Asian Journal of Computer Science and Technology
ISSN: 2249-0701 Vol.8 No.2, 2019, pp. 19-24

A Novel Digital Voting System with Integrated Technologies (DVSIT)

T. M. N. Vamsi[1], S. Sri Charan Dutta[2], K. Harika[3], V. Kiran[4] and V. Abhiram[5]
[1]Professor, [2,3,4,5]UG Student
[1,2,3,4&5] Department of Computer Science and Engineering, E & T Program,
Gayatri Vidya Parishad College for Degree and PG Courses (A), Visakhapatnam, Andhra Pradesh, India
E-Mail: biopprativamsi@gvpcdpgc.edu.in, cherrysri1997@gmail.com, harika.kornu1997@gmail.com,
kirancherry0001@gmail.com, johnsunny65@gmail.com

***Abstract* - Over the years, technology has been growing fast. With growing technology there are many modern problems being created. With innovation many novel approaches are being proposed to find a better solution. Coming to the present days, the "Electronic Voting Machines ("EVM")"based voting system is prone to much vulnerability. There were several issues regarding tampering and security of EVMs which have not been proved. With the upcoming elections the biggest challenge is to conduct a fraud-free polling. Due to vulnerabilities in current voting system the security of a vote is being compromised by many malpractices such as duplicate voters, dummy candidates, booth capturing, EVM rigging, etc. Introducing Blockchain Technology into digital voting process can minimize most of the frauds as it's almost impossible to breach the security level of Blockchain. The proposed system assures authenticity of a voter by providing Dual Authentication process.**

***Keywords:* EVM, Security, Fraud-Free Polling, Malpractices, Blockchain, Authenticity, Dual Authentication Process**

I. INTRODUCTION

The rationale of the proposed system is providing security to the details of a user as well as achieving privacy of the vote casted by the user. The technologies with which this project is being implemented are

A. Blockchain Technology

This technology came into light with the invention of bit coins and other crypto-currencies. It is more trusted because of its decentralized power i.e., Public Distributed Ledger which makes it immune to hack [1]. It uses a public and private key encryption to encrypt the transaction details which are highly impossible to decrypt. The advantage of blockchain is that it charges minimal transaction fee compared to other means such as banks, e-Wallets, etc.

B. Face Recognition

Human Beings are capable of recognizing faces without any efforts in their day-to-day life. With the present smart devices security has been a very important feature with many challenges [2]. Biometric Authentication helps us to overcome the challenges as it provides at most security. Face Recognition is one of the Biometric Authentication feature used in many sensitive areas such as bank vaults, army bases, etc.

C. OTP Verification through e-Mail

One Time Password is also an authentication process which is used as a Dual Authentication step, in general. It is mainly used online transactions, signing into online applications, etc.

D. Cloud Technologies

Cloud Technology is a pay-as-you-go service which is majorly used for storing the data in remote servers hosted by third-party companies such as Google Cloud Platform, Microsft Azure, Amazon Web Services, etc. It is a technology which provides different services such as IaaS (Infrastructure as a Service), PaaS (Platform as a Service), Saas (Software as a Service), StaaS (Storage as a Service), etc.

E. Existing Systems

Various voting methods are being used in elections. The most popular methods among them are

1. *Ballot Box:* This is the age old system for electing representatives according to people's choice. In this system a ballot paper is given to every voter which contains the list of symbols of different parties competing in the election. The voter has to choose one among the list by stamping beside the symbol. At the end the votes are counted from ballot box and the final results are announced.
2. *EVM (Electronic Voting Machine):* With growing technologies there were changes in the Voting Process and due to which EVMs were introduced into the current system. Each EVM can bareup to64 party symbols. Each voter is allowed to the polling booth after being authenticated based on their Voter Id. The votes are casted by pressing button beside the party symbol available on the machine. The maximum capacity of an EVM is 3840 votes. Though these are electronically monitored machines there are high chances of rigging and dummy candidates.

F. Proposed System

The proposed system provides security to the user's data through Encrypted Password, Face Recognition, and OTP through Mail. It also records the votes in Blockchain

through a Smart Contract which maintains the privacy of the votes and is immutable. To maintain the integrity of user data during the registration process the proposed system is connected to the Aadhar Database (which is simulated in this work). The details of a user/voter are stored in Cloud (which is simulated in our case) to maintain consistency and integrity of the collected data. The voter has to pass through the following security levels before he/she might cast a vote: Password authentication, OTP Verification which is sent to the registered e-Mail id of the voter and Face Recognition step. After the authentication process the system provides 30 seconds of time limit within which the voter has to cast his/her vote. The system records the vote in such a way that the party to which the vote belongs to is known but the voter who casted that particular vote is not known. In this way the proposed system enables high security and privacy of the details of a voter and a casted vote.

II. LITERATURE REVIEW

Several research ideas have appeared in literature for design and implementation of electronic voting machines with different computational approaches over the past decades. These approaches addressing the merits and demerits of the hitherto state-of-the-art methods and trying to developed new approaches suitable for this domain. Based on the problem discussed in this work, a summary of three different methods and their significance relevant to the problem are discussed in this section.

Ali KaanKoç, EmreYavuz, UmutCan Çabuk and GökhanDalkiliç [3], published a research paper named after "Towards Secure E-Voting Using EthereumBlockchain", which describes its abstract as "There is no doubt that the revolutionary concept of the blockchain, which is the underlying technology behind the famous crypto-currency Bitcoin and its successors, is triggering the start of a new era in the Internet and the online services. The blockchain with the smart contracts merges as a good candidate to use in developments of safer, cheaper, more secure, more transparent, and easier-to-use e-voting systems".

Aftab Ahmed, JiandongGuo, Fayaz Ali, Farah deeba[4], published a research paper named after "LBPH Based Improved Face Recognition at Low Resolution" which describes its abstract as "Automatic individual face recognition is the most challenging query from the past decade in computer vision. This paper employs the Local Binary Patterns Histogram (LBPH)[5] algorithm architecture to address the human face recognition in real time at the low level of resolution".

Friðrik Þ. Hjálmarsson and Gunnlaugur K. Hreiðarsson[6], published a research paper named after "Blockchain-Based E-Voting System" which describes its abstract as "Building an electronic voting system that satisfies the legal requirements of legislators has been a challenge for a long time. Distributed ledger technologies are an exciting technological advancement in the information technology world. Blockchain technologies offer an infinite range of applications benefiting from sharing economies. This paper aims to evaluate the application of blockchain as service to implement distributed electronic voting systems.

III. METHODOLOGY

To implement this project with the foresaid methods, the following programming languages are used to implement this system: Python (v3.6.7), Node Js (v8.11.1), Solidity (v0.4.12), HTML5, CSS Java script and Oracle SQL. Also different servers are needed for implementation and based on the purpose and requirement of the project the individual server is taken into consideration. The following are the list of servers used in the project.

1. Go Ethereum Blockchain Server and Geth Command Prompt
2. Node Js Server
3. Python Flask Server
4. Oracle Database Server

Description of each server is as follows

A. Go EthereumBlockchain and Geth Command Prompt

Go Ethereum is a blockchain server whose currency is in terms of "ETHER" and can be accessed through Node Js Server using the library named Web3.js

1. The mining commands can be given and monitored using the Geth Command Prompt
2. Commands and Instructions to start the server are

i. Go EthereumBlockchain

```
geth --datadir /ethereum-private/DVSIT --rpc -
rpccorsdomain "localhost:3000" --rpcport 8545 --rpcapi
"web3,eth,personal" --nodiscover --verbosity 6 --maxpeers
2 --networkid "124" --port "30000"
```

ii. Geth Command Prompt

1. geth attach ipc:\\.\pipe\geth.ipc
2. miner.setEtherbase(eth.accounts[0])
3. miner.start()
4. miner.getHashrate()

B. Node Js Server

Node Js is a server-side language. NodeJs is developed on Google Chrome's JavaScript Engine which is known as V8 Engine, popularly.

1. Node.js was developed by Ryan Dahl.
2. It is across-platform and an open source runtime environment for developing networking and server-side applications.

3. There is also a provision of installing different modules from Node Js library. These modules are very helpful in developing web applications with ease.
4. To install the libraries provided by Node Js a library manager is available. It is known as Node Js Package Manager (npm).
5. Commands and Instructions to start the Node Jsserver are
   a. nodemon server.js

C. Python Flask Server

1. Flask is a web frameworkwhich provides tools, libraries and technologies that allowsto build a web application.
2. A web application can be some web pages, a blog, a wiki or a commercial website.
3. Flask is a micro framework. Micro frameworks are the one which has no or little dependencies to external libraries. The advantage of Flask is that it is light and since there are little dependencies, updates are not much needed and needed less watch for security bugs. In the case of Flask, its dependencies are

a. Werkzeug a WSGI utility library
b. jinja2 which is its template engine

D. Oracle SQL Server

1. Oracle SQL Server provides Database as a Service and SQL is a language to query the database
2. Commands and Instructions to start the server

a. Goto "Start" menu
b. Search for "Oracle 11g Expresss Edition"
c. Open "Run SQL" again from the "Start" menu
d. Type the command, "connect hr/hr" and press "Enter" key

The Cloud storage service and the OTP Verification are implemented in the python flask server itself.Here, both user and voter are used synonymously. The procedure and working of the proposed system is explained with the following sections with detailed descriptions and diagrams.

E. Registration Process

The whole registration process is implemented using the Python Flask Server. The registration process is explained as follows and the respective details depicted in Fig. 1.

1. The user has to provide details such as name, date of birth, e-Mail Id, Aadhar Id, voter Id, password, security question and security answer.
2. If the above provided details match with the Aadhar Database then the system collects the face dataset using the web-cam of the machine.
3. In the backend, feature extraction process will be performed, a model will be created and stored in the Cloud including the registration details. In our case Cloud is simulated such that it provides Storage as a Service in the local system.

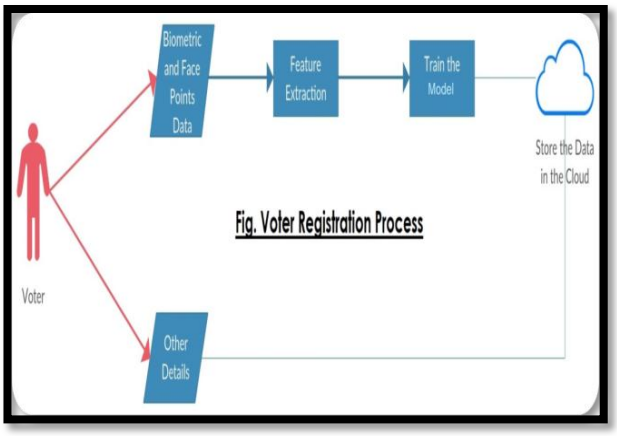

Fig. 1 Voter Registration Process

F. Voter Verification Process

Also the whole verification process is implemented using the Python Flask Server. The verification process is explained as follows and the respective details depicted in Fig. 2.

1. The process gets initiated once the user provides his/her Voter Id and password.
2. If the password is a right one, based on the Voter Id the trained model of face of that particular user is fetched from the Cloud.
3. If the face provided by the user at the verification system matches with that of the model fetched then the user is allowed to further process i.e., Voting Process.

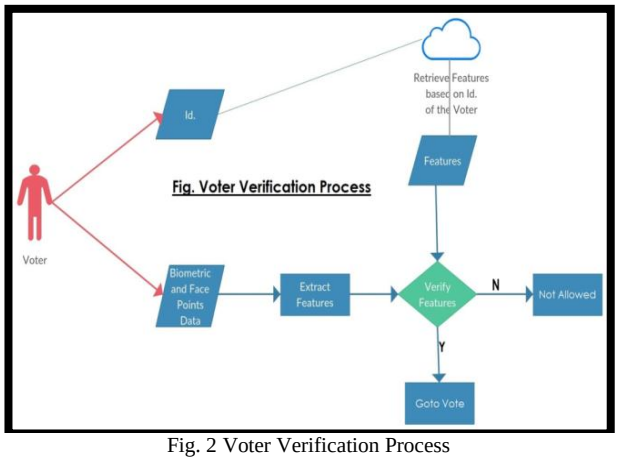

Fig. 2 Voter Verification Process

G. Voting Process

The whole Voting Process is implemented using Node Js server and Go Ethereum Blockchain Server. The voting process is explained as follows and the respective details depicted in Fig. 3.

1. The authenticated user or voter will be provided a Ballot Page in which the list of Political Parties and their symbols is shown.

2. The user will be provided a session of 30 seconds in which he/she has to cast a vote.
3. The casted vote is recorded in the Blockchain server on the command of Node Js server.
4. Also the particular voter Id will be noted in the Oracle Database as a successful voter who casted the vote so that the redundancy of the voters is eradicated.

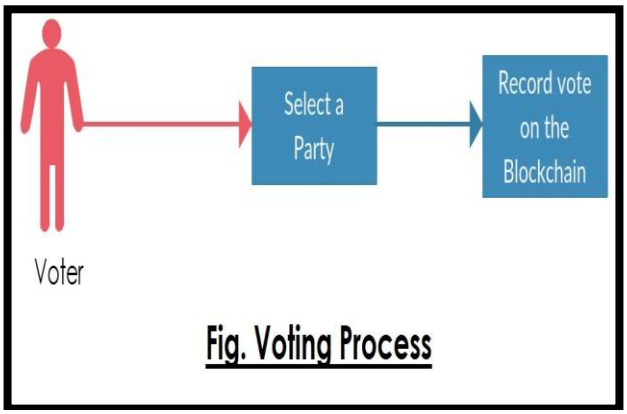

Fig. 3 Voting Process

H. Vote Counting Process

The whole Vote Counting Process is implemented using Node Js Server and Go Ethereum Blockchain Server. The vote counting process is explained as follows and the respective details depicted in Fig. 4.

1. As the blockchain is nothing but a list of blocks which can be thought of as a doubly linked list, can be traced back and access the data in each block.
2. With the help of Solidity Smart Contract the count of votes for each and every Political Party can be known.
3. And also vote casted by the voters are acknowledged that their vote has been taken into account through their registered e-Mail Ids.
4. Finally, the report is generated through chart representation.

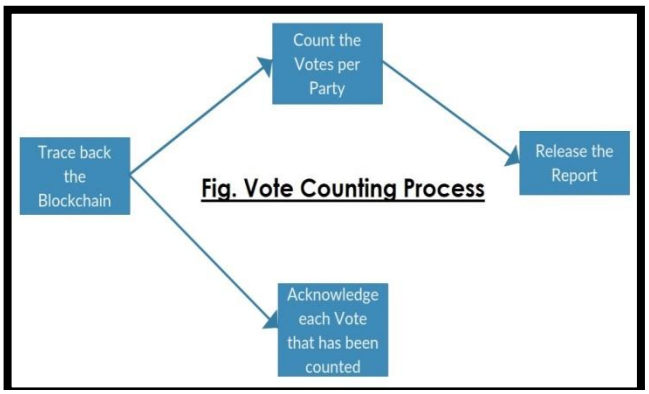

Fig. 4 Vote Counting Process

I. Algorithms

Algorithm that is used to achieve the Face Recognition is Local Binary Points Histogram (LBPH) Algorithm [2]. It is explained in the below following way.

To perform the face recognition system here the Local Binary Pattern Algorithm has been applied. The LBP operator is used in local features through Local Binary Pattern acts which shorten the local special arrangement of a face image. The LBP operator is the number of binary ratios of pixels intensities within the pixel of center and it's around eight pixels. It can be shown in below equation [2].

$$LBP\ (xc, yc) = \sum_{n=0}^{7} S(i_n - i_c)2^n \qquad (1)$$

Where ic indicates the value of the center pixel and (xc, yc), shows eight surrounding pixels information. Therefore, it is very helpful in determining the face features. From the original matrix Features of the image are extracted then these values are compared with the center pixel values, the later binary code is generated.

IV. RESULTS AND DISCUSSIONS

The implementation stages of entire system are successfully verified and the respective results are described below and each stage of system implementation is presented in following figures from 5 to 14.

A. Registration Page

The registration page as shown in figure 5 is designed in HTML and CSS and the backend is developed with Python Flask web framework.

Oracle Databse (simulated Aadhar Database) is connected to the Flask server and also Cloud Server is simulated using flask. On clicking the register button on the screen, immediately an OTP is generated to the mail proivided which is shown in the Fig. 6 .

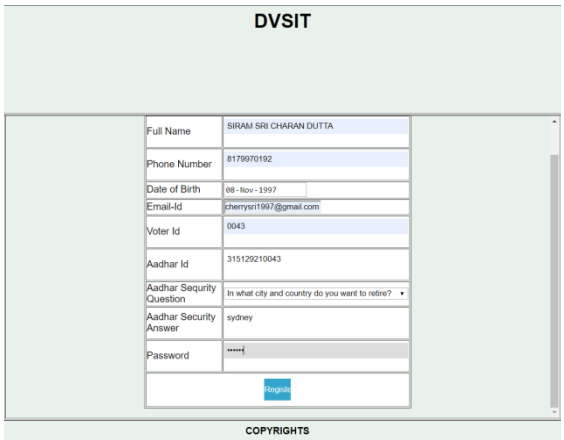

Fig. 5 Registration Page

B. OTP through eMail

An OTP is sent to the eMail Id provided in the registration page as shown in the Fig. 5. And this OTP should be entered in the text field given.

If the user doesn't provide a valid OTP an error page appears showing the same. The recived OTP from DVSIT wiil be enter in the page provided which was shown in the Fig. 7.

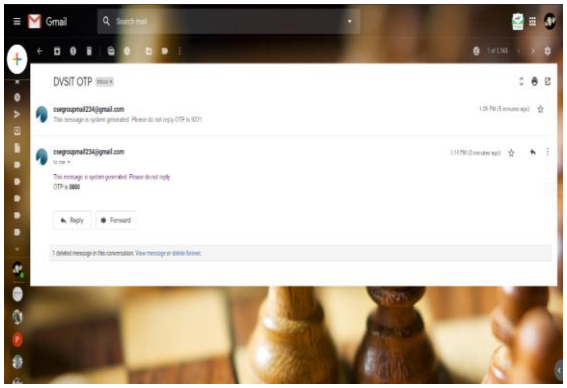

Fig. 6 OTP sent to E-Mail

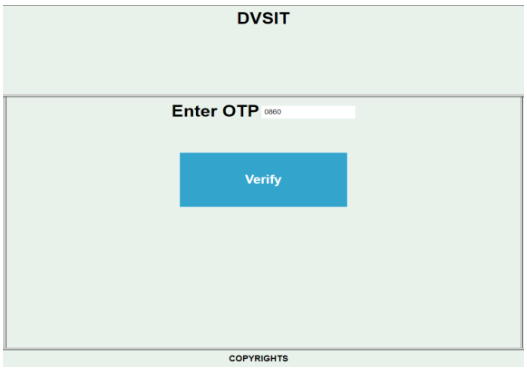

Fig. 7 Enter OTP Page

C. Registration Details Storage File in Simulated Cloud Space

The registration details are stored in the simulated Cloud space in the form of a text file as shown in the below figure 8. These are stored as Comma Separated Values. This file is stored in a directory which will be named as that of the voter Id of the user. The last value in the file is nothing but the encrypted form of the password. The password will be hashed and stored in the file.

Fig. 8 Registration Details stored in Cloud

D. Face Dataset Collection

Upon passing through the OTP page, the user is supposed to sit erect in front of the camera of the system and the surroundings must be under minimal brightness. The system captures 100 images of the user's face and stores them in the Cloud into the directory created with his/her voterId. And after the collection of the dataset the system prompts the user to click the train button. Upon clicking the Train button a model is created in the Cloud which is further used to recognize the user during the authentication process.

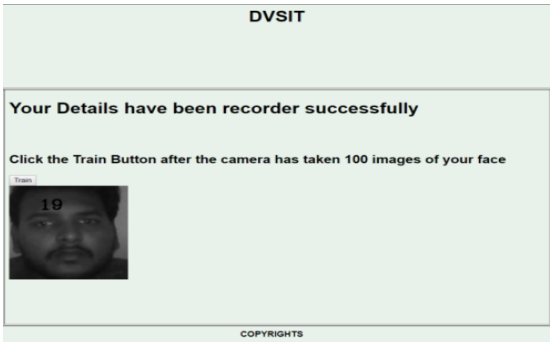

Fig. 9 Face Dataset Collection

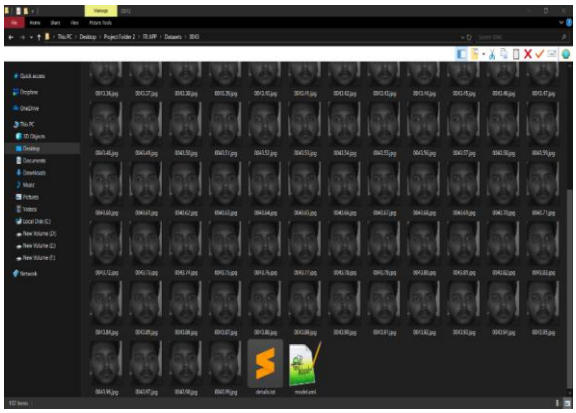

Fig. 10 Dataset in simulated Cloud Space

E. Login Page

The login page is to authenticate the user with his/her voterId as username and a password which is provided by the user during the registration phase. The current systems login page is shown in Fig. 11.

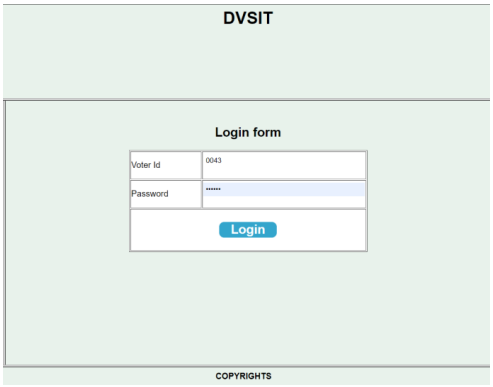

Fig. 11 Login Page

F. Face Recognition Page

After providing the correct credentials in the login page as shown in figure 11, the system will be re-directed to the Face Recognition page. The face recognizer shows the percentage of confidence of legitimacy of the user. And if the user face recognition result crosses a threshold of 85% then he/she is a legitimate user. The detailed results are shown in figures 12 and 13.

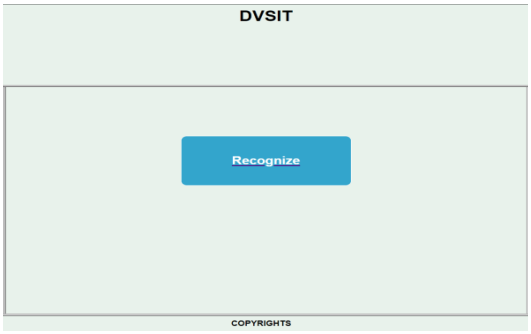

Fig. 12 After Login Page

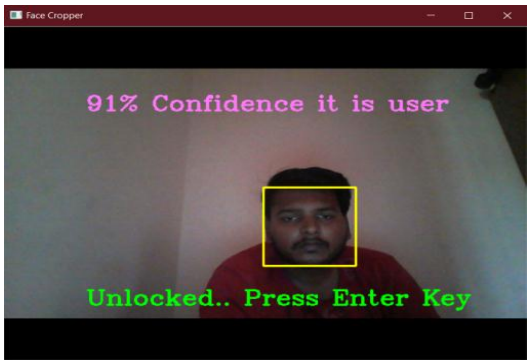

Fig. 13 Face Recognizer

G. Proceed to Vote Page

If a user passes through the face recognizer page then he/she is a legitimate voter and is allowed to cast a vote. The link to the voting page is provided in this page. And the respective result is shown in Fig.14.

Fig. 14 Proceed to Vote Page

V. CONCLUSION

Digital Voting System with Integrated Technologies (DVSIT) system can reduce the malpractices involved in present day's voting system by dual authentication. The confidentiality of the vote casted by the Voter and details of the Voter is maintained. Each and every casted vote will be counted and will be acknowledged to the Voter. The system generates a result chart of the elections. This proposed system operates better at the minimum low resolution of 35px to identify the human face in various angles, side poses and tracking the face during human motion. We designed the dataset (LR500) for training and classification. With the proposed methodology a better performance of the system is achieved on the designed dataset and this performance can be much improved in future by using updated blockchain servers. Other biometric and security levels can be involved to improve the security of the system in future.

REFERENCES

[1] P. Fredrik, Hjálmarsson and Gunnlaugur K. Hreiðarsson, "Block chain-Based E-Voting System", *IEEE 11th International Conference on Cloud Computing (CLOUD)*, pp.983-986, 2018.

[2] VarunGarg and KritikaGarg, "Face Recognition Using Haar Cascade Classifier", *Journal of Emerging Technologies and Innovative Research (JETIR)*, Vol. 3, No. 12, December 2016.

[3] Ali KaanKoç, EmreYavuz, Umut Can Çabuk and GökhanDalkiliç, "Towards Secure E-Voting Using EthereumBlockchain", *6th International Symposium on Digital Forensic and Security (ISDFS)*, pp. 1-6, 2018.

[4] Aftab Ahmed, JiandongGuo, Fayaz Ali and Farah deeba, "LBPH Based Improved Face Recognition At Low Resolution", *in International Conference on Artificial Intelligence and Big Data (ICAIBD)*, pp. 144-146, 2018.

[5] J. W. L. Chao, J. J. Ding, J. Z. Liu,"Facial expression recognition based on improved local binary pattern and class-regularized locality preserving projection", *Elsevier-Signal Processing*, Vol. 117, pp. 1-10, 2015.

[6] J. B. A. Olshausan and D. Field, "Emergence of simple-cell receptive field properties by learning a sparse code for natural images", *Nature Publishing*, Vol. 381, No. 6583, pp. 607-609, 1996.