iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 8 **Issue:** VI **Month of publication:** June 2020

DOI: http://doi.org/10.22214/ijraset.2020.6224

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 8 Issue VI June 2020- Available at www.ijraset.com

An IoT and Blockchain based Electronic Voting System

Asst. Prof. K. Raguvaran[1], Santhoshkumar R[2], Sowmiya K[3], Tharun Raj J[4], Vasanthapriyan C[5]
[1, 2, 3, 4, 5]*Electronics and Communication Engineering, K.S. Rangasamy College of Technology, Tiruchengode-636215*

Abstract: ***The objective of voting is to permit voters to exercise their right to precise their choices regarding specific issues, pieces of legislation, citizen initiatives, constitutional amendments, recalls and/or to settle on their government and political representatives. It has always been an onerous task for the election commission to conduct free and fair polls in our country, the largest democracy in the world. A lot of cash has been spent on this to form sure that the elections are rampage free. But, now- a -days it's become very usual for a few forces to enjoys rigging which can eventually cause a result contrary to the particular verdict given by the people. In order to provide inexpensive solutions to the above, this project will be implemented with biometric system i.e. finger print scanning. This is wont to make sure the security to avoid fake, repeated voting etc. It also enhances the accuracy and speed of the method . The system uses thumb impression for voter identification as we all know that the thumb impression of each person features a unique pattern. Thus it might have a foothold over this day voting systems.***
Nowadays, crypto currency has become a trending theme within the software package globe. Crypto currency may be a digital quality that's meant to operate as a dealings medium that utilizes sturdy cryptography to secure asset exchange and make sure plus transfer. Crypto currency is in addition spoken as digital suburbanized cash. Block chain stores knowledge concerning dealings which will be accustomed assess transaction trait. This voting system deals with multi chain block chain technology. We can define block chain as a digital transaction which is used to record financial transactions also as totally different transactions. As a result of the knowledge keep within the block chain isn't related to personal identifiable information, it's such a anonymity attribute. Blockchain allows dealings and verification to be clear. The options of this block chain technology are useful in powerful voting system, robustness, obscurity and transparency. The electoral system is our country's core. Verification of fingerprints employed in this theme to authenticate identity of electors.
Keywords: Blockchain, Voting machine, Fingerprint module (R307),Electronic voting

I. INTRODUCTION

Biometrics is that the science and technology of measuring and analyzing biological data. In information technology, biometrics refers to technologies that measure and analyze human body characteristics, like DNA, fingerprints, eye retinas and irises, voice patterns, facial patterns and hand measurements, for authentication purposes. In this paper we have used thumb impression for the purpose of voter identification or authentication. As the thumb impression of each individual is exclusive , it helps in maximizing the accuracy. A database is made containing the thumb impressions of all the voters within the constituency. Illegal votes and repetition of votes is checked for in this system. Hence if this technique is used the elections would be fair and free from rigging. Thanks to this technique that conducting elections would not be a tedious and expensive job.

II. LITERATURE SURVEY

Voting process is understood as a process for a gaggle by means of a gathering or democratic choose orders to require a free decision. This manner considers as the best normally found in republic and democratic governments (IDEA international, 2012).
Election systems have already existed in the past hundred years. All those earlier election systems, however had been considered being acceptable in past days, they started to reveal its disadvantages, day after day. These disadvantages, cause an enormous development within the design and elegance of electronic mechanical device . During 1961, the planning of electoral system s developed from manual base to electronic base where the primary electronic voting system was the electronic punched card system.
Currently information and communication technologies (ICT) have grown and became an important in every aspect of human been lives. The Information and communication technologies have big choice of applications starting from the entertainment, to applications within the areas of business, transportation, communications and etc.The supporters of the technology may believe that computer systems are effective, trusted and far more accurate, than humans, while the others believe that getting the humans guidance out of the scenario will increase the likelihood big errors may occur unnoticed. It is vital to face over what the previous researchers have already done before to be ready to defeat the issues of their e-voting machines and minimizing the problems may perhaps occur during the election process (Cetinnkaya, 2007).
Electronic voting machines contains three actors: people that will make the votes, registration authorities and tallying authorities.

All the Voters have the proper for voting; need to be register before the polling day so as to be eligible voters. These authorities confirm of only authorized people give their vote and that they must vote just one time during the election and then all the votes will be casted and show the final results of the voting (Anthony L, 2007).

III. PROPOSED SYSTEM

A biometric system is really a pattern recognition system that operates by acquiring biometric data from a personal , extracting a feature set from the acquired data, and comparing this feature set against the template set within the database. Depending on the appliance context, a biometric system may operate either in verification mode or identification mode. In addition, different from the manual approach for fingerprint recognition by experts, the fingerprint recognition here is referred as AFRS (Automatic Fingerprint Recognition System), which is program-based. An block chain technology incorporated with the system so the security is high.

System Architecture

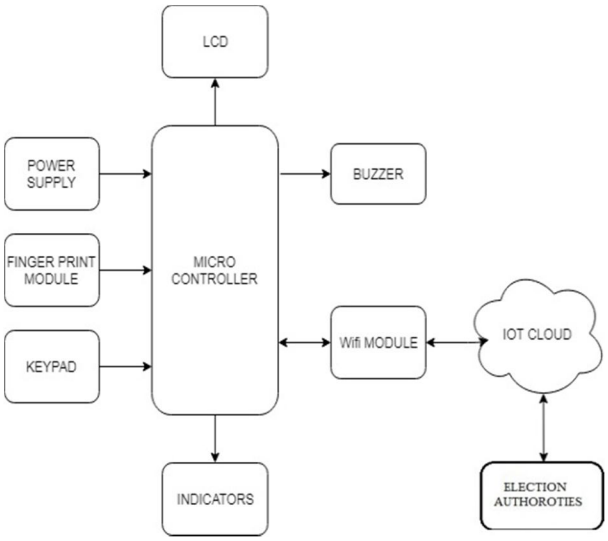


Fig. 1: Architecture of the System

A. Authentication using R307 Fingerprint module

Fingerprint processing technique consists of two stages-fingerprint enrollment and fingerprint matching [11].While enrolling; the user has to place the finger on fingerprint scanner two times. The system will process the two ti me finger image and will generate a template of the finger based on processing results and store the template in database.

Fig. 2: R307 Fingerprint module

Deployed on the cloud. While matching the fingerprint user needs to scan the finger through optical sensor and system will generate a template of the finger. Then it will compare it with templates of the fingerprint library in the central database .

In this process, the system will compare the live finger with specific template designated within the Module and in specific cases the system will search the whole fingerprint library for the matching finger. In both situations, system will return the matching result, whether it's success or failure.

B. Voting Process

Initially, the power supply is given to the system. Hence, the system is connected to the server through a wifi module. The server has the database of the votes such as voter Aadhar number and their personal details they are date of birth, name and address. Two ways of authentication are used to verify the voters. Who is voting for the first time and to identify the correct identify of the voters .The first authentication is fingerprint verification. Before that, all the voters' fingerprint details are enrolled and stored in the fingerprint module. The unique number is allocated for the each fingerprint template. At the time of voting, the voters scan their fingerprint by place the finger over a glass of the fingerprint module. It starts, scanning the current fingerprint and converted into a template. It matched with the already stored template. If both are matched, the voters are eligible to vote or else not. If suppose the voters is already votedthey try to vote again, the alarm or buzzer starts ringing. In another case, the voter database is not in the database, the message will display on the LCD, that is informed to the supervisor.

After this first step authentication, the voting switch are enabled. Next step authentication is for disabled people or who have injured in the finger. The person who has injured in the fingerprint, unable to vote. If a person has an injury, the scanner scans the finger and it does not give the correct output because the template is not matched .So to avoid this problem .The keypad is interfaced with microcontroller for verifying the voters identify. The voter has to enter their other number in that keypad. Those who will use the keypad for verification, they have to verify their details with supervisor before voting. If the voter identity is identified by either fingerprint or keypad, their details will display in the monitor.

The parties' names are displayed on the LCD. The voter can vote for any one of the party what they wish to vote. If the voter once press the button of the respective party. Then, the button again moves to unable state. Because this is to avoid, the voter to vote the multiple parties. The buttons are interfaced to wifi module. Each button has a unique number with that number the count of respective party will store in the server. The data which are sent to the server is in the form of encryption. The hacker cannot change the count of vote at the time of data transferring to the server. The wireless communication is established between the system and the server .The server has a specific IP address through that IP address the server can be accessed. Each switch connects to the wifi, through that only it can send the data, so each button has a specific directory to store the data in the server.

After the data stores in the server. The hackers can change the count off if the each party. To overcome this problem, block chain is used to protect the data from the hackers. The data's are stored in the form of blocks. If the data is stored in the server using block chain technology . The copy of the data sends to the nearby system. The copy of the data is in the form of log file and it stored in that system. The copy of data may be shared with any number of systems. The owner of the system does not know that he has the copy of the data .Suppose if they find the data where it is shared the copy of the data. The their person cannot change the data of the file. Because the data is not in the normal format .The data is not shared with the same system at all the time, it varies. For example, if first Data is sent to the server then connect it to some system for sharing and then next data is sent to the server, it may or may not connect the same system for sharing. The nearby system should enable the firewall option, then only, block chain will connect to the nearby system and send the data to that system. If the hacker change, the change the count of the party, block chain will cross check the data. Suppose if there any changes, the data will change according to the copy of the data which is shared to peer systems. The block chain technology used to prevent the change in the vote counting and provide security to the stored data.

C. TM4C123GXL(Microcontroller)

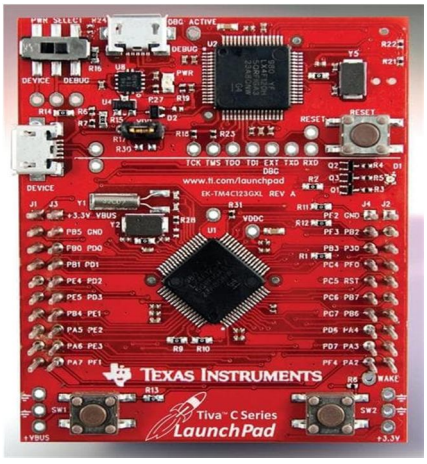


Fig. 3: Raspberry Pi 3B+ module

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 8 Issue VI June 2020- Available at www.ijraset.com

The design of the TM4C123G LaunchPad with a USB 2.0 device interface and hibernation module.The stackable headers of the Tiva C Series TM4C123G LaunchPad BoosterPack XL Interface make it easy.

1) Features

a) Low-cost evaluation platform

b) Includes a USB 2.0 device interface and hibernation module

D. LCD Display

It is combination of two states of matter, the solid and therefore the liquid. LCD uses a liquid to supply a clear image. LCD's technologies allow displays to be much thinner in comparison to beam tube (CRT) technology. This combination of colored light with the grayscale image of the crystal (formed as current flows through the crystal) forms the coloured image. This image is then displayed on the screen.

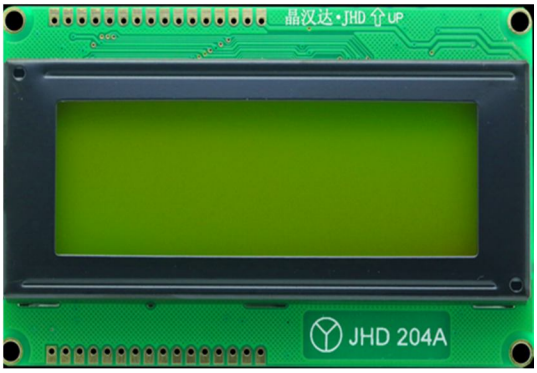


Fig 3:LCD display

E. IOT Cloud

For developers, an IoT platform provides a group of ready-to-use features that greatly speed up development of applications for connected devices also as lookout of scalability and cross- device-compatibility.Thus, an IoT platform are often wearing different hats counting on how you check out it. It is commonly mentioned as middle ware when mention how it connects remote devices to user applications (or other devices) and manages all the interactions between the hardware and the application layers.

F. BLOCKCHAIN

How Does a Blockchain Work?

Picture a spreadsheet that's duplicated thousands of times across a network of computers. Information persisted a block chain exists as a shared and continually reconciled database. This is how of using the network that has obvious benefits. The block chain database isn't stored in any single location, meaning the records it keeps are truly public and simply verifiable. Hosted by many computers simultaneously, its data is accessible to anyone on the web .To go in deeper with the Google spreadsheet analogy, i might such as you to read this piece from a block chain specialist.

G. 4X4 Matrix Keypad

There are 4 push buttons in each of 4 rows. And the terminals of the push buttons are connected consistent with diagram. In first row, one terminal of all the 4 push buttons are connected together and another terminal of 4 push buttons are representing each of 4 columns, same goes for each row. So we are getting 8 terminals to connect with a micro controller.

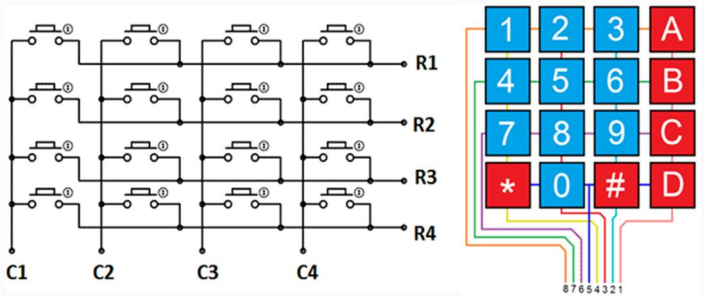


Fig 4: 4X4 matrix keypad

H. ESP8266

SP8266 comes with capabilities of

1) 2.4 GHz Wi-Fi (802.11 b/g/n, supporting WPA/WPA2),
2) General-purpose input/output (16 GPIO),
3) Inter-Integrated Circuit (I²C) serial communication protocol,
4) Analog-to-digital conversion (10-bit ADC)
5) Serial Peripheral Interface (SPI) serial communication protocol,
6) Pulse-width modulation (PWM).

It employs a 32-bit RISC CPU supported the Tensilica Xtensa L106 running at 80 MHz (or over-clocked to 160 MHz). External non-volatile storage are often accessed through SPI.ESP8266 module is low cost standalone wireless transceiver which will be used for end-point IoT developments.To communicate with the ESP8266 module, microcontroller needs to use set of AT commands.

a) V3: - 3.3 V Power Pin.
b) GND: - Ground Pin.
c) RST: - Active Low Reset Pin.
d) EN: - Active High Enable Pin.
e) TX: - Serial Transmit Pin of UART.
f) RX: - Serial Receive Pin of UART.
g) GPIO0 & GPIO2: - General Purpose I/O Pins.

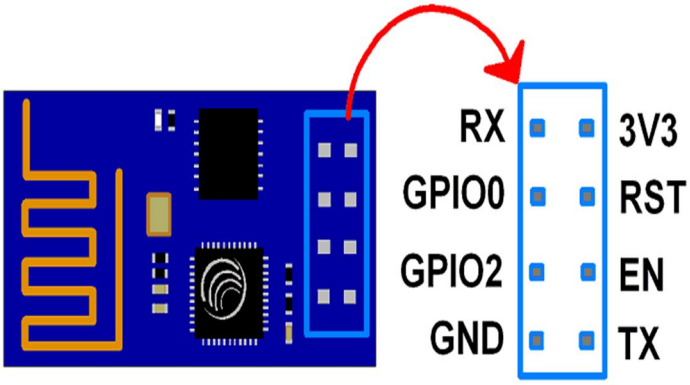


Fig 5: ESP8266

IV. CONCLUSION

Thus, here a voting system is discussed considering fingerprint matching process. The enrollment and authentication process is discussed in the proposed system. Also different techniques are analyzed. The main objective included developing strong matching algorithm using Digital Persona fingerprint algorithm and connect it to database for identification process and also used to store the data in database.

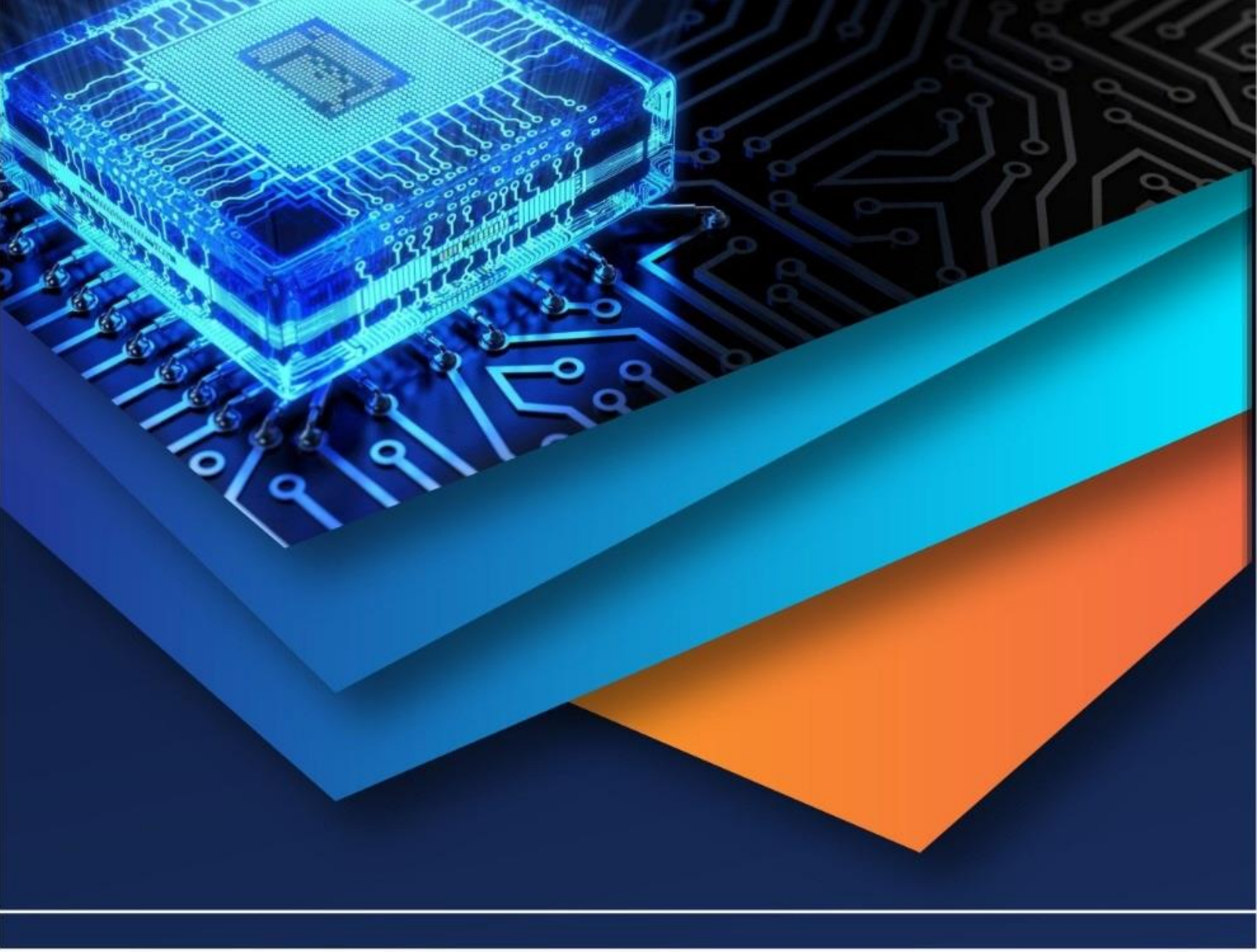
The accuracy of voter's identity and results are ensured with this voting system.The fingerprint module consists of high-performance fingerprint alignment algorithm and low power consumption. Because of the unique identity of every individual users, It is found that the fingerprint based voting system is best suitable in designing a proposed architecture.

Hence, a proposed system will implement a voting system with privacy & security using block chain technology. In block chain, each block contains a cryptographic hash of the previous block, a timestamp, and transaction data. A block chain is usually managed by a peer-to-peer network collectively adhering to a protocol for inter-node communication and validating new blocks. Although block chain records aren't unalterable, block chains could also be considered secure intentionally . The block chain database isn't stored in any single location, meaning the records it keeps are truly public and simply verifiable. An IoT platform is used.It helps for enrollment and authentication process.

It is used to store the data in the database. The voter casted their votes through the IoT based block chain technology, if there is any illegal activities happen or any changes happen it shows notification or alert message.This project can be used for secure voting since it overcome all the draw backs of ordinary voting machine also provide additional security. The system are often manufactured simply also as cheap.

REFERENCE

[1] Sathya v, “Block Chain Based Cloud Computing Model on EVM Transactions for Secure Voting’’,2019.
[2] Dong Zheng, "A Traceable Block chain Based Access Authentication System With Privacy Preservation in VANETs”,2019.
[3] Shitang Yu, "A High Performance Block chain Platform Intelligent Devices,"2018.
[4] N.Moses Babu, “Malware Detection for Multi cloud Server using Intermediate Monitoring Server,” 2017
[5] Kai Zhou, “PassBio: Privacy-Preserving User-Centric Biometric Authentication”, 2016
[6] Basit Shahzad, “Survey Trustworthy Electronic Voting Using Adjusted Blockchain Technology,” 2019.
[7] Y.Xiang, “Protection of Privacy in Biometric Data,” 2016.
[8] shafiqahmad, “Performance Analysis of Personal Cloud Storage Services For Mobile Multimedia Health Record Management”, 2018.
[9] Yao sun “Blockchain-Enabled Wireless Internet of Things: Performance Analysis and Optimal Communication Node Deployment”, 2019.
[10] Vijay Varadharajan “Security as a Service Model for Cloud Environment”, 2014.
[11] Muhammad Raisul Alam, “Design and Implementation of Microprocessor Based Electronic Voting System’’,2015.
[12] Orhan Cetinkaya, " Analysis of Security Requirements for Cryptographic Voting Protocols”,2014.
[13] Supeno Djanali, Design and Development of Voting Data Security for Electronic Voting (E-Voting),"2016.
[14] Kanika Garg, “A Comparitive Analysis on E-Voting System Using Blockchain,” 2019.
[15] A.M.Jagtap,“ Electronic Voting System using Biometrics, Raspberry Pi and TFT module.”, 2019.
[16] Lucie Langer, “Towards a Framework on the Security Requirements for Electronic Voting Protocols,” 2015.
[17] Haijun Pan, “E-NOTE:An E-voting System ThatEnsures VoterConfidentiality and VotingAccuracy,” 2012.
[18] Adria Rodriguez-Perez, “Secret Suffrage in Remote Electronic Voting Systems” , 2017.
[19] Z.A. Usmani “Multi-purpose platform independent online voting system”, 2017.
[20] Melanie Volkamer “Vote casting device with VV-SV-PAT for elections with complicated ballot papers”, 2014.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY