IJCAT - International Journal of Computing and Technology, Volume 7, Issue 4, April 2020
ISSN (Online) : 2348-6090
www.IJCAT.org
Impact Factor: 0.835

Secure File Transfer Using Blockchain Technology

[1] Trupti Kulkarni; [2] Vandana Nemane; [3] Madhuri Darekar; [4] Jyoti Bachhav

[1, 2, 3, 4] Computer Science, Savitribai Phule Pune University, Assistant Professor,
Dr.D.Y.Patil Arts,Commerce & Science College,
Pimpri, Pune, 411018, India

Abstract - Growth in blockchain technology has been witnessed through the event of bitcoins and another necessary application that involves the idea of distributed cloud storage. A more practical employment would be to alter file sharing through the idea of Blockchain. This might facilitate in reducing the 2 step method of uploading a file to the drive and downloading it from a similar to one step method of simply transferring it from a sender to a receiver during a Blockchain network. Even if there square measure many applications which offer file sharing, it cannot match the one that's supported Blockchain technology in terms of security. Our focus is to alter a secured file sharing application by employing a personal Blockchain network so it will be used at intervals tiny organizations. A larger level of security is achieved by applying some important algorithms from the world of cryptography to powerfully encode the file thereby ensuring that none aside from the receiver will gain access to the file

Keywords: *Peer to peer, Decentralized, Round Robin Mining, Blockchain, P2P, Merkle Tree***.**

1. Introduction

The Blockchain could be a precocious spread-out information system that conserves a continuing increasing of record blocks secured from meddling. Every block incorporates a timestamp and a link to a former block, during a Merkle Tree Structure. The decentralized cloud is that the advanced and next level cloud wherever the difficulties of traditional centralized cloud area unit thought-about and brought care of. usually Cloud storage is centralized wherever area unit all information area unit hold on one server or a laptop in order that if the server is hacked or broken, the confidential information may be accessed thereby interrupting the service. It's not a good suggestion to trust the third party service in transferring confidential file in sector like Military Secrets, Bank Transaction etc.

By constructing a personal blockchain network for file sharing, hacking into the blockchain network becomes terribly laborious to Associate in Nursing extent that even the network administrator cannot intercept or tamper any a part of the file. Blockchain could be a new and rising technology and it in the main deals with the Cryptocurrency transactions wherever the entire transactions area unit absolutely secured and anonymous. The common example of public blockchain is bitcoins. During this project, rather than victimization Bitcoins, we have a tendency to area unit transferring files in order that even the massive files may be sent from one node to a different node safely.

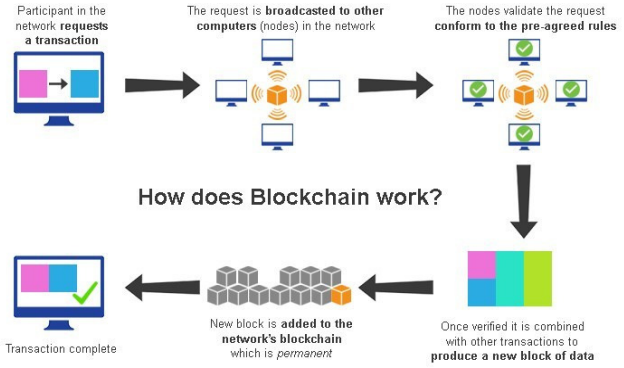


Figure 1

1.1 Merkle Tree Data Structure

To confirm the data transferred between two nodes, Merkle tree data structure make use of a hash value. It is very essential in a P2P networks because here we rely on unknown nodes. Consider if there are 4 messages namely 'a', 'b' , 'c' & 'd' , each message is hashed individually, then hashed values of a and b is combined into "ab", and the hashed values of c and d is combined into "cd". Again these are united into "abcd" which is top most root hash.
Any changes in a sole message also results in incorrect hash values, and these hash values are compared with hash values of another nodes. If the values are not same, it assumes that some tampering has taken place and the

transaction will not get confirmed. This maintains Stability as well as Reliability in Pear to Pear networks.

1.2 Multichain Framework

One of the famous open source framework is Multichain . By using this Framework user can deploy private Blockchain for any organization. Operating System Supported by Multichain are Linux ,Windows and Mac servers and it also provides interface through Command Line interface and simple application program interface. Multichain resolves the co-related problems of mining, privacy and openness via integrated management of user permissions. Multichain is permission based private blockchain. Using Multichain framework any number of nodes can join to form a network.

1.3 Mining and Miners

New Transactions are validated by **Miners** and then these transactions are recorded on the global ledger (**blockchain**). On an average, after every 10 minutes a block which contains transaction is excavated (**mined**) . Cryptographic hash algorithm are used by Miners to solve difficult mathematical problem. There will be two set of block data out of which one is temporary and the other is permanent. The improvised blocks are generated immediately when the transaction is initiated. Once the mining is done, the improvised block gets linked to permanent block which is the existent block used by all the nodes. Since blockchain built is private, mining need not be very complex and hard like the one performed for bitcoins.

The initial block is called the "genesis" block which acquire all the approval initially. The administrator has to grant the permissions to the other users joining the network. After requesting permission from admin any node from the network are able to become miner but the network which has been set by us provides permission as an miner to all the nodes which are the part of the network and the new nodes which will be part of the network in after joining the network in future. so that the transaction can be confirmed quickly and the files can be received immediately. The mining theory has been enforced in a round-robin fashion.

2. Deployment Scenarios

Consider a scenario for creating a private blockchain for an educational organization. If the file transfer mechanism has to be established between two parties then the circumstances is that the sender and the receiver both should have multichain framework installed in it.

2.1 Environment Setup

2.1.1 Consider that the private blockchain for an educational organization is created initially with 4 nodes. One is the local host itself, and the other nodes are three instances bought on AWS and set up in various locations such as Pune, New York and Berlin. So this results into, a private blockchain network . This new network is created by connecting the instance. This conveys the brief of network like count of blocks created , count of connected nodes , it also gives information about version of mutichain and a masked burn address.

2.1.2 Private Blockchain web Explorer

As a bitcoin explorer we also have an explorer which accounts all the transactions made in our private blockchain.

The image given below gives the list of nodes connected with its address. It also provides nodes address which are using multichain framework across the country. It does not require any technicalized or traditional hardware to work with it as it is fully independent of hardware. Normal laptop or PC is enough to conduct the test. It also runs in various cross platforms and supports different operating systems such as Linux, OSX and Windows.

1.

2.1.3 Connecting an instance to a private blockchain

```
root@blockchain3:~# multichaind chain1 -daemon

MultiChain Core Daemon build 1.0 alpha 27 protocol 10007

MultiChain server starting
Looking for genesis block...
Genesis block found

Other nodes can connect to this node using:
multichaind chain1@139.59.10.187:4793


This host has multiple IP addresses, so from some networks:
multichaind chain1@10.47.0.5:4793

multichaind chain1@10.139.96.112:4793

Node started
root@blockchain3:~#
```

Figure 1. Starting the blockchain service

Once the “genesis” block is found the multichain framework on that particular node starts.

```
MultiChain Core Daemon build 1.0 alpha 28 protocol 10007

MultiChain server starting
Other nodes can connect to this node using:
multichaind chain1@192.168.43.217:4793

Node started
root@srii-Alienware-15:/home/srii# multichain-cli chain1 getinfo
{"method":"getinfo","params":[],"id":1,"chain_name":"chain1"}

{
    "version" : "1.0 alpha 28",
    "nodeversion" : 10000128,
    "protocolversion" : 10007,
    "chainname" : "chain1",
    "description" : "MultiChain chain1",
    "protocol" : "multichain",
    "port" : 4793,
    "setupblocks" : 60,
    "nodeaddress" : "chain1@192.168.43.217:4793",
    "burnaddress" : "1XXXXXXWWXXXXXXXTuXXXXXXLZXXXXXXUoJmpZ",
    "incomingpaused" : false,
    "miningpaused" : false,
    "walletversion" : 60000,
    "balance" : 0.00000000,
    "walletdbversion" : 2,
    "reindex" : false,
    "blocks" : 5725,
    "timeoffset" : 0,
    "connections" : 0,
    "proxy" : "",
    "difficulty" : 0.00001526,
    "testnet" : false,
    "keypoololdest" : 1491411485,
    "keypoolsize" : 2,
    "paytxfee" : 0.00000000,
    "relayfee" : 0.00000000,
    "errors" : ""
}
```

Figure 2.Chain information

Publishers	1N9fSNLihuuKSvzJNUAFxHfc8VDFHCxyuivhV3
Key	my_key1N9fSNLihuuKSvzJNUAFxHfc8VDFHCxyuivhV3
Data	ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAAAgQCCX9V/Fez09f3V4z49vGoseDyklzo49S0Leuy36GHKSnioGGcFSMm /EpXopbXBTPASF45468WbPbOz9JSyFGf73KS8fOcV9/q4etiG6Q/x/Tgpboq+mQdLKXjNv7 /qrHjURWJHki9fUa9FSUpsDHCrcQ7TYsOuMECt1BZiC0RAsw== phpseclib-generated-key
Added	2017-04-05 17:38:17 GMT (confirmed)

Publishers	192vuW4VQcyKTsT82zj8Tm6TpaVdQS6WZy877M
Key	my_key192vuW4VQcyKTsT82zj8Tm6TpaVdQS6WZy877M
Data	ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAAAgQDAjFiys56z4lMUybpptaLOmdlBvpmL3coFT1iHw4QuWL/w3D2eBl2vc41eicdy0GteYrJf4zaRogXmyLh /Kj5wlvg73TlzqdUzFlzOsaT7FjnLPRKSD8Li9vVzm0bU2yej02eNcrt0yhlGsi3H /wcTMkGYSF27H3Xk5YqkyW/LQ== phpseclib-generated-key
Added	2017-03-27 16:36:46 GMT (confirmed)

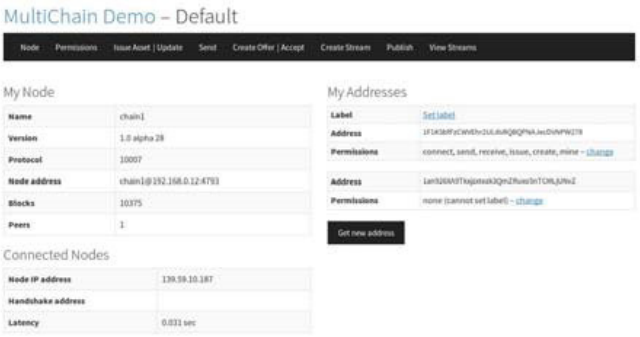


Figure 3. Explorer home page

The blocks here are called as streams. It shows number of streams available such as public key which will store the subscribed users Public key to used for RSA encryption. It does not provide with delete operation i.e it is not possible to delete data in streams only many streams can be created.

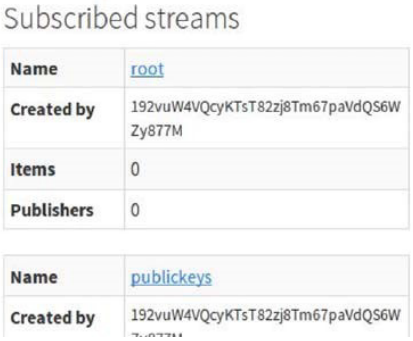
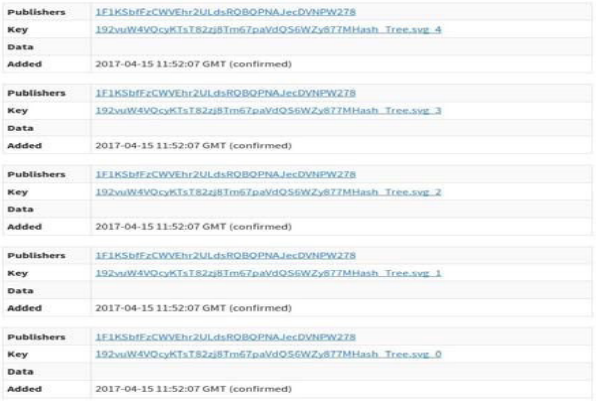


Figure 4. Public key system

It stores the public key of all subscribed users. Any new user must subscribe into this stream and must distribute their public key.



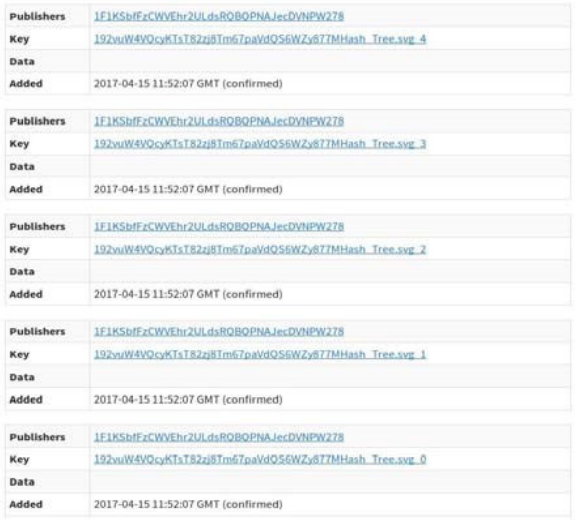


Fig. 5 Data Streams

Here the separate files are named from 0 to 4. Also the fourth row shows that the transaction is confirmed. All the parts of the file must be confirmed and only then the transaction will be added to the blocks and the receiver can receive and file.

2.2 Implementation Architecture

In this theory a sender cannot directly send a file to the receiver. Whenever the user wants to receive a file, he can explicitly send a request to the sender. With the request, the receiver also shares his burn address along with its public key to the sender. Burn address is essentially the address to which the file has to be sent which will be generated by multichain framework on all nodes.

While the receiver requests sender for the file, he can share his burn address along with it through by any means such as email or Facebook etc.

2.2.1 Modular Design

Modular design defines the structure of the overall module. The overall system consists of the following modules:

1. Encryption/Decryption
2. Split/Merge
3. Hex Encode/Decode

Encryption / Decryption At the sender's end, the input file is encrypted with symmetric cryptographic mechanism called AES+KEY, the keys are randomly generated then the randomly generated keys are encrypted with the Asymmetric cryptographic mechanism RSA.

File Split/ Merge
The AES encrypted file is split into five equal halves. At the receiver each part is decrypted and then the decrypted parts are merged together.
Hex Encoding/ Decoding
Now the split parts are encoded with Hex encoding and then encoded values of five parts along with the RSA encrypted key will get stored on each blocks, created by miners.
Step 1: By sharing his burn address the receiver will have to request for the file initially.
Step 2: The sender will upload the file with the receiver's address.
Step 3: The uploaded file moves through different modules.
Step 4: At the receivers side the file can be seen and the receiver can download it from his stream.

2.3 Security levels

There are various levels of security provided:

Level 0: There is an Encryption of AES key with RSA which allows file can be access only by the receiver. Even if the files are existing at all the blocks only the receiver can access the file. That's beauty of the blockchain.

Level 1: File is splitted into equal sized portions and encoded with Hex encoding which is capable way of sending files in the streams. Streams are nothing but blocks here.

Level 2: This is the most important level of security and the highest that can ever be obtained. Block chain network provides the highest form of security by making sure of the fact that when a file transfer takes place, the same has to be established by all the nodes which are present in the network. All the nodes can see that a transaction is going on between the sender and the receiver. But they can not alter the file anyhow. Any node can not snoop into the file and observe what is being sent. This level of security provides a assurance that only legitimate files can be transferred through the network. This legitimacy can be assured through the process of mining. Generally in a public bitcoin network, miners needs the capability to perform highly rigorous and sophisticated mathematical operations. In this case, since it is a private blockchain mining is not that complicated and hard. Also the more number of miners the faster the file transfers will occur. In a file sharing application, miners have to find out who are the real senders of files_and then confirm the transaction that is taking place. We have constructed a private block chain network with few nodes at different places of the world and used a mechanism of mining which takes in any node which joins a block chain network to be a miner. Like a bitcoin explorer we also have an explorer to account all the transactions made. Each transaction contains values such as size, received time, mined time and whether or not the transaction is included in a block. By default, the transaction is unconfirmed. In this case the file is split into five equal 0parts so all the five parts has to be confirmed by the miners only then the receiver can receive the file.

Level 3: At the receiver's side, to avoid leakage, strong algorithms from cryptography are implemented. Since the file is encrypted and split, the hackers or intruders cannot get access to the original file. It provides maximum integrity as well as security. Even if the file is tampered anywhere in between any nodes the root hash value will change using the Merkle tree data structure. The root hash will not match with the original hash and therefore the transaction does not get confirmed and remains tamper proof.

Thus all these levels of security will provide the most secure form of a file transfer. Even after the implementation of various algorithms that span a diverse and wide area of cryptography as well as Blockchain technology, it is still faster and more secure than SFTP and TOR. In spite of the sophisticated methodology involved, the process clearly worked out to be much quicker than the normal file sharing applications which are less secure. From the time taken for file transfer, it is even possible to expect blockchain to be an essential technology in shaping tomorrow's applications as long as security is perceived to be the primary concern in the world.

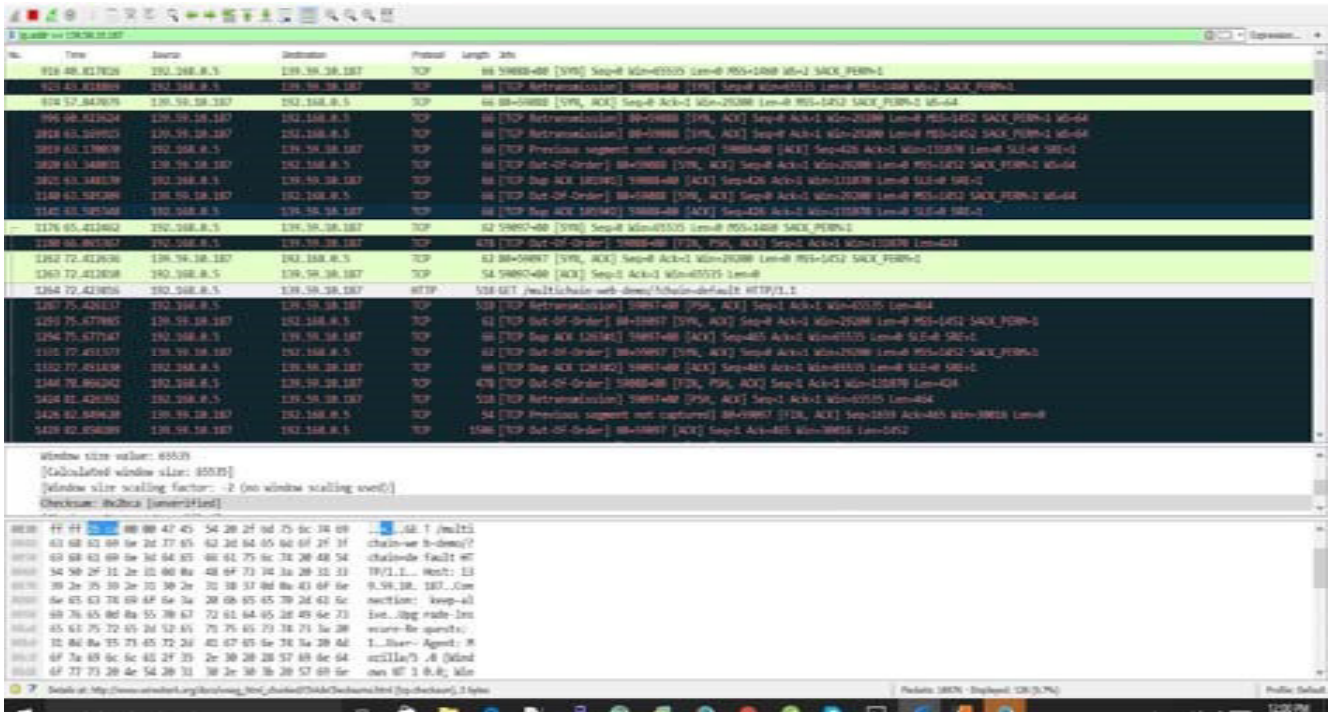
3. Proof Of Concept (POC)

The security proof of Concept can be measured using a popular packet sniffing tool called wireshark. When tried with normal FTP file transfer and SFTP the blockchain file transfer is much secured. In FTP the username and passwords are sent in plain text and can be easily seen.

3.1. Wireshark Sniffing

Wireshark is an open source and very powerful packet analyser.
While examining the packet it is seen that the blockchain file transfer doesn't simply use FTP protocol. Also the files from the stream can be downloaded using Curl request in Java/PHP. Curl is faster and secure than FTP. Also it is secure and faster than SFTP.

Consider a scenario where a rogue node or hacker tries to pretend as a legitimate node in a private blockchain and tries to sniff traffic and decodes the data passed between the nodes. As a result a hacker cannot decode the packet and it seems unbreakable.



4. Speed comparison

The speed comparison is tested with the input file size of 250MB pdf file at the internet speed rate of 30 MBPS. In the blockchain test environment it has 4 nodes and all the nodes were given miners permission.

Table 4.1. Speed comparison

FTP	STFP	Blockchain
2 min 30 seconds	3 min 10 seconds	2 min 5 seconds

It is important that the more the number of miners, faster is the file transfer. The receiver can receive the file only if the transaction is confirmed by the miners.

5. Advantages of blockchain technology

1. The blockchain technology permit for confirmation without dependent on third-parties.
2. The data structure in a blockchain is append-only. So, the data cannot be deleted and changed .
3. It makes use of protected cryptography to secure the data ledgers.
4. After maximum trust confirmation process, all the transactions and data are attached to the block.
5. All the blocks in the blockchain are time stamped, as the transactions are recorded in sequential order.
6. The ledger is scattered across each and every single node in the blockchain who are the participants. So, it is distributed.
7. The transactions stored in the blocks are present in millions of computers participating in the chain. Therefore it is decentralized. So if there is data lost, it can be recovered.
8. The transactions which takes place are clear. So the individuals who are provided authority can see the transaction.
9. The source of any ledger can be traced along the chain to its point of source.
10. There are no chances of duplicate entry or fraud , as various consensus protocols are used to validate the entry.

6. Disadvantages of blockchain technology

As every coin has two sides, blockchain technology also has a few disadvantages as follows.

6.1. Extremely Volatile :

The virtual currencies that are based on blockchain technology are very unpredictability. Good example for that is the fluctuating prices of Bitcoin that vary from day to day.

6.2. Problem for Not Tech Savvy

To store virtual currencies which are based on blockchain technology is a big headache for people who are not-so tech savvy. So people may face a problem while creating a Bitcoin or Ethereum wallet and then transferring coins from a digital wallet to a cold storage wallet**.**

7. Comparison between FTP and FTP using blockchain :-

The table gives an overview of comparison between the FTP and FTP using blockchain technology**.**

Table: Overview of FTP & FTP using blockchain

FTP	FTP using Blockchain
Dependent on third party	Not dependent on third party
Not much transparent	Transparent.
Not so secure as not using encryption	Is Secure as using encryption.
Speed is 2 min 30 seconds	Speed is ie 2 min 5 seconds
Compliance is an Issue.	Compliance is not an Issue.
It can be vulnerable to attack.	It can not be vulnerable to attack.

8. Conclusion

Since this concept is open source, we have implemented it using PHP and Java. It can also be integrated into an android environment and developed into an Android app. The only problem with deployment in Android smartphone is memory handling.. Mobile does not have a large memory to create and handle ‘n’ number of blocks. It is very challenging and if it is implemented in the future, it will create a new revolution in android. Also this

Blockchain concept can be integrated into various banking transactions to make them more secure and anonymous. Since the file is split and encoded with hex encoding, this could also create a possibility for compressing huge volumes of data into smaller sizes to further enhance the performance of file transfer in future.

9. Future Scope

This Blockchain technology is used in every escort of life such as in the meadow of Manufacturing, Banking, Healthcare, educational etc. While crisp on certainty regarding file transfer is not far away from this transformational change. The adoption of Blockchain will truly have a powerful and secured impact while saving our files more safely. To provide security at the time of file transfer in this technique and we have also a great impact to enhance the process. Thus it allow efficient data security while transferring files. For the moment comparing speed between FTP and SFTP they always try to increase their miners to make file transfer more faster. This same concepts can also be applied for maintaining our data more secured in all types of fields.

References

[1] https://www.ibm.com/blogs/blockchain/2018/05/securing-your-cross-domain-file-transfers-with-blockchain/
[2] www.quora.com
[3] www.wikipedia.org
[4] https://www.blockchain.com
[5] https://interparestrust.org/terminology/citations/844
[6] https://troindia.in/journal/ijcesr/vol4iss4/169-175.pdf
[7] https://www.smartdatacollective.com/top-advantages-blockchain-for-businesses/
[8] https://www.eff.org

First Author biography –
I Mrs. Trupti Anil Kulkarni have completed my M.Sc.(Computer Science) in year 2003, BSc(Electronics) in year 2001,HSC & SSC in year 1998 & 1996 respectively. I am currently working as Assistant Professor in Dr. D.Y. Patil Arts, Commerce & Science college, pimpri, Pune-411018..I published 12 research papers in different UGC approved Journals at National & International level. My current research era is in IOT & Blockchain.

Second Author biography-
I am Mrs. Vandana Nemane completed my M.Sc.(Computer Software) degree and currently working as Assistant Professor in Dr. D.Y.Patil Arts ,Commerce & Science college, pimpri,Pune-411018.