IMPLEMENTING BLOCKCHAIN TECHNOLOGY FOR MULTIMODAL BIOMETRIC SYSTEM USING ADAPTIVE FEATURE SET UPDATE ALGORITHM

[1]Dr. Vinayak A. Bharadi, [2]Ms. Purva P. Ghag, [3]Ms. Sukanya R. Chavan, [4]Ms. Shivani S. Gawas
Asst. Professor[1], Student[2,3,4] at Finolex academy of management and technology, Ratnagiri.
vinayak.bharadi@famt.ac.in[1], purvaghag86@gmail.com[2], chavansukanya16@gmail.com[3],
gawasshivani@gmail.com[4]

ABSTRACT

Multimodal biometric system is an important part of biometric system which is consist of multiple biometric traits for human identification. These biometric traits are varying as per ageing and some are unchanged. Therefore, combination of human biometric traits is used for better performance. These changes are identifying using adaptive feature set algorithm which will trigger when there updating is required.

For security purpose we implementing Blockchain technology using Hyperledger fabric on Multimodal biometric system to track the entire system and reduced frauds. Once the transactions are recorded in the ledger then it is hard to modify or delete the record. Blockchain technology is unalterable.

***Keywords*—Blockchain technology, Hyperledger fabric, Smart Contract, Multimodal Biometric, AFSU algorithm, Docker.**

I. INTRODUCTION

Multimodal Biometrics is a combination of multiple biometric feature for human identification. A biometric-based authentication process is done by using two modes: Enrollment and Authentication. In enrollment mode, a user's biometric data is read by biometric and stored in a database. In authentication mode, data which is acquired using enrollment mode is use to verify the claimed identity of the user or identify who the user is. While this verification is done using data corresponding to all users in the database. There are two types of user's biometric feature: Un-changed and Varying. In this system, the data which is use for user's biometric identification is stored in the database by implementing blockchain technology on it [1].

In Multimodal biometric system, system authentication is done by using combination of human features. There are two types of human features: Changed and Unchanged human biometric features. The changed features like face, voice, signature have low degree of permanence and they vary with time whereas unchanged features like Iris, retina, fingerprint have high degree of permanence and do not vary with time. Adaptive Feature Set Algorithm is used to monitor the changes occurring in the human biometric features due to some reason, identify need of replace the feature and triggered update module.

Biometric system is use for human identification. This verification is done using data corresponding to all users in the database. Biometric system is secured itself but it is totally dependent on the database therefore there is need of database security and by identifying this drawback we implementing blockchain technology on it. The data is stored through blockchain technology is secured and unalterable, therefore anyone cannot modify or delete the data from database.

Blockchain technology is referred as Distributed Ledger Technology (DLT), makes the record or history of transactions happened between two parties or any digital asset unalterable and transparent through the use of decentralization and cryptographic hashing [2].

A smart contract used in blockchain technology is nothing but a set of rules written in programming language. A smart contract is referred as an agreement between the two parties to perform any transaction over internet. A smart contract executes independently by the blockchain, there is no third-party involvement is present [3].

Hyperledger fabric is a blockchain framework on which you can build your own blockchain applications. Hyperledger fabric is open source project which is founded by Linux Foundation in 2015. In Hyperledger fabric, all participants must enroll through a trusted Membership Service Provider (MSP), before they can be part of the network, so it provides proof of trusted party. No transaction is allowed without verifying the participant. It is not a public network like Ethereum or bitcoin, it is a permissioned network or private network. In this, participants can be allowed to invoke smart contract, but not allowed to deploy any new smart contract. The smart contract written in Hyperledger fabric is called as Chaincode. No specific currency is required there is freedom for token/ coin [3].

II. EXISTING SYSTEM

In existing system, multimodal biometrics which is an emerging domain in biometric technology for enhance the performance of combination of more than one biometric trait that is used to adapt future changes in biometrics like face, iris, thumb, signature, voice and gait with respect to time. These biometric-based systems use two modes that are enrollment and authentication. Author Ujwalla Gawand [4] proposed a system that adapts a unified viewpoint to extract singular points (core and delta) that determine the topological structure and largely influence the orientation field by using the principle of Gabor basis functions.

Author Shyam Sundar Yadav [5] proposed five important modules that: The Sensor module which is interface between real world and system, the Feature Extraction module which removes artifacts from sensor, the Matching module extracts features which we have to choose with certain efficiency to create a template and match the input pattern and the database pattern with the pattern matching technique, Decision module and System Database module, authentication occurs based on pattern matching techniques.

Author Dr. Vinayak Bharadi [1] proposed a system that uses Adaptive Feature Set Update Algorithm to track the changes in biometrics and update the feature set securely which can take different biometric inputs for face recognition, finger print scan for finger identification for future extraction and representation. Biometric uses features related to human body which are change with age or some physical changes. Some high degree performance features like fingerprint, iris do not vary with respect to time but features like voice, face have low degree of performance which can be vary with time due to some physical changes. The existing system takes these types of features for enrolling feature set for multimodal biometric that can adopt changes in biometric traits with AI which are used for human identification.

Author Senthil Nathan proposed a system that design and implement first-ever decentralized replicated relational database with Blockchain properties that we term blockchain relational database. Author Shu Yun Lim [6] proposed a blockchain system that perform identity management and authentication which is distributed, fault tolerance and decentralized. The system facilitates peer-to-peer exchange of sensitive data, maintain privacy to providing efficiency and cost-effective identity management framework.

III. PROPOSED SYSTEM

Here, we are explaining our proposed systemFig. 3.1 which used multimodal biometric features like face, voice, signature, thumb, iris, etc. which are changed or unchanged for human identification. Face, voice, signature is changing features and thumb, iris are unchanging features. When these features are used for system authentication as an input with the help of biometric devices. That authenticate results comes from changing and unchanging feature traits which are monitored with the help of Adaptive feature Set Update Algorithm which is used for feature extraction. If there is a need to replace the features which are change due to some physical changes or ageing then update is triggered with the help of update module. Update module invokes those changes. When system authentication is done successfully then biometric system record that entries with date, time, %matrix and timestamps, so anybody cannot be denying the entries [1]. When user performs any transaction then smart contract is execute or trigger by blockchain which is written in Hyperledger fabric.

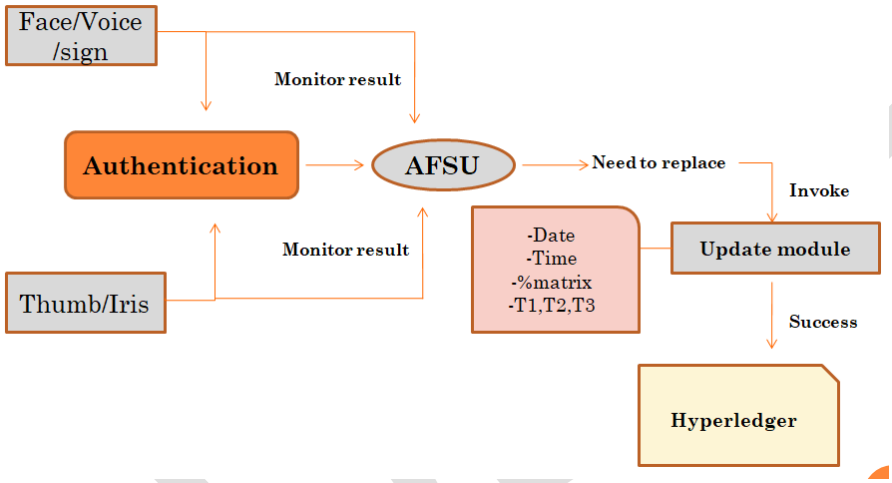


Fig. 3.1 Architecture of proposed system

❖ The Hyperledger contains 3 main components:

A. **Endorser Peer –** Receives data entries request from client application and validates the data and roles of requester. This executes the chain code (i.e. smart contract) and simulates the transaction but, it does not update the ledger. It approves and disapproves the transaction.

B. **Anchor Peer –** It configures the secret channels among the peer and data among the peer of that channel is visible only to them. It receives the updates and broadcast the updates to the other peers.

C. **Ordering Peer –** It is the central communication channel for Hyperledger network. It is responsible for consistent ledger state across the network. It creates the blocks and delivers that to all the peers.

❖ The Hyperledger workflow Fig. 3.2 is given as follows:

Step 1: User request for data entry to client application.

Step 2: Client Application broadcast data entry invocation entry to Endorser peer.

Step 3: Endorser peer validate that data entries and generate Chaincode i.e. smartcontract to client application.

Step 4: Client application send validate data entries to the Ordering peer which generates blocks of data.

Step 5: Ordering peer forwards these blocks of different members to Anchor peer of Hyperledger network.

Step 6: Anchor peer broadcast blocks to other General peers.

Step 7: These individual peers then updates their local ledger with latest block.

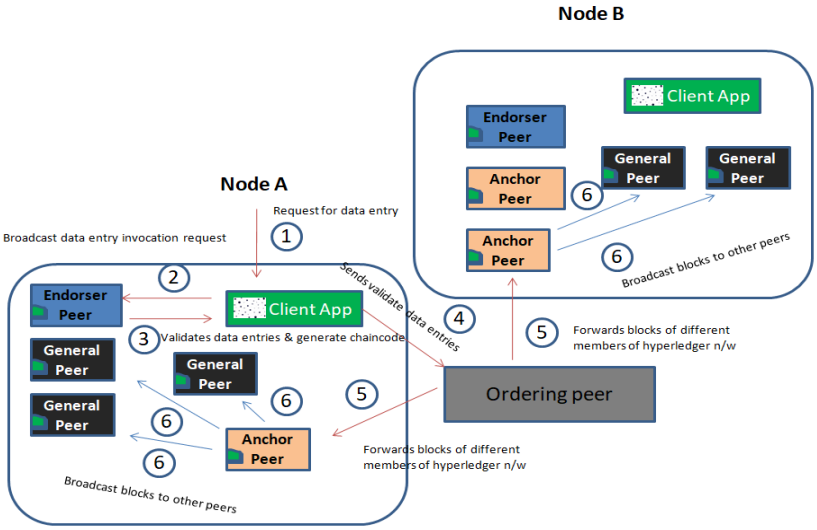


Fig. 3.2 Data Flow Diagram

IV. RESULT

❖ **To install Hyperledger Fabric on Linux:**

1. Execute the following commands to update the software on your system:

sudo apt-get update

2. Install curl and the golang software package:

sudo apt-get install curl

sudo apt-get install golang

export GOPATH=$HOME/go

export PATH=$PATH:$GOPATH/bin

3. Install Node.js, npm, and Python

sudo apt-get install nodejs

sudo apt-get install npm

sudo apt-get install python

4. Install and upgrade docker and docker-compose:

$ sudo apt-get install docker

curl -fsSL https://download.docker.com/linux/ubuntu/gpg | sudo apt-key add -

sudo add-apt-repository "deb [arch=amd64] https://download.docker.com/linux/ubuntu

$(lsb_release -cs) stable"

$ sudo apt-get update

$ apt-cache policy docker-ce

sudo apt-get install -y docker-ce

sudo apt-get install docker-compose

sudo apt-get upgrade

```
curl 7.47.0 (x86_64-pc-linux-gnu) libcurl/7.47.0 GnuTLS/3.4.10 zlib/1.2.8 libidn/1.32 librtmp/2.3
Protocols: dict file ftp ftps gopher http https imap imaps ldap ldaps pop3 pop3s rtmp rtsp smb smbs smtp smtps telnet tftp
Features: AsynchDNS IDN IPv6 Largefile GSS-API Kerberos SPNEGO NTLM NTLM_WB SSL libz TLS-SRP UnixSockets
go version go1.11.2 linux/amd64
Python 2.7.12
v8.15.0
6.4.1
Docker version 18.09.0, build 4d60db4
docker-compose version 1.8.0, build unknown
```

5. Install Hyperledger Fabric 1.3:

$ curl -sSL http://bit.ly/2ysbOFE | sudo bash -s 1.3.0

Download Docker images:

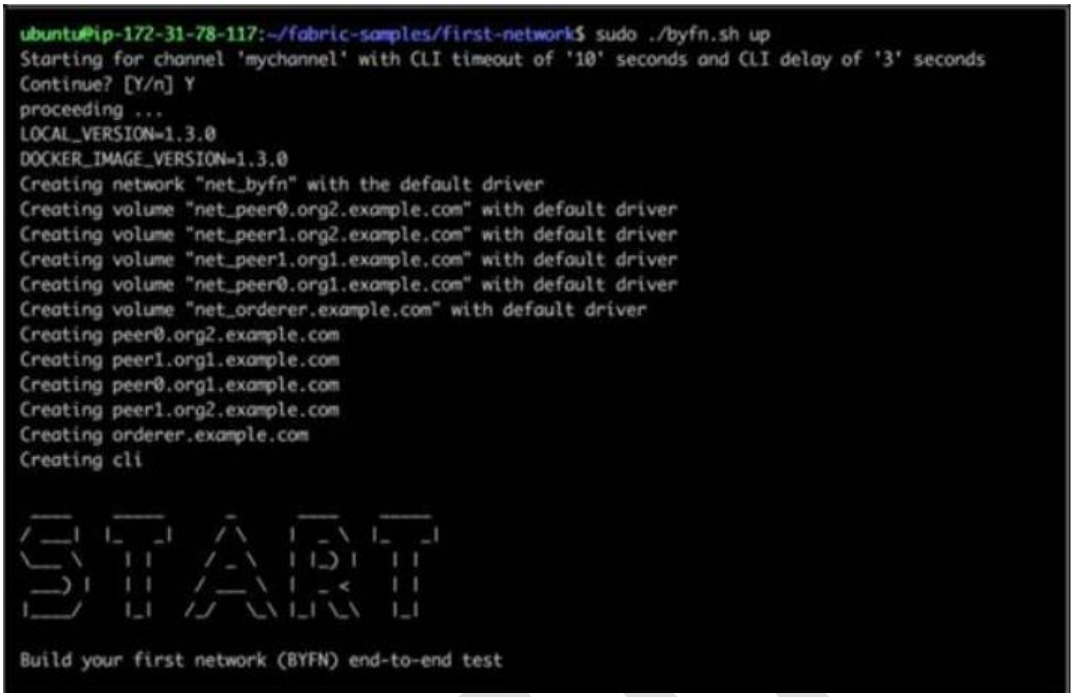
```
===> List out hyperledger docker images
hyperledger/fabric-ca           1.4.0-rc2           921e03d2731e        2 weeks ago         244MB
hyperledger/fabric-ca           latest              921e03d2731e        2 weeks ago         244MB
hyperledger/fabric-zookeeper    0.4.14              d36da0db87a4        2 months ago        1.43GB
hyperledger/fabric-zookeeper    latest              d36da0db87a4        2 months ago        1.43GB
hyperledger/fabric-kafka        0.4.14              a3b095201c66        2 months ago        1.44GB
hyperledger/fabric-kafka        latest              a3b095201c66        2 months ago        1.44GB
hyperledger/fabric-couchdb      0.4.14              f14f97292b4c        2 months ago        1.5GB
hyperledger/fabric-couchdb      latest              f14f97292b4c        2 months ago        1.5GB
hyperledger/fabric-javaenv      1.3.0               2476cefaf833        2 months ago        1.7GB
hyperledger/fabric-javaenv      latest              2476cefaf833        2 months ago        1.7GB
hyperledger/fabric-tools        1.3.0               c056cd9890e7        2 months ago        1.5GB
hyperledger/fabric-tools        latest              c056cd9890e7        2 months ago        1.5GB
hyperledger/fabric-ccenv        1.3.0               953124d80237        2 months ago        1.38GB
hyperledger/fabric-ccenv        latest              953124d80237        2 months ago        1.38GB
hyperledger/fabric-orderer      1.3.0               f430f581b46b        2 months ago        145MB
hyperledger/fabric-orderer      latest              f430f581b46b        2 months ago        145MB
hyperledger/fabric-peer         1.3.0               f3ea63abddaa        2 months ago        151MB
hyperledger/fabric-peer         latest              f3ea63abddaa        2 months ago        151MB
```

❖ **Build Hyperledger Fabric Network:**

1. Log in as a default user and execute the byfn.sh script to generate certificates and keys for the network:
$ cd ~
sudo chmod 777 -R fabric-samples
cd fabric-samples/first-network
sudo ./byfn.sh generate

2. Bring up the Fabric network by executing the byfn.sh script using the up option:
$ cd ~
cd fabric-samples/first-network
sudo ./byfn.sh up

The network has started successfully:



3. Bring down the Fabric network by executing the byfn.sh script using the down option to shut down and clean up the network. This kills the containers, removes the crypto material and artifacts, and deletes the chaincode images. The following code shows how to do this:

$ cd ~
cd fabric-samples/first-network
sudo ./byfn.sh down

The byfn.sh script, shown as follows. This script is well documented, and you should read about it in detail to understand each execution step during the network startup process:

The following command will generate the YAML file:

$ cd ~
$ cd fabric-samples/first-network
$ sudo ../bin/cryptogen generate –config=./crypto-config.yaml

We write the blockchain genesis block, create the first channel transaction, and write anchor peer updates. You may not care how exactly it is done, but this is how Fabric is built from the bottom up. You can see that four new files are generated and stored in the channel-artifacts directory:

- genesis.block
- channel.tx
- Org1MSPanchors.tx
- Org2MSPanchors.tx

$ export FABRIC_CFG_PATH=$PWD
sudo ../bin/configtxgen -profile TwoOrgsOrdererGenesis – outputBlock ./channel-artifacts/genesis.block
export CHANNEL_NAME=mychannel
sudo ../bin/configtxgen -profile TwoOrgsChannel

-outputCreateChannelTx ./channel-artifacts/channel.tx -channelID $CHANNEL_NAME
sudo ../bin/configtxgen -profile TwoOrgsChannel

-outputAnchorPeersUpdate ./channel-artifacts/Org1MSPanchors.tx -channelID $CHANNEL_NAME -asOrg Org1MSP
sudo ../bin/configtxgen -profile TwoOrgsChannel
-outputAnchorPeersUpdate ./channel-artifacts/Org2MSPanchors.tx -channelID $CHANNEL_NAME -asOrg Org2MSP

6. The Docker Compose tool is used to bring up Docker containers. We usde docker-compose-cli.yaml to keep track of all Docker containers that we bring up:
$ cd ~
$ cd fabric-samples/first-network
$ sudo docker-compose -f docker-compose-cli.yaml up –d

7. We have brought up six nodes: cli, orderer.example.com, peer0.org1.example.com, peer0.org2.example.com, peer1.org1.example.com, and peer1.org2.example.com:

CONCLUSION

The multimodal biometric systems overcome the problems in unimodal biometric systems. To facilitate peer-to-peer exchange of data and consent, mechanisms for discovery and recording of biometric traits, a decentralized network that is publicly accessible, immutable and resistant to faults and tampering is needed. Distributed ledger technology and Blockchain is the revolution that makes this possible. The approach used here is to increase accountability and efficiency as well as security of the entire system. Blockchain based solution is to produce integrity and protect system from single-point-of-failure. The Hyperledger of the blockchain, contains all the transactions information, is distributed and available to every member of the blockchain network. So, the blockchain-based identity management for user authentication using Adaptive Feature Set Update Algorithm is proposed for preserving privacy. This is the novel key management mechanism for blockchain-based security for user authentication. Performance and the advanced security level with blockchain technology made the multi-modal biometric systems popular in nowadays.

REFERENCES

[1] H B Kekre, V A Bharadi, **"Ageing Adaptation for Multimodal Biometrics using Adaptive Feature Set Update Algorithm"**, 2009 IEEE International Advance Computing Conference (IACC 2009),

Patiala, India, 6-7 March 2009.

[2] https://builtin.com/blockchain

[3] Sven Mitt, **"Blockchain Application - Case Study on Hyperledger Fabric"**, UNIVERSITY OF TARTU Institute of Computer Science Software Engineering Curriculum, 2018.

[4] Ujwalla Gawande, Sreejith R Nair, Harsha Balani, Nikhil Pawar & Manjiri Kotpalliwar, **"A High-Speed Frequency Based Multimodal Biometric System Using Iris and Fingerprint"** International Journal on Advanced Computer Engineering and Communication Technology (IJACECT)

[5] Shyam Sunder Yadav, Jitendra Kumar Gothwal, Prof. (Dr.) Ram Singh, **"Multimodal Biometric Authentication System:Challenges and Solutions"** Global Journal of Computer Science and Technology Volume 11 Issue 16 Version 1.0 September 2011.

[6] Shu Yun Lim1, Pascal Tankam Fotsing1, Abdullah Almasri1, Omar Musa1, Miss Laiha Mat Kiah2, Tan Fong Ang2, Reza Ismail3, **"Blockchain Technology the Identity Management and Authentication Service Disruptor: A Survey"** International Journal on Advance Science Engineering Information Technology.