Journal of Research Administration
Society of Research Administrators International

DESIGN OF A USER AUTHENTICATION SYSTEM & DATA SECURED HARDWARE PROTOTYPE MODEL OF A NEXT-GEN INTELLIGENT VOTING SYSTEM BASED ON BLOCKCHAIN & IOT

Sandeep. K.V. & Dr. T.C. Manjunath

[1]Research Scholar, VTU Research Centre, Dept. of Electronics & Communication Engineering,
Dayananda Sagar College of Engineering, Bengaluru-560111, Karnataka
Visvesvaraya Technological University, Belagavi-590018, Karnataka &
Assistant Professor, Electronics & Telecommunication Engineering,
Dayananda Sagar College of Engineering, Bengaluru-560111, Karnataka
Email: sandeep.kv38@gmail.com

[2]Research Supervisor, Professor & HOD, Dept. of Electronics & Communication Engineering,
Dayananda Sagar College of Engineering, Bengaluru-560111, Karnataka
Visvesvaraya Technological University, Belagavi-590018
Email: tcmanju@iitbombay.org

Abstract:

On this day, abstention rates continue to rise, primarily due to the inconvenience of traveling to vote. This is why the implementation of remote e-voting is crucial in increasing voter turnout. By enabling everyone to vote without the need for travel, remote e-voting not only addresses this issue but also streamlines the voting process, delivering faster and more accurate results compared to traditional paper ballots. Given the significant importance of elections, it is imperative that any remote e-voting solution meets the highest standards of security, reliability, and transparency to instill trust among citizens. In the realm of literature, numerous remote e-voting solutions based on blockchain technology have been proposed. Blockchain technology is increasingly recognized as a cutting-edge technical infrastructure for various IT applications, as it eliminates the need for a trusted third party and decentralizes transactions, all while ensuring transparent and highly secure data storage. Moreover, it offers the capability to incorporate smart-contracts technology, which automates and executes agreements between users. In this paper, our focus lies in critically examining the most promising e-voting solutions based on blockchain technology. By doing so, we aim to shed light on the potential of these solutions and their ability to revolutionize the voting process. We are currently working on addressing the challenges within the current systems by integrating them with Arduino, a microcontroller that facilitates communication with peripherals. Our objective is to enhance efficiency and prevent any fraudulent activities like unauthorized voters. Additionally, we have incorporated a fingerprint sensor and assigned a unique identification number for authentication purposes. These measures ensure a seamless secured voting process, allowing voters to conveniently cast their votes from any location. This user-friendly approach ensures that all participants can easily exercise their voting rights safely without going to their actual location.

Keywords - Security, Internet of Things, Elections, Voting system, Blockchain technology, Unique identification number, Fingerprint sensor decryption, encryption,

1. Introduction

If an advanced electronic recognition method is created to detect the voter, then the acts of neglect can be halted and it will encourage the surveying authorities in their work. In that course for helpful voting this paper is proposed and Radio-Frequency Identification (FPR) based native ID is used. Voting apparatus are the aggregate mix up of the mechanical, hardware, or electromechanical together with software and records required to control the program which is utilized to characterize votes; to cast and count votes; to report or show election outcomes and to keep up and deliver any review trail data. The principal of voting machines was mechanical yet it is progressively more regular to utilize EVMs.

Generally, option mechanisms are 1 by the instrument the framework uses to allow votes and to boot sorted by the world wherever the framework organizes the votes. Option equipment have distinctive levels of simple use, security, productivity and preciseness. Bound frameworks may well be just about hospitable all voters, or not on the market to those voters with bound kinds of handicaps. They'll likewise have an effect on folks in general's capability to control elections.

At present some individual makes the pretend citizen IDs and to evade creating such IDs, FPR tag is employed as citizen ID card which boosts the safety execution and keeps faraway from pretend option. FPR reader sends the data to the P89V51RD2 s. The P89V51RD2 s is given the data of each and every person. Following FPR reader causing the ID to the s, it tries to match up the ID with its info base. On the off probability that the ID is matched it permits the individual to vote.

If it's incorrect, 16*2 liquid crystal presentation LCD numerical display s display} interfaced with an s can display "Unauthorized User/Finger" with beeper wide- ranging. At the top the controller program can calculate the full option. At that time by victimization GSM technology the full option info is distributed to Taluk workplace information base or central station so it'll be displayed on the laptops at the central station.

(A) Authentication

Prior to granting access to a system or resource, authentication is the process of confirming a user or device. Its a procedure for confirming a user's or piece of information's identification. Confirming a person's identity when they connect into a computer system is known as user authentication. This assures that only user's with authorized credentials gain access to secure systems. When a user attempts to access the info on a network, they must provide secret credentials to prove their identity. Upon authentication, can be granted permission to the user with confidence. Authentication is part of a three-step process for gaining access to digital resources:

(i) Identification - who are you?

(ii) Authentication -Prove it.

(iii) Authorization - Do you have permission?

Identification requires a user ID like a username. But without identity authentication, there's no way to know if that username actually belongs to them. That's where authentication comes in—pairing the username with a password or other verifying credentials. In this proposed method, authentication is a done by verifying login username and password.

(B) Authorization

A server assesses if a client has permission to utilize a resource or access a file through the authorization procedure. Authorization with authentication are frequently combined so as to server can identify the client making the access request. Different types of authentication may be required for authorization; some may not require passwords. In some circumstances, authorization is not required; any user may access a resource or a file by requesting it. Most Internet web sites don't need authorization or authentication. Once a person or process is authenticated, they're often put through an authorization procedure to assess if they should be granted permission to a certain protected resource or system. If fails in user authorization, not permitted to access data.

Lot of confusion between the words authorization and authentication. Before granting access to secure networks and systems, an authenticated user or process's identity is verified. Authorization, a more detailed procedure, verifies that the authenticated user or process has been given authorization to access the requested resource. Access control describes the procedure used to limit particular users' access to such resources. Always, the authorization procedure happens after the authentication step.

2. LITERATURE REVIEW

Year	Author	Technique	Paper Title	Work Focused	Future Work
2014	"Jhani Bhasha Shaik, Mazhar HussainShaik"	OTP	Elector identification also Detection System consuming FPR and GSM to halt Rigging in the elections	To develop the election Development and to avoid rigging expending FPR & GSM technologies	Face detection technologyto identify the voter
2015	B. Madan Mohan Reddy, D. Srihari	Finger Print Technology and Alcoholic sensor	FPR Based Biometric 1 Voting's Machine Linked To Aadhaar For Safe & Secure Voting	Using sensors alcoholic persons are detected at the polling station	Face recognition based retinal scan method

2014	Ashok Nalluri, B. BhanuTej, A.Balakri hna	Finger Print Technology	FPR and Thumbprint Acknowledgment based Electronic Voting System for Real Time Application	Human finger print is used to caste the vote	Touch screen systems
2014	Vaibhav Bhatia, Rahul Gupta	GSM technology	"Design of a GSM Based Electronic Voting Machinewith Voter Tracking"	"All votes are sent to themonitoring station via GSM"	Further improved in terms of power consumption using advanced VLSI application
2013	Sanjay Kumar, ManpreetSingh	Fingerprint biometrics	"Design secure electronic voting system using fingerprint technique"	Eliminating bogus voting andvote repetition	FPR and GSM technologies
2014	ChinnaV Gowdar, P alle Jeevan Kumar,A kash Reddy R. S, Santosh Kumar, Sameena	.NET with cryptography technique	Convenient voting machine	On-Line and Offline e- voting	Facial recognitio n, Finger Veinand iris matching detection

3. Overview of Voting System

A voting system is a technique that the people resolve on a choice stuck between alternatives, regularly during a contest. A selection framework upholds guidelines to have substantial voting, how the votes are counted and aggregative in the direction of giving very last result. The Common voting techniques are standard, relative depiction or majority balloting with an assortment of varieties. Through greater measurement governing, individuals who are fresh to the ballot vote hypothesis can be generally stunned that there is another voting framework, or differences can exist over the meaning of what that it intends to be upheld by a majority. On the off chance that each decision had exclusively two options, the title holder would be resolved utilizing majority govern alone. However, when there are three or additional choices, there may not be a single option

that is most liked or most disliked by a majority. Convenient voting system innovation can increase speed of work and save money from government also can give! Improved availability to the disability voters. In any case, there has remained dispute, mainly in the US, DRE voting, could encourage appointive misrepresentation.

Moment spillover voting was formulated in 1871 by American planner William Robert, despite the fact that it is, essentially, an exceptional instance of the single transferable vote framework, which developed freely in 1850.Not at all like the single transferable vote in multi-seat races, in any case, are the main poll exchanges from customers of applicants who have been disposed of. The principal known utilization of an IRV-like framework in a legislative decision was in 1893 in a race for the frontier legislature of Queensland. The variation utilized for this race was an "unforeseen vote". IRV in its actual structure was initially utilized as a part of 1908 in a State race in Australia. A selection framework upholds guidelines to have substantial voting, how the votes are counted and aggregative in the direction of giving very last result. The Common voting techniques are standard, relative depiction or majority balloting with an assortment of varieties.

IRV was presented broadly in Australia in 1918 after by-election, because of the ascent of the traditionalist country party, speaking to little agriculturists. Country party tears the counter labor vote in moderate nation regions, permitting Labor contender to succeed on marginal vote. The preservationist administration of Hughes presented particular voting as a method for permitting rivalry between the two traditionalist gatherings without putting seats at danger. It was initially utilized at the by-election in 1918. Thomas and Andrew had already presented it in the assembly of Tasmanian House. The people in an IRV race rank hopeful on a particular voucher. IRV frameworks being used in various nations fluctuate both as to tally plan and in the matter of regardless of whether voters are obliged to give a full rundown of inclinations.

The behaviors of elections have been changed from numerous points of view in the course of recent years. The degree of these progressions is pleasantly delineated by a correlation of today's voting rehearses with those represented in George Bingham's sketch as appeared in Fig 1. Notwithstanding being a critical craftsman, George was a fruitful government official; this artistic creation demonstrates a surveying place on the progressions of the courthouse in Missouri during 1846.

Fig. 1: The country election.

In this sketch, the judge (top focus) directing a promise to a voter. The person (wearing red shirt) is swearing, by means of his hand on the book of scriptures, that he is qualified for vote and has not officially done as such. There was no arrangement of voter enrollment, so this vow and the likelihood that the judge or another person in the region of the surveys may remember him on the off chance that he returned was all that kept a voter from voting over and over.

Here it was no privilege to a mystery ticket; having been confirmed, the voter basically got out his decisions to the election representatives who sit on the patio behind the judge counting the vote. Every assistant will be having poll book where he composes the voter's name and records his votes; different poll books are a typical barrier against administrative blunder. There are a few people in the work of art grasping paper tickets. These were not paper tallies since Missouri kept on utilizing voice voting until 1863. In a general decision, in any case, numerous voters may have needed to convey their own notes to the surveying place.

(A) BALLOT VOTING

Voting using the gadget when votes are cast during an election. It can be a bit of paper or ball used as part of a secret ballot. In British English, this is often referred to as a "ballot paper" as shown in fig. 2.

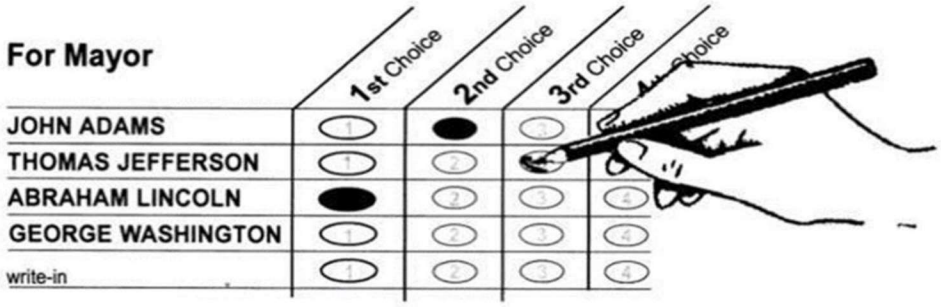

Fig. 2: Paper ballot

The term voting is used in an election method within an organization. Every voter uses 1ballot, and voting is not a separate ballot. In a primary election, voting can be the beginning of a direct thesis that each voter names the candidate; but administrative decisions make use of pre-print use to protect the confidentiality of votes. The voter throws his vote into the crate at the polling station. The normal approach to rundown candidates on a tally paper is one after another in order or by arbitrary part. At times hopefuls may likewise be gathered by political gathering. On the other hand, Robson rotation includes the arbitrarily changing competitor request for every turn out run. Wherever the special voting is utilized for the decision of a gathering or committee, gatherings and competitors frequently guide their followers on their minor inclinations, particularly in Australia in which an elector have to grade all contender to cast a legitimate ticket. This can prompt "inclination bargains", a type of pre-decision dealing, in which littler gatherings consent to coordinate their voters consequently for backing from the triumphant party on issues essential to the little party. Though, this depends on the supposition that followers of minor gathering will check inclinations for another gathering in light of the counsel which is given to them. Most IRV decisions truly have been tallied by manually. In the advanced period, voting hardware can be utilized to control the tally either in part or completely.

(B) ELECTRONIC VOTING MACHINE

EVMs are controlled by a normal 6v alkaline battery This configuration permits the utilization of electronic voting machine (EVM) all through the nation with no interferences in light of the fact that few sections of India can't have power supply and/or flighty force supply. In electronic voting machine (EVM) the person should go to particular voting station for voting where he got the voter ID. EVM consists of 2 units: A Balloting unit which is used by the voter caters up to 16 candidates are control units which is monitored by polling/higher officers. Rather than giving ballot sheet, polling officials accountable for the control unit going to squeeze button on the ballot. It helps the voters to make he/her choice by squeezing the blue color key/switch on balloting units adjacent to his preferred applicant and picture Utilized as a part of EVMs is programmed forever on the silicon at the period of fabricating by the producer. Nobody (as well as the producer) can alter the controller program after fabricating the controller. At present, an EVM will record the greater part of 3840 votes, which is adequate for a surveying station as they for the most part have close to 1400 voters doled out as shown in Fig 3.

Fig 3: Electronic voting machine

Here first the thumb impression is taken in a register. Election officer puts an ink mark on the finger of the voter and gives slip that has voter enlistment number. This slip is given over to the managing officer who affirms the series number and allows the voter to vote. In the balloting unit voter needs to press the blue switch. When it is pressed LED will blink and machine makes a sound. This shows that vote has been casted correctly and choice has been enrolled in the control unit. The quantity of votes in favor of particular competitors figured naturally and at the tallying place, just the control unit is required for delivering the aftereffect of the survey at the surveying station. It is impractical to vote for the 2nd time by squeezing the switch more than once. When a specific switch on balloting unit is squeezed, vote is counted for that specific competitor then device is automatically locked. Regardless of the possibility that one squeezes the switch further or some other switch, no more votes are counted.

EVMs are can't be pre-modified to support a gathering or a hopeful in light of the fact that the request in which the candidate's name shows up on the voting station relies on upon the request of documenting of selections and legitimacy of the candidature, this succession can't be anticipated ahead of time. EVM for surveying stations is customized by PC choice keeping the development learning of task of particular EVMs to surveying stations. As the EVMs make use of a battery of 6V, so that truly no danger of any voter getting an electric stun. EVM costs up to 5,500rs during the time of 1989- 1990. Despite the fact that the early venture was very costly it was more than killed by the funds in the matter of creation and printing of tally sheets in lakhs and the significant diminishment in the numbering employees and the compensation paid to them.

(C) Direct Recording Electronic Voting Machine

The DRE ("Direct Recording Electronic") voting machine polls by means of a voting displays needed electronically by a voter that provides information on the PC programs and controls the voting information's and memory components are used as shown in Fig. 4.Subsequent to the election it generates an organization of the voting information put present in a removable recollection segment and also as printed duplicate copy. Scheme may similarly give a way to

communicating singular polls or vote sums to a focal area for merging and exposure results from areas at the important area. These schemes utilize a region number strategy that classifies the tickets at the surveying place. They commonly organize the tallies as they are thrown and print the outcomes after the end of surveying.

(D) Punched Card Voting Machine

Voting by punching openings on paper or cards began during 1890s and creators kept on investigating these cards during the days that were followed. The primary real accomplishment of punched cards introduced during 1965, with Harris. Improvement of the Votomatic punched card framework. It is depended on IBM's Port-A innovation. Harris authorized the Votomatic to IBM Rouverol fabricated the model framework.

Fig. 5 Punched card voting machine

4. Implementation and Methodology

The aim of the applications of this development is to providing a facility for public to the cast their valuable vote from whichever location they are. During election process, if voters are not in their town and they want to cast their vote for candidates of their choice then they can vote from whichever location they are using this proposed system. It is not necessary for them to come and cast their vote in their particular polling station.

Here first the thumb impression is taken in a register. Election officer puts an ink mark on the finger of the voter and gives slip that has voter enlistment number. This slip is given over to the managing officer who affirms the series number and allows the voter to vote. In the balloting unit voter needs to press the blue switch. When it is pressed LED will blink and machine makes a sound. This shows that in existing system ballot is finished by victimization electronic mechanical device (EVM) during which the person ought to visit specific ballot station for ballot wherever he got the citizen ID. EVM consists of two units: a voting unit that is employed by the citizen caters

up to sixteen candidates and an effect unit that is monitored by polling officers. Vote has been casted correctly and choice has been enrolled in the control unit.

Figure 5 below indicates the design flow of the proposed system. First the LCD, UART and GSM are initialized. Swipe the card in the FPR reader if the card is invalid then swipe again otherwise LCD will display the station to which the voter belongs to and candidates of his/her station. Then press any key to cast a vote. After pressing the key it is incremented so that no one can press the key for the second time which avoids fake voting. If the voting is over then wait for the acknowledgement from the central station and message is send to the central/Taluk station. Results are exposed in the PC and acknowledgement is sent to both the stations.

To overcome from these disadvantages of electronic voting machine this system is proposed. Here FPR tag is used which has the unique ID that avoids malpractice and person can vote to his choice of candidate from any voting station irrespective of the place he belongs to. LCD can be used for the proper display of information and to avoid losing of voting information s can be used to store information about the voter. The System has details of all elector. System receives the main points from the FPR reader that it tries to match these details with its hold on info disreputable. If these specifics match then it permits the individual to vote. If it's incorrect, 16*2 liquid crystal display connected to a can display as “unauthorized finger” with buzzer sound. At the tip the controller program can calculate the overall balloting then by victimization GSM technology the overall 1 info is shipped to central station information base then this info is displayed on computer at the central station.

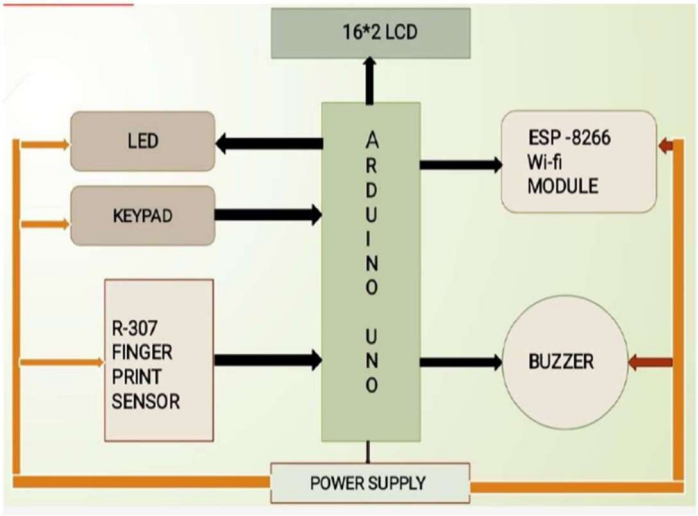

Fig 5: Block diagram for voting system

Voting station 1 or city 1

Here the two stations area unit thought of to indicate the person will vote from any balloting station. In existing system if the person has citizens identifying happiness to balloting station one he has got to choose that exact station for balloting, albeit he's out of station.

But in this proposed system person is provided with FPR tag which has a unique finger identified so that he can cast his vote in voting station 2 even though he belongs to voting station 1 as revealed in Fig 3.5. The Fig 3.6 shows central or Taluk office/district office.

5. FLOW CHART & ALGORITHM

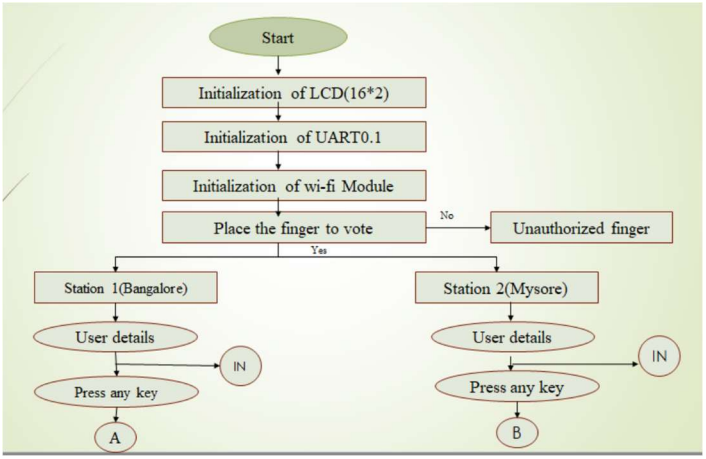

Fig. 6: Flow chart

In this work, 16*2 LCD is the output module that has been controlled by Arduino Uno. When citizen places finger print reader, the scanner can read the images of the finger and sends to the Arduino Uno controller. It has details of every citizens receives the data from the finger print reader, that it tries to check these details with its hold on information to base on the system. If an information match it permits somebody to vote. If incorrect finger LCD digital displays interface with an s display "Unauthorized finger" with beeper sound. Keys or Switches are used for choosing the option preferences voters. After completion of the voting process.

The database is printed victimization of Embedded C language. This program is Arduino sketch software are used and damping to the Arduino Uno controller. On the tip of the generation the Arduino uno controller software package can calculate the entire option. At that time by victimization GSM. Technology the entire option details is distributed to central/Taluk office sation and these particulars are square messure show on laptop.

6. Results & Discussion

The outcomes of the work is equivalent as proposed system hardware model and the components that are interfaced are discussed in this section. The proposed system hardware perfect is shown in below Figure 7 & 8. In this proposed system person is provided with finger scanner which has a unique ID so that he/she can cast his vote in Voting station 1 even though he/she belongs to Voting station 2.

System is designed with 4 switches i.e., 4 candidates BJP, Congress, JDS and Others. When voter's finger place to the finger scanners his/her information stored in arduino mega 2560 system will be

displayed on LCD and after pressing particular switch vote has been casted to the particular candidate.

Fig 7: Voting station 1

Fig 8: Voting station 2

All the components such as FINGER PRINT, WI-FI Module, LCD and switches are interfaced with the Arduino UNO s is as shown in Fig 9.

Fig 10: Status when power switch is turned on.

Fig 11: Voting System readiness status

After some delay LCD shows the ready status by showing the information as in fig. 11. If the user is biometric authenticated & valid, then LCD shows the voter information such as his/her name and station he/she belongs to. For example Bangalore south as shown in fig 11.

Fig. 11: Voter Information

If the person is a unauthenticated user, or invalid person who does not match with Arduino UNO system database, then LCD displays as Unauthorized Finger with the buzzer sound as shown in fig 12.

Fig 12: Unauthorized Voter

Next, the voter named UMM EA ASFIYA, even though he is from Station 1, he can vote from station 2 showing that the voter can vote from any voting station as shown in fig 12. Vote can be casted by pressing on the particular switch to the candidates of his/her station as shown in Fig 14.

Fig. 13: Voter Information after Authentication

Fig. 14: Parties in station

If voter tries to vote for the 2nd time LCD displays as “You already Voted” as shown in Fig 15. This system avoids fake voting.

Fig. 15: Warning details of 2nd vote

After all the votes have been casted at the particular station, polling officials must Place the finger and authenticate themselves. If the officials are authorized, system will communicate with server

or significant station as shown in Fig 16. Voting information is transferred or sending results to central station

Fig. 16: Polling results

8. Conclusion

The proposed system shows promising results, as the active FPR technique used for identification purposes contains voter details. Arduino maga2560 system is used which has special features like ISP and IAP. This system is designed with some advantages that the voter can vote for the constituency related to any station. So that 100 percent polling can be done, human intervention is reduced and chances of reunification are also less. Data centralization is used, that is, after polling all polling details are sent to the respective server. Therefore, it avoids human intervention. GSM technology is used to transmit polling details. This system avoids fake voting, it can definitely identify who all are voting and not even ballot.

9. Future Scope

The system security can be improved using face recognition, eye-ray scanner, and touch screen systems in future. For creating large database, the server-based system can be used. Battery can be used instead of AC supply because battery is a good option in case of power failure while voting.

REFERENCES

[1] Jena Catherine Bel.D, Savithra.K ,Divya.M , “A Secure Approach for E-Voting Using Encryption and Digital Signature”, *International Journal of Engineering Development and Research., JETIR*, Vol. 8, Issue 1, January 2021.

[2] Cosmas Krisna Adiputra, Rikard Hjort, and Hiroyuki Sato, “A Proposal of Blockchain-based Electronic Voting System”, *Second World Conference on Smart Trends in Systems, Security and Sustainability* , Oct 1 ,2018.

[3] Ashish Singh,Kakali Chatterjee, “Secure Electronic Voting System Using Blockchain Technology”, *International conference on Computing, Power and Communication Technologies (GUCON),* Galgotias University, Greater Noida, UP, India. Sep 2018.

[4] G.Saranya, R.Mahalakshmi, J.Ramprabu, “Smart Electronic Voting Machine surveillance”, *International Journal of Engineering and Advanced Technology (IJEAT),* ISSN: 2249 8958, Volume-8, Issue- 2S, December 2018.

[5] Girish H S, Gowtham R, Harsha K N, Manjunatha B, "Smart Voting System", *International Research Journal of Engineering and Technology (IRJET)*, Volume: 06 Issue: 05, May 2019.

[6] B.Mary Havilah Haque, G.M.Owais Ahmed, D.Sukruthi, K.Venu Gopal Achary, C.Mahendra Naidu, "Fingerprint and RFID Based Electronic Voting System Linked with AADHAAR for Rigging Free Elections", International journal of advanced research in electrical, electronics and instrumentation engineering, Vol. 5, Issue 3, March 2016.

[7] X. Sun, Q. Wang, P. Kulicki, and M. Sopek, "A simple voting protocol on quantum blockchain", *International Journal of Theoretical Physics,* vol. 58, no. 1, pp. 275–281, 2019.

[8] Sandeep K.V., Dr. T.C.Manjunath, "Design and implementation of security mechanism by user authentication for voting system based on Fernet encryption and Blockchain technique", Scopus Indexed Journal Article, SCImago Journal & Country Rank - Quartile 3 (Q3) Journal, SJR 2022 Rating 0.25, *Journal of European Chemical Bulletin*, Section A-Research paper, e-ISSN 2063-5346, H-Index 11, Vol. 12, Special Issue 6 (Si6), pp. 3354 – 3369, 2023.

[9] Sandeep K V, Dr.Sayed Abdulhayan, "Implementation of Data Integrity using MD5 and MD2 Algorithms in IoT Devices", *Palarch's Journal Of Archaeology Of Egypt/Egyptology-PJAEE(Scopus Q3), vol. 17, no. 7, pp. 7388 - 7395, ISSN: 1567-214X, Nov. 2020.*

[10] Sandeep K.V., Manjuanth T.C., "A Novel Mechanism for Design and Implementation of Confidentiality in Data for the Internet of Things with DES Technique", *6th IEEE International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)*, I-SMAC 2022, Dharan, Tribhuvan University, Purwanchal Campus, Nepal, IEEE XPLORE COMPLIANT ISBN: 978-1-6654-6941-8, IEEE DVD Part Number: CFP22OSV-DVD; ISBN: 978-1-6654-6940-1, Paper ID 561, 10-12, pp. 109-114, November 2022. DOI:10.1109/I-SMAC55078.2022.9987268.

[11] Dr. T C Manjuanth., Dr. Sandeep K.V., "Development of the Implementation of Secured Data Communication on IoT Applications with hardware prototype development in IoT Devices", *Indian Patent No. 202341067445*, October 13th 2023.

[12] "Design & implementation of security mechanism by user authentication for voting system based on Fernet encryption and blockchain technique", *adapted from Copyright by Dr. Sandeep K.V., Dr. T C Manjuanth*, Oct 2023, Diary No. 27462/2023-CO/L

[13] Sandeep K.V. & Dr. T.C. Manjunath, "Design & Implementation of data privacy & security using IoT sensors in remote health monitoring system", Tuijin Jishu / Journal of Propulsion Technology, ISSN: 1001-4055, Indexed by Elsevier Scopus, SCI Q3, SJR 2022 – 0.32, SNIP 2022 1.069, H-Index 24, CiteScore 2022 1.1, DOI : 10.52783/tjjpt.v44.i4.1837, Vol. 44, Issue 4, pp. 4996 – 5007, Oct-Dec. 2023