IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2320-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 10, Issue 6, June 2021

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.512

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 10, Issue 6, June 2021 ||

| DOI:10.15680/IJIRSET.2021.1006435|

A Decentralized Approach for Generate E-Document over the Secure Network using Blockchain

Saber Nasir Take, Prof.Monika D. Rokade

PG Student, Department of Computer Engineering, Sharadchandra Pawar College of Engineering, Junnar Pune, India

Assistant Professor, Department of Computer Engineering, Sharadchandra Pawar College of Engineering, Junnar Pune, India

ABSTRACT: The existing methods for the use and maintenance of traditional certificates are already risk of forging and retrieving data. This establishing of authorization data is becoming a very easy task, which decreases the legitimacy of physical certificates. There is therefore a need for an important pre-forge measure to reduce the falsification of certificates. The implemented E-certificate iteration and authentication system is based on cryptocurrency. Blockchain offers impartial, uninitialized and encrypted feature vectors. Thus, by using cryptocurrency, an E-certificate with features such as pro-counterfeit, anti-forge and repeatability is produced. People will not be able to forge the concentrations of the E-certificates at all. The system, due to blockchain technology, would then help to solve the scam certification major issue by improving the legitimacy of the certificates. The system would also save on paper and overhead expenses. Electronically, the potential loss of credentials will be decreased. In brief, the system is all very beneficial to us. The system shall operate in brief: a valid electronic certificate file, i.e. an E-certificate, shall be initiated at the request of both the student. At the very same moment, the student record is stored in blockchain blocks by using hash values. In addition to the E-certificate, a related QR code or a unique serial number is also provided to the student. Then, the request unit (e.g. the service provider to which the student applied to work) can inspect the legitimacy of the electronic document using the QR code or the unique security code based on the information recorded on the blockchain. The proposed system has implemented in custom blockchain with own defined algorithms with peer to peer node networks. Experimental analysis shows the effectiveness of system and how it's better than other available blockchain.

KEYWORDS: E-Certificates, Blockchain, Mining,

I. INTRODUCTION

Educational certificates and transcripts contain confidential personal information which should not be easily accessible to others. Therefore, a mechanism is highly needed to ensure that the information contained in such a document is original, meaning that document originated from an authorized source and is not fake. The details in the document should therefore be kept confidential, so that only authorized individuals can access it. 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.

Digital Certification

The digital certificate, which adopts digital signature technology, gives the authority to confirm the user himself in the digital fields used for validating a user's identity and authorizing access to the network resources[1]. Digital certificates

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 10, Issue 6, June 2021 ||

| DOI:10.15680/IJIRSET.2021.1006435|

can be applied to Internet and e-government e-commerce activities, including traditional business, manufacturing, online retail transactions, public utilities, etc.**Blockchain**

Blockchain is the basic technology that underpins emerging crypto currencies like Bitcoin[2]. The key advantage of blockchain is largely regarded to be decentralization, and it can help establish peer-to - peer (P2P) intermediate transactions, coordination , and cooperation in distributed systems without mutual trust and centralized control among individual nodes, based on techniques such as data encryption, time stamping, distributed consensus algorithms, and economic incentive mechanism. As such, blockchain in traditional centralized systems can offer a novel solution to the long-standing problems of high operating costs , low efficiency and potential data storage security risks. Blockchain can be considered the next generation of cloud computing and is expected to radically reshape the behavioural model of individuals and organizations, making the transition from today's information internet to the future value internet possible. Blockchain is a distributed database, which is commonly used to record different transactions. Once a consensus among different nodes is reached, the transaction is added to a block that already holds records of multiple transactions. Each block contains its last counterpart hash value for connection. All of the blocks are connected and form a blockchain together. The data are distributed between different nodes (distributed data storage) and are therefore decentralized. Therefore the nodes hold the database intact. Under blockchain, a block becomes validated only after multiple parties have verified it. In addition , the data in blocks cannot be arbitrarily changed. For example , a smart contract based on blockchain provides a secure mechanism as it dispels doubts about the veracity of the information.

II. LITERATURE SURVEY

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.

Hao Wang et Mate Al [4] 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 VipulGoyalet.Al [5] develops new cryptosystems to share encrypted data properly, which we call key-policy attribute-based encryption (KPABE).In our cryptosystem, Cefhettextis labeled 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

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 10, Issue 6, June 2021 ||

| DOI:10.15680/IJIRSET.2021.1006435|

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).

Miners, a collaborative consumer network, verify and check transactions and set up specialized computation equipment called "hashes." They vote with their CPU strength, demonstrating their approval of legitimate blocks by working to expand them and by declining to operate on invalid blocks[6]. These record strings (hashes) that keep track of any Bitcoin transaction and are repeated on any device in the Bitcoin network.

Blockchain is a decentralized LEDGER used for safe trading of digital currencies, deals and transactions[7], and peer-to-peer network management. All nodes adopt the same internode contact protocol, and verify new objects. If the data is validated in every block no block will change it. To modify individual block data, all corresponding block data will be modified, resulting in network cooperation and denial of the transaction by all nodes.

The The power used to "farm" the cryptocurrency is a key aspect since its costs are rising. According to the Bitcoin statistics site Digiconomist, citizens worldwide use more than 30 terawatts-hours of electricity are mining the crypto-currency. This is greater than, at least, the human energy use 159 countries like Hungary, Oman, Ireland, and Lebanon [8].

Bitcoin mining is a Creation of new Bitcoin process by verifying Bitcoin Network transactions. That transaction is stored in a shared ledger, and all of the machines involved in the Bitcoin network check and manage the ledger. This "net" of transactions is known as the ledger, and. transaction is basically a timestamp for the database that may involve data [9].

Narayanan et al. [10] Describe a block string as a data structure composed of a related array of hash pointers. Every entity in the list is a block containing some previous block data and hash. This renders it a tamper-evident file, implying the data can only be applied to the list and the prior data can not be changed without detection.

Monika Rokade and Yogesh Patil [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. Yogesh Patil 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 Yogesh kumar 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 Yogesh kumar 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.

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 10, Issue 6, June 2021 ||

| DOI:10.15680/IJIRSET.2021.1006435|

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.

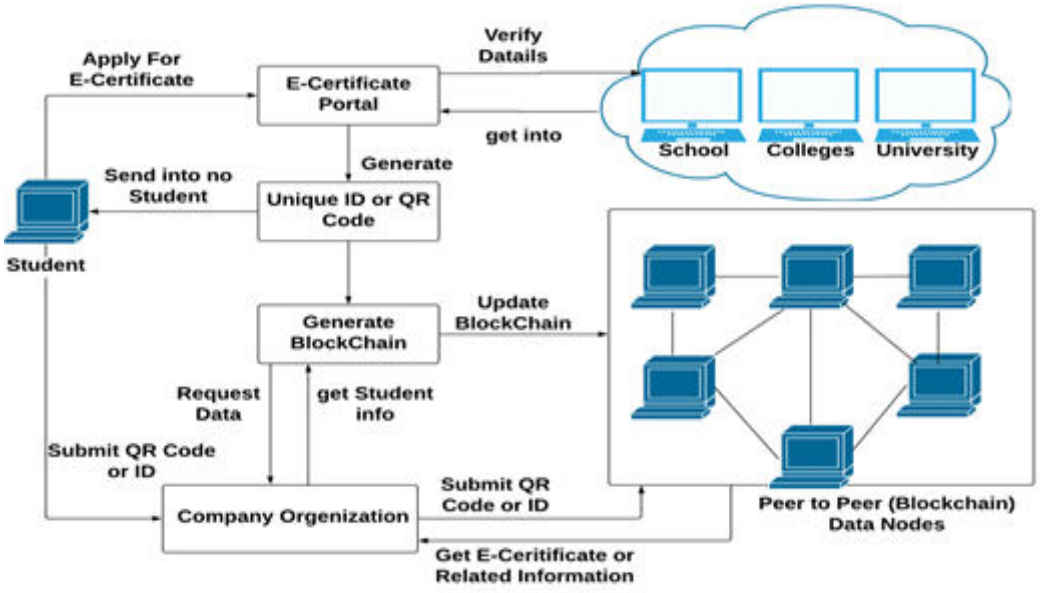

Figure 1 : Proposed system architecture

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 hash Ph, 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 : New Hash= SHA256(data[])

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 10, Issue 6, June 2021 ||

| DOI:10.15680/IJIRSET.2021.1006435|

Step 4 : Retrun String(**New**Hash)

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 (!.equals NodeChain[i] with (Cchain))

Flag 1

Else Continue Commit query

Step 5 : if (Flag == 1)

CCount = SimilaryNodesBlockchian()

Step 6 : Determine the majority of server

Recover inacceptable blockchin 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

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 10, Issue 6, June 2021 ||

| DOI:10.15680/IJIRSET.2021.1006435|

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.

Method	Hash Generation	Mining	Smart Contract Validation (Min 4 Nodes)
A blockchain-based access control system for cloud storage [3]	500	424	1025
Secure cloud-based EHR system using attribute-based cryptosystem and blockchain [4]	450	390	1120
SmartInspect: solidity smart contract inspector[8]	510	400	1640
blockchain and smart contract for digital certificate[17]	450	318	1450
Certificate Validation Through Public Ledgers and Blockchains [18]	401	350	1200
Proposed	250	170	980

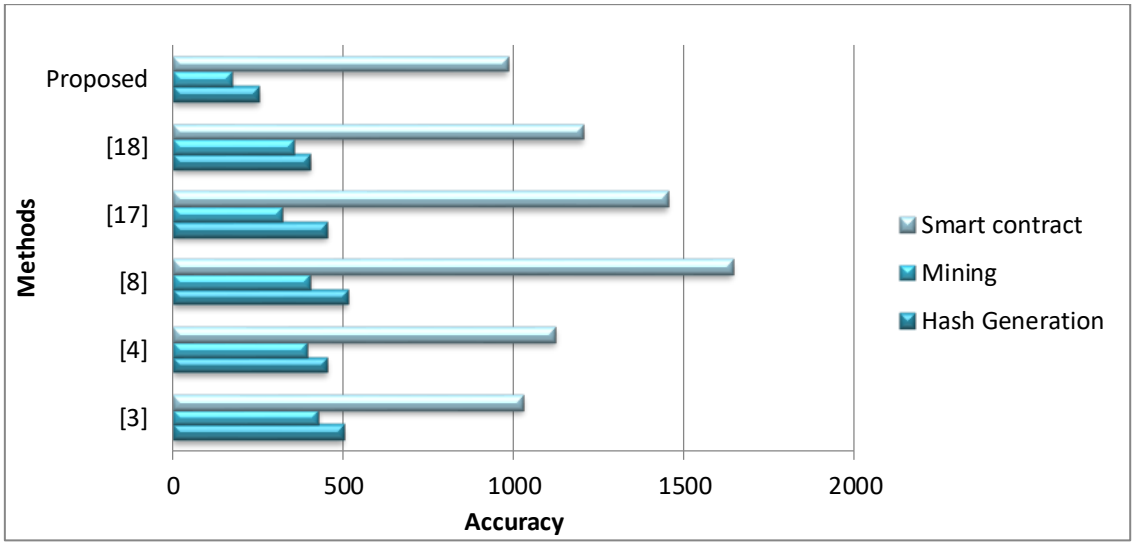

Figure 2 : Time required for blockchain

In another test case we evaluate the proposed system with smart contract validation by consensus algorithm in different number of peer to peer node.

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.

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 10, Issue 6, June 2021 ||

| DOI:10.15680/IJIRSET.2021.1006435|

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.
[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] Wang, Hao, and Yujiao Song. "Secure cloud-based EHR system using attribute-based cryptosystem and blockchain." Journal of medical systems 42.8 (2018): 152.
[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] Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, 2008, White Paper.
[7] Nirmala Singh and Sachchidanand Singh, "Blockchain: Future of financial and cyber security," in IEEE, Noida, 2016.
[8] Henrique Rocha ,Marcus Denker and Stephane Ducasse Santiago Bragagnolo, "SmartInspect: solidity smart contract inspector," in IEEE, Itly, p. 2018.
[9] GWYN D'MELLO. (2017, Dec.) https://www.indiatimes.com/technology/news. [Online]. https://www.indiatimes.com/technology/news/bitcoin-miners-are-using-more-electricity-than-irelandother-159-countries-no-kidding-335114.html
[10] Narayanan A., Bonneau J., Felten E., Miller A. & Goldfeder S. (2016) Bitcoin andCryptocurrency Technologies: A Comprehensive Introduction. Princeton: Princeton University Press
[11] Monika D.Rokade ,Dr.Yogesh kumar Sharma,"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.Yogesh kumar Sharma"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.Yogesh kumar 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.Yogesh kumar Sharma, "Data Hiding In Audio-Video Using Anti Forensics Technique ForAuthentication ", IJSRDV4I50349, Volume : 4, Issue : 5
[16]Sunil S.Khatal Dr. 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.

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor:
7.512

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर
NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details