

Blockchain based Cryptocurrency Wallet

Ayush Gimekar¹, Abhay Pawar², Vaishnavi Patil³, Zuveriya Tamboli⁴, Prof.M.S.Kale⁵

Department of Information Technology, Sinhgad Academy of Engineering, SPPU, Pune,
Maharashtra, India

ABSTRACT: Blockchain is a technology that is developed using a combination of various techniques such as mathematics, algorithms, cryptography, economic models, and so on. Blockchain is a public ledger of all cryptocurrency transactions that are digitized and decentralized. All the transactions of cryptocurrencies are stored in chronological order to help users in tracking the transactions without maintaining any central record of the transactions. Application prospects of blockchain are promising and have been delivering the result since its inception. Blockchain technology has evolved from initial cryptocurrency to new age smart contracts and has been implemented and applied in many fields.

KEYWORDS: *Blockchain, ledger, cryptocurrencies*

I. INTRODUCTION

Traditional banking systems pose several problems for doing any transaction. For one thing, transactions are often slow. For another, any transaction has to pass through an intermediary, like a bank, meaning there is a central point of failure. And there are issues in keeping track of all accounts and balances; data can get jeopardized, manipulated, or even corrupted across multiple systems where the accounts and balances are maintained. Blockchain wallets reduce or eliminate these problems. A blockchain wallet is a cryptocurrency wallet that allows users to manage different kinds of cryptocurrencies—for example, Bitcoin or Ethereum. A blockchain wallet helps someone exchange funds easily. Transactions are secure, as they are cryptographically signed. The wallet is accessible from web devices, including mobile ones, and the privacy and identity of the user are maintained. So a blockchain wallet provides all the features that are necessary for safe and secure transfers and exchanges of funds between different parties. It is very similar to the process of sending or receiving money through PayPal or any other gateway used today, but you use cryptocurrency instead. Examples of blockchain wallets include Electrum, Blockchain.info, Jaxx, Mycelium, Samurai, and Bitcoin paper wallet. There are many more based on the needs you have and the security you require. E-wallets allow individuals to store cryptocurrencies and other digital assets. In the case of Blockchain Wallet, users can manage their balances of various cryptocurrencies such as the well-known Bitcoin and Ether as well as stellar, Tether, and Paxos Standard. Creating an e-wallet with Blockchain Wallet is free, and the account setup process is done online. Individuals must provide an email address and password that will be used to manage the account, and the system will send an automated email requesting that the account be verified.

II. KEY CONCEPTS

A) Blockchain

A block chain is a publicly accessible type of record between technology nodes in the network. A block chain serves as a digital database for storing data in digital form. The most well-known use of blockchain technology is for preserving a secure and decentralized record of transactions in cryptocurrency systems like Bitcoin. The novelty of a blockchain is that it fosters confidence without the necessity for a reliable third party by ensuring the integrity and security of a record of data. Blockchains are a specific kind of common ledger that vary from conventional databases as in manner they gather information. Blockchains hold data in blocks that are subsequently connected via cryptography. Cryptocurrency is utilized in the context of Bitcoin in a decentralized manner, allowing all users to jointly maintain control rather than any one individual or organization. The data cannot be changed since it is decentralized. This implies that payment done using Bitcoin are publicly visible and forever recorded.

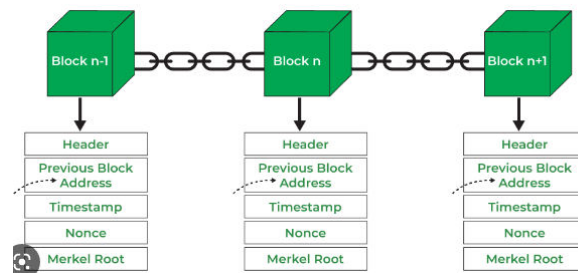


Fig 1. Blockchain Structure

B) Cryptography

Data security using cryptography prevents illegal access. As was already said, the two primary ideas in a cryptocurrency are cryptographic and hashing. Cryptography is a method of protecting information and communications through the use of codes, so that only those for whom the information is intended can read and process it.

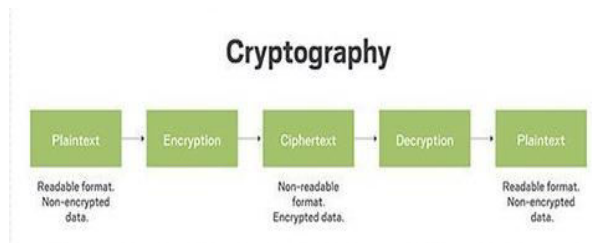


Fig 2. Cryptography Structure

- **Encryption:** Conversion of normal text to a random sequence of bits.
- **Keys:** Some of the amount of information is required to give the information for cryptographic algorithm.
- **Decryption:** The inverse process of encryption, conversion of a Random sequence of bits to plaintext
- **Cipher:** The mathematical function, i.e. A cryptographic algorithm which is used to convert plaintext to ciphertext (Random sequence of bits).

C] Cryptocurrencies:

Cryptocurrencies are a form of digital money operated via a decentralised system, meaning they aren't regulated by banks or governments. Their value, like traditional money, is based on supply and demand, and then secured by algorithms. Cryptocurrencies went mainstream with the launch of Bitcoin in 2009.

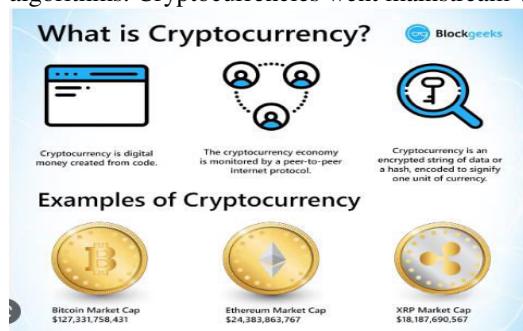


Fig 3. Cryptocurrency



Fig.4. Public and private key

D] Public key and Private key :

A key is a long string of random, unpredictable characters. While a public key is like a bank account number and can be shared widely, the private key is like a bank account password or pin and should be kept secret. In public-key cryptography, every public key is paired with one corresponding private key. Together, they are used to encrypt and decrypt data

E) Mining:

The process of adding transaction records to the bitcoin blockchain This process of Blockchain mining is performed by a community of people around the world called ‘Blockchain miners.’ Anyone can apply to become a Blockchain miner. These Blockchain miners install and run a special Blockchain mining software that enables their computers to communicate securely with one another. Once a computer installs the software, joins the network, and begins mining bitcoins, it becomes what is called a ‘node.’ Together, all these nodes communicate with one another and process transactions to add new blocks to the blockchain which is commonly known as the bitcoin net



Fig5. Bitcoin mining

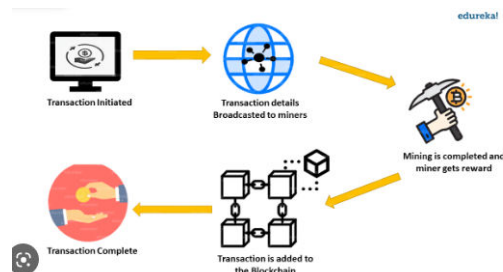


Fig 6. Mining Process

F) Ethereum:

Ethereum is a decentralized blockchain platform that establishes a peer-to-peer network that securely executes and verifies application code, called smart contracts. Smart contracts allow participants to transact with each other without a trusted central authority.

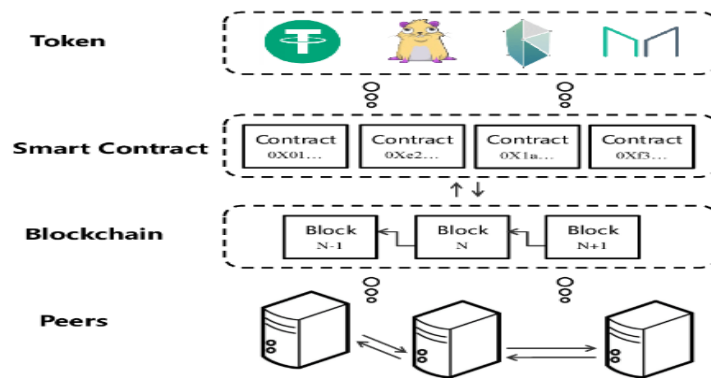


Fig 7. overview of ethereum

G) Hashing :

A hash is a function that meets the encrypted demands needed to secure information. Hashes are of a fixed length, making it nearly impossible to guess the hash if someone was trying to crack a blockchain. The same data will always produce the same hashed value. Hashes are one of the backbones of the blockchain network



Fig. 8. Hashing

III. LITERATURE SURVEY

A blockchain can be referred to as a collection of records or open records that can be shared among the participating parties. Every transaction that gets incorporated is first verified by all participants of that transaction. Once the data gets recorded by the blockchain can never be rewritten or changed. Thus blockchain can be termed as record book of all transactions held Cryptocurrencies, the decentralized bitcoin or say Ethereum which can be termed as peer-to-peer computerized cash also uses the blockchain technology. [1] This paper proposed by Siddharth Rajput and Archana Singh includes history of bitcoin, a few literary reviews, working of the blockchain and its application.[2]The paper proposed by Zhou Jian, Qu Ran, Sun Liyuan in Securing Blockchain Wallets Efficiently Based on Threshold ECDSA Scheme Without Trusted Center proposes a blockchain wallet protection scheme against single point failure based on threshold elliptic curve digital signature without trusted center. In this scheme, participants cooperate to generate public and private keys and sharing private key without the participation of trusted center. The participants who exceed the threshold number can sign the transaction by constant rounds, which can effectively resist single point attack and ensure the security of wallet.

Cong Li and Shihao Li [3], In this paper the authors have studied the security risks of Android-based cryptocurrency wallet and proposed the adversary model, analyzed the attack surface originated from the Android OS, and demonstrated several attack vectors by conducting experiments on multiple popular cryptocurrency wallets in Google Play Store. Finally, they have presented several security defense strategies in response to the security risks. Weiqi Dai, Jun Deng [4], In this paper, the analyst have designed a secure blockchain lightweight wallet based on Trust zone to protect SPV. It is more portable compared with the hardware wallet, and safer than the software wallet. Through the isolation, it can also protect the private key and the wallet's address from being stolen by the attackers no matter whether the Rich OS is malicious or not. Meanwhile, it can protect the verification process by verifying transactions in the secure execution environment (SEE), and keep the local block headers unreadable directly from the Rich OS through encryption

In the paper, SBLWT: A Secure Blockchain Lightweight Wallet Based on Trustzone by Weiqi Dai; Jun Deng; Qinyuan Wang; Changze Cui; Deqing Zou; Hai Jin [5], The software-based wallet is convenient but the safety cannot be guaranteed, whereas the hardware-based wallet is secure but inconvenient because users must carry an additional physical device. In this article, we build a Secure Blockchain Lightweight Wallet based on Trustzone (SBLWT), which provides comprehensive protection for the private key, the wallet address, the block headers stored in the local database, and the transaction verification mechanisms.S. Nagaprasad et al. [13], Ajay S. Laddkat et al. [14], S. L. Bangare et al. [15-20], K. Gulati et al. [21], P. S. Bangare et al. [22-23], Xu Wu et al. [24], V. Durga Prasad Jasti et al. [25], A. S. Zamani et al. [26], M. L. Bangare et al. [27] and S. Mall et al. [28] have proposed various research models which were referred here.

IV. METHODOLOGY

Blockchain wallets follow a similar process using a public key and a private key together. A public key is similar to your email address; you can give it to anyone. When your wallet is generated, a public key is generated, and you can share the public key with anyone in order to receive funds.

The private key is top secret. It's similar to your password; it should not get hacked and you should not disclose it to anyone. You use this private key to spend your funds. If someone gets access to your private key, there is a high possibility that your account is compromised, and you might end up losing all the cryptocurrency deposits in your account.

Project dependencies:

A. Open CV:

OpenCV stands for Open-Source Computer Vision which is a library in which is written in C++ used for Computer Vision. It is cross-platform and free to use. It provides real-time GPU acceleration features which are used in wide areas like 3D and 2D feature toolkits, Faces and gesture recognition systems.

B. Ganache:

Is a personal blockchain for rapid Ethereum and Corda distributed application development. You can use Ganache across the entire development cycle; enabling you to develop, deploy, and test your Apps in a safe and deterministic environment. In short it is your local blockchain simulator.

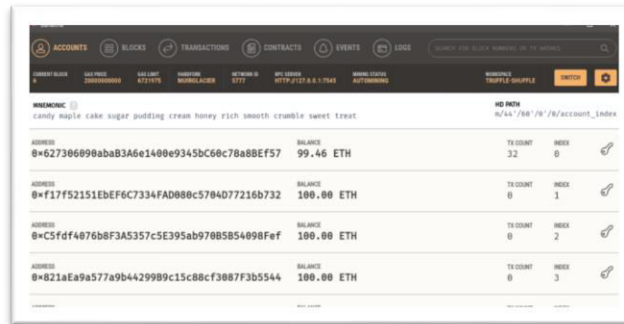
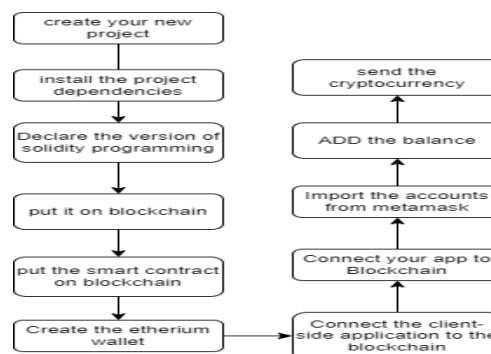


Fig. 1.1 Ganache

C. Metamask

Meta Mask is a software cryptocurrency wallet used to interact with the Ethereum blockchain. It allows users to access their Ethereum wallet through a browser extension or mobile app, which can then be used to interact with decentralized applications. Meta Mask is developed by ConsenSys Software Inc., a blockchain software company focusing on Ethereum-based tools and infrastructure. MetaMask allows users to store and manage account keys, broadcast transactions, send and receive Ethereum-based cryptocurrencies and tokens, and securely connect to decentralized applications through a compatible web browser or the mobile app's built-in browser. Websites or other decentralized applications are able to connect, authenticate, and/or integrate other smart contract functionality with a user's MetaMask wallet (and any other similar blockchain wallet browser extensions) via JavaScript code that allows the website to send action prompts, signature requests, or transaction requests to the user through MetaMask as an intermediary

Steps :-



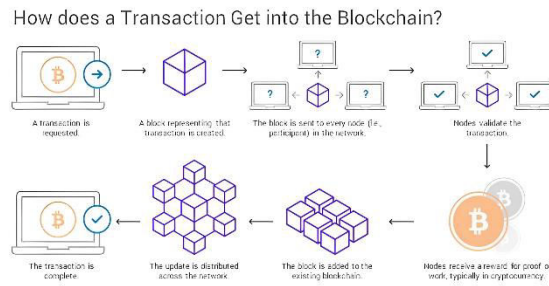


Fig. 1.2. Transaction in Blockchain

Blockchain Wallet Features:

- Easy to use. It's just like any other software or a wallet that you use for your day-to-day transactions.
- Highly secure. It is just a matter of securing your private key.
- Allows instant transactions across geographies. And these are barrier-free, without intermediaries.
- Low transaction fees. The cost of transferring funds is much lower than with traditional banks.
- Allows transactions across multiple cryptocurrencies. This helps you do easy currency conversions.

V. RESULTS

First, we have to connect to MetaMask in order to access the Ethereum wallet.

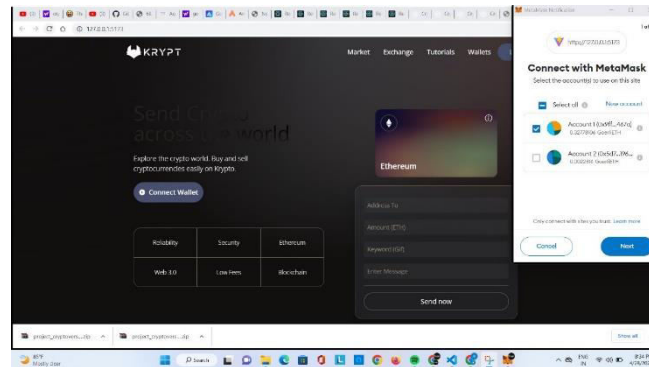


Fig. 1.3. Connection with Metamask

We then connect to the account

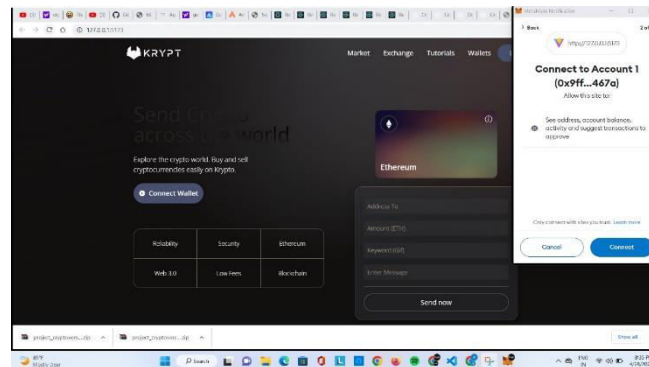


Fig. 1.4. Home Screen

Type or copy paste the Address to which you want to sent the amount. Enter the amount you want to send and if you want to give any additional information related transaction or send any message you can do that as well. Sending message is optional.

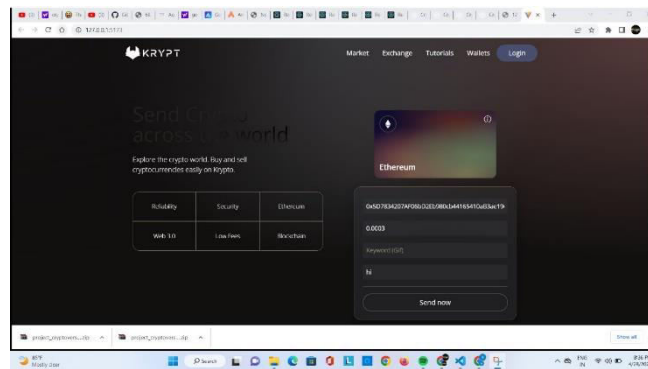


Fig. 1.5. Filling the details

If you scroll a little down you would be able to see the features of this crypto wallet.

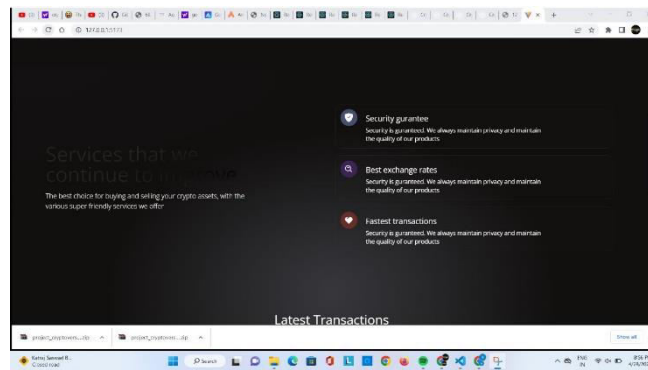


Fig.1.6. Features of website

And scrolling more down you would be able to see the transaction history as well.

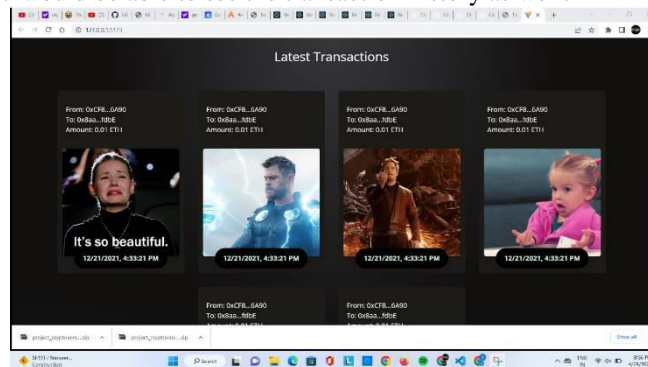


Fig.1.7 Transaction History

VI. CONCLUSION

The two most popular and valuable cryptocurrencies in existence today are Bitcoin and Ethereum. They are built on blockchain technology, which aims to support a done to assure in a peer-to-peer network based on the consensus of the majority of nodes. In this article, we. present an overview of the foundations of blockchain technology, the most successful (or well-liked) blockchain applications, Bitcoin and Ethereum, as well as the early phases of the introduction of digital money. We have created a web- based wallet for the DAI stable coin on the ethereum network using truffle, Ganache, Web3.js and React.js. Cost is what drives day-to-day company operations; thus, banks must carefully consider this before implementing this technology. When blockchain is used to power the banking system, it becomes more tolerant.

REFERENCES

1. M. Marchesi, "Why blockchain is important for programming designers, and why programming building is crucial for blockchain programming (Keynote)", 2018 International Workshop on Blockchain orientating software system Engineering (IWBOSE), Campobasso, 2018, pp. 1-1.
2. Ehab Zaghloul, Tongtong Li, Matt W. Mutka, Jian Ren. "Bitcoin and Blockchain: Security and Privacy", (2020).3004273, IEEE Internet of Things Journal
3. Hossein Rezaeighaleh, Cliff C. Zou, Multilayered Defense-in-Depth Architecture for Cryptocurrency Wallet 2020 IEEE 6th International Conference on Computer and Communications
4. Gokay Saldamli, Sohil S. Mehta, Pranjali S. Raje, Madhuri S. Kumar, Sumedh S. Deshpande. "Identity management using blockchain", preprint, (2019)
5. N. Kshetri and J. Voas, "Blockchain-Enabled E-Voting," in IEEE Software, vol. 35, no. 4, pp. 95-99, 2018.
6. D. Mill operator, "Blockchain and therefore thenet of Things within the Industrial Sector," in IT skilled, vol. 20, no. 3, pp. 15-18, May./Jun. 2018.
7. Popova, N.A., Butakova, N.G. (2019). technology without tokens to protect banking transactions Proceedings of the 2019 IEEE Institute of Electrical and Electronics Engineers Inc
8. T. N. Dinh and M. T. Thai, "AI and Blockchain: A turbulent Integration," vol. 51, no. 9, pp. 48-53, Gregorian calendar month 2018.
9. L. Kan, Y. Wei, A. Hafiz Muhammad, W. Siyuan, G. Linchao and H. Kai, "A Multiple Blockchains design on Inter Blockchain Communication," 2018 IEEE International Conference on software system Quality, responsibility and Security Companion (QRS-C), L'isbon, 2018, pp. 139-145.
10. Corina Sas and Irni Eliana Khairuddin, "Exploring Trust in Bitcoin Technology: A Framework for HCI Research" in , ACM, 2015.
11. Stanislaw Jarecki, Aggelos Kiayias, Hugo Krawczyk and Jiayu Xu, "Highly Efficient and Composable Password-Protected Secret Sharing (Or: How to Protect Your Bitcoin Wallet Online)" in , IEEE, 2016
12. Nelisiwe Peaceness DLAMINI, Mfundo Shakes SCOTT and Kishor Krish-nan NAIR, "Development of an SMS System Used to Access Bitcoin Wallets".
13. S. Nagaprasad, D. L. Padmaja, Yaser Quereshi, S.L. Bangare, Manmohan Mishra, Mazumdar B. D., "Investigating the Impact of Machine Learning in Pharmaceutical Industry", Journal of Pharmaceutical Research International (Past name: British Journal of Pharmaceutical Research, Past ISSN: 2231-2919, NLM ID: 101631759), Volume 33, Issue 46A, Pages 6-14, Publisher: JPRI <https://www.journaljpri.com/index.php/JPRI/article/view/32834>
14. Ajay S. Ladkat, Sunil L. Bangare, Vishal Jagota, Sumaya Sanober, Shehab Mohamed Beram, Kantilal Rane, Bhupesh Kumar Singh, "Deep Neural Network-Based Novel Mathematical Model for 3D Brain Tumor Segmentation", Computational Intelligence and Neuroscience, vol. 2022, Article ID 4271711, 8 pages, 2022. <https://doi.org/10.1155/2022/4271711>
15. S. L. Bangare, "Brain Tumor Detection Using Machine Learning Approach", Design Engineering ISSN: 0011-9342, Scopus Index- Q4, Ei Compendex, Volume 2021, Issue 7, Pages 7557-7566, Publisher Design Engineering.
16. S. L. Bangare, and P. S. Bangare. "Automated testing in development phase." International Journal of Engineering Science and Technology 4.2 (2012): 677-680.
17. S. L. Bangare, N. B. Dhawas, V. S. Taware, S. K. Dighe, & P. S. Bagmare, (2017). "Implementation of fabric fault detection system using image processing", International Journal of Research in Advent Technology, Vol.5, No.6, June 2017, E-ISSN: 2321-9637.
18. S. L. Bangare, N. B. Dhawas, V. S. Taware, S. K. Dighe, & P. S. Bagmare (2017). "Fabric fault detection using image processing method", International Journal of Advanced Research in Computer and Communication Engineering, 6(4), 405-409.
19. S. L. Bangare, S., H. Rajankar, P. Patil, K. Nakum, G. Paraskar, (2022). "Pneumonia detection and classification using CNN and VGG16". International Journal of Advanced Research in Science, Communication and Technology, 12, 771-779.
20. Sunil L. Bangare, Deepali Virmani, Girija Rani Karetla, Pankaj Chaudhary, Harveen Kaur, Syed Nisar Hussain Bukhari, Shahajan Miah, "Forecasting the Applied Deep Learning Tools in Enhancing Food Quality for Heart Related Diseases Effectively: A Study Using Structural Equation Model Analysis", Journal of Food Quality, vol. 2022, Article ID 6987569, 8 pages, 2022. <https://doi.org/10.1155/2022/6987569>
21. K. Gulati, M. Sharma, S. Eliyas, & Sunil L. Bangare (2021), "Use for graphical user tools in data analytics and machine learning application", Turkish Journal of Physiotherapy and Rehabilitation, 32(3), 2651-4451.

22. P. S. Bangare, Ashwini Pote, Sunil L. Bangare, Pooja Kurhekar, and Dhanraj Patil, "The online home security system: ways to protect home from intruders & thefts." International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN (2013): 2278-3075.
23. P. S. Bangare, S. L. Bangare, R. U. Yawle and S. T. Patil, "Detection of human feature in abandoned object with modern security alert system using Android Application," 2017 International Conference on Emerging Trends & Innovation in ICT (ICEI), Pune, India, 2017, pp. 139-144, doi: 10.1109/ETIICT.2017.7977025.
24. Xu Wu, Dezhi Wei, Bharati P. Vasgi, Ahmed Kareem Oleiwi, Sunil L. Bangare, Evans Asenso, "Research on Network Security Situational Awareness Based on Crawler Algorithm", Security and Communication Networks, vol. 2022, Article ID 3639174, 9 pages, 2022. <https://doi.org/10.1155/2022/3639174>.
25. V. Durga Prasad Jasti, Enagandula Prasad, Manish Sawale, Shivilal Mewada, Manoj L. Bangare, Pushpa M. Bangare, Sunil L. Bangare, F. Sammy, "Image Processing and Machine Learning-Based Classification and Detection of Liver Tumor", BioMed Research International, vol. 2022, Article ID 3398156, 7 pages, 2022. <https://doi.org/10.1155/2022/3398156>
26. Zamani, A. S., Dr. Seema H. Rajput, Dr. Harjeet Kaur, Dr. Meenakshi, Dr. Sunil L. Bangare, & Samrat Ray. (2022). Towards Applicability of Information Communication Technologies in Automated Disease Detection. International Journal of Next-Generation Computing, 13(3). <https://doi.org/10.47164/ijngc.v13i3.705>.
27. M. L. Bangare, P. M. Bangare, R. S. Apare, & S. L. Bangare, (2021). "Fog computing-based security of IoT application", Design Engineering, 7, 7542-7549.
28. S. Mall, A. Srivastava, B. D. Mazumdar, M. Mishra, S. L. Bangare, & A. Deepak, (2022). "Implementation of machine learning techniques for disease diagnosis", Materials Today: Proceedings, 51, 2198-2201. <https://www.sciencedirect.com/science/article/abs/pii/S2214785321072679#!>