International Journal of Scientific Research in Science and Technology
Print ISSN: 2395-6011 | Online ISSN: 2395-602X (www.ijsrst.com)
doi : https://doi.org/10.32628/IJSRST229441

Blockchain and Inter Planetary File System based Secured KYC Document Verification for Banking System

Sowmya B. K.[1], Manikandan H[2], Naveen Kumar A[2], Nagaraj Adibatti[2], Pradeep Kumar V[2]

[1]Assistant Professor, Department of Computer Science and Engineering, AMC Engineering College, Bannerghatta Main Road, Bangalore, Karnataka, India

[2]Department of Computer Science and Engineering, AMC Engineering College, Bannerghatta Main Road, Bangalore, Karnataka, India

Article Info
Volume 9, Issue 4
Page Number : 248-259

Publication Issue
July-August 2022

Article History
Accepted : 05 July 2022
Published : 20 July 2022

ABSTRACT

Know your client (KYC) is a requirement for the banking system to validate a customer using identity, appropriateness, and risk assessment in establishing a banking relationship. With the developed concern for security, the KYC process is complex and involves a high cost for completing for a single customer. In this paper, we propose a reasonable, abrupt, secure, and transparent platform for KYC document verification for the Banking system through Inter Planetary File System (IPFS) and blockchain technology. The proposed system allows a customer to open an account at any Bank, complete the KYC process there, generate a hash value using the IPFS network and share it with other banks using the blockchain technique. Using a private key, any Bank/financial organization can retrieve, and store customer data (i.e., KYC) securely using the IPFS network if the customer wants to open another account in that Bank/financial organization. The proposed system can avoid repetitive work and save time, and money during the KYC process when someone tries to open an account at multiple Banks. In this paper, we have focused on how the present banking industry, especially the KYC document verification process, can be impacted after using blockchain to store and track the records.

Keywords : Blockchain, KYC, Interplanetary File System, Security

I. INTRODUCTION

Digital technologies have transformed media content production and distribution in the global entertainment and media industry over the last two decades. Many challenges still remain, though, especially relating to the way in which digital content can be distributed on the Internet, and how content contributors are compensated when their materials are used or bought through legitimate channels. One of the latest experiments in this specific industry involves the use of blockchains and cryptocurrencies for micropayments— payments by consumers of very small sums of money to access specific content.

Blockchain technology and cryptocurrencies can provide an ideal, cost-effective framework for payments, preserving privacy, with low commission fees and instant financial transactions without intermediaries. Blockchain technology become famous due to the introduction of blockbuster cryptocurrencies like BitCoin and Ethereum, which are still the individual applications of blockchains at scale. As the interest of the financial services industry increased in Both Bitcoin and Ethereum, this gave rise to the introduction of additional cryptocurrencies (AltCoins) such as LightCoin, PrimeCoin, NameCoin. Thus, it leads to the emergence of an entirely new concept for funding innovative ideas and products, namely the Initial Coin Offering (ICO) mechanism. Over the last few years, there has been a surge of interest in other applications of blockchains beyond cryptocurrencies, mainly applications that attempt to exploit the decentralized characterisitic and security, transparency and anti-tampering properties of distributed ledger technologies (DLT). Many applications take advantage of these properties in the scope of permissioned blockchain infrastructures, which offer strong authentication and authorization, while at the same time it removes the need for complex and time-consuming Proof-of-Work (PoW) processes. The main thing is a key to supporting applications that need to support faster transaction completion than what is supported by conventional public blockchains such as BitCoin and Ethereum.

This leads to the emergence of platforms that support permissioned blockchains such as R3/Corda and Hyperledger Fabric, which support hundreds of transactions per second (TPS).

Many financial sectors dismiss several long-lasting important issues by enabling the use of blockchain technologies. One of the major problems associated with bank credit is the lack of information regarding credit scores, which causes difficulties for individuals and SMEs to obtain loans from financial institutions. Due to a lack of proper and clear information financial institutions are unable to conduct accurate customer profiling such that they can efficiently conduct product differentiation and personalization. Even insurance products offered by the financial sector enclose a complex insurance claims process, which requires the involvement of numerous stakeholders before the finalization and payment of a claim. Thus, the primary targets for cyber attacks are the existing infrastructures that facilitate the majority of the transactions of financial organizations.

All financial sectors started KYC and KYB processes whenever they onboard a customer.

In the above process, the customer is identified and verified against applicable laws and rules set by regulators at the national and international levels (e.g., Central Banks, Banking Associations, Securities and Futures Commissions). Also, an original profile for the retail or commercial customer is offered, as means of personalizing service offerings. As KYC/KYB process is dynamic both customer information and applicable regulations need to be evolved over time, which makes the process quite challenging. Moreover, customers are requested to provide a batch of documents each time they are onboarded by a financial sector. To reduce this demand customer documentation can be centralized with authority. In this way, a solution is exposed to cyber-attacks and data breaches.

The Know your customer (KYC) is a very popular term in the banking and financial sector. For better results now it's necessary to automate the KYC verification process. Thus Blockchain technology recently draws the attention of the public, as a dispute that leads to the foundation that the trust-free economical transaction is possible with its distinctive method.

The blockchain allows unknown and assured transactions of digital currencies (such as Bitcoin, Litecoin, etc) and preserves the metadata regarding the transaction details in a database. The cryptography techniques are used to secure the database and to block the alteration in the transaction history. The banks or financial sector require diverse policies and multi-steps processing between parties. It also requires secure transactions and short processing/settlement time. To facilitate these concerns, the researcher has proposed a blockchain-based distributed platform and a decentralized framework that allows sharing and integration of all distributed actors for financial transaction processing in the insurance industry. This will help the industry to analyze the spread and plan further development.

Ever since Satoshi Nakamoto exited the scene and two-handed over Bitcoin development to different core developers, the digital ledger technology has evolved leading to new applications that structure the blockchain History planned an e-transaction system of the coin created exploitation digital signatures. The system is in a position to trace the history of the dealings, and it will stop double payment drawbacks. Since then, researchers are attempting to search out the potential sectors to use the Blockchain. notwithstanding, sharing transaction info over bitcoin is pricey. Currently, miners square measure charging around $7 per one hundred K of knowledge.

Blockchain networks will be more expensive, so they cannot be used to upload KYC documents. So as an alternative solution, KYC documents are shared using the InterPlanetary File System (IPFS) and then documents are shared over the Blockchain network. Thus, IPFS is a shared distributed document framework that associate all registering computing devices with a similar system of files. By the use of IPFS users can store their transaction history and hash to the IPFS network, and then stare it to the This process will reduce the blockchain data size significantly.

II. Literature Survey

Blockchains are recognized as distributed systems to store data. The irreversibility and transparency properties of blockchain are unsuitable for personal data. For the sake of data privacy, data stored in the blockchain cannot be changed, which means that the personal data they contain cannot be removed, so the blockchain is designed in order to protect users' privacy. One method to use blockchain is to provide a timestamp for information held elsewhere. If any content needs to be removed from a public source, the fact that the content existed at a given point would still remain in the blockchain but the stored hash would now point to other content that has been changed or simply removed. This approach of using blockchains purely as a time-stamping mechanism has more benefits of scaling a large amount of data to be recorded. Thus, additional encryption of data is possible in blockchain before it is pushed. The major problem with this method is that the decryption key is made public, for the encrypted data and the encrypted content is readable by anyone with that key; and the data cannot be encrypted with a different key once it is embedded within the blockchain. Every blockchain contains transaction data and all privacy by design principles have to be taken into consideration before letting any transaction into the ledgers of public/private blockchain implementations.

The technology behind blockchain has significantly evolved 0since it was originally proposed as an accounting method for Bitcoin cryptocurrency Naughton suggests that blockchain technology could be "the most important IT invention of our age", while Mougayar says that it is "at the same level as the World Wide Web in terms of importance". The main step for the course of blockchain technology was the

development of the Ethereum project, which gives new solutions by Implementation and executing the smart contract. It is a tool and protocol for the creation and operation of decentralized (DApps)," applications that run exactly as programmed without any possibility of fraud or third-party interference". It also supports a contract-oriented, high-level, Turing-complete programming language, allowing anyone to write smart contracts and create DApps.

Nowadays after realizing that the potential goes beyond cryptocurrencies, research has been conducted. Blockchain technology and smart contracts have applications in different domains. Smart contracts are (mainly) written in the programming language in Ethereum Solidity and numerous distributed applications (DApps) have been proposed in research works such as for the government sector, funding mechanisms, and many more.

By blending Blockchain with the Internet many distributed applications have been introduced, Decentralized applications have been proposed based on blockchain technology for sharing Internet of Things (IoT) sensors' data. Papadodimas et al. gave a platform for sharing (buying and selling) measurements of IoT weather sensors operating on the Ethereum blockchain, acting as a marketplace for IoT sensor data, exploiting the Sensing-as-a-Service (S2aaS) business model, which blends blockchain and IoT for monetization and extracting value from IoT data.

Over the last few years, many digital cryptocurrencies have also been introduced, as also presented on a technical survey on digital cryptocurrencies and smart contracts implementing value tokens as well. The use of different smart contracts in the media industry, by combining blockchain, web technologies and user-generated multimedia content, allowing direct monetization for the content creator, is examined. Every day a huge number of transactions take place in financial banking sectors. In July 2019 the Society for Worldwide Interbank Financial Telecommunication (SWIFT) recorded an average of approximately 32 million transactions per day. Blockchain can enable parties to exchange digital data with no particular trust on a peer-to-peer basis with fewer or no third parties. Blockchain based identity management and authentication frameworks are proposed for recognizing the decentralized ownership credentials and offers universally available protocol for verifying one's record in an immutable chain of data. Mikula et al. proposed an authorization and authentication proof-of-concept system for identity managements, where an immutable and auditable history is desired for data concerning patients. Widick et al.presented a blockchain-based authentication and authorization framework to control access to the resources of an IoT device, while Mudliar et al. examine the integration of identity with blockchain technology.

The KYC verification process is an integral part of regulation for the financial industry. The KYC process is started when a client wants a financial transaction with a financial institution.

Arasa et al. direct an investigation of the expense of KYC dependent on the complexity level of the compliance required for the instance of business banks in Kenya, building up to four variables that clarify 78.3% of the consistence necessities. The data in ound us is increasing day by day, including the KYC documents. Soni and Duggal proposed a solution using big data analytic techniques to solve the big data problem of KYC focused on Indian banks. Y. Lootsma et al. proposed to implement the Regtech (regulatory technology) like Blockchain in the banking sector to reduce the burden of the KYC process for a financial institution as well as the regulatory institution. Using the approach tax reporting can also be done. However, they did not show the full implementation of Blockchain and the cost involved with the process.

When a client wants to do the financial transaction through a payment provider, they will check the customer identity by his name from Bank if the provided information is correct through Blockchain smart contract . The author provided an assumption on using the blockchain to make the identity and financial transaction through blockchain, though they did not provide any use case for document sharing like KYC docs. A typical KYC framework could be that a client goes to a bank, the bank performs KYC, stores KYC in the Blockchain, give a customer a token and then customer give access to another bank to check the KYC information. The other bank then crosschecks the information from Blockchain. Because of a range of configuration parameters, the blockchain is somewhat uncontrollable. For example, testnets like Rinkby, Ethereum cannot be adjusted easily because of their parameters like Gas limit, Mining difficulty and so on. Authors suggested using Grid'5000, as they found it highly controllable and reconñgurable testbed. Again, the authors did not provide a practical use case scenario with cost calculation. J. Parra Moyano et al. has shown the design of centralized and decentralized Blockchain KYC solution with the division of processing cost among different banks. To minimize the cost of core KYC verification and improve the customer experience, they proposed a new scheme based on distributed ledger technology (DLT). They Focused on four main points. The first is proportionality: the cost will be shared proportionally by all the institutions involved with a partic- ular KYC verification process. They focused on Irrelevance secondly. The one who avoids the KYC process will not get any incentive. The third point of focus was Privacy. The KYC verification process has to be secured so that user privacy is not violated. Finally, they focused on No-minting. As the process is online-based, they need to focus that no false can be made during KYC verification. Whenever someone tries to edit any portion of KYC data, that editing process will automatically be void from the authoritative side.

III. Problem Statements

The progressive cost of the KYC process is planned to reduce by tackling the cost problem of KYC from a financial institution perspective by using blockchain. Currently, many third-party data providers and external validation agencies offer data and interfaces to extract the required customer information. But, banks struggle to integrate this data to obtain a consolidated view of the customers. This increases instances of banks' failure to comply with regulatory requirements, resulting in huge penalties and reputational damage. Thus, before investigation banks need to digitize data in the documents to feed it into the repositories. This is an immoderate exercise, as it uses advanced technology platforms.

The KYC aspect is regularly facing new rules and regulations across different aspects. therefore, utilities need to update their guidelines. This led to increasing the need for banks to improve their data collection mechanisms for effective risk management and timely compliance. Banks do not have a centralized or single unified KYC system for their various lines of business-like wealth management, asset management, and brokerage. Hence, maintaining these multiple systems and integrating different interfaces puts banks under immense pressure and adds costs. This paper solves the problem based on three assumptions: First, all the financial institutions in the same country and therefore obliged to respect the same KYC regulations and agree on the standards for granting core KYC verification to a customer. Second, all the financial institutions cooperating with the system agree on the average costs of conducting a core KYC verification process. This cost may depend on the complexity of each individual customer, based on predetermined parameters. Third, the national regulator keeps the system and approves financial institutions to work with the system in order to conduct a more efficient and transparent KYC verification process. These three

assumptions are necessary to ensure a correct structure across the participating financial institutions.

IV. Objectives

When customers approach two different banks they have to go through with following stages. In the first stage, the customer went to Bank A to provide the Bank with his KYC document for verification. Bank A goes through our proposed system design and provides the customer with a hash value and if the hash value of the sending bank matches the hash value of the customer. Then Bank A will send the customer document to both Bank B and Bank C thus both banks will testify the KYC doc in a blink. Banks used the IPFS network to upload and retrieve KYC docs at the banks end. Nevertheless, before sharing out KYC docs into the IPFS network, we considered encrypting the file for extra security and reducing file size. So anyone can access the KYC docs from the IPFS network by just knowing their hash values.

4.1 Requirement Analysis

This project will analyze the design of many applications to make the application more users friendly.TO do user-friendly it's important to navigate in good order from one screen to the other and at the same time reduce the amount of typing the user needs to do. The application will be more accessible if the browser version is chosen so that it is compatible with most of the Browsers.

V. Proposed Methodology

Figure 1 shows an illustration of the process that occurs when one customer has to work with three different financial institutions. It can be clearly observed from the diagram that the same process is recurred three times. Also the total verification costs are generated thrice, though the core process is in reality, the same. It is important to note here that the "core" process means the minimum KYC verification that all financial institutes are obliged by law to conduct

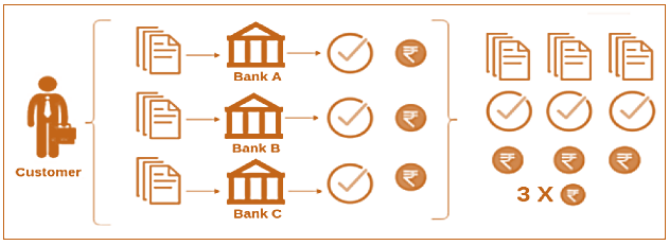

Figure 1. Current KYC Verification Process

Blockchain: is a purely peer-to-peer version online transaction, where a customer directly sends money to others without the help of a financial organization. All transactions will be hashed to an ongoing proof-of-work chain. Each of this called a block; the running block contains the hash of previous all blocks. Therefore, the whole process is tempered proof, as a single peer cannot add a new block without the proof-of-work . Bitcoin was the first fully decentralized cryptocurrency. While the central purpose of DLT was to create digital money and sending and receiving via the Internet, the technology can also be used to authenticate online document sharing using smart contracts. The smartcontract aims to involve them in properties, which are expensive and controlled in a digital manner.

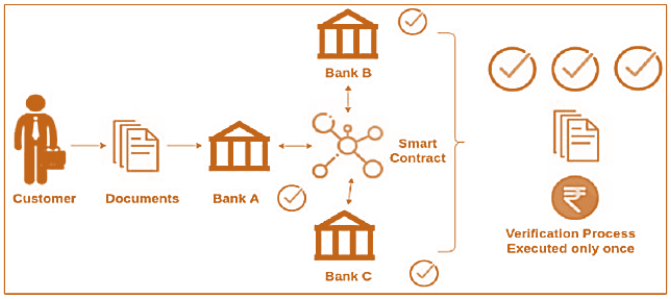

Figure 2. KYC Verification Process after implementation of blockchain

The Interplanetary File System is a peer-to-peer hypermedia protocol, which connects computing devices for sharing/storing files/data. The content in the file is distinctively recognized in the global namespace using the hash code of the file. If the hash

code differs, the data can not be verified which will be identified by IPFS. Besides, IPFS identifies duplication if files with the same content are stored.

5.1 KYC Verification

We considered a scenario in which, a customer wants to open an account in bank A. The customer submitted the account information along with KYC docs to the Bank. The bank then observed the whole information, and if it is found correct, will encrypt information using the system's application l which is available to all banks to share documents with other banks and store a copy in a local database. Afterward, the encryption file will be stored in the private IPFS network by bank A. Later, the bank will upload the hash value from IPFS, a very small in-memory size, to the Blockchain network. Bank A also keeps a copy of the customer's KYC docs to the local database of it.

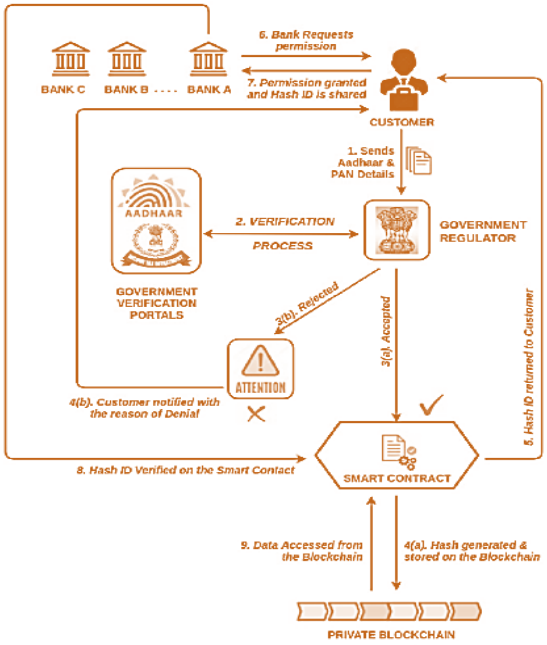

Figure 3. Workflow of the Proposed System

Finally, Bank A will share the hash value of Blockchain and IPFS to the customer. Later on, the customer can give access to the KYC doc package by just sharing the hash value to any other institution he intended to work with. However, now the customer can go to another bank to open another account. The customer will share his hash value from IPFS, and Blockchain to Bank B. Since Bank B will be granted access to the hash value of the document package by the customer, the Bank will get access to the Blockchain network for the required hash value. Subsequently, the bank will download the encrypted KYC docs from the IPFS network using the hash value retrieved from Blockchain. Lastly, with the help of the private key of the customer, the Bank will retrieve the KYC docs and keeps a copy of KYC docs to the bank's local database. The regulatory bank defined in the proposed solution in the central bank.

VI. Conclusion

This paper has suggested a distributed ledger technology based architecture which attempts to minimize the total KYC costs for banks working together in a jurisdiction. With this, the major advantage achieved is the avoidance of redundant tasks by different financial institutions. This paper also gives a solution for the distribution of proportionally divided costs incurred for that group of financial institutions which are working with the same customer.

VII. REFERENCES

[1]. F. Glaser, "Pervasive Decentralisation of Digital Infrastructures: A Framework for Blockchain Enabled System and Use Case Analysis," Social Science Research Network, Rochester, NY, SSRN Scholarly Paper ID 3052165, Jan. 2017.

[2]. A. Rahman, S. Roy, M. S. Kaiser, and M. S. Islam, "A lightweight multi-tier s-mqtt framework to secure communication between low-end ioi nodes," in 2016 5th International Conference

[3]. M. Raikwar, S. Mazumdar, S. Ruj, S. Sengupta, A. Chattopadhyay, and K.-Y. Lain, "A Blockchain Framework for Insurance Processes." 20/h 9tñ HIP Ititernutionul

Conference on New Tec hnc›lc›gies, Mobility und Security (NTMS), 2018.

[4]. D. Puthal, N. Malik, S. Mohanty, E. Kougianos, and C. Yang, "The Blockchain as a Decentralized Security Framework [Future Directions]," IEEE Consumer Electronics Magazine, scd. 7, pp. 18—21, 2018.

[5]. Rahman, M. A. Rahman, A. Shabut, S. AlMamun, and A. Hussain, "A Brain-Inspired Trust Management Model to Assure Security in a Cloud Based IoT Framework for Neuroscience Applications," Cognitive C‹›myututi‹›n, vol. 10, no. 5, pp. b64— b73, Oct. 201 b. [Online]. Available: [6] l4tt|as://cloi .t / 1 IL I 007/S 1 25 I "9- 0 I S- °)fi43-3 S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2010, library Catalog' bitcoin.org. Online].

[6]. D. Tonin, "Money Button CEO: How to upload large hles to Bitcoin SV blockchain," Mar. 2019, library Catalog: coingeek.com Section: Tech. [Online].

[7]. M. Irvine an‹l D. King, "The Money Laundering Control Act of 19b6: Tainted Money and the Criminal Defense Lawyer," McGeorpe Law' Review, vol. 19, no. 1, pp. 171—192, Jan. 1987. [Online].

[8]. Kapoor, S. AltCoins: Cryptocurrencies beyond BitCoin. Available online: https://www.itexchangeweb.com/blog/altcoi ns-cryptocurrencies-beyond-bitcoin/ (accessed on 30 July 2019).

[9]. Guo, Y.; Liang, C. Blockchain application and outlook in the banking industry. Financial Innovation 2016, 2, 24.

[10]. Rosati, P.; Cuk, T. Blockchain Beyond Cryptocurrencies: FinTech and Strategy in the 21st Century. In Disrupting Finance, Lynn, T., Mooney, J.G., Rosati, P., Cummins, M. (Eds.), pp.149-170, 2016.

[11]. Divya. R and Dr.R. Chinnaiyan, "Reliable Constrained Application Protocol to Sense and Avoid attacks in WSN for IoT Devices," 2019 International Conference on Communication and Electronics Systems (ICCES), Coimbatore, India, 2019, pp. 1898-1901

[12]. Dr.R.Chinnaiyan , M.S.Nidhya (2018), " Reliability Evaluation of Wireless Sensor Networks using EERN Algorithm" , Lecture Notes on Data Engineering and Communications Technologies, Springer International conference on Computer Networks and Inventive Communication Technologies (ICCNCT - 2018), August 2018 (Online)

[13]. Dr.R.Chinnaiyan , R.Divya (2018), " Reliable AI Based Smart Sensors for Managing Irrigation Resources in Agriculture" , Lecture Notes on Data Engineering and Communications Technologies, Springer International conference on Computer Networks and Inventive Communication Technologies (ICCNCT - 2018), August 2018 (Online)

[14]. Dr.R.Chinnaiyan , S.Balachandar (2018) , " Reliable Digital Twin for Connected Footballer" , Lecture Notes on Data Engineering and Communications Technologies, Springer International conference on Computer Networks and Inventive Communication Technologies (ICCNCT - 2018), August 2018 (Online)

[15]. Dr.R.Chinnaiyan , S.Balachandar (2018) , " Centralized Reliability and Security Management of Data in Internet of Things (IoT) with Rule Builder" , Lecture Notes on Data Engineering and Communications Technologies, Springer International conference on Computer Networks and Inventive Communication Technologies (ICCNCT - 2018), August 2018 (Online)

[16]. Dr.R.Chinnaiyan, Abishek Kumar (2017) " Reliability Assessment of Component Based Software Systems using Basis Path Testing" , IEEE International Conference on Intelligent

Computing and Control Systems, ICICCS 2017, 512 – 517

[17]. Dr.R.Chinnaiyan, Abishek Kumar(2017) ,"Construction of Estimated Level Based Balanced Binary Search Tree", 2017 IEEE International Conference on Electronics,Communication, and Aerospace Technology (ICECA 2017), 344 - 348, 978-1-5090-5686-6.

[18]. Dr.R.Chinnaiyan, Abishek Kumar(2017), Estimation of Optimal Path in Wireless Sensor Networks based on Adjancy List, 2017 IEEE International Conference on Telecommunication,Power Analysis and Computing Techniques (ICTPACT2017) ,6,7,8th April 2017,IEEE 978-1-5090-3381-2.

[19]. Dr.R.Chinnaiyan, R.Divya (2017)," Reliability Evaluation of Wireless Sensor Networks", IEEE International Conference on Intelligent Computing and Control Systems, ICICCS 2017, 847 – 852

[20]. Dr.R.Chinnaiyan, Sabarmathi.G (2017)," Investigations on Big Data Features , Research Challenges and Applications", IEEE International Conference on Intelligent Computing and Control Systems, ICICCS 2017, 782 – 786

[21]. Dr.S.Nirmala ,R.Chinnaiyan et.al. (2021). Blockchain based Secured Framework for Road Traffic Management using Fog Computing . International Journal of Computational Intelligence in Control 13(2)

[22]. G. Sabarmathi and Dr.R. Chinnaiyan, "Reliable Machine Learning Approach to Predict Patient Satisfaction for Optimal Decision Making and Quality Health Care," 2019 International Conference on Communication and Electronics Systems (ICCES), Coimbatore, India, 2019, pp. 1489-1493.

[23]. G. Sabarmathi and Dr.R. Chinnaiyan, "Big Data Analytics Framework for Opinion Mining of Patient Health Care Experience" International Conference on Computing Methodologies and Communication (ICCMC 2020), IEEE Xplore Digital Library

[24]. G. Sabarmathi and R. Chinnaiyan, "Reliable feature selection model for evaluating patient home health care services opinion mining systems," 2021 International Conference on Advancements in Electrical, Electronics, Communication, Computing and Automation (ICAECA), 2021, pp. 1-4, doi: 10.1109/ICAECA52838.2021.9675485.

[25]. G.Sabarmathi , Dr.R.Chinnaiyan (2018), "Envisagation and Analysis of Mosquito Borne Fevers – A Health Monitoring System by Envisagative Computing using Big Data Analytics" in ICCBI 2018 – Springer on 19.12.2018 to 20.12.2018 (Recommended for Scopus Indexed Publication IEEE Xplore digital library)

[26]. G.Sabarmathi , Dr.R.Chinnaiyan, Reliable Data Mining Tasks and Techniques for Industrial Applications, IAETSD JOURNAL FOR ADVANCED RESEARCH IN APPLIED SCIENCES, VOLUME 4, ISSUE 7, DEC/2017,PP- 138-142, ISSN NO: 2394-8442

[27]. G.Sabarmathi, Dr.R.Chinnaiyan "Mining Patient Health Care Service Opinions for Hospital Recommendations" International Journal of Engineering Trends and Technology 69.9(2021):161-167

[28]. Hari Pranav A; M. Latha; Ashwin. M. S; R. Chinnaiyan, "BlockchainAs a Service (BaaS) Framework for Government Funded Projects e-Tendering Process Administration and Quality Assurance using Smart Contracts," 2021 International Conference on Computer Communication and Informatics (ICCCI), 2021, pp. 1-4, doi: 10.1109/ICCCI50826.2021.9402348.

[29]. Hari Pranav A;M. Senthilmurugan;Pradyumna Rahul K;R. Chinnaiyan , "IoT and Machine Learning based Peer to Peer Platform for Crop Growth and Disease Monitoring System using

Blockchain," 2021 International Conference on Computer Communication and Informatics (ICCCI), 2021, pp. 1-5, doi: 10.1109/ICCCI50826.2021.9402435.

[30]. M. Latha, M. Senthilmurugan and R. Chinnaiyan, "Brain Tumor Detection and Classification using Convolution Neural Network Models," 2021 International Conference on Advancements in Electrical, Electronics, Communication, Computing and Automation (ICAECA), 2021, pp. 1-5, doi: 10.1109/ICAECA52838.2021.9675585.

[31]. M. Senthilmurugan, M. Latha and R. Chinnaiyan, "Analysis and Prediction of Tuberculosis using Machine Learning Classifiers," 2021 International Conference on Advancements in Electrical, Electronics, Communication, Computing and Automation (ICAECA), 2021, pp. 1-4, doi: 10.1109/ICAECA52838.2021.9675482.

[32]. M. Swarnamugi & R. Chinnaiyan (2021). CNN based Vehicle Classification for Intelligent Transportation System in Unstructured Environments. International Journal of Computational

[33]. Intelligence in Control 13(2)

[34]. M. Swarnamugi & R. Chinnaiyan (2021). CNN based Single-level and Multi-level Vehicle Classification Framework in Intelligent Transportation System. International Journal of Computational Intelligence in Control 13(2)

[35]. M.S.Nidhya and R.Chinnaiyan, Shortest Reliable path for Wireless Sensor Network, International Journal of Pure and Applied Mathematics, Volume 117 No. 20 2017, 105-109, ISSN: 1311-8080 (printed version); ISSN: 1314-3395 (on-line version).

[36]. M.S.Nidhya, Dr.R.Chinnaiyan (2017), Conniving Energy and Time Delay Factor to model Reliability for Wireless Sensor Networks , 2016 IEEE International Conference on Advances in Computer Applications (ICACA) , 978-1-5090-3770-4/16/$31.00©2016 IEEE, pp 213-216.

[37]. M.Swarnamugi , Dr.R.Chinnaiyan(2019) , Smart and Reliable Transport System based on Message Queing Telemetry Transport Protocol, ICICCS 2019 , 15-17 May 2019, Madurai. (Recommended for Publication Scopus indexed IEEE Xplore digital library)

[38]. Manoj Challa , Dr.R.Chinnaiyan (2019) "Optimized Machine Learning Approach for the Prediction Of Diabetes-Mellitus (Recommended for Scopus Indexed Publication in Springer - Advances in Intelligent Systems and Computing Series)

[39]. Preetika B, ; M. Latha; M. Senthilmurugan; R. Chinnaiyan, , "MRI Image based Brain Tumour Segmentation using Machine Learning Classifiers," 2021 International Conference on Computer Communication and Informatics (ICCCI), 2021, pp. 1-9, doi: 10.1109/ICCCI50826.2021.9402508

[40]. Preetika B; R. Chinnaiyan, "An Open Source Distributed Virtualization for Enterprise Infrastructure using OVIRT," 2021 International Conference on Computer Communication and Informatics (ICCCI), 2021, pp. 1-5, doi: 10.1109/ICCCI50826.2021.9402547.

[41]. R. Chinnaiyan and D. Stalin Alex, "Early Analysis and Prediction of Fetal Abnormalities Using Machine Learning Classifiers," 2021 2nd International Conference on Smart Electronics and Communication (ICOSEC), 2021, pp. 1764-1767, doi: 10.1109/ICOSEC51865.2021.9591828.

[42]. R. Chinnaiyan and S. Alex, "Machine Learning Approaches for Early Diagnosis and Prediction of Fetal Abnormalities," 2021 International Conference on Computer Communication and Informatics (ICCCI), 2021, pp. 1-3, doi: 10.1109/ICCCI50826.2021.9402317.

[43]. R. Chinnaiyan et.al., "Smart Vehicle Tracking System Using Internet of Things", International Journal of Scientific Research in Science and

Technology (IJSRST), Online ISSN : 2395-602X, Print ISSN : 2395-6011, Volume 9 Issue 2, pp. 351-355, March-April 2022.

[44]. R. Chinnaiyan, M. Shashwat, S. Shashank and P. Hemanth, "Convolutional Neural Network Model based Analysis and Prediction of Oral Cancer," 2021 International Conference on Advancements in Electrical, Electronics, Communication, Computing and Automation (ICAECA), 2021, pp. 1-4, doi: 10.1109/ICAECA52838.2021.9675533.

[45]. R.Chinnaiyan et.al, " Intelligent Hospital Monitoring System using Internet of

[46]. Things"International Journal of All Research Education and Scientific Methods (IJARESM), ISSN: 2455-6211 Volume 10, Issue 4, April-2022, Impact Factor: 7.429

[47]. R.Chinnaiyan, Dr.Stalin Alex (2021). Optimized Machine Learning Classifier for EarlyPrediction of Fetal Abnormalities . International Journal of ComputationalIntelligence in Control 13(2)

[48]. R.Divya , Dr.R.Chinnaiyan (2018) "Reliable AI Based Small Sensors for Managing Irrigation Resources in Agriculture – a review, International Conference on Computer Networks and Communication Technologies. Lecture Notes on Data Engineering and Communications Technologies, Vol 15. Springer, Singapore, 978-981-10-8681-6, September 2018

[49]. R.Divya , Dr.R.Chinnaiyan (2019) ,"Reliable Constrained Application Protocol to sense and avoid attacks in WSN for IoT Devices (Recommended for Scopus Indexed Publication IEEE Xplore digital library)

[50]. Reliable Machine Learning Approach to Predict Patient Satisfaction for optimal Decision Making and Quality of Health Care on 17-19 July 2019, Coimbatore (Recommended for Scopus Indexed Publication IEEE Xplore digital library)

[51]. S. Balachandar , Dr.R.Chinnaiyan , A Reliable Troubleshooting Model for IoT Devices with Sensors and Voice Based Chatbot Application, International Journal for Research in Applied Science & Engineering Technology (IJRASET), Volume 6 Issue II, February 2018, PP.1406-1409 ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887

[52]. S.Balachandar, Dr. R.Chinnaiyan, A RELIABLE AGNOSTIC DATA COMPRESSION MODEL BETWEEN EDGE AND CLOUD IOT PLATFORM, International Journal of Computer Engineering and Applications, Volume XII, Issue I, Jan. 18,PP.139-143. ISSN 2321-3469

[53]. S.Balachandar, Dr.R.Chinnaiyan, "Reliable Admin Framework of Drones and IOT Sensors in Agriculture Farmstead using Blockchain & Smart Contracts " BDET 2020 @ NTU – SINGAPORE on 3-5 January 2020

[54]. S.Balachander , Dr.R.Chinnaiyan (2019)," Internet of Things based Agro based Monitoring using Drones with Block Chain , ICICCS 2019 , 15-17 May 2019, Madurai. (Recommended for Publication Scopus indexed IEEE Xplore digital library)

[55]. S.Balachander , Dr.R.Chinnaiyan(2018) , "Internet of Things based Reliable Real –Time Disease Monitoring of Poultry Farming Imagery Analytics" in ICCBI 2018 – Springer on 19.12.2018 to 20.12.2018 (Recommended for Scopus Indexed Publication IEEE Xplore digital library)

[56]. Sabarmathi . G and R.Chinnaiyan (2021). Sentiment Analysis for Evaluating the Patient Medicine Satisfaction. International Journal of Computational Intelligence in Control 13(2), pp.113-118.

[57]. Swarnamugi , Dr.R.Chinnaiyan (2019) Context-Aware Smart Reliable Service Model for Intelligent Transport System, ICRIC 2019, SCOPUS indexed , 8th 9th March 2019, Jammu & Kashmir.

[58]. Tilak, Dr.R.Chinnaiyan et.al , " IOT based Leaf Disease Detection and Fertilized Recommendation" International Journal of Innovative Technology and Exploring Engineering (IJITEE), Volume-9 Issue-2, December2019.

[59]. Vardhini B;Shreyas N Dass;Sahana R;R. Chinnaiyan, "A Blockchain based Electronic Medical Health Records Framework using Smart Contracts," 2021 International Conference on Computer Communication and Informatics (ICCCI), 2021, pp. 1-4, doi: 10.1109/ICCCI50826.2021.9402689.

[60]. Yamini, Dr.R.Chinnaiyan et.al, "Smart Crop Monitor using Internet of Things, Cloud, Machine Learning and Android App" International Journal of Engineering and Advanced Technology (IJEAT), Volume- 9 Issue-3, February, 2020.

Cite this article as :

Sowmya B. K., Manikandan H, Naveen Kumar A, Nagaraj Adibatti, Pradeep Kumar V, "Blockchain and Inter Planetary File System based Secured KYC Document Verification for Banking System", International Journal of Scientific Research in Science and Technology (IJSRST), Online ISSN : 2395-602X, Print ISSN : 2395-6011, Volume 9 Issue 4, pp. 248-259, July-August 2022. Available at doi : https://doi.org/10.32628/IJSRST229441
Journal URL : https://ijsrst.com/IJSRST229441