A Conceptual Framework for the Integrated, Smart and Secure Remote Public Voting System (SSRPVS)

Vinayachandra[1,2], Geetha Poornima K[1,2], Rajeshwari M[1,2] & Krishna Prasad K[3]

[1]Research Scholar, College of Computer Science and Information Science, Srinivas University, Mangalore, India

[2]Assistant Professor, Dept of Computer Science, St Philomena College, Puttur, India

[3]College of Computer Science and Information Science, Srinivas University, Mangalore, India

E-mail: veeciashu@gmail.com

Area/Section: Information Technology.
Type of the Paper: Conceptual Research.
Type of Review: Peer Reviewed as per |C|O|P|E| guidance.
Indexed in: OpenAIRE.
DOI: http://doi.org/10.5281/zenodo.3934459.
Google Scholar Citation: IJMTS.

How to Cite this Paper:
Vinayachandra, K., Geetha Poornima, M., Rajeshwari & Krishna Prasad, K. (2020). A Conceptual Framework for the Integrated, Smart and Secure Remote Public Voting System (SSRPVS). *International Journal of Management, Technology, and Social Sciences (IJMTS), 5*(1), 318-334. DOI: http://doi.org/10.5281/zenodo.3934459.

International Journal of Management, Technology, and Social Sciences (IJMTS)
A Refereed International Journal of Srinivas University, India.

A Conceptual Framework for the Integrated, Smart and Secure Remote Public Voting System (SSRPVS)

Vinayachandra[1,2], Geetha Poornima K[1,2], Rajeshwari M[1,2]& Krishna Prasad K[3]

[1]Research Scholar, College of Computer Science and Information Science, Srinivas University, Mangalore, India

[2]Assistant Professor, Dept of Computer Science, St Philomena College, Puttur, India

[3]College of Computer Science and Information Science, Srinivas University, Mangalore, India

E-mail: veeciashu@gmail.com

ABSTRACT

Elections are the backbone of democracy. It is through elections that individuals assert their voice, their perspectives, and choose a person whose philosophies most complement them. Elections allow citizens to choose their representatives. They are also important for the people to express their resentment at the ruling government. When there is high voter participation, the election process is considered successful. Unfortunately, developing countries such as India are facing a decline in the turnout. People in rural areas move to metropolitan cities or other countries, in most developing countries to make their livelihood or schooling. During elections, visiting their hometown and casting their votes becomes burdensome for them because of their commitment to their workplace. Challenges in moving to poll places and sometimes adverse weather conditions, cause people to miss the chance to choose the candidate of their choice. People with disabilities and senior citizens also refuse to go to the polling station due to travel-related difficulty. Therefore, many elections record only 50-70 percent electoral turnout, sometimes, even less than 50%. Only when all eligible voters are granted fair opportunities to exercise their franchise then only such a democratic system is considered fool proof. The need for the hour is such a fool proof framework that enables all eligible voters to cast their vote by visiting Polling Station or doing so remotely. This paper proposes a conceptual framework for the Integrated, Smart, and Secure Remote Public Voting System (SSRPVS) that allows voters from any part of India to exercise their franchise without moving place to place and wasting time and money. To develop the Framework, emerging technologies such as IoT, Cloud Computing, Edge Computing, Blockchain, and Data Analytics are included. The system will guarantee security through four different levels, Smart Voting Card based on RFID, One Time Password, Thumb Recognition, and Retina Recognition. The only theoretical model of the system that is open for further analysis and development is provided here.

Keywords: Electronic Voting, E-Voting, Security, Blockchain, Cloud, IoT, Remote Voting, RFID.

1. INTRODUCTION :

India is considered the world's largest democracy with over 130 billion population and over 92 billion eligible voters. True to its spirit of democracy, the legislature and executive powers are decentralized and distributed to different administrative settings, from central to local governance. Parliament at the helm is supported by State Assemblies, Municipal Corporations, Zilla Panchayats, Taluk Panchayats, Town Municipal Councils, and Gram Panchayats. Representatives of these different administrative institutions are elected through the general election process. Though the term of these elected bodies is either five or six years, mid-term elections may necessitate on several occasions due to political or administrative reasons. Thus, in general, one in any part of India may witness major elections every six months. Because of the logistics involved in the

process, it is a herculean task for the Election Commission to coordinate the election process. According to the current framework, the Commission is opening Polling Stations in designated places based on the number of eligible voters, where the voters have to come and vote. Any other voters must physically come to the polling station to exercise their ballot, other than the people participating in the voting process and the State serving personnel; they have the option of postal ballot. They have no other option left out in exercising their franchise. Most of the time, voters may be working in different locations, or they may be traveling, or they may be studying in faraway places, losing their chances of voting because it's not so convenient for them to come to the polling stations and caste voting. Also, there may be a fear of getting bullied into voting for someone who is not of their choice. The reasons may be administrative or economic.

As technology usage increases every passing day, transaction security is needed more. Secure Internet-based transactions include online shopping banking, tax payment to payment of instalments, and license renewal for vehicle insurance. The Internet can also be used in a certain way to allow secure elections. Many classes of people, including military personnel, overseas citizens, businessmen, physically challenged people, elderly people, sportsmen, college students, etc. will benefit from the chance to vote from anywhere. Due to its remarkable limitations, conventional paper-based ballots have become outmoded. But apart from the performance aspect, electronic voting machines raise issues like security, privacy, digital divide, etc. The system is to be commissioned with limited control and operated by people with limited technical expertise. The e-voting system is convenient as it is accurate, faster, and requires less labour compared to printed ballots. Technologies such as encryption are used to ensure the security of every vote. But e-voting systems still exhibit several technical imperfections. Studies reveal that several times the implementation of e-voting machines was not as convinced as expected. Fairness and e-voting authentication can only be achieved when all the specifications of voting procedures are fulfilled. The election officials are expected to follow a powerful verification procedure [1].

Utilizing technology in voting procedures can make it quicker, more efficient, and less susceptible to security breaches. The technology can ensure the safety of every vote, better and faster and much more accurate counting and automatic tallying. The process uses minimum paper documents and is therefore environmentally friendly. Bio-metric or retina scans can be used as security measures [2]. The e-voting system is vulnerable to several serious attacks from external sources. There is indeed a likelihood that anybody who has immediate access to the e-voting system can access it suspiciously. Malevolent software can steal one candidate's votes and assign them to some other. An attacker may deny officials access to the e-voting system or render an e-voting system unavailable for the Election Day voting process. This is known as a service denial (DoS) attack. Such an attack is extremely complicated to identify. [3]. The major problem with conventional paper-ballot based voting system is a large number of doubtful and invalid votes. This phenomenon will be eliminated if the e-voting system is used. In addition to the speed of counting and reduction of errors the e-voting system offers some more advantages such as accessibility, verifiability, and availability. When the e-voting system is integrated with the Internet, any eligible voter can vote from anywhere as there will be two or more levels of authenticity checks [4].

2. OBJECTIVES OF THE STUDY :

This paper mainly focuses on various issues related to the development of SSRPVS. The main objectives include:

- To comprehend the need of SSRPVS
- To comprehend the function of different technologies used in SSRPVS
- To scrutinize the benefits and challenges associated with SSRPVS
- To design a conceptual model that addresses security issues of remote voting system
- To foretell the future of SSRPVS

3. METHODOLOGY :

In this paper, the secondary data available from a

good number of articles, peer-reviewed journals, magazines, and a few official websites is used to discern different issues related to SSRPVS. An attempt is made to know about different technologies used to build a smart and secure remote voting system that consists of several emerging technologies such as the Internet of Things (IoT), smart sensors, cloud platforms, Blockchain, etc. The design of a conceptual model for SSRPVS is also proposed. Finally, this paper tries to propose some suggestions to employ research activities.

4. RELATED WORK :

Table-1: Contribution of Researchers to devise technology adapted secured Voting System

SN	Authors	Year	Inventions/Findings/Results
1	Weldemariam *et al*. [1]	2010	Developed a reliable e-voting system consisting of direct electronic machine recording, real-time audit log that functions as VVPAT (voter-verified paper audit trail), custom-made electronic ballot, and tiny / flashcard. The system was designed using ASTRAL language and used the touch screen.
2	Gentles *et al*. [2]	2011	Developed a framework for a safe and secure mobile voting system in which smartphones can access the remote voting machine. Finger-print based bio-metric is used to ensure safety.
3	Kadbe *et al*. [5]	2013	Proposed a model utilizing automatic identification method based on RFID, and biometric identification. All voter data and all constituencies and the respective candidates' details are stored in a centralized database. The system also features a dynamic user interface.
4	Hussien & Aboelnaga [6]	2013	Designed an RFID-based embedded voting system in which cryptography, blind signature, and homomorphic methods are used to maintain integrity and privacy.
5	Agarwal & Pandey [7]	2013	Constructed a secure voting system to be used in India based on the unique identification of the user, named the Aadhaar number. Password provided to guarantee safety.
6	Ujir *et al*. [8]	2014	Recommended 3D face recognition based secure voting system using the basic expressions namely rage, repulsion, horror, gladness, grief, and surprise. Three different types of modules called 2-module, 6-module, and 10-module are used and their performance is compared. Support vector machines are used as classification models.
7	Nikam *et al.* [9]	2015	The innovative framework was proposed to ensure verification, confidentiality, security, and integrity. The system uses a technology called Near Field Communication (NFC).
8	Matharu *et al.* [10]	2015	Envisaged cloud-based model named I-Voting which uses cloud computing power where all the necessary information is stored in a cloud environment. With additional features such as scalability and cost-effectiveness, the program guarantees quick and efficient data transfer. Since the system allows voting from anywhere, it can accomplish a higher percentage of turn-out.
9	Malladi *et al.* [11]	2015	Suggested e-voting system that uses terminals with automatic teller machine ATM). OTP and Random Security Question (RSQ) are used to confirm security and authentication. The process provides robustness, scalability, and cost-effectiveness.

10	Patil *et al.* [12]	2015	Intended a secure voting device that includes the Aadhaar database and an iris scanner at the polling station for elections in India. To check for the person's identity, the scanned image of the iris is compared with that of the Aadhaar database.
11	Stem *et al.* [13]	2015	Proposed a technique that compares the image of the iris to that stored in the database. It uses a micro-controller to compare and, if a discrepancy occurs, an alarm buzzes, and an error message is displayed.
12	Barnes *et al.* [14]	2016	A fast and fool proof remote e-voting system that uses Blockchain technology has been designed. Because Blockchain is immutable, the votes are kept safe. The voting process makes the deletion and modification of votes impossible.
13	Anik*et al.* [15]	2017	Designed a cost-effective e-voting solar power system that could efficiently store the data. The system uses both the touch-screen and the audio instructions.
14	Selvarani *et al.* [16]	2017	Designed a secure e-voting system based on SMS which uses both SMS for voting and voter registration. Cryptography is used to provide the security that is needed. OTP will be provided to the user both at registration and during voting time.
15	Deepika *et al.* [17]	2017	Devised a smart electronic voting system that uses RFID as well as fingerprint technology for the Indian scenario. Aadhaar, EPIC, fingerprint, and iris details are stored in a single database which makes the verification process quick and efficient.
16	Mello-Stark & Lamagna [18]	2017	Developed an e-voting system that uses authenticity and integrity from end to end. The system uses the open-source platform and is capable of auditing.
17	Alam *et al.* [19]	2018	Developed an e-voting system using Blockchain that utilizes zero-knowledge non-interactive technology.
18	Shaw *et al.* [20]	2018	Developed an intelligent e-voting mechanism using Arduino Uno that contains fingerprint-based authentication
19	Khoury *et al.* [21]	2019	Designed a smart voting system that uses private Blockchain and Ethereum protocol.
20	Abirami [22]	2019	Developed a retina-based smart voting system that uses fuzzy logic and hamming distance.

5. EXISTING SYSTEM :

5.1 Electronic Voting Machine (EVM)

The e-voting plan is meant to be used by the entire population of eligible voters irrespective of background and physical disability. People with less technical know-how handle the devices. So, they are expected to be handy and easy to manage. The e-voting system has to be secure and tamper-free. Flows within the voting device lead to inaccurate results. Hence, the system must be secure, transparent, and reliable. The EVM is developed and tested under the Indian election

commission administration by the two government-owned companies Electronics Corporation of India Limited (ECIL) and Bharath Electronics. In Indian elections introduces were made in a phased manner. Since 2004 they have been used in all general and state assembly elections of India.

The EVM consists of two units-a ballot unit and one control unit, as shown in Figure-1. The ballot unit displays the name of the candidate and the corresponding symbol. The voter must press the

respective button on the right-hand side of the symbol. The controller is a onetime programmed device where the manufacturer loads the program. It also includes a seven-segment LED displaying the status and the number of votes polled. The two units are connected using a short-length cable. These days, the EVMs used to contain a provision to accommodate a maximum of 384 candidates and "no of the above" (NOTA). The voting program commences when the voter identity is confirmed by the operator and the ballot unit is activated to issue a new operation. Once the elector casts his / her vote, the controller displays the count and the machine is locked to prevent multiple votes casting by the voter. EVMs are powered by an ordinary 6volt alkaline battery, and therefore do not require an external power source to operate. The VVPAT facility had EVMs used in the 2019 elections [23].

5.2 EVM Model

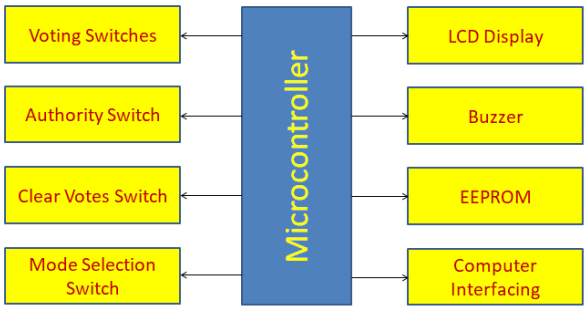


Fig. 1: Block diagram of EVM [24]

Figure-1 shows the EVM block diagram. Hitachi 6305 microcontrollers and firmware were used by the first generation EVM's. The software for processing the cast votes was housed in external VU-erasable PROM and 64 kb EEPROM. The next generation had a CPU, rather than a microcontroller. The controller stores the accumulated votes, and voters use the ballot unit to cast their votes. Once the election process is finished, the memory is sealed in the control unit. Officials remove the seal and test the votes during the counting process, and announce the result. The computer is tested during the election cycle until it is put into service. The voter must press a button on the ballot box to cast his/her vote [24].

5.3 Security features of EVM

The election commission of India (ECI) follows strict administrative procedures to verify the functioning of EVMs. These procedures are used to ensure proper functionality and to prevent potential misuse. To ensure transparency ECI includes candidates, their backers, and elected officials at different hierarchical levels. The safety measures are taken by the ECI include:

1. A first-level check (FLC) is performed before each election in the presence of candidates, their supporters, and election officers and engineers of the manufacturers.
2. Manufacturers at the end of FLC certify the EVM stating all components used in the EVMs are genuine. Upon completion of this process, the control unit is sealed with a "pink seal." Once completed, the control unit's plastic armoire cannot be opened.
3. The mock poll is conducted using about 1000 votes, and the results of the VVPAT and count are shown on the control panel are counted together. Anyone present in the FLC will be shown the test. Candidate supporters are allowed to cast a mock vote and ECI officials document the entire procedure.
4. EVMs are randomized twice with computer software before being distributed to the polling stations in question. The entire process, including candidates and their supporters, is carried out transparently.
5. The next step is called "Setting the candidate" The ballot paper is set on EVM's ballot unit arranging candidates' names in alphabetic order. This system is achieved using the software. Hence the candidate's serial number is not based on their political party. This method rules out the risk of any influence or abuse.
6. Once the candidate setting is done, the ballot box is also sealed using a “pink seal”. The seal will contain the signatures of officials and the candidates.
7. At the next level, 5% of EVMs are randomly chosen to verify the functioning of the ballot box and VVPAT. This process is made transparent as it is carried out in the presence of candidates and their supporters.
8. On Election Day the presiding officer performs a mock poll in the presence of party supporters or polling officers. All officials and the people who participated in the mock poll are expected to sign the mock poll paper.

9. At the control unit, green paper seals are placed after the mock poll. The presiding officer presses the "Close" button in the presence of the polling agent once the election process is over. The EVMs are transported from the poll station to the strong rooms.
10. With the aid of the Central Armed Police Force (CAPF), the strong rooms where EVMs are kept are sealed and secured all round the clock. In CC Cameras all activity near the strong room is captured [25].

5.4 Benefits and Limitations of EVM

Benefits:

- Approximately 10,000 tons of ballot papers are saved in national elections. This saves around two lakhs of trees
- Present generation EVMs cost around Rs 2000 per unit, the amount is smaller when compared to the printing of ballot documents during every election
- Compact and portable when compared to ballot boxes
- Counting of votes takes place much fast and accurate. The results can be announced within 3-5 hours
- Tallying of votes can be done automatically
- A person cannot cast more than one vote. This decreases the likelihood of fake votes.
- EVMs use battery hence they can be used in places where there is no electricity
- EVMs are durable and can be used for more than 15 years
- They eliminate the possibility of doubtful and invalid votes
- A vote stored in the memory of the control box cannot be deleted or altered
- No one can link any ballot to an individual. This way it ensures privacy

Limitations

- EVMs handled by people with minimum technical expertise, they require training for effective use.
- They are vulnerable to hacking.
- The touch screen is not-efficient for physically challenged people. It leads to voting someone who is not of their choice [26].
- No scope for the voters to cast a vote of his/her chosen constituency other than the designated constituency.

6. PROPOSED SSRPVS FRAMEWORK :

The proposed Smart and Secure Remote Public Voting Systems (SSRPVS) consists of evolving technologies such as Smart Sensing and Automatic Functioning Internet of Things and Edge Computing, Cloud Framework for Remote Processing and Data Storage, Blockchain for the safety and security of Sensitive Information, 5 G as a Network Infrastructure, and many additional elements. The reason for implementing such a relatively involved remote voting system rests heavily on voters' perception of security and inherently simple insider attacks.

Besides providing a framework that a voter would trust, our system should offer far stronger defenses against viruses and intruder attacks than other systems proposed. This helps voters to cast their votes from the remote place where they live, where they are working, where they are learning, and where they are getting training or treatment rather than driving to their designated Polling Station wasting precious time, resources, and energy. This also guarantees to electioneer 100 percent fool proof because it as it provides an opportunity for all the eligible voters to exercise their franchise. The motivation behind proposing this framework is to address the following requirements of the election process.

***Accuracy*:** The system must ensure that none of the voting parties will change any of the votes cast. It must prohibit anyone from deleting valid votes from the final count and also the invalid votes must not be considered in the final count. It should also be remembered that the steps taken to prevent hostile parties from muddling the mechanism do not interfere with the privacy of the electorate [27]

***Equality*:** The system should allow only eligible voters to vote; this means the system must ensure that only registered citizens can vote, recognizing eligibility is tested during the registration process and every registered voter can only vote once and that every vote is weighted equally [27].

***Privacy*:** Ensures the confidentiality of ballot contents by encrypting the ballots using a specific cryptographic technique. The method preserves

privacy by preventing either the election authorities or someone else who can connect any ballot to the voter who casts it, and by not allowing the elector to show that he/she has voted in a particular way [28].

Verifiability: A system is verifiable because all voters can independently check that their votes have been correctly counted without losing privacy, each voter must also be able to verify the final results of the count to ensure that each party can be assured that all legitimate votes have been included in the final count.

Convenience: A system is considered as a convenient one if it allows voters to cast their votes with the minimal equipment or skills. This property will increase the turnout, predominantly in government elections that rely on a large number of voters, and it is not feasible to expect this huge number of voters to get into training.

Robustness: The voting system must operate properly even if the system is partly failing. This must be avoided that a small coalition of electors, talliers, and other groups participating in the election to disrupt elections should not, for example, be able to write an encrypted vote in an unauthorized format, which can go unnoticed at first and then prevent the mechanism from functioning effectively.

Voter Independence: In certain voting schemes, a voter may copy the vote of another voter without necessarily understanding the vote being copied, for example, if a vote is simply encrypted using the voting server's public key such encryption may be copied, such duplication of votes must be avoided by the voting system.

***Efficiency*:** The amount of computation capability and communication is proportional to the number of voters.

***Fairness*:** No partial results are known before the election is closed.

The proposed system is composed of the following elements

a. Remote access
b. Five-factor security checks
c. Encryption of data using Blockchain
d. Secured Cloud Storage
e. High-speed 5G network

a. Remote Access: This provides a way for the eligible voters to cast their votes to their choice of the candidate from a remote location. It is assumed that the Commission will install several SSRPVS units in the major cities spread across India. So that whenever an election is scheduled for any of the constituency or area of India, the legitimate voter needs not to travel to his constituency, city, town, or village, instead, one can exercise his franchise directly by visiting one of the SSRPVS units installed in his place.

b. Five-factor of security checks: The system ensures safety and security through 5-factor security checks – Voter ID number, One Time Password (OTP), Fingerprint recognition, Iris recognition, and face recognition. Every Voter ID card consists of a unique Voter ID also barcoded, which is used to initiate the process of voting. The preliminary process generates an OTP and sends it to the register mobile of the voter. This is used as the second-factor security.

Fingerprint recognition is considered ad the most advanced authentication known to date because the ridge pattern on each individual's finger is identical and does not change while the finger measurements change concerning each individual's finger growth and heyday. There is seldom a situation where, so far, two fingerprints are found identical among the billions available. Thus, this type of authentication will make the system more efficient and fool-proof. Of the entire available algorithms, the minutiae algorithm is commonly used to recognize fingerprints [29].

Iris recognition or iris scanning is the process of taking a high-quality photograph of a person's iris using visible and near-infrared light. It is in the same category as face recognition and fingerprinting, a form of biometric technology. Iris scanning tests the distinctive patterns in irises, the circles of colour in the eyes of men. Biometric iris recognition scanners operate by lighting the iris with invisible infrared light to detect special patterns that are not apparent to the naked eye.

Face recognition another way of biometric authentication that is most commonly used for computational methods it can evade manipulation of voting can as it avoids attempts by individuals to cast multiple ballots under various names and IDs. A large part of this problem can be overcome by identifying an individual's face and then determining whether it matches any of the

previously registered voters' faces in the voting database, thereby eliminating duplicate votes. Due to different factors such as the context of the image, lighting of the image, facial expressions, angles and postures, face recognition is arguably the most challenging and difficult form of computing. There are many algorithms available that tend to meet the above purpose, yet facial recognition based on the Eigen-face is considered more viable [29].

c. Encryption of data using Blockchain: Once it comes to Blockchain voting, each vote will be considered equivalent to a transaction, and by using multiple Blockchains along with public key encryption, the decentralized voting process can be safeguarded while maintaining the voting process's anonymity function. The votes can be randomized in the digital ballot box more than three times in the Blockchain voting process ensuring the identity of the voters is never revealed. When the voting is closed a separate Blockchain program is installed in the digital ballot box for the counting of votes. The specific Blockchain matches the Blockchain of the public newsletter board and thus shows that the online voting system correctly worked. The Blockchain voting system combines the transaction audit trail with the public key encryption which solves the auditability problem [30].

d. Secured Cloud Storage: The main concept cloud database means that the database is run on a cloud platform (DaaS-Database as a Service). By using the private cloud database, it becomes simpler to store, access, and retrieve data, as it can be accessed anywhere. The user details are encrypted and stored using md5 in the cloud database, and it is decrypted during recovery. The database services typically make all of the underlying software stack clear to all users.

Describing the security of cloud data storage is nothing other than data protection, applications, and infrastructure involved in cloud computing. An effective form of security architecture will be able to identify any problems that could occur with management protection, and recently information management should fix the problems with protection controls. The controls will be put in place to protect all sorts of weaknesses that occur in the allotted system and will attempt to reduce all effects of any kind of attack. The proof-of-work which in the Blockchain technology is generally also known as the Consensus Algorithm is that it makes it difficult for fraudulent nodes to catch up with honest nodes. The main benefit is that it does not require the Denial of Service (DoS) attack and also impact on mining possibilities from the low stake. Attack the Do defense: proof of work imposes such constraints or limitations in network behavior. It takes lots of potential effort to be put into action. To apply the calculations, the attacks need lots of computational or computing resources and therefore a lot of time [28].

e. High-speed 5G network: 5 G is the next generation of mobile communication technology that guarantees download and upload speeds extraordinarily faster. Latency, or the time it takes for apps to connect with wireless networks, also reduces considerably. This element ensures seamless, high speed, and low latency communications between every component of the system [27].

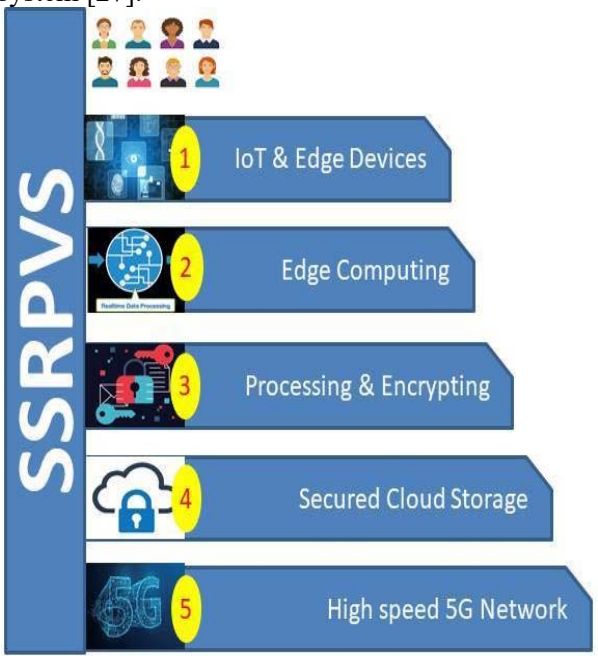


Fig. 2: 5-layer Framework of proposed SSRPVS

The framework of the proposed system consists of 5 layers which is explained in Figure-2. IoT and Edge Devises are appearing in the first layers. The smart sensors include Barcode reader, biometrics scanners, automatic height adjusters, tilt controllers, light controllers, and smart surveillance cameras. Data so scanned will be compared and authenticated by matching them with the cloud data by applying edge computing

techniques in the second layer. All processing, decision making, and encryption, etc, are happening in the third layer. Data processed using analytical tools and Blockchain technology finally gets stored in a secured way at cloud storage. All communication between the edge devices, cloud, and administers is channelled through a seamless high-speed 5G network.

7. ARCHITECTURE OF THE PROPOSED SYSTEM :

The architecture of the proposed SSRPVS contains several components. It concludes barcode reader, fingerprint scanner, iris scanner camera, face capture camera, receipt printer, light illumination controllers, height adjustment sensors, and 3D sensors for liveness and lighting adaption. Components and their uses are listed below.

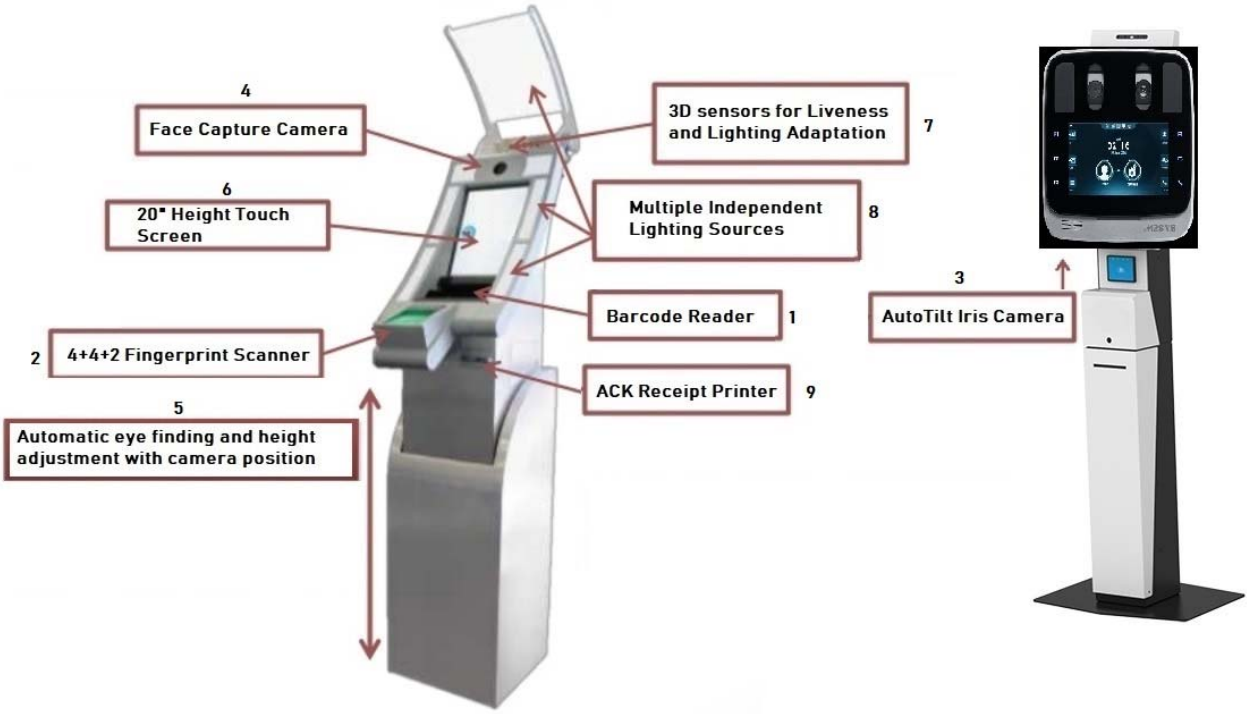


Fig. 3: Architecture of the proposed system

1. Barcode Reader – to read unique ID recorded in the Voter ID card
2. 4+4+2 Finger Scanner – reads fingerprints of left and right-hand fingers and two thumbs
3. Auto Tilt Iris Camera – reads the Iris image of the voter. The camera is automatically adjustable to the height of the voter as it is featured with AutoTilt option
4. Face Capture Camera – scans a facial image of the voter
5. Automatic Height adjustment – the height of the unit gets adjusted to the height of the voter as directed by the smart camera
6. 20" height touch screen – vote to the candidate of his/her choice is made through this screen.
7. 3D sensors – detect objects, changes in exterior conditions, and other objects through a variety of optical properties.
8. Lighting sources – illumine light as expected by other sensors
9. ACK Receipt Printer – prints acknowledge slip upon the completion voting transaction

8. ADAPTIVE TECHNOLOGIES :

8.1 IOT & EDGE DEVICES

IoT is an evolving technology that links 'people' and 'things' with 'anytime,' 'anywhere', and 'anyone.' The modern technologies would make an individual's day-to-day life easier, simpler, and better. IoT infrastructure uses multiple 'smart' interconnected devices that use sensors. Unless the

sensors do not have the computational capacity, the sensed data will be forwarded to the cloud for further review. That is a time-consuming process. Devices with computational power are used to make the transactions quick and efficient. Those are called edge devices [31].

8.2 EDGE COMPUTING

Edge computing provides tools for open storage. The data is stored at the place where it is required. Complex solutions require huge data. The storage infrastructure which contains computational capabilities is used with edge computing. When there is a computational feature of the storage device, data can be analyzed quickly. The edge computing also comes with the feature of visualizing the data. It's the way the resources are optimized by bringing the computational process closer to the data source. This feature optimizes the process by reducing the contact between client and server over long distances. The technology is cost-efficient and reduces latency, too. Large data-intensive applications can efficiently process the stored data by using parallelization t. Edge data centers are rising in popularity and hold great promise for the future [32].

8.3 CLOUD INFRASTRUCTURE

If vast volumes of data obtained from various sources are to be efficiently processed, use is made of cloud infrastructure. It requires a massive archive to store this information, which includes text, images, audio, etc. DBMS cannot be used. A centralized warehouse is a facility used to store different forms of data for analytical purposes. When data is collected in a centralized data center it is easy to analyze. Cloud computing provides the consumer with on-demand tools exclusively for data storage and processing power. It is the best example of resource sharing. It ensures agility, flexibility, and scalability for storing voluminous information needed to be stored for analysis. Cloud can be public, private, or hybrid. Public cloud can be accessed by anyone and it is available free of cost. A private cloud is owned by a single organization and a hybrid cloud coalesces the features of both. Usually, a private cloud owned by a trusted third-party is made used. The use of a data warehouse enables any system to automatically extract and analyze data stored [33].

8.4 BLOCKCHAIN

To efficiently store a huge amount of containing text, images, etc. Blockchain technology is extensively used. Blockchain is a method by which data is securely stored in a decentralized network. It is an alternative to conventional cloud storage. The incontrovertible feature of Blockchain is drawing the attention when data to be saved safely. Voluminous information can be stored effectively ensuring their security and privacy. When many entities need to use the stored data this technology can be used to manage interoperability effectively. Blockchain consists of block formatted data such as text, images, audio, or a video file. Several blocks with interconnections are called nodes. The information stored in the interconnected blocks forms a chain-like process governing data transfer. Cryptographic hashing is used to provide much-needed protection for the stored data. Blockchain may be private or public. In the case of a decentralized Blockchain, anyone can read or write data without having to wait for permission from an authority. Private Blockchain, the popular one between the two is a permission-based one involving familiar participants [34].

8.5 5G NETWORK

In the current scenario, the fifth generation (5 G) mobile network is meeting the growing demand for the data. Once billions of devices are interconnected, it transmits huge quantities of data. 5 G allows trillions of devices to be seamlessly connected. It provides outstanding speed, incredibly low latency, and omnipresent connectivity. It acts as next-generation communications technology. 5 G apparatuses are much quicker. Every type of content is quickly uploaded or downloaded using 5G [35].

8.6 DATA ANALYTICS

Data analytics is a dynamic method of analyzing large datasets to uncover hidden patterns or unknown relationships, whose analysis can assist an organization in the decision-making process. It has brought radical changes in many industries. The enormous data collected must be analyzed using algorithms and converted to the information required that can be used for further analysis to reach a conclusion or make a decision. The main difficulty is getting relevant information out of a broad data set. Using data analytics reduces overheads for data processing. The hidden relation

or association with either two or more events or attributes is easy to figure out with the aid of big data analytics. The data analytics can also be used to provide solutions [36]

9. FUNCTIONING OF THE PROPOSED SYSTEM :

The flow of execution of the proposed SSRPVS is illustrated in Figure-4with the help of the flowchart or work flow and the same is explained below.

Step-1. Eligible voter visit any of the SSRPVS unit placed in his nearby location

Step-2. Either he enters Voter ID through touchscreen keypad or let barcode reader read ID tagged to his card

Step-3. The system validates Voter ID entered by comparing the same with data stored in the Voter Database

Step-4. If not valid or the voter already cast his vote then by displaying the error message system terminates the flow

Step-5. If the ID is valid and he is entering as a fresh voter then the system produces an OTP and sends it to his registered mobile. Also, it initiates the timer so that the voter must enter the OTP he received within the given time window

Step-6. If the time elapsed before the Voter enter the OTP, by flashing a message terminate the flow

Step-7. It accepts OTP and validates the same. If it found invalid then by flashing a message terminate the flow

Step-8. If validation succeeds then the system search Voter record in the Aadhaar database using linked Voter ID

Step-9. The system will scan fingerprints of all fingers; four of the left hand, four of the right hand, and two thumbs.

Step-10. It will compare scanned fingerprint images with Aadhaar biometrics

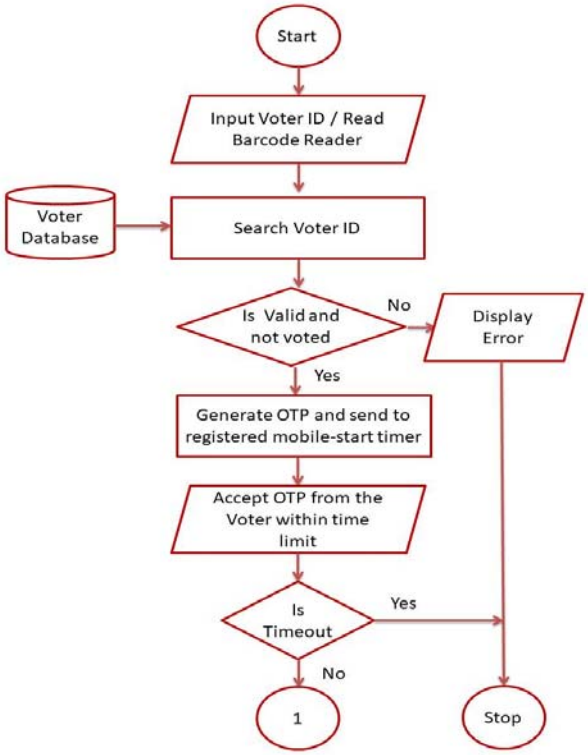
Step-11. If the matching is successful then it proceeds otherwise by flashing a message system terminates the process

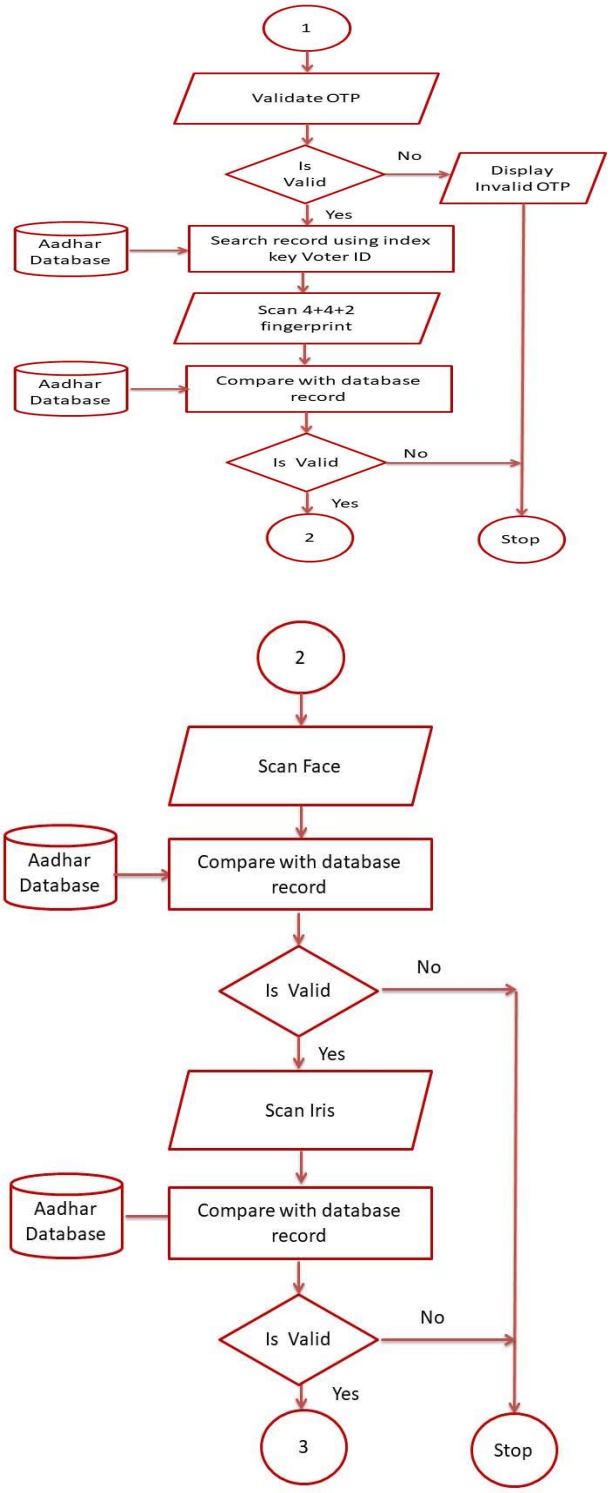
Step-12. Now the system will scan voters' face image. Before doing so the system automatically adjust its height and light illumination to create the best scenario for the face scanning

Step-13. It will compare scanned face image with Aadhaar biometrics

Step-14. If the matching is successful then it processes otherwise by flashing a message he system terminates the process.

Step-15. As the last authentication step, the system will scan voters Iris. Auto tilt iris scan cameras automatically get adjusted to the voter's height





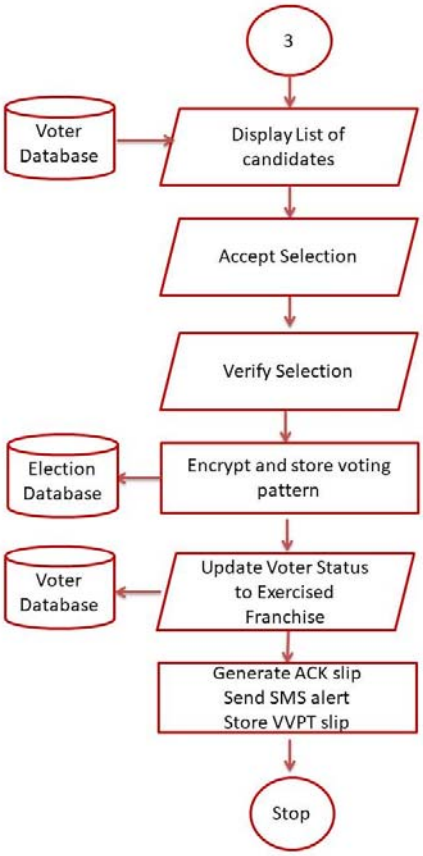


Fig. 4: SSRPVS Work Flow Diagram

Step-16. It will compare the captured iris image with Aadhaar biometrics

Step-17. If the matching is successful then it processes otherwise by flashing a message he system terminates the process.

Step-18. With this all authentication procedures are validated, the system comes to the understanding that the voter is genuine and valid so it displays a roll of candidates and permits the voter to make a choice

Step-19. Now the voter is making a selection by touching the Party Symbol displayed against the candidate name

Step-20. It allows the voter to e-verify his selection by allowing him to make the selection for the second time

Step-21. With this voting is done, the system encrypts the data by using appropriate

algorithms and technology and store in the database

Step-22. It also changes the status of the voter to franchise exercises as he already made voting

Step-23. It generates an ACK slip that contains basic details such as Voter ID, constitution details, Unit ID, date, time, etc.

Step-24. Also, the system sends an SMS voter's registered mobile

Step-25. Generate VVPT slip and stores the same in its container for future reference to the administrators

Step-26. With this the voting process is completed, the system automatically logout the voter. Now new voter can come and use the system

10. BENEFITS& CHALLENGES OF SSRPVS :

Benefits

- It contributes a lot for the increase in voter turnout
- It saves money, time and hardship involved in moving from place to place to cast a vote
- Votes can cast their votes from anywhere thereby eliminating the problems associated with commuting
- It is faster, as people need not have to wait in queues to get their turn to vote.
- It will be secured and well-controlled than that of the manual work or way of monitoring, voting, and safeguarding the votes.
- By just using pre-recorded details voters can easily login to the voting system and cast his/her vote.
- It uses Blockchain technology for giving higher security makes it more reliable than that of the existing system.
- It reduces the dependence on human resources to manage the voting process
- It makes all the processes involved in voting are made fool-proof, tamperproof and automatic
- Greater accessibility for voters with special needs

Challenges

- The system is only useful for remote voters. Not the voters who are residing in the area in which voting is held
- A huge initial investment is required to setup units in different locations across India
- The biometric authentication process may consume little more time as it involves several processes
- Biometric authentication some time fail to identify even genuine voter and deny the right to vote
- It is functioning largely depends on the sophisticated network infrastructure as most of the operations are cloud-based
- As almost all the processes are happening using cloud infrastructure, there may be cause to worry about security and safety of data

11. DISCUSSION & FUTURE WORK :

For India having fairly easily adopted technology originating in the West, it is only reasonable to use the accepted technological aspects to solve real-world problems. Now, concerning India's new technical buzzword, we feel that this is undoubtedly the Internet-of-Things (IoT), the Cloud and Blockchain, and related smart aspects viz. Artificial Intelligence, Deep Learning, and Machine Learning. To communicate and share data with other devices and systems over the Internet, the Internet of Things introduces a new world of connected objects that are loaded with sensors, programs, and other technologies. Cloud computing facilitates on-demand computing resources over the Internet and on a pay-as-you-go basis. Organizations can rent computing resources rather than having their own. Blockchain is the latest technology that has the potential to have a massive effect on different industries. Voting is one of the applications benefiting from Blockchain technology implementation. Some of the reasons why the voting system needs Blockchain to include trouble-free voting, utmost confidence for voters, greater transparency, privacy for voters, cost-effectiveness, legitimacy, factual outcome, higher security, and east for tootling. In this work by using these three versatile technologies was used to develop a conceptual model that provides a framework for remote voting safely and securely. The framework is made up of five different inter-

linked layers that embrace different adaptive technologies. The architecture of the proposed system is presented in the paper for a clear understanding of its functioning. Smart sensors are proposed to gather user data and they are processed using edge and cloud computing techniques. To ensure security and robustness Blockchain technology is proposed. This is used to encrypt using a particular algorithm that is very hard for one to decode without the key being used. The functioning of the system is also detailed using a flowchart. In this work, only the conceptual model of the proposed system is presented. Its development and technicalities were not discussed. In our future work, this model will be implemented with specific algorithm, technique and hardware inferences

12. CONCLUSION :

In this paper, the authors proposed a smart and safe remote public voting system that adapted five-factor security checks and the latest technologies to provide a more convenient and efficient voting environment for voters scattered across India. It was estimated that over 300 million registered voters didn't cast their votes in the 2019 general election. There are many reasons. But any method that offers a way for the elector to cast his vote from the position where he is positioned is impossible for one of the most important reasons. Other than in the service staff, government officials who are directly linked to electioneering and citizens of more than certain age groups have to appear in their designated polling station to exercise their franchise. Because of this many genuine and legitimate voters who placed in different parts of India lose the chance to vote. This model is proposed to tackle this particular problem. That cannot be considered as an alternative to the current system of elections. It is merely a supplement to the existing structure. The framework being proposed has several strong features such as reliability, verifiability, usability, security, etc. For this system, only the unit, internet access, and one supervisory officer are necessary. Besides, it is tamper-proof and fraudulent-proof because the device uses IoT and Blockchain technologies. As it is merely conceptualized here, in our future work we will implement this model in a phased manner.

REFERENCES :

[1] Weldemariam, K., Kemmerer, R. A., & Villafiorita, A. (2010). Formal specification and analysis of an e-voting system. *ARES 2010 - 5th International Conference on Availability, Reliability, and Security*, 164–171. DOI: https://doi.org/10.1109/ARES.2010.83

[2] Gentles, D., & Sankaranarayanan, S. (2011). Biometric secured mobile voting. *Asian Himalayas International Conference on Internet*. DOI: https://doi.org/10.1109/ AHICI. 2011.6113931

[3] Lavanya, S. (2011). Trusted secure electronic voting machine. *Proceedings of the International Conference on Nanoscience, Engineering and Technology, ICONSET 2011*, 505–507. DOI: https://doi.org/10.1109/ICONSET.2011.6168014

[4] Kumar, D. A., & Begum, T. U. S. (2012). Electronic voting machine - A review. *International Conference on Pattern Recognition, Informatics and Medical Engineering, PRIME 2012*, 41–48. DOI: https://doi.org/10.1109/ICPRIME.2012.6208285

[5] Kadbe, A., Balgujar, S., & Chimote, S. (2013). *Biometric and RFID Secured Centralised Voting System*. *4*(2), 255–258.

[6] Hussien, H., & Aboelnaga, H. (2013). Design of a secured e-voting system. *International Conference on Computer Applications Technology, ICCAT 2013*. DOI: https://doi.org/ 10.1109/ICCAT.2013.6521985

[7] Agarwal, H., &Pandey, G. N. (2013). Online voting system for India based on AADHAAR ID. *International Conference on ICT and Knowledge Engineering*, 1–4. DOI: https://doi.org/10.1109/ICTKE.2013.6756265

[8] Ujir, H., Sing, L. C., & Hipiny, I. (2014). A modular approach and voting scheme on 3D face recognition. *2014 International Symposium on Intelligent Signal Processing and Communication Systems, ISPACS 2014*, 196–199. DOI: https://doi.org/10.1109 /ISPACS.2014.7024451

[9] Nikam, R., Rankhambe, M., Raikwar, D., &Kashyap, A. (2014). *Secured E-Voting Using NFC Technology*. *5*(6), 8325–8327.

[10] Matharu, G. S., Mishra, A., & Chhikara, P. (2015). CIEVS: A cloud-based framework to modernize the Indian election voting system. 2014 IEEE International Conference on Computational *Intelligence and Computing Research, IEEE ICCIC 2014*. DOI: https://doi.org/10.1109/ICCIC.2014.7238454

[11] Malladi, K., Sridharan, S., & Jayprakash, L. T. (2015). Architecting a large-scale ubiquitous e-voting solution for conducting government elections. *2014 International Conference on Advances in Electronics, Computers and Communications, ICAECC 2014*. DOI: https://doi.org/10.1109/ICAECC.2014.7002445

[12] Patil, P. S. A., & Kote, P. G. (2015). IRIS Detection in Voting System. *International Journal for Research in Applied Science & Engineering Technology (IJRASET)*, 3(8). 469-473, ISSN: 2321-9653

[13] Stem, I.-, Nithya, M. J., Abinaya, G., Sankareswari, B., & Lakshmi, M. S. (2015). *Iris recognition-based voting system International Conference on Science, Technology, Engineering & Management*, (10), 44–51.

[14] Barnes, A., Brake, C., & Perry, T. (2016). Digital Voting with the use of Blockchain Technology. *Computing with Plymouth University*, 1–19.

[15] Anik, A. A., Jameel, R., Anik, A. F., & Akter, N. (2017). Design of a solar power Electronic Voting Machine. *Proceedings of 2017 International Conference on Networking, Systems and Security, NSysS 2017*, 127–131. DOI: https://doi.org/10.1109 /NSysS.2017.7885813

[16] Selvarani, X. I., Shruthi, M., Geethanjali, R., Syamala, R., & Pavithra, S. (2017). Secure voting system through SMS and using smart phone application. *2017 International Conference on Algorithms, Methodology, Models and Applications in Emerging Technologies, ICAMMAET 2017*, *2017-Janua*, 1–3. DOI: https://doi.org/ 10.1109/ ICAMMAET.2017.8186724

[17] Deepika, J., Kalaiselvi, S., Mahalakshmi, S., & Agnes Shifani, S. (2017). Smart electronic voting system based on biometric identification-survey. *ICONSTEM 2017 - Proceedings: 3rd IEEE International Conference on Science Technology, Engineering and Management*, *2018-Janua*, 939–942. DOI: https://doi.org/10.1109/ICONSTEM.2017.8261341

[18] Mello-Stark, S., & Lamagna, E. A. (2017). The need for audit-capable E-voting systems. *Proceedings - 31st IEEE International Conference on Advanced Information Networking and Applications Workshops, WAINA 2017*, 535–540. DOI: https://doi.org/ 10.1109/WAINA.2017.87

[19] Alam, A., Zia Ur Rashid, S. M., Abdus Salam, M., & Islam, A. (2018). Towards Blockchain-Based E-voting System. *2018 International Conference on Innovations in Science, Engineering and Technology, ICISET 2018*, 351–354. DOI: https://doi.org/10.1109/ICISET.2018.8745613

[20] Shaw, S. K., Poddar, S., Singh, V., &Dogra, S. (2018). Design and Implementation of Arduino Based Voting Machine. *Proceedings of International Conference on 2018 IEEE Electron Device Kolkata Conference, EDKCON 2018*, 450–454. DOI: https://doi.org/10.1109/EDKCON.2018.8770474

[21] Khoury, D., Kfoury, E. F., Kassem, A., & Harb, H. (2019). Decentralized Voting Platform Based on Ethereum Blockchain. *2018 IEEE International Multidisciplinary Conference on Engineering Technology, IMCET 2018*, 1–6. DOI: https://doi.org/10.1109/IMCET.2018.8603050

[22] Abirami, P. (2019). Retina based E-voting system using fuzzy logic and hamming distance. International Journal of Advance Research, Ideas and Innovations in Technology. *4*(4). 218-222.

[23] Wolchok, S., Wustrow, E., Halderman, J. A., Prasad, H. K., Kankipati, A., Sakhamuri, S. K., Gonggrijp, R. (2010). Security analysis of India's electronic voting machines. *Proceedings of the ACM Conference on Computer and Communications Security*, 1–14. DOI: https://doi.org/10.1145/1866307.1866309

[24] Hoquec, M. M. (2014). *A Simplified Electronic Voting Machine System. International Journal of Advanced Science and Technology, 62, 97–102.* DOI: https://doi.org/10.14257/ijast.2014.62.07

[25] Election Commission of India. (2018). *Status Paper on Electronic Voting Machine(Ed-3)*. Retrieved from https://eci.gov.in/files/file/8756-status-paper-on-evm-edition-3/

[26] Bhuyan, D. J. (2019). Effectiveness of electronic voting machine in the electoral system of India: New opportunities and challenges. *International Journal of Recent Technology and Engineering*, *8*(2), 192–199. DOI: https://doi.org/10.35940/ijrte.A2199.078219

[27] Bhattacharrya, S., Roy, D., Pramanik, E., Nath, T., &Kundu, S. (2019). Wireless voting machine.*2019 International Conference on Opto-Electronics and Applied Optics, Optronix 2019*, 1–3. DOI: https://doi.org/10.1109/OPTRONIX.2019.8862393

[28] Shakkeera, L., C, H. P. K., Begum, S., &Vali, S. (2020). Cloud Database Security in E-Voting System using Blockchain Technology. *International Journal of Recent Technology and Engineering*, *8*(5), 1361–1370. DOI: https://doi.org/10.35940/ijrte.e6292.018520

[29] Komatineni, S., &Lingala, G. (2020). Secured E-voting System Using Two-factor Biometric Authentication. *Proceedings of the 4th International Conference on Computing Methodologies and Communication, ICCMC 2020*, *Iccmc*, 245–248. DOI: https://doi.org/10.1109/ICCMC48092.2020.ICCMC-00046

[30] Alam, M., Yusuf, M. O., &Sani, N. A. (2020). Blockchain technology for the electoral process in Africa: a short review. *International Journal of Information Technology*, 1–7.DOI: https://doi.org/10.1007/s41870-020-00440-w

[31] Srikrishnaswetha, K., Kumar, S., & Rashid Mahmood, M. (2019). *A Study on Smart Electronics Voting Machine Using Face Recognition and Aadhaar Verification with IOT. Topics in Heterocyclic Chemistry*, 87–95. DOI: https://doi.org/10.1007/978-981-13-3765-9_10

[32] Weinman, J. (2011). The future of cloud computing. *IEEE Technology Time Machine Symposium on Technologies Beyond 2020, TTM 2011*. DOI: https://doi.org/10.1109/ TTM.2011.6005157

[33] Vidhya, P. (2013). *Transforming Election Polling from Electronic Voting to Cloud as a Software Service in India. Advances in Intelligent Systems and Computing*, 225–232.DOI: https://doi.org/ 10.1007/978-3-642-31552-7_24

[34] KaziSadia, MdMasuduzzaman, Kumar Paul, & Anik Islam. (2019). Blockchain Based Secured E-voting by Using the Assistance of Smart Contract. *Springer IETE International Conference on Blockchain Technology (IC-BCT 2019)*, 1–15.

[35] EMF - 5G Explained - How 5G Works (n.d.). Retrieved from http://www.emfexplained.info/?ID=25916on 28-06-2020.

****