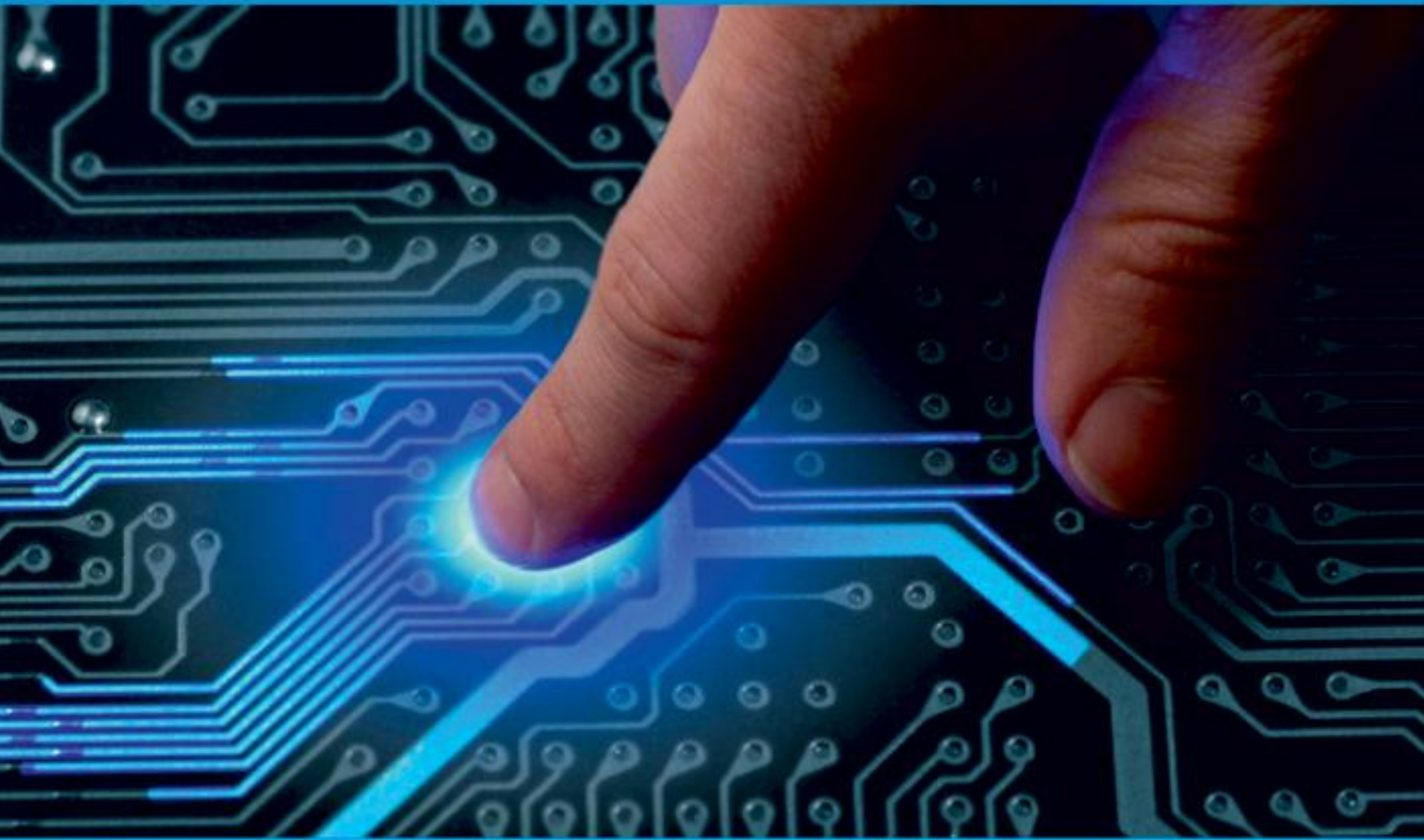
IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 9, Issue 7, July 2021

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.542

| DOI: 10.15680/IJIRCCE.2021.0907012 |

Online Document Generation using Blockchain Technology for P2PNetwork

Saber Nasir Take , Prof.Monika D. Rokade

[1]PG Student, Sharadchandra Pawar College of Engineering, Junnar, Pune, India

[2]Assistant Professor, Sharadchandra Pawar College of Engineering, Junnar, Pune, India

ABSTRACT: In order to solve the problem of forged certificates, the digital certificate system based on blockchain technology would be proposed. By the immutable property of blockchain, the digital certificate with anti-counterfeit and verifiability could be made. During the course of education, the students achieve many certificates. While applying for jobs students produce these certificates, where these are verified manually. There can be incidents where students may produce the fake certificate and it is difficult to identify them. This problem of fake academic certificates has been a longstanding issue in the academic community. It is possible to create such certificates at low cost and the process to verify them is very complex. This problem can be solved by generating the digital certificates on the blockchain. The blockchain technology provides immutability and publicly verifiable transactions. These properties of Blockchain can be used to generate the digital certificate which are anti-counterfeit and easy to verify. It is because the generated digital certificate cannot be edited or modified since it is generated through blockchain, which makes it unchangeable.

KEYWORDS: E-Certificates, Blockchain, Mining, Hyperledger, Digital Certificate, Hashing

I.INTRODUCTION

Blockchain technology is used to reduce the incidence of certificate forgeries and to ensure improvement of the security, validity and confidentiality of graduation certificates. Technologies exist in related domains such as digital signatures which are used in electronic documents to provide verification, integrity, and non-repudiation. However, for the requirements of an electronic qualification certificate it has critical safety holes and missing functions: for instance, it uses the keys to verify document modification, but does not automatically start validation of the status of the public key certificates. This may result in a forgery being recognized if the key has been compromised. However, only the signer's public key certificate has been authenticated but it does not have the signed document itself. In our case of an e-qualification certificate, the signed document itself is also a certificate which may have a legitimate duration issue, so a simple digital signing of the document alone does not solve the problem.

Smart Contracts [1] Also called crypto-contract, it is a computer program used for transferring / controlling the property or digital currents in specific parties. It does not only determine the terms and conditions but may also implement that policy / agreement. These smart contracts are stored on block-chain and BC is an ideal technology to store these contracts due to the ambiguity and security. Whenever a transaction is considered, the smart-contract determines where the transaction should be transferred / returned or since the transaction actually happened.

Currently CSIRRO team has proposed a new approach to integrate BlockOn IOT with [2]. In its initial endeavor, he uses smart-home technology to understand how IOT can be blocked. Blockwheels are especially used to provide access control system for Smart-Devices Transactions located on Smart-Home. Introducing BC technology in IOT, this search again provides some additional security features, however, every mainstream BC technology must have a concept that does not include the concept of comprehensive algorithms. Moreover, this technology can not provide a general form of block-chain solution in case of IOT usage.

According to IlyaSukhodolski. The Al [3] system presents a prototype of multi-user system for access control over datasets stored in incredible cloud environments. Like other unreliable environments, cloud storage requires the ability to share information securely. Our approach provides access control over data stored in the cloud without the provider's investment. Access Control Mechanism The main tool is the dynamic feature-based feature-based encryption scheme, which has dynamic features. Using BlockChain based decentralized badgers; Our systems provide an irrevocable log for accessibility requests for all meaningful security incidents like large financing, access policy assignment, alteration or cancellation. We offer a set of cryptographic protocols that make the secret or secret key of cryptographic operation

confidential. The hash code of the sifter text is only transmitted by the block on laser. Our system has been tested on prototype smart contracts and tested on IteriumBlockchan platforms.
According to Huehuangenet. Al [4] they offer a blockchain and a MedRec-based approach by enabling encryption and attribute based authentication to enable secure sharing of healthcare data. By applying this approach:
1) The fragmented EHR fragment of all patients can be seen as a complete record and can be safely stored against tampering;
2) The authenticity of patients' EHR can be verified;
3) Flexible and finer access control can be provided and 4) it is possible to maintain a cleared audit trail.
According to VipulGoyalet.Al [5] develops new cryptosystems to share encrypted data properly, which we call key-policy attribute-based encryption (KPABE).In our cryptosystem, Cefhettextislabeled with a set of properties and controls that it connects to private key access configurations that a user can decrypt the encryption. We display the utility of our product to share audit log information and broadcast encryption. Our creation supports private key providers, which subscribe to categorized identification-based encryption (HIBE).

Hao Wang et Mate Al [6] They offer a secure electronic health record (EHR) system based on special-based cryptococcurs and blockchan technology. In our system, we use attribute-based encryption (ABE) and identity-based encryption (IBE) to encrypt medical data and to use identity-based signature (IBS) to apply digital signatures. . In order to obtain various functions of ABI, IBE and IBS in crypto, we present a new cryptographic primitive, it is called a joint feature-based / identity-based encryption and signature (C-AB / IB-ES). It simplifies system maintenance and does not require the installation of separate cryptographic system for various security requirements. In addition, we use blockconne techniques to ensure the integrity and inspection of medical data. Finally, we offer a demonstration application for medical insurance business.

According to Yan Michalevskyet. Al [7] system introduces the first practical decentralized ABE scheme with proof of policy-hiding.Our creation is based on the basic encryption of decentralized internal product, which is an encryption strategy launched in this paper. This ABB scheme supports results, disputes, and threshold policies, which protect the access policies of those parties that are not authorized to decrypt content. In addition, we handle the receiver's privacy issue.

Using our plan with Vector Commitment, we hide a complete set of attributes presented by the individual with the recipient; Just disclose the feature that regulates the authority. Finally, we propose random-polynomial encoding that immerses this scheme in the presence of corrupt officials. Al [8]they successfully address these issues by offering a clearepolicy feature-based data sharing plan with direct cancellation and keyword search. In the proposed scheme, the non-terminated users' private key is not required to be updated during the cancellation of direct revocation of features. In addition, a keyword search has been realized in our plan, and the search is stable with the increase in time features. Specifically, the policy is hidden in our plan, and therefore, the privacy of users is preserved. Our security and performance analysis show that the proposed plan can deal with security and efficiency concerns in cloud computing.

According to SarmadullahKhanet.Al [9] embedded power transactions in blockchain are based on their defined characteristics through the signature of many manufacturers. These signatures have been verified and customers are satisfied with the features that do not open any information that meet those features. The public and private key manufacturers have been created for these customers and using this key ensures that the support process is authorized by customers. There is no central authority required in this perspective. To protest against collision attacks, the makers are given secret pseudo-functional work seeds. Comparative analysis shows the efficiency of the proposed approach to existing people.

According to Ruuguet. Al [10] To guarantee the validity of the EHR surrounding the block channel, he has submitted a special-based signature scheme with multiple officials, in which the patient supports the message according to the specifications, but there is no evidence that he does not have any other information. In addition, there are many officers without generating a reliable individual or a central person in order to generate and deliver a public / private key, which avoids the escrow problem and adapt to the mode of data storage distributed in the Block Block. By sharing the secrecy of the secret pseudo-festive festivals in the authorities, this protocol opposed the attack of N-1 affiliated with officials.Under the computational BillineDiffie-Hellman concept, we also formally demonstrate that, in relation to the specialty-signatory's enforceability and complete privacy, this specialty-based signature scheme is safe in random decorative models. Comparison shows the efficiency and qualities among the proposed methods and methods in other studies.

II.LITERATURE SURVEY

HyperledgerSawtooth employs a flexible design, which distinguishes different sections of the device. This means the degree of blockchain is decoupled from stage of implementation. The flexible architecture often ensures that it is possible to modify various elements of the network, based on the project requirement. Examples of the modules that can be modified involve transaction laws, making and consensus algorithm. Most systems present algorithms Under different circumstances, that let the generals reach consensus. In a structure where the generals can send recorded, unforgeable letters, the writers illustrate that the dilemma can be solved with any number of generals and traitors. Nonetheless, because of the huge number of communications this approach would be very costly necessary.
Monika Rokade and YogeshPatil [11] proposed a system deep learning classification using nomaly detection from network dataset. The Recurrent Neural Network (RNN) has classification algorithm has used for detection and classifying the abnormal activities. The major benefit of system it can works on structured as well as unstructured imbalance dataset.

The MLIDS A Machine Learning Approach for Intrusion Detection for Real Time Network Dataset has proposed by Monika Rokade and Dr.YogeshPatil in [12]. The numerous soft computing and machine learning classification algorithms have been used for detection the malicious activity from network dataset. The system depicts around 95% accuracy ok KDDCUP and NSLKDD dataset.

Monika D. Rokade and Yogesh Kumar Sharma [13] proposed a system to identification of Malicious Activity for Network Packet using Deep Learning. 6 standard dataset has sued for detection of malicious attacks with minimum three machine learning algorithms.

Sunil S. Khatal and Yogeshkumar Sharma [14] proposed a system Health Care Patient Monitoring using IoT and Machine Learning for detection of heart and chronic diseases of human body. The IoT environment has used for collection of real data while machine learning technique has used for classification those data, as it normal or abnormal.

Data Hiding In Audio-Video Using Anti Forensics Technique For Authentication has proposed by Sunil S.Khatal and Yogeshkumar Sharma [15]. This is a secure data hiding approach for hide the text data into video as well as image. Once sender hide data into specific objects while receivers does same operation for authentication. The major benefit of this system can eliminate zero day attacks in untrusted environments.

Sunil S.Khatal and Yogesh Kumar Sharma [16] proposed a system to analyzing the role of Heart Disease Prediction System using IoT and Machine Learning. This is the analytical based system to detection and prediction of heart disease from IoT dataset. This system can able to detect the disease and predict accordingly. The system E-Certificate Authentication System Using BlockchainIn short, the program's purpose is: a valid registry with electronic certificates, i.e. an electronic credential is generated at the applicant's request. At the same time, that student's record is preserved by using hash values in blockchain blocks. The customer is also presented with a particular QR code or serial number, in accordance with the E-certificate. And instead the demand unit (e.g. company to which the applicant has applied for a job) must verify the authenticity of the electronic file using the QR code or the relevant serial number based on the reported details in the blockchain.

Jiin-Chiou Cheng et. al. [17] proposed a system Blockchain and smart contract for digital certificate, Then build an electronic paper document file that follows those related details into the database and thus decides the hash value of the electronic file. Finally, the hash value within the ring is stored in the chain process. To be affixed to the paper credential, the software will produce a related QR code and question string data. It will involve the demand device for paper certificate validity verification via mobile phone scanning or web site inquiries. Since of the blockchain's unchangeable property, the network not only increases the credibility of unique paper-based certificates but also the authentication risks of various types of certificates electronically types of certificates.

Marco Baldiet. al. [18] Certificate Validation The program solves the problem through Shared Ledgers and Blockchains by introducing a mechanism in which several CAs share a transparent, shared and stable database where CRLs are received. To this end, we find the concept of blockchain-based shared ledgers implemented for use of cryptocurrencies, which is becoming a common solution for many web applications of high protection and reliability requirements.

Oliver et. al. [19] illustrates Using blockchain as a Government degree tracking and assessment tool: a business analysis based on two financial factors comparing the service price as the main players between the customer and the employer. Students need a low-cost and easy-to-check evidence of competence, and employers also need swift and accurate documentation of their degree before recruiting. All models are built for growing regional markets and shares to discover ways of extending this sector in the European Union.

Because of the The arbitrary existence of hashing is never a guarantee of producing an appropriate object. Thus, Bitcoin mining is a competitive enterprise where miners are effectively hashed and admitted into the blockchain by awarding new Bitcoin for each block[20].

III.PROPOSED SYSTEM DESIGN

The system proposed blockchain-based e certificate generation for educational documents. The below figure 1 illustrates the propose system execution to generate a certificate as well as a unique Identification number for specific education students. The verification process per organization has also described in propose execution, the basic objective of the system to eliminate traditional certificate verification and documentation verification time-consuming process. The system follows the blockchain architecture to distribute the data in different data nodes like a distributed environment, in which insurance data can be extracted from different nodes using consensus algorithms. In the below section, we briefly explain our propose system execution with the strategic process.

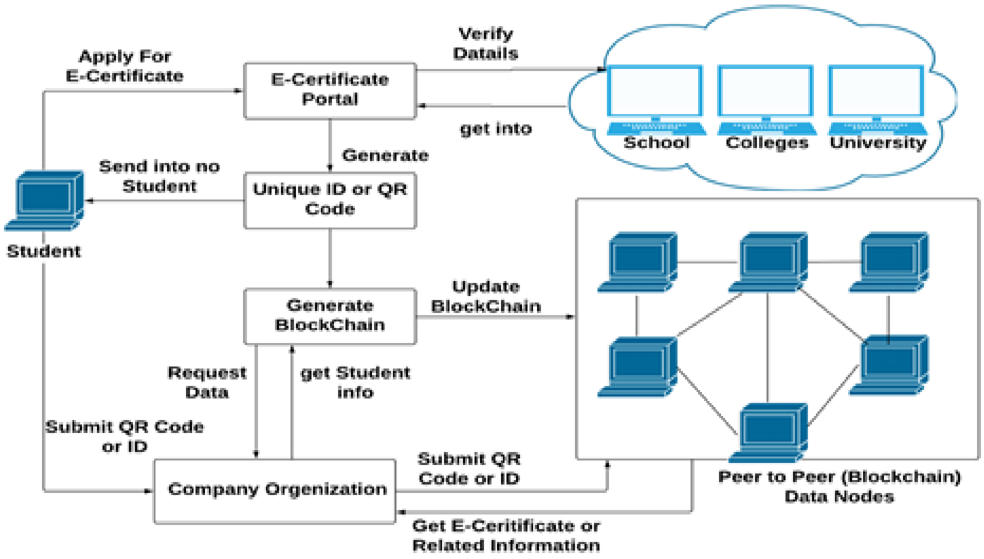


Figure 1 : Proposed system architecture

The above Figure 1 shows e certificate generation using blockchain in P2P environment. In the first phase user or student upload educational documentary on the web portal, the basic assumption behind the system web portal is the trustworthy organization which provide an authentic process of document verification from respective organizations. This process system follows once whenever user submit his documents. According to the verification process web, admin generates unique Identification (UID) number and QR code for a particular user. When the system generates those documents data has been automatically stored in different data nodes, and such data should be immutable. When data has Store into the blockchain it follows entire blockchain process as well as algorithms simultaneously. When specific organisation once to validate any user's educational history then they can only submit UID or can returned QR code and access the E-certificate from the blockchain.This processing difficulty eliminates traditional document verification time-consuming processes and provides a trustworthy framework for organizations.

Algorithm Design

Algorithm 1 : Hash Generation

Input : initial genesis block Gb, Previous hashPh, Data data[],

Output :Hash generation using SHA256 algorithm on data

```
    Step 1 :Input data data[]
    Step 2 :Perform SHA 256 from SHA suitable algorithms
    Step 3 :NewHash= SHA256(data[])
    Step 4 :Retrun String(NewHash)
```

Algorithm 2 : Protocol for peer to Peer nodeverification
Input : User Transaction query, Current Node Chain CNode[chain], AdditionalOutstanding Nodes blockchain NodesChain[Nodeid] [chain],
Output : Recover if any chain is invalid else execute current query

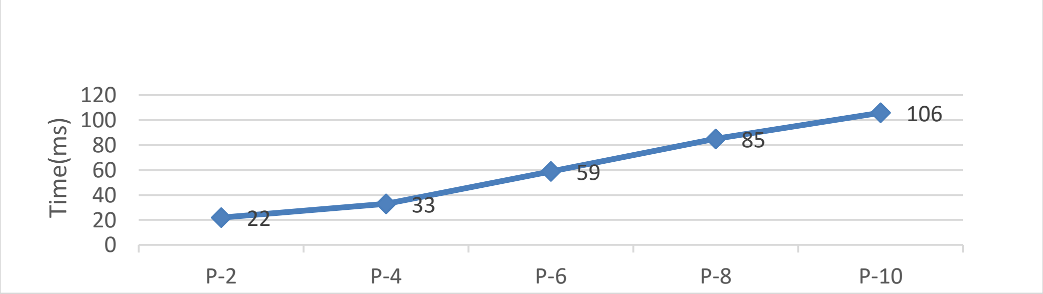
```
Step 1 :Transactional data or any event data for input to blockchain
Step 2 :Extract current server blockchain of time[t]
Cchain←Cnode[Chain]
Step 3 :For'each
                    $NodesChain\ [Nodeid, Chain] \sum_{i=1}^{n} (GetChain)$
  End for
Step 4 :Foreach (read I into NodeChain)
          If (!.equalsNodeChain[i] with (Cchain))
              Flag 1
Else Continue Commit query
Step 5 :if (Flag == 1)
CCount = SimilaryNodesBlockchian()
Step 6 :Determine the majority of server
          Recover inacceptableblockchin from precise node
 Step 7: End if
          End for
          End for
```

Mining Algorithm for valid hash creation
Input : Hash Validation Policy smart_contract[], Current Hash Values hash_Val
Output : Valid hash generation according to smart contract

```
Step 1 :System generate the hash_Value for ith transaction using Algorithm no. 1
Step 2 :if (hash_Value.valid with smart_contract[])
          Valid hash
           Flag =1
Else
        Flag=0
Mine the current hashagain randomly
Step 3 : Return valid_hash when flag=1
```

IV.RESULTS AND DISCUSSION

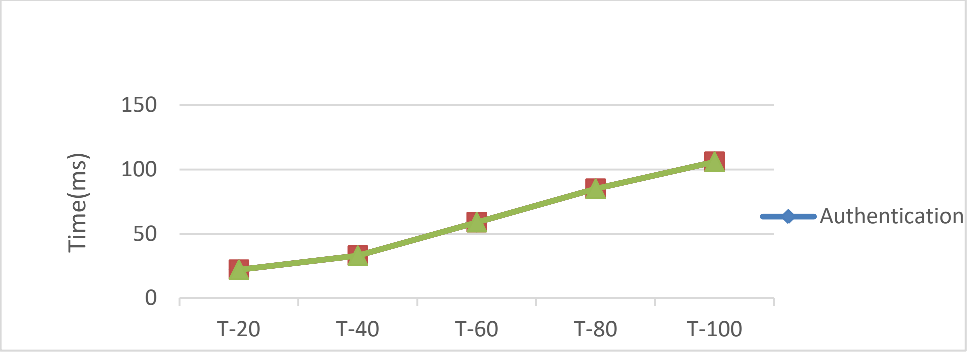
For the system performance evaluation, the system calculates the matrices for accuracy. The system is executed on java 3-tier architecture framework with INTEL 2.8 GHz i3 processor and 4 GB RAM with a distributed environment. The below figure (b) shows the time required for a consensus algorithm to validate the blockchain in 4 nodes. The x-axis shows the size of blockchain and Y shows the time required in milliseconds for validation.



Size of Blockchain

Figure 2: Time required for smart contract validation with different no. of P2P network in blockchain

The number of variation taken by algorithm from propose SHA value are evaluated in the third test case. Basically this has been done to evaluate the propose hash string is valid or not according to given mining policy. In many times when system generates SHA code for given transactional data its never fulfill the mining policy. To fulfillthe propose mining policy according to given scenario mining to generate the multiple variation on given string. The below figure (d) shows the time required to generate the valid SHA string for specific transaction.



No. of Transactions

Figure 3: Time required for mining for number of transactions in milliseconds

V.CONCLUSION

The program proposed uses blockchain technology that is a Distributed ledger means its stores for each node and validates the same statistics. Because of the blockchain function, our system is Improves the integrity of digital documents, that is to say Certificates, but also reduces the chances of falsification of certificates. E-certificate approval process and its automated system extremely efficient and clear generation. The units in demand Then (i.e. company or organisation) can ask for the Authentication of E-certificate specifications with QR code or serialunique identification number. The overall system provides for Exactness and security of the information. To implement the system based custom blockchain and some existing clock change like it Ethereum, Ripple, Cordono, etc, ensure the effectiveness of how custom blockchain provide additional significance over the available blockchain frameworks.

REFERENCES

[1] "Smart Contracts," http://searchcompliance.techtarget.com/definition/ smart-contract, 2017, [Online; accessed 4-Dec- 2017]

[2] A. Dorri, S. S. Kanhere, and R. Jurdak, "Blockchainin internet of things: Challenges and Solutions,"arXiv:1608.05187 [cs], 2016. [Online]. Available:http://arxiv.org/abs/1608.05187%5Cnhttp://www.arxiv.org/pdf/1608.05187.pd

[3] Sukhodolskiy, Ilya, and Sergey Zapechnikov. "A blockchain-based access control system for cloud storage." Young Researchers in Electrical and Electronic Engineering (EIConRus), 2018 IEEE Conference of Russian.IEEE, 2018.

[4] Yang, Huihui, and Bian Yang. "A Blockchain-based Approach to the Secure Sharing of Healthcare Data."Proceedings of the Norwegian Information Security Conference. 2017.

[5] Goyal, Vipul, et al. "Attribute-based encryption for fine-grained access control of encrypted data." Proceedings of the 13th ACM conference on Computer and communications security.Acm, 2006.

[6] Wang, Hao, and Yujiao Song. "Secure cloud-based EHR system using attribute-based cryptosystem and blockchain." Journal of medical systems 42.8 (2018): 152.

[7] Michalevsky Y, Joye M. Decentralized Policy-Hiding Attribute-Based Encryption with Receiver Privacy.

[8] Wu, Axin, et al. "Hidden policy attribute-based data sharing with direct revocation and keyword search in cloud computing." Sensors 18.7 (2018): 2158.

[9] Khan S, Khan R. Multiple authorities attribute-based verification mechanism for Blockchain mircogrid transactions. Energies. 2018 May;11(5):1154.

[10] Guo, Rui, et al. "Secure attribute-based signature scheme with multiple authorities for Blockchain in electronic health records systems." IEEE Access 776.99 (2018): 1-12.

[11] Monika D.Rokade ,Dr.YogeshkumarSharma,"Deep and machine learning approaches for anomaly-based intrusion detection of imbalanced network traffic."IOSR Journal of Engineering (IOSR JEN),ISSN (e): 2250-3021, ISSN (p): 2278-8719

[12] Monika D.Rokade ,Dr.YogeshkumarSharma"MLIDS: A Machine Learning Approach for Intrusion Detection for Real Time Network Dataset", 2021 International Conference on Emerging Smart Computing and Informatics (ESCI), IEEE

[13]Monika D.Rokade, Dr.Yogesh Kumar Sharma. (2020). Identification of Malicious Activity for Network Packet using Deep Learning. *International Journal of Advanced Science and Technology*, *29*(9s), 2324 - 2331.

[14] Sunil S.Khatal ,Dr.Yogeshkumar Sharma, "Health Care Patient Monitoring using IoT and Machine Learning.", IOSR Journal of Engineering (IOSR JEN), ISSN (e): 2250-3021, ISSN (p): 2278-8719

[15]Sunil S.Khatal ,Dr.Yogeshkumar Sharma, "Data Hiding In Audio-Video Using Anti Forensics Technique ForAuthentication ", IJSRDV4I50349, Volume : 4, Issue : 5

[16]Sunil S.KhatalDr.Yogesh Kumar Sharma. (2020). Analyzing the role of Heart Disease Prediction System using IoT and Machine Learning. *International Journal of Advanced Science and Technology*, *29*(9s), 2340 - 2346.

[17] Cheng JC, Lee NY, Chi C, Chen YH. Blockchain and smart contract for digital certificate.In2018 IEEE international conference on applied system invention (ICASI) 2018 Apr 13 (pp. 1046-1051).IEEE.

[18] Baldi M, Chiaraluce F, Frontoni E, Gottardi G, Sciarroni D, Spalazzi L. Certificate Validation Through Public Ledgers and Blockchains. InITASEC 2017 (pp. 156-165).

[19] Oliver M, Moreno J, Prieto G, Benítez D. Using blockchain as a tool for tracking and verification of official degrees: business model.

[20] George F. Hurlburt and Irena Bojanova, "Bitcoin: Benefit or Curse?," in IEEE, 2014

INNO SPACE
SJIF Scientific Journal Impact Factor
Impact Factor: 7.542

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर
NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details