Trading Platform Powered by Blockchain

Siva Vignesh K[a], Shashwat Shukla[b], R.Naresh[c]

[a,b] UG Scholar, Department of Computer Science and Engineering, SRM Institute of Science and Technology, Kattankulathur, Chengalpattu, Chennai, Tamil Nadu, India-603 203.
[c] Associate Professor, Department of Computer Science and Engineering, SRM Institute of Science and Technology, Kattankulathur, Chengalpattu, Chennai, Tamil Nadu, India-603 203.
[a]siva_vignesh@outlook.com, [b]shashwatshukla194@gmail.com , [c]nareshr@srmist.edu.in .

***Corresponding Author: R. Naresh**

Article History: Received: 11 January 2021; Revised: 12 February 2021; Accepted: 27 March 2021; Published online: 10 May 2021

Abstract: Blockchain, the distributed ledger System advances in emerging decentralized systems that simplify paper processes and disrupt long-settled business models [1]. In Blockchain, data are encrypted, documented, dealing blocks together with timestamps are joined along to create an extensive, deep-seated record. Blockchain is a distributed ledger technology that aims to ensure transparency, integrity, and data security so that it cannot tamper. Blockchain technology is best notable for its association with cryptocurrency Bitcoin. It will have enormous applications in government, finance trade, accounting, and Business method Management. Therefore, an attempt is made to investigate its scope within the trading Sector by the decentralized and distributed ledger technology in this study. This paper examines the further improvement of trade finance utilizing blockchain technology.

Keywords: Blockchain, Hyperledger Fabric, smart contract, consensus mechanism.

1. Introduction

The Traditional way of online trading or any other E-Commerce platform is centralized. There are many problems like the high potential to threat, data leaks, data mutability, and under par responsibility. Blockchain is an advancing technology that facilitates every business model to the next level of advancement by providing a decentralized system. A decentralized, permissioned ledger means that every order and every shipment could be tracked in real-time, all while preventing competitors from accessing sensitive information. This model would reduce duplicate data entries, minimize human error, and expedite the investigation, as each transaction's provenance could easily be demonstrated. Whereas the traditional method has a centralized body that accesses all the sensitive information, and if there is any problem between the client and the customer or between the customer and the platform, it is a slight disadvantage for the customer because the central body of the platform may tamper or modify the data which breaks the trust. So this proposed model eliminates all these problems with blockchain property which is decentralized, immutable, and tamper-proof. This model proposed is implemented on a permissioned blockchain called Hyperledger Fabric launched by Linux Foundation. Hyperledger fabric has the edge over other blockchain technology like Ethereum as it is a permission-less blockchain and limited to solidity programming language. But in the case of Hyperledger fabric, it supports NodeJS, Java, or GO.

2. Related Work

In this segment, we will investigate the already proposed blockchain-based approach in the field of trading.

P. Krishna Karthik and R. Anand [1] have given us an idea about how Blockchain can be used in energy trading, and thereby smart contracts are made for the motivation behind P2P energy trading using Ethereum. When there is software aggregation with the energy trading, there is time utilization in getting the ideal outcomes.

Nizamuddin Arifin and Ahmad Zahiri Ismail [2] have given us another dimension about how the Trade finance application can be implemented with the Permissioned Blockchain Platform. This study differentiates between the traditional trading method and newly proposed blockchain-based trading methods and how it facilitates to ease this process and the idea of software connectors as a medium.

In 2018, Top to bottom examination and discussion of blockchain technologies like Hyperledger Fabric, Smart contract, Consensus mechanism, and protocols in network trading system had been done by Yu Wenjun and Wu Yuan [3]. But the author could not clearly explain the reliability of the encryption algorithm and its authentication. So this has been left for future work.

3. Overview of the Blockchain

In simple terms, a blockchain is a combination of technological invocation such as distributed ledger and cryptography. There are many advantages: immutability of data, transparency, decentralization, enhanced security, and easier traceability. A blockchain that supports a cryptocurrency like Bitcoin [4], Ethereum [5] is a permission-

less Blockchain where random people can participate in the network transactions. But in the case of permissioned Blockchain (example – Hyperledger Fabric), only a group of people who have a common motive to do some specific task but are new to each other and cannot trust each other fully participate. In this way, Permissioned Blockchain has evolved as an alternative way for permission-less Blockchain, leading to a secure transaction with each other.

3.1 Blockchain and its Data Structure.

Cryptography is one of the core building blocks of a blockchain [6]. The bitcoin blockchain's fundamental security is the elegant cryptographic linkage of all significant components of the ledger.

Blocks in a blockchain are linked with each other through the Merkle tree. A Merkle tree is based on the concept of a tree data structure where every leaf node has a hash calculated of its data and where the non-leaf node has a hash of all their underlying child [7].To preserve the tree's righteousness, the leaf that is denoted as private is removed, and hash is left as it is. The Merkle tree has its roots incorporated into the block header. The block header includes a reference to the block headers that precede it.

—At any point, if a link between any of the components is broken, it leaves them exposed to malicious attacks. Figure 1 shows how blocks are connected and the attributes present inside each block.

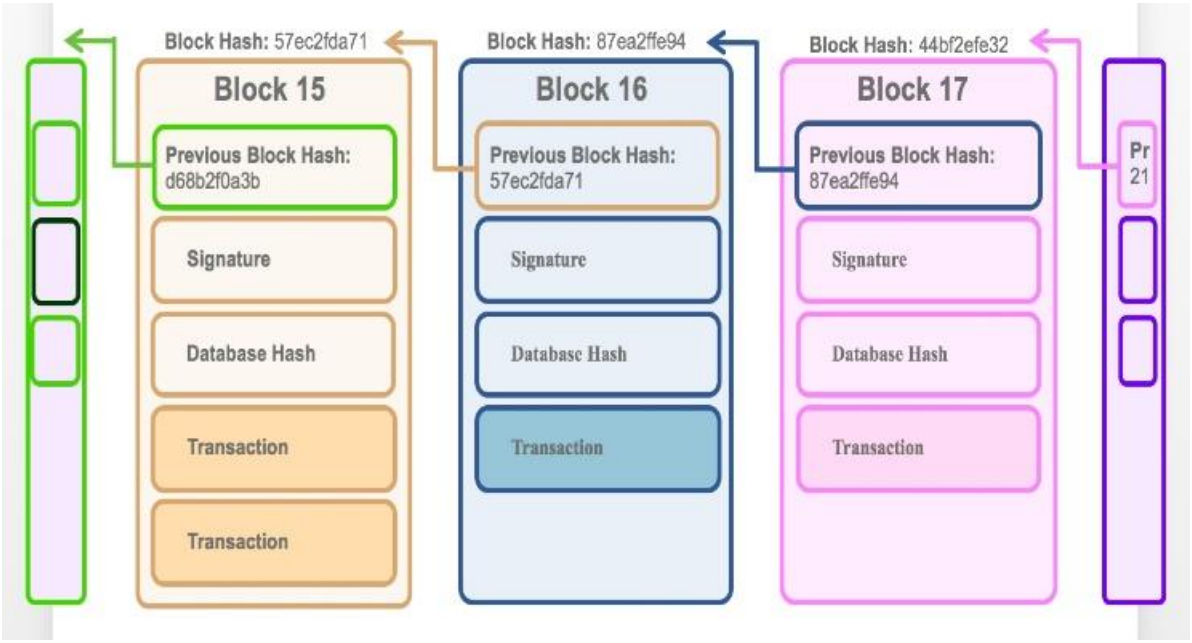

Figure 1. Blockchain data structure diagram

When a new transaction is done in the network, these are cryptographically connected to the already existing block with the previous hash linked to its header. These connections happen mainly through the Merkle tree. Once a network transaction has been changed in a block, with all other parts remaining stable, the relationship between all network transactions of the block and its header is broken. Figure 2 has the definition of the attributes present inside the block.

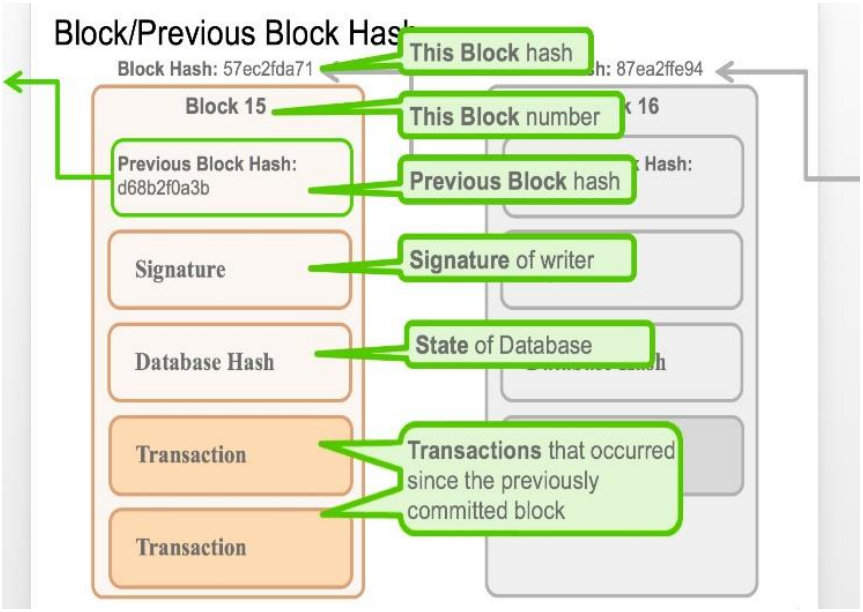

Figure 2. Definition of the attribute inside the block

As a result, when the chain is broken, and there arises a new Merkle tree root that will not match with the one already in the block header, this leads to breaking the connectivity for the rest of the Blockchain. By this, we can achieve tamper-proof. This the security model of the Blockchain.

3.2 Building Blocks of Blockchain

Distributed ledger, Cryptography, Consensus (Trust System), and Smart Contracts (Business rules) are the four building blocks of the Blockchain. All these have existed before the Blockchain. The combination of these innovations is termed Blockchain and making revolutions in the real-world Business model.

3.3 Distributed Ledger

The distributed ledger is a database that is shared and Synchronized across the organization. This allows the transaction to have strong evidence, allowing the network participants to access the information with a time stamp on it. Additionally, if an insertion, deletion, or updation is done inside the ledger, it immediately reflects all the network participants. As a result, decentralization in the network is achieved.

3.4 Cryptography

Cryptography is the technology of storing the data safe and secret by modifying it into the hash code. There are many crypto algorithms and encryption technology. They are Asymmetric (example: Rivest Shamir Adleman(1024- 8192), Digital Signature Algorithm (1024-3072)), Symmetric (example: Advanced Encryption Standard, Ron's Code 2, Data Encryption Standard, Triple Data Encryption Standard), Hash Algorithm (example: Secure hash algorithm-256).

3.4.1.Data Signing.

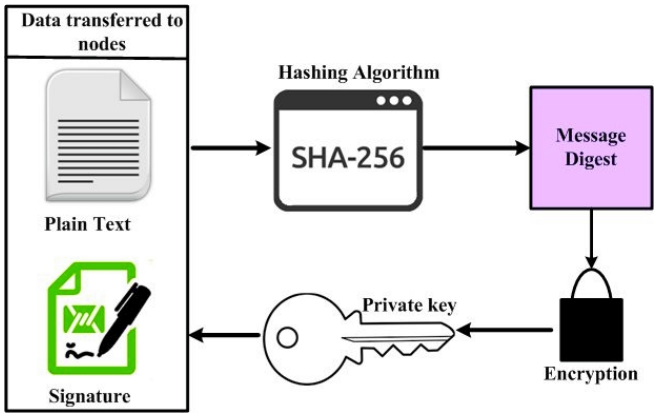

Figure 3. Data Signing Procedure

Each node is allocated with a public key and private key. The public key can be accessed all over the network, whereas the private key is used for message decryption and must be in safer hands. The first process is to encrypt the data and then broadcast it to all the nodes in the network. Public key information, node-specific private key information is made available in each node [8]. A message digest is created by plain text and signature processed inside the transferred data with the Secure Hash Algorithm (SHA) help. Figure 3. gives an outline of the initial process of data signing in the network.

3.4.2.Data Verification and Authentication.

After the data signing procedure, encrypted data is sent to the node in the network, and this encrypted data needs to undergo a verification procedure. The plaintext is hashed to message digest1 (MD1), and the signature is hashed to message digest 2 (MD2) as a part of the verification procedure. This procedure is done with the help of a broadcaster's public key information. The Authentication procedure is done by checking the similarity of the MD1 and MD2, and if they match with each other, then the data received is true. Else, it is false. Figure 4. gives the outline of data verification.

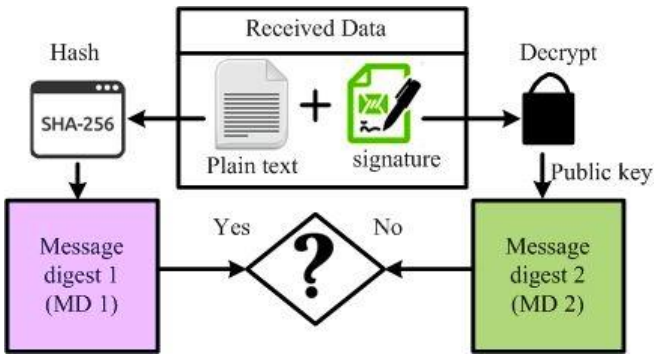

Figure 4. Data Verification Procedure

Privacy through cryptography is essential for ensuring that transactions are authenticated and verified. It is imperative to include cryptography in blockchain design to harden security and make it more difficult to breach the distributed system. By combining cryptography and Blockchain, the system ensures no duplicate recording of the same transaction.

3.5 Consensus:

Trust systems refer to using the power of the network to verify transactions. Consensus is the strategy for verifying and validating a data or transaction on a shared ledger without the need to depend on or trust any governing body. Consensus mechanisms are the key factor for the working of Blockchain. This foundational element of trust dictates the overall design and investment in a blockchain infrastructure. Trust, trade, and ownership are staples of blockchain technology. For intercompany transactions, the trust system governs transactions for trade between participating companies. Kafka [9] is a Voting-based algorithm that provides crash fault tolerance (CFT). This Consensus Algorithm is Permissioned, used in Fabric Blockchain. But there is one disadvantage associated with crash fault tolerance. The algorithm can stop the malicious nodes from reaching an agreement. But this can be prevented in the Sumeragi Consensus algorithm, which uses Byzantine fault tolerance (BFT) [10].

3.6 Smart Contracts:

Smart Contracts can also be referred to as business rules. Smart contracts are executable software module that is installed in the Blockchain itself. There will be terms and agreements between the client and customer when there is a business need, and they must be signed as a digital agreement via smart contracts. A blockchain can monitor the running status of a smart contract progressively. Transactions are executed as per the smart contract. Any decision taken inside the blockchain transaction is pre-defined in the Smart Contract as all the requirements, conditions, and exceptions are written in the form of code in the Smart Contract only[11]. Various business needs can be written in the form of code to reassure one party that the other will fulfill their promise. A smart contract is written in a high-level language, such as GO, solidity, or JavaScript.

4. Implementation

We cannot certainly conclude that designing an application in a blockchain or decentralized environment solves all the problems that prevail in the existing model. In the traditional method, the database is used to store, process, and serve data at the backend. Due to this, performance gets affected. Additionally, a Fabric blockchain application has peers keeping a common recreated record as the database's equivalent[12].

4.1 Characteristics of Hyperledger Fabric Application

Linux Foundation introduced an open-source project called Hyperledger [13]. There are five blockchain frameworks, and Hyperledger Fabric is one among them. We have used Hyperledger Fabric in our proposed work because it is the permissioned Blockchain.

4.2 Hyperledger Fabric runtime architecture

- Transaction Proposal
- Transaction endorsement
- Transaction submitted to the ordering service
- Transaction validation

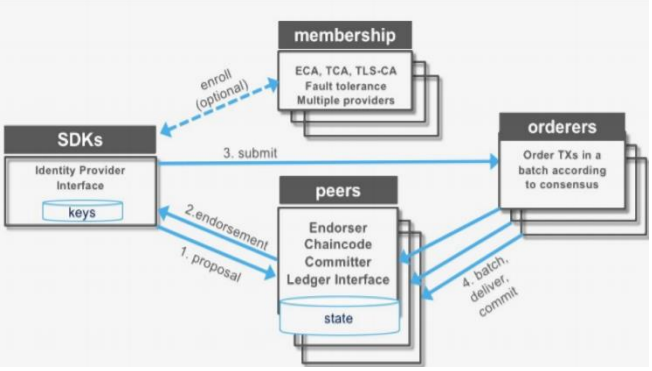

Figure 5. Runtime Architecture of Hyperledger Fabric

Application SDK submits the transaction proposal that includes ReadWrite set to the Ordering service. The transaction is then received by counter-parties that have been represented by endorsing peers on their channel. By calling the demanded chaincode function, the transactions are executed by each peer. Then the approved transactions are sent to the ordering service, and according to the consensus algorithm and validation, the orders are committed to the ledger. In the final step, transactions, endorsement policies, ReadSet data are validated and executes in the Blockchain block.

4.3 Application Architecture.

- At the Bottom layer, smart contract functions on the distributed ledger. Service API is exposed for notifying the transaction results and changes occurring on the channel.
- Operations such a chaincode setup and queries, Registration and enrollment, Transaction, and Event submission of a blockchain are performed in the middle layer.
- At the Topmost layer lies a user interface for the ease of use of the end-users.

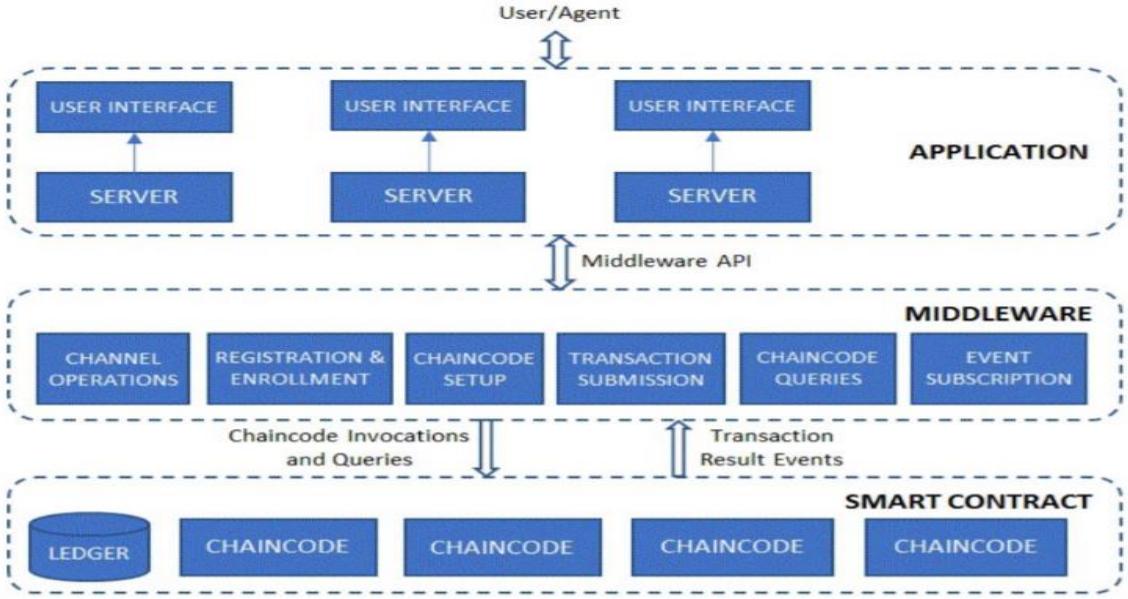

Figure 6. Application Architecture

5. Results discussion

Let us discuss the actual workflow with the working attributes present inside the application. Create a channel for trade. Join peers on the trade channel. Install and Initialize the trade Chaincode on the channel. Add or remove new organization, peers, new orders. Modification of smart contract.

Further explanation of the use case of this application is explained with an example. Person A wanted to buy a Mobile Phone from Person B and used the letter of credit process to initiate the trade process. Person B shipped the product to Person A with their respective banks' trust, which is also present in the Blockchain network. Their banks were aware of every step in the business process.

5.1 Platform Performance Characteristics

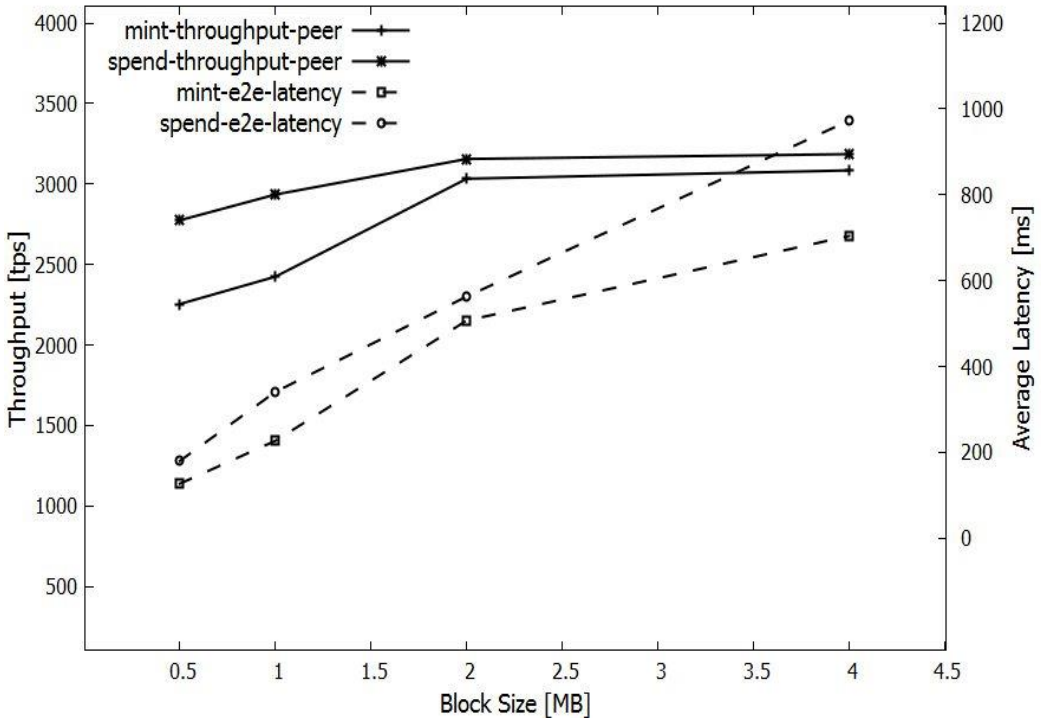

Figure 7. Effect of Block size on throughput and latency of the transaction in Blockchain.

The system's performance depends on many factors like the size of the block, transaction, fabric network, and hardware capabilities. Choosing the block size is the most crucial factor because it impacts the platform's throughput and latency. The network has been tested with block sizes varying from 0.5MB to 4MB. When block size is increased beyond 2MB, we could notice no significant improvement in the throughput. Hence block size of 2MB has been adopted to our network. Figure 7 shows the effect of block size on throughput and latency of the transaction in the Blockchain. The blockchain network has also been tested with two different hashing algorithms. By default, Hyperledger Fabric uses SHA-256 for its encryption, but the default hashing algorithm has also been tested with SHA-1 because many authors in the past have used SHA-1 in their work. Table 1 shows the difference between SHA-1 and SHA-256. By comparing both the algorithms, SHA-256 can result in the best encryption algorithm that is effective and efficient[14].

Attributes	**SHA-1**	**SHA-256**
Hash Size	160	256
Message Block size	512	512
Complexity of best attack	2^{80}	2^{128}
Attack possibilities	Easier to attack than SHA-256	Difficult to attack
Latency	60 ms	62 ms

Table 1. Comparison of hash algorithm

6. Conclusion

This study provides a comprehensive view of Blockchain and its building blocks like a shared ledger, Cryptography, Consensus Mechanism, and Smart contracts through its use case in trading. Hyperledger Fabric, a permissioned blockchain, is used. As a result, only a desired peer can participate in the network, and a control authority is present in the network who administers the activities performed by the permitted members. The integrity, immutability of the data, and its decentralization nature make the Blockchain a powerful upcoming technology. But each coin has two sides. Lower Transaction Processing, minimization of computation overhead, and scalability is the critical challenge in the Blockchain. Nevertheless, many major financial firms focus on shifting their business model entirely or partially to the Blockchain [15]. We could expect many business models would change to Blockchain in the future

References

1. P. Krishna Karthik, R. Anand, "Energy Trading in Microgrids using BlockChain Technology", IEEE 2020.

2. A.Saranya, R.Naresh "Cloud Based Efficient Authentication for Mobile Payments using Key Distribution Method", Journal of Ambient Intelligence and Humanized Computing, Springer, 02 January, 2021. DOI: 10.1007/s12652-020-02765-7

3. R.Naresh, P.Vijayakumar, L. Jegatha Deborah, R. Sivakumar, "A Novel Trust Model for Secure Group Communication in Distributed Computing", Special Issue for Security and Privacy in Cloud Computing, Journal of Organizational and End User Computing, IGI Global, Vol.32, No. 3, Septemer 2020, Pp. 1-14. DOI: 10.4018/JOEUC.2020070101

4. A.Saranya, R.Naresh "Efficient mobile security for E health care application in cloud for secure payment using key distribution", Neural Processing Letters, Springer, 2021, DOI: 10.1007/s11063-021-10482-1

5. R.Naresh, M.Sayeekumar, G.M.Karthick, P.Supraja, "Attribute-based hierarchical file encryption for efficient retrieval of files by DV index tree from cloud using crossover genetic algorithm",Soft Computing, Springer, Vol.23, No. 8, 2019, Pp. 2561-2574. Doi: https://doi.org/10.1007/s00500-019-03790-1

6. P.Vijayakumar, R.Naresh, L. Jegatha Deborah, SK Hafizul Islam, "An efficient group key agreement protocol for secure P2P communication", Security and Communication Networks, Wiley, Vol.9, No.17, pp.3952–3965, 2016. http://onlinelibrary.wiley.com/doi/10.1002/sec.1578/abstract

7. P.Vijayakumar, R.Naresh, SK Hafizul Islam, L. Jegatha Deborah "An Effective Key Distribution for Secure Internet Pay-TV using Access Key Hierarchies", Security and Communication Networks, Wiley, Vol.9, No.18, pp.5085–5097, 2016. http://onlinelibrary.wiley.com/doi/10.1002/sec.1578/full

8. R. Naresh, M Meenakshi, G Niranjana, "Efficient study of Smart Garbage Collection for Ecofriendly Environment", Journal of Green Engineering, Vol.10, No.1, pp.1-10, Feb 2020.

9. R Divya Mounika, R.Naresh, "The concept of Privacy and Standardization of Microservice Architectures in cloud computing", European Journal of Molecular & Clinical Medicine, Vol 7, No 2, Pages 5349-5370, Dec 2020.

10. R.Naresh, AyonGupta, Sanghamitra, "MALICIOUS URL DETECTION SYSTEM USING COMBINED SVM AND LOGISTIC REGRESSION MODEL", International Journal of Advanced Research in Engineering and Technology (IJARET), Vol.10, No.4, pp. 63-73, May 2020.

11. Meenakshi, R Naresh, S Pradeep "Smart Home: Security and Acuteness in Automation of IOT Sensors", International Journal of Innovative Technology and Exploring Engineering

(IJITEE), Vol. 9, No. 1 , pp. 3271- 3274 , Nov 2019.

12. Younis, S.B., Naresh, R. "Opinion mining on web-based communities using optimised clustering algorithms", Turkish Journal of Computer and Mathematics Education, Vol. 12, No.9, pp. 438–447, 2021

13. Mounika, R.D., Naresh, R. "A benchmarking application on workload and performance forecasting of micro services" , Turkish Journal of Computer and Mathematics Education, Vol. 12, No.2, pp. 3232–3238, 2021

14. Nizamuddin Ariffin, Ahmad Zuhairi Ismail, "The Design and Implementation of Trade Finance Application based on Hyperledger Fabric Permissioned Blockchain Platform", ISRITI 2019.

15. Yu Wanjun, Wu Yuan, "Research on Network Trading System Using Blockchain Technology", ICIIBMS 2018.

16. Nakamoto S.Bitcoin: A peer-to-peer electronic cash system.WhitePaper,2008.

17. E. Kosba, A. Miller, E. Shi, Z. Wen, and C. Papamanthou. Hawk: The blockchain model of cryptography and privacy-preserving smart contracts. In 37th IEEE Symposium on Security & Privacy, 2016.

18. "Efficient Registration of Land using BlockChain Technology", International Journal of Recent Technology and Engineering, 2019.

19. Sheikh, V. Kamuni, A. Urooj, S. Wagh, N. Singh, Dhiren Patel. "Secured Energy Trading Using Byzantine-Based Blockchain Consensus", IEEE Access, 2020.

20. Han Wei, Liu Yamin. Research on Consensus Mechanism in Blockchain Technology[J]. Information Network Security, 2017(9):147-152.

21. Androulaki E.Barger, Bortnikov on Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains[J].2018.

22. K. Venkatesh, S. Parthiban, P. Santhosh Kumar, C.N.S. Vinoth Kumar, "IoT based Unified approach for Women safety alert using GSM", Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV 2021), IEEE Xplore Part Number: CFP21ONG-ART; 978-0-7381-1183-4, pp.no. 388-392, 978-1-6654-1960-4/21/$31.00 © April 2021 IEEE

23. R Ramasamy, V Rajavel, M Vasim Babu, C.N.S Vinoth Kumar, S Parthiban, "Design and Analysis of Multiband Bloom Shaped Patch Antenna for IoT Applications", Turkish Journal of Computer and Mathematics Education (TURCOMAT), Vol.12 Issue No.3, 4578-4585, April 2021.

24. Seethal Sasikumar, Abhay K S, C.N.S.Vinoth kumar," Network Intrusion Detection and Deduce System", Turkish Journal of Computer and Mathematics Education (TURCOMAT), Vol.12, Issue No.9, 404 – 410, April 2021.

25. Rupesh Kumar, Shreyas Parakh, C.N.S.Vinoth kumar, " Detection of Cyberbullying using Machine Learning", Turkish Journal of Computer and Mathematics Education (TURCOMAT), Vol.12, Issue No.9, 656 – 661, April 2021.

26. Raghav Rathi, Nishant Balyan, C.N.S Vinoth Kumar," Pneumonia Detection Using Chest X-Ray", International Journal of Pharmaceutical Research (IJPR), Volume 12, issue 3, ISSN: 0975-2366 July - Sept, 2020

27. Praharsha Sarma, Utkarsh Kumar, C.N.S. Vinoth Kumar, M.Vasim Babu, "Accident Detection And Prevention Using Iot & Python Opencv", International Journal Of Scientific & Technology Research(IJSTR), Volume 9, Issue 04,pp no. 2677-2681, ISSN No: 2277-8616 April 2020.

28. Gautam Srivastava, C.N.S. Vinoth Kumar, V Kavitha, N Parthiban, Revathi Venkataraman, "Two-Stage Data Encryption using Chaotic Neural Networks", Journal of Intelligent and Fuzzy systems, Vol. no.38, Issue. No.3, pp no.2561-2568, ISSN No: 1875-8967. March 2020

29. M.Vasim Babu, C.N.S. Vinoth Kumar, M.Venu, International journal entitled "Improvisation of localization accuracy using ERSSI based on ADV-HOP algorithm in wireless sensor network", International journal of innovative technology and exploring engineering (IJITEE), ISSN No.2278-3075 Feb 2019.

30. C.N.S. Vinoth Kumar, A.Suhasini, "Secured Three-Tier Architecture for Wireless Sensor Networks Using Chaotic Neural Networks", 'Advances in Intelligent Systems and Computing' AISC Series, Springer Science + Business Media Singapore 2017 Vol. No. 507, Chapter No. 13, pp. No. 129-136, ISSN 2194-5357, DOI 10.1007/978-981-10-2471-9_13