

A BLOCKCHAIN-BASED FAKE ITEM IDENTIFICATION SYSTEM

Mrs. M. Anusha¹, S. Rachana², A. Supriya³, J. Chandrika⁴, P. Naga Meghana⁵, M. Himaja⁶

¹Assistant Professor in Department of Computer Science and Engineering, Santhiram Engineering College, Nandyal, Kurnool, AndhraPradesh, India.

^{2,3,4,5,6}Student, Department of Computer Science and Engineering, Santhiram Engineering College, Nandyal-518501, AndhraPradesh, India.

¹Corresponding Author: anusha.cse@srecnandyal.edu.in

DOI: <https://www.doi.org/10.58257/IJPREMS33546>

ABSTRACT

The fusion of Quick Response (QR) codes with blockchain technology creates a robust solution against counterfeit goods in the supply chain. QR codes, widely used in web applications, streamline verification processes. When linked to blockchain, they establish an immutable ledger, storing vital product details. Upon scanning, users input their unique code, cross-referenced with blockchain records. Matching codes yield comprehensive product information, ensuring authenticity. Conversely, mismatches signal counterfeit status. This integration enhances trust and transparency, empowering stakeholders to track and verify product authenticity, mitigating risks associated with counterfeit goods. In summary, this innovative approach combines supply chain management, blockchain, and QR technology to combat counterfeiting effectively.

1. INTRODUCTION

In the contemporary marketplace, counterfeit goods pose a pervasive and multifaceted challenge, threatening consumer safety, undermining brand integrity, and eroding trust in online commerce. Defined as low-quality replicas of original products, counterfeits are designed to imitate luxury items at a fraction of the cost, enticing consumers with the promise of savings. The quality of counterfeit goods has evolved to closely resemble their authentic counterparts, exacerbating the difficulty of discerning between genuine and fake products. According to the Organization for Economic Co-operation and Development (OECD), the global trade in counterfeit goods has witnessed a steady rise, comprising 3.3% of global trade [1]. This flourishing illicit trade not only siphons revenue away from legitimate brands but also jeopardizes consumer health, particularly in sectors such as medicine and beauty products.

In response to the escalating prevalence of counterfeit goods, online retailers are intensifying their efforts to combat this menace and safeguard consumer interests. Notably, e-commerce giant Amazon has implemented initiatives such as Project Zero, leveraging machine learning technology to detect and eliminate counterfeit listings from its platform [2]. With a substantial investment of resources and manpower, Amazon endeavors to uphold the integrity of its marketplace and protect consumers from fraudulent products. Despite these measures, the proliferation of counterfeit goods continues to plague the global market, perpetuating consumer skepticism and undermining the competitiveness of authentic brands.

Within the European Union, a significant proportion of consumers have fallen victim to counterfeit products, unwittingly purchasing items they believed to be genuine [3]. This alarming trend not only erodes consumer trust but also jeopardizes the viability of authentic brands, as disillusioned consumers retreat from online commerce. Moreover, the unchecked proliferation of counterfeit goods not only diminishes the profitability of legitimate businesses but also facilitates the enrichment of counterfeiters at the expense of genuine manufacturers.

Amidst these challenges, there emerges an urgent imperative for a robust and reliable mechanism to authenticate products and restore consumer confidence in online transactions. Blockchain technology emerges as a promising solution, offering a decentralized platform of trust that empowers consumers to verify the authenticity of goods seamlessly. By leveraging blockchain's inherent attributes such as consensus, provenance, immutability, and finality, stakeholders can establish a transparent and tamper-proof ledger of product information, thereby mitigating the risks associated with counterfeiting.

This introduction lays the groundwork for a comprehensive examination of the impact of counterfeit goods on consumer trust and brand integrity in the digital age. Through an analysis of industry trends, regulatory frameworks, and technological innovations, this paper aims to elucidate the potential of blockchain technology to combat counterfeit goods effectively. By exploring the benefits and challenges of blockchain-based authentication systems, this study seeks to inform policymakers, businesses, and consumers alike on strategies to mitigate the risks posed by counterfeit products and foster a more secure and trustworthy marketplace.

2. EXISTING SYSTEM

Counterfeit products are unauthorized or fake replicas of genuine products, often produced and sold with the intent to deceive consumers or profit from the reputation of the genuine product. The primary goal of this project is to enhance product authentication and combat counterfeits. Traditional product authentication methods have two main problems. First, they're not very good at stopping fake products from being sold, resulting in economic losses and potential risks to consumers.. Second, they often depend on middlemen or authorities that might not always be honest, making it hard to trust the authentication process.

Disadvantages of the existing system:

- Their effectiveness in preventing the sale of counterfeit goods is questionable, leading to financial losses and possible hazards for buyers.
- It is difficult to trust the authentication process because they frequently rely on intermediaries or authorities who may not always be trustworthy.

3. PROPOSED SYSTEM

To overcome these challenges, we are integrating blockchain technology. Blockchain is like a digital ledger that records transactions securely and transparently. In our case, it's used to store information regarding product origins, verification processes, and authenticity checks. Instead of having all the data in one place, blockchain stores records as blocks of data, each with a unique code called a hash. These blocks are distributed across multiple computers (nodes), making it much harder for anyone to tamper with the data or compromise the entire system.

4. WORKING PRINCIPLE

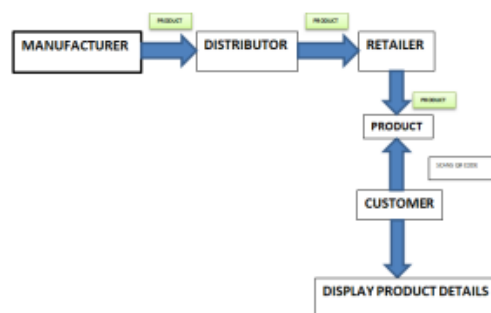


Fig 1: Work Flow

Advantages of the Proposed System:

- First, it's decentralized, meaning the data isn't stored in one vulnerable location.
- Second, it enhances security because the data is stored in encrypted format that's very difficult to alter or hack.
- Third, it promotes transparency, as all transactions are recorded and visible to authorized users.
- Fourth, it ensures data immutability, meaning once something is recorded in the blockchain, it can't be easily changed.
- Finally, it's resilient to failures because even if some nodes go down, others continue to maintain the data.

5. RESULTS

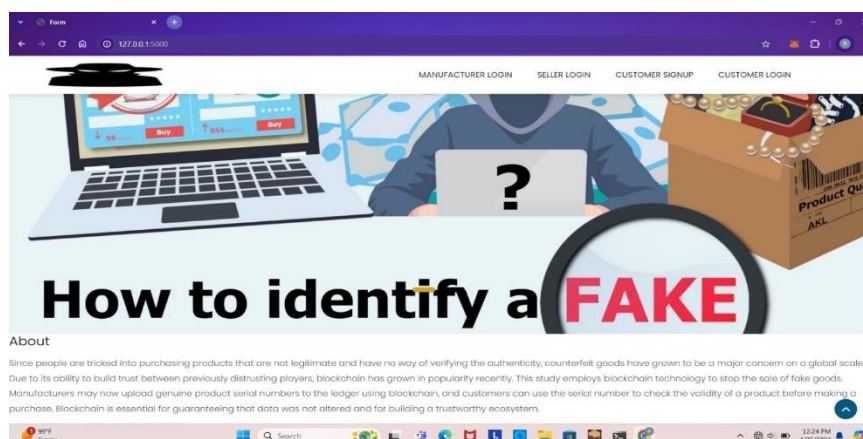


Fig 2: Home Page

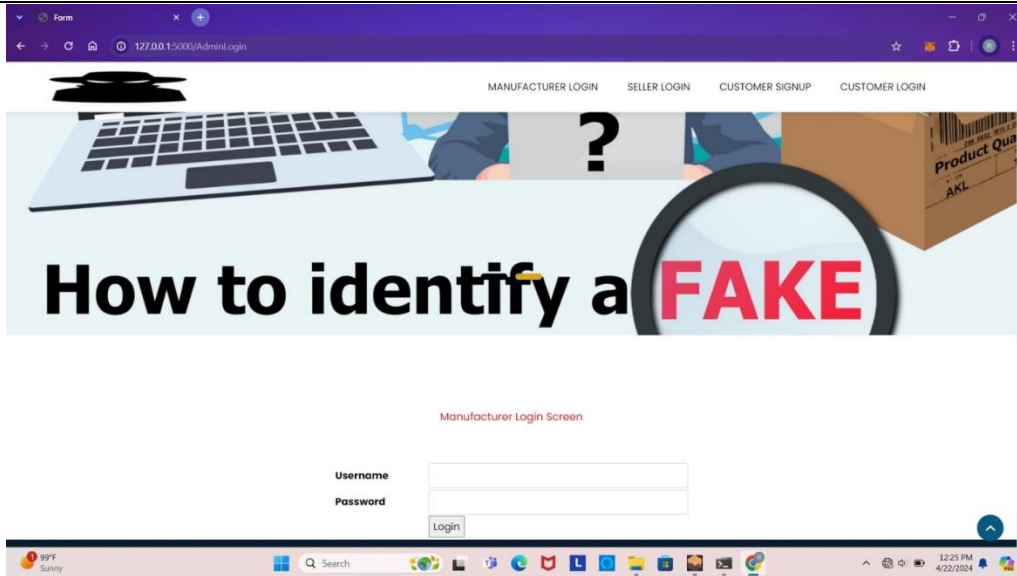


Fig 3: Manufacturer Login Screen

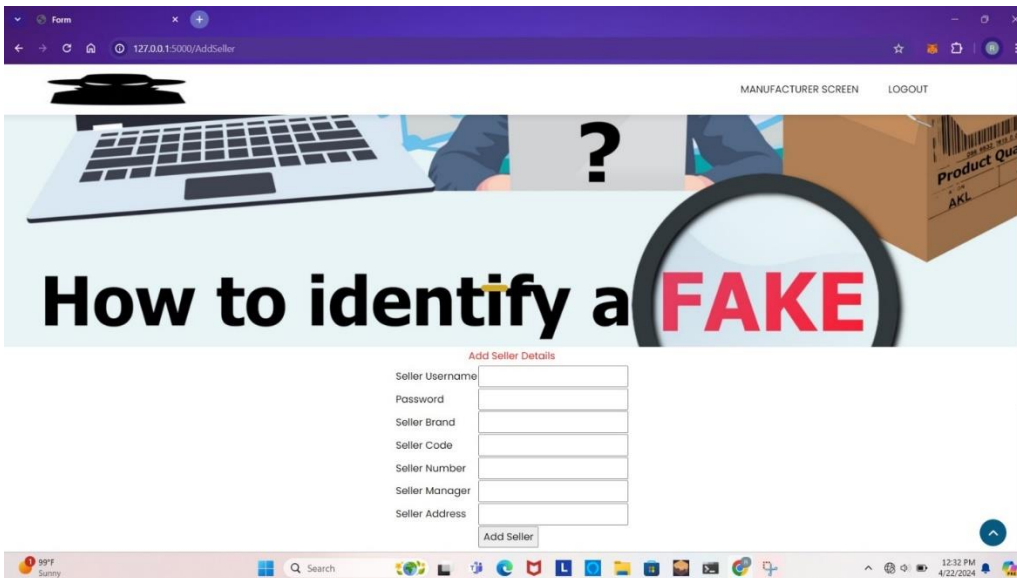


Fig 4: Add Seller Details Screen

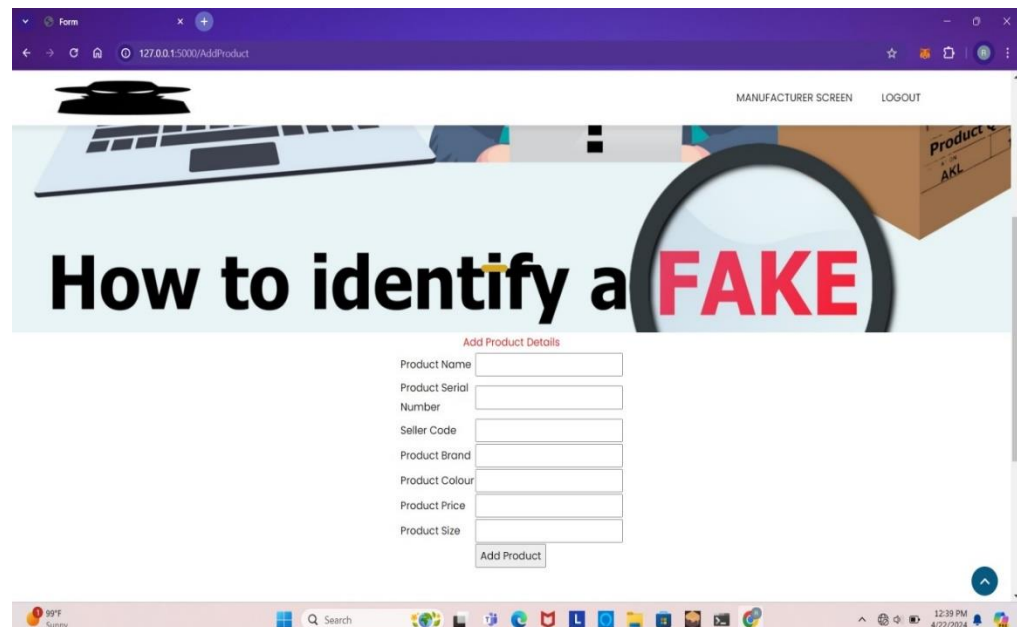


Fig 5: Add Product Details Screen

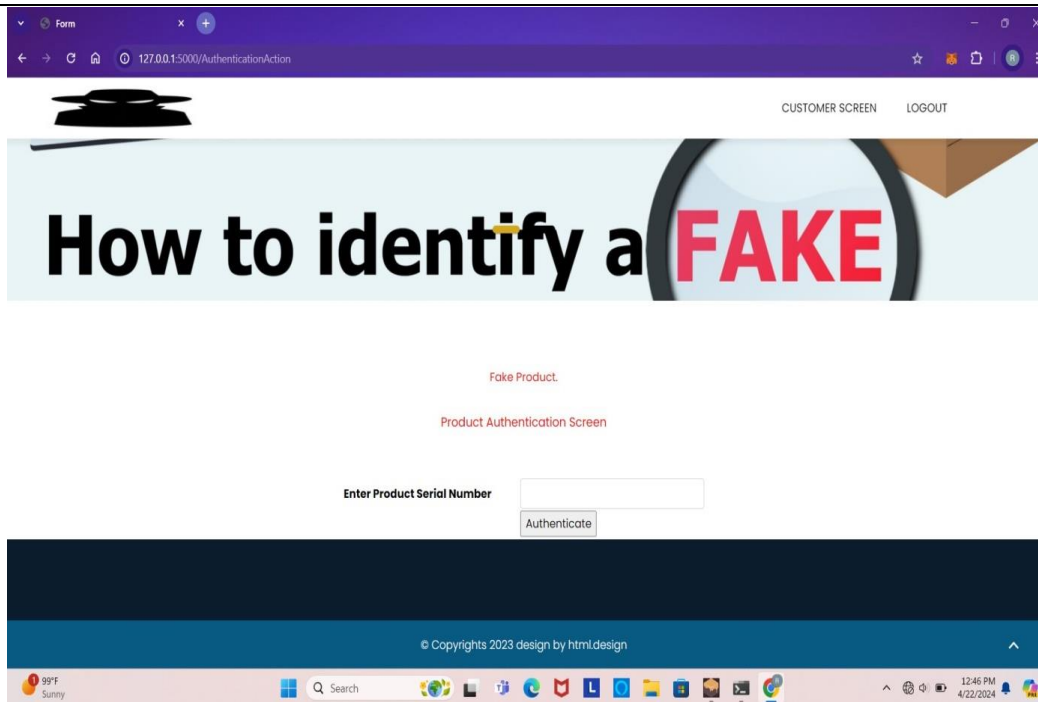


Fig 6: Fake Product Identification Screen

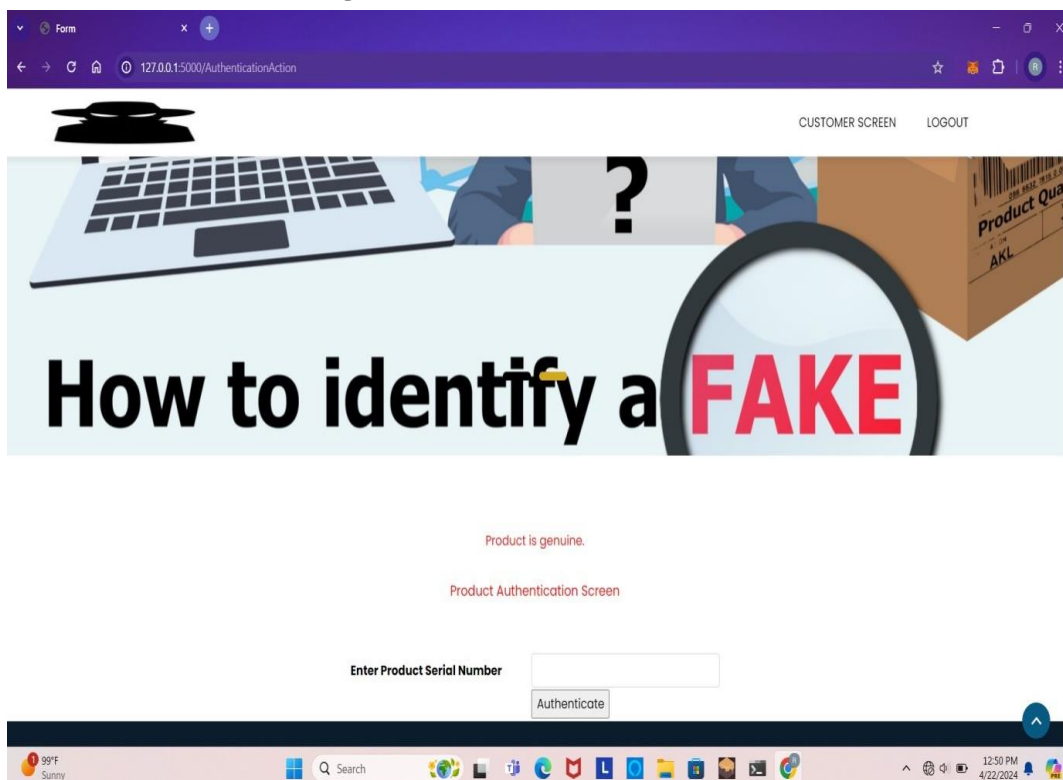


Fig 7: Real Product Identification Screen

6. CONCLUSION

In conclusion, the project harnesses blockchain technology to empower consumers in distinguishing genuine items from counterfeits, fostering trust and confidence in their purchases. By integrating blockchain within supply chains, the initiative effectively combats counterfeit products, elevating transparency and reliability across industries. Collaborative efforts with stakeholders promote standardized blockchain integration protocols, further enhancing counterfeit prevention measures.

Through a user-friendly interface, consumers can easily verify product authenticity, instilling confidence in everyday purchases. Ultimately, by diminishing counterfeit products and associated risks, the project emerges as a pivotal guardian for consumers and markets, while highlighting the sustainability benefits of its support.

7. REFERENCES

- [1] Mahammad, F. S., & Viswanatham, V. M. (2020). Performance Analysis Of Data Compression Algorithms For Heterogeneous Architecture Through Parallel Approach. *The Journal Of Supercomputing*, 76(4), 2275-2288.
- [2] Karukula, N. R., & Farooq, S. M. (2013). A Route Map For Detecting Sybil Attacks In Urban Vehicular Networks. *Journal Of Information, Knowledge, And Research In Computer Engineering*, 2(2), 540-544.
- [3] Farook, S. M., & Nageswarareddy, K. (2015). Implementation Of Intrusion Detection Systems For High Performance Computing Environment Applications. *Inter National Journal Of Scientific Engineering And Technology Research*, 4(0), 41.
- [4] Sunar, M. F., & Viswanatham, V. M. (2018). A Fast Approach To Encrypt And Decrypt Of Video Streams For Secure Channel Transmission. *World Review Of Science, Technology And Sustainable Development*, 14(1), 11-28.
- [5] Mahammad, F. S., & Viswanatham, V. M. (2017). A Study On H. 26x Family Of Video Streaming Compression Techniques. *International Journal Of Pure And Applied Mathematics*, 117(10), 63-66.
- [6] Devi, S. M. S., Mahammad, F. S., Bhavana, D., Sukanya, D., Thanusha, T. S., Chandrakala, M., & Swathi, P. V. (2022). "Machine Learning Based Classification And Clustering Analysis Of Efficiency Of Exercise Against Covid-19 Infection." *Journal Of Algebraic Statistics*, 13(3), 112-117.
- [7] Devi, M. M. S., & Gangadhar, M. Y. (2012). "A Comparative Study Of Classification Algorithm For Printed Telugu Character Recognition." *International Journal Of Electronics Communication And Computer Engineering*, 3(3), 633-641.
- [8] Devi, M. S., Meghana, A. I., Susmitha, M., Mounika, G., Vineela, G., & Padmavathi, M. Missing Child Identification System Using Deep Learning.
- [9] V. Lakshmi Chaitanya. "Machine Learning Based Predictive Model For Data Fusion Based Intruder Alert System." *Journal Of Algebraic Statistics* 13, No. 2 (2022): 2477-2483.
- [10] Chaitanya, V. L., & Bhaskar, G. V. (2014). Apriori Vs Genetic Algorithms For Identifying Frequent Item Sets. *International Journal Of Innovative Research & Development*, 3(6), 249-254.
- [11] Chaitanya, V. L., Sutraye, N., Praveena, A. S., Niharika, U. N., Ulfath, P., & Rani, D. P. (2023). Experimental Investigation Of Machine Learning Techniques For Predicting Software Quality.
- [12] Lakshmi, B. S., Pranavi, S., Jayalakshmi, C., Gayatri, K., Sireesha, M., & Akhila, A. Detecting Android Malware With An Enhanced Genetic Algorithm For Feature Selection And Machine Learning.
- [13] Lakshmi, B. S., & Kumar, A. S. (2018). Identity-Based Proxy-Oriented Data Uploading And Remote Data Integrity Checking In Public Cloud. *International Journal Of Research*, 5(22), 744-757.
- [14] Lakshmi, B. S. (2021). Fire Detection Using Image Processing. *Asian Journal Of Computer Science And Technology*, 10(2), 14-19.
- [15] Devi, M. S., Poojitha, M., Sucharitha, R., Keerthi, K., Manideepika, P., & Vasudha, C. Extracting And Analyzing Features In Natural Language Processing For Deep Learning With English Language.
- [16] Kumar Jds, Subramanyam Mv, Kumar Aps. Hybrid Chameleon Search And Remora Optimization Algorithm-Based Dynamic Heterogeneous Load Balancing Clustering Protocol For Extending The Lifetime Of Wireless Sensor Networks. *Int J Commun Syst.* 2023; 36(17):E5609. Doi:10.1002/Dac.5609
- [17] David Sukeerthi Kumar, J., Subramanyam, M.V., Siva Kumar, A.P. (2023). A Hybrid Spotted Hyena And Whale Optimization Algorithm-Based Load-Balanced Clustering Technique In Wsns. In: Mahapatra, R.P., Peddoju, S.K., Roy, S., Parwekar, P. (Eds) *Proceedings Of International Conference On Recent Trends In Computing. Lecture Notes In Networks And Systems, Vol 600.* Springer, Singapore. https://doi.org/10.1007/978-981-19-8825-7_68
- [18] Murali Kanthi, J. David Sukeerthi Kumar, K. Venkateshwara Rao, Mohamad Ahmed Ali, Sudha Pavani K, Nuthanakanti Bhaskar, T. Hitendra Sarma, "A Fused 3d-2d Convolution Neural Network For Spatial-Spectral Feature Learning And Hyperspectral Image Classification," *J Theor Appl Inf Technol*, Vol. 15, No. 5, 2024, Accessed: Apr. 03, 2024. [Online]. Available: [Www.Jatit.Org](http://www.jatit.org)
- [19] Prediction Of Covid-19 Infection Based On Lifestyle Habits Employing Random Forest Algorithm Fs Mahammad, P Bhaskar, A Prudvi, Ny Reddy, Pj Reddy *Journal Of Algebraic Statistics* 13 (3), 40-45
- [20] Machine Learning Based Predictive Model For Closed Loop Air Filtering System P Bhaskar, Fs Mahammad,

-
- Ah Kumar, Dr Kumar, Sma Khadar, ...Journal Of Algebraic Statistics 13 (3), 609-616
- [21] Kumar, M. A., Mahammad, F. S., Dhanush, M. N., Rahul, D. P., Sreedhara, K. L., Rabi, B. A., & Reddy, A. K. (2022). Traffic Length Data Based Signal Timing Calculation For Road Traffic Signals Employing Proportionality Machine Learning. *Journal Of Algebraic Statistics*, 13(3), 25-32.
- [22] Kumar, M. A., Pullama, K. B., & Reddy, B. S. V. M. (2013). Energy Efficient Routing In Wireless Sensor Networks. *International Journal Of Emerging Technology And Advanced Engineering*, 9(9), 172-176.
- [23] Kumar, M. M. A., Sivaraman, G., Charan Sai, P., Dinesh, T., Vivekananda, S. S., Rakesh, G., & Peer, S. D. Building Search Engine Using Machine Learning Techniques.
- [24] “ Providing Security In Iot Using Watermarking And Partial Encryption. Issn No:
- [25] 2250-1797 Issue 1, Volume 2 (December 2011)
- [26] The Dissemination Architecture Of Streaming Media Information On Integrated Cdn And P2p, Issn 2249-6149 Issue 2, Vol.2 (March-2012)
- [27] Provably Secure And Blind Sort Of Biometric Authentication Protocol Using Kerberos, Issn: 2249-9954, Issue 2, Vol 2 (April 2012)
- [28] D.Lakshmaiah, Dr.M.Subramanyam, Dr.K.Satya Prasad,” Design Of Low Power 4- Bit Cmos Braun Multiplier Based On Threshold Voltage Techniques”, *Global Journal Of Research In Engineering*, Vol.14(9),Pp.1125-1131,2014.
- [29] R Sumalatha, Dr.M.Subramanyam, “Image Denoising Using Spatial Adaptive Mask Filter”, *Ieee International Conference On Electrical, Electronics, Signals, Communication & Optimization (Eesco-2015)*, Organized Byvignans Institute Of Information Technology, Vishakapatnam, 24 Th To 26th January 2015. (Scopus Indexed)
- [30] P.Balamurali Krishna, Dr.M.V.Subramanyam, Dr.K.Satya Prasad, “Hybrid Genetic Optimization To Mitigate Starvation In Wireless Mesh Networks”, *Indian Journal Of Science And Technology*, Vol.8, No.23, 2015. (Scopus Indexed)
- [31] Y.Murali Mohan Babu, Dr.M.V.Subramanyam, M.N. Giri Prasad,” Fusion And Texure Based Classification Of Indian Microwave Data – A Comparative Study”, *International Journal Of Applied Engineering Research*, Vol.10 No.1, Pp. 1003-1009, 2015. (Scopus Indexed)