumers to verify the authenticity by scanning them with their smartphones. The implementation process includes the development of a user interface for consumers to interact with the system and receive instant feedback on the authenticity of the products.

5. Product Validation: The final phase of the research methodology focuses on product validation. This phase involves testing the system's effectiveness in accurately identifying counterfeit products. The validation process requires consumers to input the digital product identity, batch number, and manufacturing location when scanning the QR code. The system cross-references this information with the blockchain database using the BLAKE2b-512 algorithm. If the scanned data matches the records in the blockchain, the system confirms the product's authenticity; otherwise, it alerts the consumer to the possibility of a counterfeit item. This phase also evaluates the system's performance in terms of speed, accuracy, and user experience.

Through these phases, the research methodology ensures a systematic and rigorous approach to developing a blockchain-based solution for combating counterfeit goods in the eCommerce industry. The use of the BLAKE2b-512 algorithm, combined with the secure storage of product information in the blockchain, provides a robust and reliable framework for product authentication.

IV. IMPLEMENTATION AND RESULT ANALYSIS

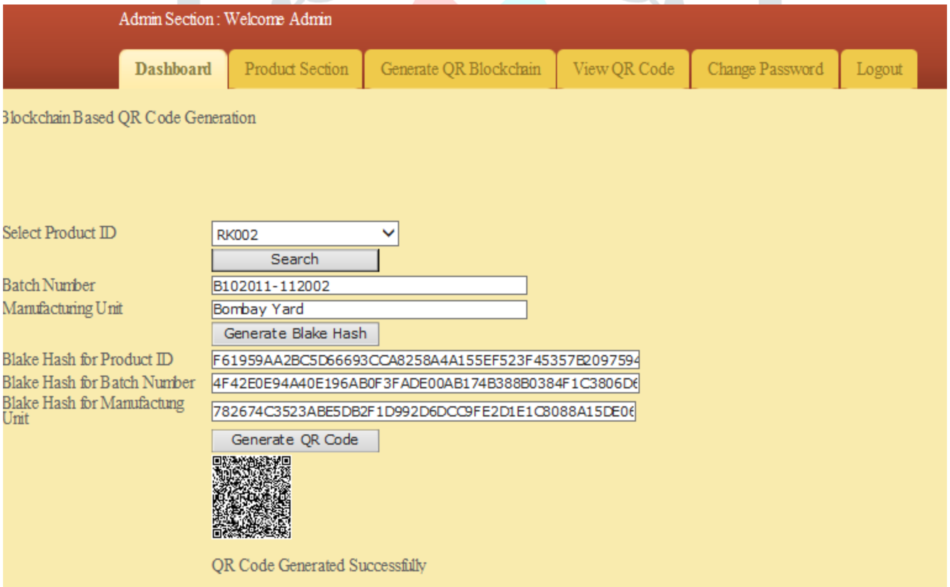

Fig 1. Implementation

The research paper of F.Z. Glory et. Al 2019, password or OTP generated according to their concept is,

{urAn29iRfan- 0

Blockchain generated using the proposed work,

87A560A15DA6E340094BFF4FBA55D527EDB54E72_024A6C1B63681D5647F43A9689B08D0A2A8EBB8E_E8E2EC029D35E5A5E0328692DE92357F0C101BFA

The results of the base research paper and the pattern generated from the proposed work are compared using the various available tools for the password strength calculation or estimation.

Table 1 Years Calculation using My1Login

	Base Approach	Proposed Approach
Years Taken to Break	49 billion years	1 billion trillion trillion trillion trillion trillion trillion trillion trillion trillion trillion trillion years

Table 2 Years Calculation using Security.org-Base 1

	Base Approach	Proposed Approach
Years Taken to Break	9 hundred billion years	16 million sexagintillion years

Table 3 Entropy Calculation using Password. Blue

	Base Approach	Proposed Approach
Entropy	49 bits	399 bits

Table 4 Entropy Calculation using Cryptool2

	Base Approach	Proposed Approach
Entropy	68.5	533.7

V. Conclusion

This research paper presents a comprehensive solution to the growing problem of counterfeit products in the eCommerce industry by leveraging blockchain technology and QR code-based authentication. The proposed system addresses the critical need for a reliable method to ensure product authenticity, thereby protecting consumers and preserving brand reputation. By embedding unique QR codes into products during the manufacturing process and linking them to a secure blockchain database, the system offers a robust mechanism for verifying the authenticity of products in real time.

The integration of the BLAKE2b-512 hashing algorithm plays a pivotal role in securing the product data within the blockchain, ensuring that each entry is tamper-proof and accurately reflects the product's identity. This approach not only enhances the security of the authentication process but also offers scalability and efficiency, making it suitable for widespread adoption in the fast-growing eCommerce sector.

The validation phase demonstrated the system's effectiveness in distinguishing genuine products from counterfeits, providing consumers with a reliable tool for making informed purchasing decisions. The user-friendly interface and the seamless interaction between the QR code and blockchain technology further enhance the system's practicality and accessibility for everyday use.

In conclusion, the research successfully develops a cutting-edge solution that significantly mitigates the risks associated with counterfeit products in the eCommerce industry. By combining the transparency and immutability of blockchain technology with the convenience of QR code scanning, the proposed system offers a promising approach to safeguarding both consumers and brands against the pervasive threat of counterfeit goods. Future work could explore the expansion of this technology to other sectors, as well as the integration of additional security features to further enhance the system's robustness and versatility..

References

[1] Ahmad Almulhem "A Graphical Password Authentication System" World Congress on Internet Security (WorldCIS-2011) February 21–23 2011.

[2] G-C Yang H. Kim "A New Graphical Password Scheme based on Universal Design" The Journal of Digital Convergence vol. 15 no. 5 2014.

[3] Ahmad Almulhem "A Graphical Password Authentication System" World Congress on Internet Security (WorldCIS-2011) February 21–23 2011

[4] Sh. Doiphode J. Jadhav P. Shelke M.S. Pokale et al. "Novel Security Method Using Captcha as Graphical Password" International Journal of Emerging Engineering Research and Technology vol. 3 no. 2 pp. 18-24 February 2015.

[5] N. Asmat and H. S. A. Qasim, "Conundrum-Pass: A New Graphical Password Approach," *2019 2nd International Conference on Communication, Computing and Digital systems (C-CODE)*, 2019, pp. 282-287.

[6] A. Khan and A. G. Chefranov, "A Captcha-Based Graphical Password With Strong Password Space and Usability Study," *2020 International Conference on Electrical, Communication, and Computer Engineering (ICECCE)*, 2020, pp. 1-6.

[7] Y. Mu and B. YAo, "Construction Of Topological Graphic Passwords By Hanzi-gpws," *2019 IEEE 3rd Information Technology, Networking, Electronic and Automation Control Conference (ITNEC)*, 2019, pp. 1957-1961.

[8] B. Bilgi and B. Tugrul, "A Shoulder-Surfing Resistant Graphical Authentication Method," *2018 International Conference on Artificial Intelligence and Data Processing (IDAP)*, 2018, pp. 1-4.

[9] D. Gupta, A. P. Singh, V. Goar and S. Mathur, "Combination of textual and graphical based authentication scheme through virtual environment," *2017 3rd International Conference on Advances in Computing,Communication & Automation (ICACCA) (Fall)*, 2017, pp. 1-4.

[10] J. A. Jaffar and A. M. Zeki, "Evaluation of Graphical Password Schemes in Terms of Attack Resistance and Usability," *2020 International Conference on Innovation and Intelligence for Informatics, Computing and Technologies (3ICT)*, 2020, pp. 1-5.

[11] S. Yang, M. Zhang, B. Yao, J. Guo and Z. Bai, "Topological Graphic Passwords Made By Series Sun-graphs On Odd-graceful Property," *2019 IEEE 8th Joint International Information Technology and Artificial Intelligence Conference (ITAIC)*, 2019, pp. 1617-1621

[12] S. Shen, T. Kang, S. Lin and W. Chien, "Random graphic user password authentication scheme in mobile devices," *2017 International Conference on Applied System Innovation (ICASI)*, 2017, pp. 1251-1254.

[13] K. Irfan, A. Anas, S. Malik and S. Amir, "Text based graphical password system to obscure shoulder surfing," *2018 15th International Bhurban Conference on Applied Sciences and Technology (IBCAST)*, 2018, pp. 422-426.

[14] A. I. Shaban and N. Haryani Zakaria, "The Impact Of Cultural Familiarity On Choosing Images For Recognition-Based Graphical Passwords," *2018 4th International Conference on Computer and Information Sciences (ICCOINS)*, 2018, pp. 1-5.