Role of Technology in the Development of Smart and Secure Public Voting Systems – a Review of Literatures

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: Review Paper.
Type of Review: Peer Reviewed as per |C|O|P|E| guidance.
Indexed in: OpenAIRE.
DOI: http://doi.org/10.5281/zenodo.3934439.
Google Scholar Citation: IJMTS.

How to Cite this Paper:

Vinayachandra, K., Geetha Poornima, M., Rajeshwari & Krishna Prasad, K. (2020). Role of Technology in the Development of Smart and Secure Public Voting Systems – a Review of Literatures. *International Journal of Management, Technology, and Social Sciences (IJMTS), 5*(1), 298-317. DOI: http://doi.org/10.5281/zenodo.3934439.

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

International Journal of Management, Technology, and Social Sciences (IJMTS), ISSN: 2581-6012, Vol. 5, No. 1, June 2020.

SRINIVAS PUBLICATION

Role of Technology in the Development of Smart and Secure Public Voting Systems – a Review of Literatures

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

The goal of the election is not only to determine the outcomes but also to lend credence to the winners, even for those voters who did not bother voting for them. This underlines the necessity of holding free, fair, and hidden elections. Component of all this is that elections are controlled by open and accountable, neutral, and autonomous electoral-management bodies. 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 design of a sophisticated voting system is a complex task as it has to fulfill several essential criteria. The secrecy of an elector's poll is to be well-preserved. The voting system should not give any evidence that proves which candidate receives a particular voter's vote. The process uses minimum paper documents and is therefore environmentally friendly. Bio-metric or retina scans can be used to ensure security. 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 arrangement or render an e-voting structure unavailable for the Election Day voting process. This is known as a service denial (DoS) attack. But this kind of threat is hard to detect. A large number of questionable and invalid votes are the big problem with traditional paper-ballot based voting system. 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. In this paper, the authors reviewed the application of technology in the development of smart, secure, and versatile public voting systems. Also, they outlined research gaps and recommend new approaches to the existing systems.

Keywords: Voting, Digital Voting, IoT, Blockchain, RFID, NFC, Internet, Web, EVM.

1. INTRODUCTION :

In the last decade, emerging technologies have played an instrumental role in organizing a growing number of elections around the world. Numerous countries have moved to several innovative solutions in a bid to make voting more efficient and cost-effective and to enhance the confidence of the public in each stage of the cycle. Services ranging from the use of geographical information systems for delimiting boundaries and defining polling stations to the use of advanced databases for holding voter registers, communication technology for transmitting exit polls or digital voting machines to allow citizens to

cast their votes [1]. Utilizing digital technology is a way of bringing revolutionary changes in many aspects of life and elections are no exception to the same. Document digitalization makes them easy to access and update. Because of this functionality, it is possible to update electoral rolls. Updating paper-based electoral rolls are time-consuming and hazardous. Electoral corruption may happen. Some people do not have clear proof in developing countries to maintain their identification. There is a risk that the same person may register in two or more locations. A record can be easily checked in case of digitalization and this kind of circumstance can be avoided by using bio-metric based verification. If the polling officer has an up-to-date copy of the digital electoral roll on Election Day, the verification process becomes smooth and fast [2]. Recently, in various countries around the world, the question of using new technologies to improve the election process has arisen. Although electronic voting modes could be useful in improving turnout or helping with the counting and tabulation procedure, their use creates questions of governance of electoral processes. A choice in which technology is used requires more technological know-how [3]. As technology usage increases every passing day, transaction security is needed more. 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 [4]. The technology-enabled voting system is convenient as it is accurate, faster, and requires less labor compared to printed ballots. Technologies such as encryption are used to ensure the security of every vote. But digital 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 [5]. When years go by, scholars have suggested new concepts that could be integrated into the smooth conduct of democratic voting. Emerging technologies such as RFID, Internet, Internet, Biometrics, Smart Cards, NFC, Cloud Services, IoT, Blockchain, and so on have been introduced. Model numbers have also been suggested. Yet none of the schemes proposed met any requirement of a free and transparent voting procedure. In this study, authors are endeavoured to highlight the involvement of various researchers within voting and system implementation of digital technology, established some research goals, and proposed some solutions based on the study. The work contains research aim & methodology, literature review, a summary of findings, research agenda based on the study, recommendations based on the study, and conclusion.

2. RESEARCH AIM AND METHODOLOGY:

This paper mainly focuses on the role of different computing technologies in the development of smart and secure public voting systems. The main objectives of this research article are mentioned below:

- To understand the role of technology on voting systems
- To review the contribution of researches on the topic of study
- To familiarize with technologies adapted in construction of voting systems
- To identify the Research Gaps in comparison with existing systems
- To recommend new approaches based on the study

This literature review paper discusses and explores technology applications on the development of Voting Systems. The adaptive technologies include RFID, Smart Card, IoT, Blockchain, Cloud Architecture, Artificial Intelligence, connecting options, etc are analyzed. This literature analysis is shaped using the secondary data collected by revising a good number of articles published in reputable journals and internet sources. The paper also includes outlined research gaps and recommendations for fool proof voting systems.

3. LITERATURE REVIEW :

An electoral system or voting scheme is a set of instructions that govern how elections and referendums are to be performed and their

outcomes decided. It involves time to conduct the election, eligible electors, appropriate candidates, how ballots are marked and cast, way of conducting the election, limitation of the election campaign, factors affecting results of an election, etc. Democratic electoral systems are defined by constitutions and electoral laws, are typically run by election commissions, and multiple forms of elections may be used for different offices. Free and fair-minded elections are the foundation stone of every sound democracy. Yet free and fair elections are easier than it sounds. It is much more complex and difficult in a vast and diverse country, like India. The whole process entails humongous logistical problems in terms of both resources and manpower. Free and equal elections all participants in the game must have a level playing field. The electoral mechanism as a whole will catch a true voter mood. The incorporation of information and communications technology (ICT) into the democratic process creates consciousness and apprehension among electors around the world, as well as specialists. Today, most Electoral Management Bodies (EMBs) around the world are using new technology to improve the electoral process.

The author suggested a new electronic voting process using Election systems and ATSRAL language-functioning software machines. It consists of a Direct Recording Electronic Voting Machine (DRE) called iVotranic, a Touch Screen to cast a vote, a Real-Time Audit Log Printer (RTAL) that performs the task of a VVPAT, a Personalized Electronic Ballot (PEB), a device in use by the polling place to load a ballot, unlock the next ballot and obtain tabulated and evaluation information and a compact flash card (CFC) contains large files that do not fit inside the PEB. (Weldemariam *et al.*, 2010) [6].

Grainger Fingerprint SDK Recognition library includes the biometrically safe smartphone voting technique. Fingerprint readers were applications for collecting and storing the fingerprints. Users can register to vote anywhere using the mobile internet, and from anywhere can vote for any candidate. Even once the method of confirming and recording fingerprints needs an electoral office visit (Gentles *et al.*, 2011) [7].

Electronic voting machines are physically targeted. Vote stealing, denial of service, malicious code injection, etc. will be done on voting machines. Those threats are handled with new rigorous voting procedures by new voting machine hardware and software. Windows CE application called Ballot station handles the voting-related operations. Machine mode is often set depending on the memory card which is inserted. If a memory card is removed or a system reboot is inserted, or a new card is inserted, the machine will set new card mode. Then once the election mode has been set, power failure or system failure must return the machine to the same election mode to continue the voting without fail (Lavanya 2011) [8].

Using a centralized database, a structured user interface shows a list of all constituencies and candidates competing. The online election process is conducted using a local database at each polling station and updated to the central database once the election process is complete. RFID biometric security is provided by creating each voter with a unique 12 byte RFID code and 5 digit password as well as a multi-level fingerprint for each voter. A general structure of RFID system architecture is shown in figure 1(Ankita *et al.*, 2013) [9].

For security tools, a new voting system is implemented with the Pallier cryptosystem and blind signature scheme built on RSA. Module involves Central tabulating facility to gathering all secret ballots from local servers which communicate between polling stations and distribute them. Each server at the local polling station is connected to several embedded systems called voting terminals or machines that are used to build the ballot of the voter. The homomorphic property allows for security on Pailier cryptosystems and keeps secret ballots without description. The blind signature scheme on RSA masks the name of the elector and his vote cast. Eligibility and uniqueness are fulfilled using the RFID technique (Hussien & Aboelnaga 2013) [10].

The author proposes an online voting system for India to cast votes anywhere and to any candidate he/she wishes. Adhaar card is used for unique voter identification to prevent multiple ballots and provide high-security measures in the election process. The counting of votes and the computation of results facilitated the use of the central database established by the Indian election commission

(Agarwal & Pandey, 2013) [11].

Cloud computing technology is used to build an I-Voting system called "Cloud-based Integrated Election Voting System (CIEVS)" (shown in figure 2) to provide an additional channel for voting to Indian corporate.

Using cloud computing, online infrastructure and mobile telephone networks, it leverages new information and communication technology to combine the current Electronic Voting Machine (EVM) system by means of the I-Voting method to get an answer to the problem of low voting in Indian elections (Matharu *et al.*,2014) [12].

For voting, three different sizes of 3-D face recognition technology modules are used. The design used the Bosphorus database (one of the publicly accessible 3D Face databases) to include at least six simple facial expressions along with 3D landmarks. The notion of face decomposition for 3D face recognition is used to find the recognition rate. The researcher used two types of voting schemes to perform the modular experimentation: Majority Voting System (MVS) as well as Weighted Voting Scheme (WVS). Also, it's evident that the MVS algorithm determines the largest number of subjects voted irrespective of the recognition rate (Ujir *et al.*, 2014) [13]. The author(s) suggest that the SMS system needs more study and innovation to reach all sections of the society in order to sustain voter trust Raise and election officers become more active in conducting simple, safe and strategic choices (Mythili *et al.*, 2014) [14].

The robust e-voting system is developed using the ATM and Micro ATM terminals. This solution avoids redundant votes by using OTP and Random Security Question (RSQ) dual-tiered authentication. Contestants are issued with nominee IDs that help protect voter and candidate privacy. This also assists in the counting of ballots. RESTful web services are used by providing a fast response for all transactions to ensure the minimum load on servers. This robust voting machine is cost-effective too (Malladi *et al.*, 2014) [15].

The e-voting system is designed across multiple boundaries, such as geographical, cultural, and linguistic boundaries, descriptive of complex systems. E-voting systems focus solely on necessities, methodical configurations, and execution skills to help choices from various aspects of registration and verification, by balloting and counting outcomes (Adeshina & Ojo 2014) [16]. Secure voting is invented via Android-based mobile phones. It uses NFC technology to store voting data before a vote is cast. The NFC tag attached to the mobile phone will be used to confirm the voting information and display the list of candidates. It also helps him to cast a vote using a mobile phone to the preferred candidate. In the application, each vote is recorded and used for counting (Nikam *et al.*, 2014) [17].

The author looks at Salta's experience, the first Argentine district in 2013 to carry out e-voting for the entire voters. It analyzes the elector's knowledge and experience in the election process, based on a sample of 1,000 voters at the 2013 provincial election. He found that the overall support for e-voting and optimistic perceptions of integrity in the electoral process are strongly influenced by the capabilities of an elector to use the voting machine without extra help (Pomares *et al.*, 2014) [18].

The voting device uses an iris detection mechanism to ensure the identity of the voter before casting the vote. This application scans the iris using the Daughman algorithm. A database stores one entry for each voter and has its Adhaar card number stored. This entry stores an image of each voter's iris with other details. The database is updated once a year to add or remove the voter entries. Once the individual enters the booth to cast his vote, his iris image is scanned and checked against the data that is stored in the database. This system tests electors to avoid dummy votes. The application also helps record the total votes cast and helps determine the election winner (Shital & Pravin 2015) [19].

The authors proposed a voting system online and offline. Authenticated voters and data protection aspects of polling were discussed for the e-voting framework. Voter registration and authentication are done via online and OTP. It also ensures that unauthorized persons cannot alter the casting of votes. GSM program with cryptography technique is used to hold several voters and cast voting information is stored from time to time in the database. Offline e-voting uses iris recognition to authenticate electors to cast votes (Dixit, *et al.*, 2015) [20].

The new project uses fingerprint-based authentication to improve security by preventing fake voting and voting repetition. As an additional security measure, photo and voter information are displayed from a remote server on ARM9 LCD, and results are viewed by an approved person on the central server. The software code is built for interfacing the ARM processor with the finger-print module in WINCE6 development environment. The system provides the best solution to minimize the voter identification time taken. The FP-EVM architecture is compact, versatile, and has low power consumption (Sudhakar & Sai, 2015) [21].

Du-Vote is a modern remote electronic voting system that removes the often-demanded expectation that people trust general-use computers. Trust is distributed in Du-Vote between a simple hardware token given to the candidate, the election system, and a server run by electoral authorities. Accordingly, the author avoided designs that would require tokens to have cameras, GUIs, or operating systems for general use (Grewal *et al.,* 2015) [22].

A new EVS uses the RSA-based Pailier cryptosystem and blind signature as security instruments. It consists of CTF, which communicates with multiple servers of the local committee (each work as a polling machine) distributed among polling stations. RSA-based blind signature shades the polls and voter identification to meet security criteria for privacy and accuracy. Here RFID is used to preserve voter uniqueness (Dyta *et al.*, 2015) [23].

A voter identification card is replaced with a smart card to store the person's information in this new voting system. The smart card reader is used to read a person's information and the iris recognition is used to further verify the user. If a person tries to cast the vote multiple times, then the beep sound will be provided by the smart card reader (Nithya *et al.*, 2015) [24].

The author proposed a method for a harmless and reliable biometric voting structure based on Aadhaar, to prevent inconsistencies that would arise in elections. If an alcoholic approach a polling booth, buzzer warns approved individuals or constables in the duty. We can have peaceful surroundings at the polling stand because of the alcoholic sensor. It also gives a buzzer when an unauthorised user enters to participate or when the exact person enters with valid RFID several times, and the officer at booth level may take the appropriate action (Madan Mohan & Srihari 2015) [25].

The user has to use fingerprints in a new voting system to test the genuine vote. The fingerprint module was installed in the database for the government. This voting system was coupled to the computer that has a full database of the people who are eligible to vote. The corresponding individual identity was removed after every polling. A printer used to provide the voter with a confirmation sheet while the individual is polling the vote and use the GSM module to submit the result to the corresponding authority (Anandaraj *et al.*, 2015) [26].

The fingerprint module uses Atmega328p to authenticate the user. It operates with a real-time, embedded operating system and wireless mode of communication. Authenticated details of an adhaar card are processed and stored on the server. It will have many channels real-time or with Zigbee, handling wireless transmission, as well as other functions (Naik 2015) [27].

WinVote system is an embedded device based on Windows XP which features a touch screen, USB ports, and a minor thermal paper printer. It uses Wi-Fi to set up election contestants' voting machine, their details, and other information about the configuration. It also helps polling officers to get polling summaries of all WinVote machines placed at all booths via WiFi connection (Epstein 2015) [28].

The voter is marked with its special thumb impression, which is stored in the database. Thumb is provided by the voter as an input during elections and compared to the database to ensure the correct identification of the voter. This system detects fraudulent voters or voters who attempt to cast multiple votes and any complaint is told to the nearest police station. All voting machines are configured to the main host network. It would help make the counting process at the end of the election simpler. It uses cloud-based IoT devices to get maximum benefits with minimal costs during the election (Nithya *et al.*, 2016) [29].

The study puts a stable planning system down to

earth Voting plans to establish in this present reality a protected, creative, and freely satisfactory execution of the voting procedure (Shrivastava & Tere 2016) [30]. The biometric voting system (BVS) uses data stored in the Indian Citizens' Aadhaar Card database. Iris and fingerprint images are stored to identify unique persons on details of the Aadhaar card details. This BVS is linked to a biometric fingerprint system that uses data stored in the database to recognize authenticated voters. ASP.NET, C#, and SQL Server 2014 implement this framework (Chakraborty *et al.*, 2016) [31]. To have user authentication, fingerprint, and NFC smart card entry authenticates voting. Multiple votes are managed to avoid using the polling picture with casted voting information and printed using a POS printer to verify multiple levels (Hasan *et al.*, 2016) [32].

If a citizen decides to vote a candidate, he/she must authenticate him/herself by offering his / her identification number, registration password, and QR-code ballot card. Online voting is enabled via the Web portal where the site's URL is provided in the ballot card and the voting blockchain is used to determine whether or not he has already voted. Here blockchain is used to store the list of registered voters who have already cast votes, the information of their casted votes and the qualified persons who have not yet cast votes are confirmed (Barnes *et al.*, 2016) [33].

The author defined a hybrid voting machine using an algorithm matching hash base finger to verify the voter. Hash feature is used for voter registration and verification. Counting voting is also made easier in Pakistan utilizing high-speed techniques (Arooj & Riaz 2016) [34].

A fingerprint database is used to validate votes during elections. Numerous votes, illegal votes are denied and at minimal expense avoided. This communication is introduced by Zigbee, a wireless mesh network technology with low power and cost. Upon voting the age is checked and if the elector will not participate in voting for more than three elections the nationality will be revoked. The specially disabled would have a machine for swipe on which to vote using their AADHAR card. The results of these simulations are confirmed using Keil Vision (Dhinesh *et al.,* 2016) [35].

Next-generation high-tech techniques such as face recognition, one-time password techniques and fingerprint recognition techniques to implement the new e-voting system are being explored. This provides authentication, confidentiality, and integrity of data using the requisite electronic signature, encryption techniques, and hash functions in Voting (Bindia & Aggarwal 2016) [36].

If the elector is disappointed with all the candidates, the current system of politics or elections can be rejected by a protest vote in the system of e-voting. Every time a voter casts a ballot; the transaction is recorded and updated using Blockchain. Each voter's vote in the form of a node is connected with Blockchain from booth to booth. Decentralized voting system is created by having a network node to each district (Ayed 2016) [37].

The author suggested a new voting method in India, by connecting the fingerprint-based image database with voter Id. When the vote has been cast, an approval message will be sent to the registered phone number of the voter and information will also be stored using IoT in the local database management. To find the invalid voters or vote attempts to cast several ballots, Buzzer will be put in the voting booth (Sarankumar *et al.*, 2017) [38].

A solar-powered EVM tackles the problems triggered by the power-hungry nation. The author proposed the design of an efficient solar-powered EVM prototype that will perform all the tasks involved in voting, such as the collection, counting, and security of votes. Besides, it also removes system errors, since it is a digital device. This prototype was created by offering three stages of password protection with three-stage security encryption (Anik *et al.*, 2017) [39].

The Smart Phone app allows users to vote with full protection via mobile, supported by OTP. The app requires an Aadhaar card, barcode reader, and captcha to identify people and continue voting. The vote counting can be determined at the time of the vote itself. Option setting allows users to change personal details such as a mobile number. The App helps users to have reviewed when they vote (Baig *et al.*, 2017) [40]. Voter's cell phone gets confirmation notification of a positive vote. IoT will be used to communicate the votes cast to the

database needed for ease of complete counting (Deepika *et al.*, 2017) [41]. The digital voting system generates the list of eligible voters based on a database of Aadhaar cards. This also keeps voters monitoring to cast their ballots. Votes can quickly access their voter Id based on their number of mail ids and Aadhaar cards. Finger print-based application also offers the ability to vote online (Bhuvanapriya *et al.*, 2017) [42].

In election scheme, which uses blockchain technology, smart contracts are used to protect voter privacy. Author considers a modern method of voting that is cost efficient alternatives. With the use of Ethereum private blockchain, hundreds of transactions per second can be submitted to the network which reduces the network burden via smart contract. The turnout of voters here is theoretically improved by casting the vote to candidate belongs to his district wherever it is (Hjálmarsson *et al.*, 2018) [43].

Elections laws are regulated by open and deterministic smart contracts with blockchain technologies for each voting procedure. User mobile phone numbers are used for voting authentication and third-party servers are avoided. Results proved the program's feasibility in providing a way for the ideal environments. (Khoury *et al.*, 2018) [44].

A smart voting program provides voters with different forms of authentication, based on mobile availability. OTP is provided if the user owns a smartphone and can cast their vote from anywhere. For some, the biometric system is used to authenticate using the data stored in the server database (Oracle 9i is used for implementation). Using cryptography the casted vote is encrypted. It uses the Mix net method to perform permutation on inputs and generates an encrypted message. Only those allowed to have the decryption key may decrypt it and count the casting vote. Here the GSM modem is used to connect voters via a web server (Microsoft IIS) to the voting system (Patil *et al.*, 2018) [45].

The author suggested voting is done by providing Aadhaar and fingerprint authentication with low-cost host PIC Microcontroller control. Once the user casts their vote, the vote count will be transferred to PC directly using the Internet of Things. High level IEEE 802.15.4 based wireless communication protocol ZigBee is used and implemented here (Snega *et al.,* 2018) [46].

The E-voting based on the retina has given client authentication much more reliable security. In this task, the process of extraction of the feature is carried out by the fuzzy logic as well as the matching procedure is complete by the hamming distance and Manhattan distance to compare frequent forms in similarity measurements between the retinal pictures and to identify probabilities of detection in retina layers. Similarities of the blood vessels are observed using angular and radial partitioning techniques. This method ensures greater security and the E-voting system accomplishes optimum results (Abirami *et al.*, 2018) [47].

Linux platform based, the author proposes a new voting method for multiple candidates. Blockchain based this voting method holds voting records on the DLT to tackle voting forgery. This model makes use of the ECC public key cryptography for user authentication and non-repudiation. It forces every person to cast his or her vote. It is designed with a new function to remove the vote cast before a defined time limit. User votes are encrypted and processed using blocks, so when they have the same timestamp a block with higher signature value is selected over others. (Yi 2019) [48].

The innovations have been incorporated into traditional voting systems. This new technology includes a stable technique of data storage called a blockchain that is used for cryptocurrencies and is known for its protection. Cloud-based storage (SAAS) will update the votes that are recorded by the EVM. Any adjustments through the voting panel or interference with the votes will cause the hash to break the link and any anomalies can be avoided by marking them as NOTA by identifying the manipulated votes and therefore by no means affect the polling. Blockchain technology has played a major Proof of Work feature that prevents the continuous generation of data blocks, thereby preventing rapid manipulation of the data. This approach also includes the hashes created along with the blocks that are only to be added to a cloud hash table. The EVM data can help to define the deceptive point when tapped with the hash table (Sathya *et al.*, 2019) [49].

In the "Vote from Anywhere" system, authors

required to maintain a database that is generated based on details of the Aadhaar card. Using a fingerprint scanner, when an elector enters to cast his ballot, his fingerprint is taken and compared to the database to ensure voter identification. If he is correct, the web portal allows him to cast a vote, and increases and encrypts the count of votes; eventually, the account of voting is disabled to prevent multiple or false votes. Here, the administrator monitors, updates, and deletes the correct list of candidates and their related details that are running for election via the web portal (Jagtap *et.al.,* 2019*)* [50].

The author proposed an EVM system that catches a voter's facial image through a deep face recognition system based on CNN, verifies it with the pre-captured images in the database, the result is right, assumes the voter is a valid one and asks him to cast his vote for a political group. Upon voting, the voter's facial orientation will be removed from the system, ensuring the voter can only vote once (Mondal & Chatterjee, 2019) [51].

The author proposed a new voting method using RFID and IoT to improvise the protection mechanisms. An active RFID tag is used where, regardless of the voter id, the machine will check the tag and match the fingerprints obtained in the Aadhar database. The voter must scan the RFID tag for identification and the voter must further verify the presence with the fingerprints. If the prints matched against the gathered database, the persons could cast their votes effectively, else the buzzer would be alarmed to stop invalid voters casting out (Mansingh *et al.*, 2020) [52].

The voting system (shown in figure 3) is implemented using Blockchain technology, using the Consensus/Proof-of-Work algorithm to offer high reliability and security. The figure shows the proposed E-Voting system architecture diagram consisting mainly of software (admin), the user (electors), and the mechanism starts with user login through a web application. The admin (election authority) gathers all the details of the vote a few days before the voting and then provides the elector its unique login Id and password that the elector will use to log in to cast the vote on Election Day. Such voters use this voting information, and more details are deposited in the private cloud database that the Election Authority maintains. Later votes, using the Blockchain consensus algorithm, are stored in a block to provide greater security. This information is used by the election commission for counting to announce the results. The framework practices the MD5 algorithm for user encryption-decryption, and the vote encryption- decryption algorithm SHA-256.The core principle of the scheme is to safeguard the cloud database highly containing the exit polls from any threat or unethical activities which will destroy the entire process (Shakkeera *et al.*, 2020) [53]. The researcher has introduced a new system of voting that emphasizes on potential face detection and identification and biometric authentication features, including biometric scanning, and the execution plan that improves protection and prevents duplicate and voting fraud to make the system more efficient and cost effective. Face recognition using Eigen's face-based recognition algorithm and Minutiae based algorithm helps make the conventional voting system stronger and safer using a two-factor bio-metric authentication method with a full-pledged database as an input. (Komatineni & Lingala 2020) [54].

4. SUMMARY OF FINDINGS :

Table 1: List of contributions of researchers on Voting systems from 2010-2020.

SN	Author(s)	Year	Technology used	Findings
1	Weldemariam, *et al.* [6]	2010	ASTRAL language	To conduct an election on its day using the ES & S system.
2	Gentles, *et al.* [7]	2011	Android 3.0 (Honeycomb)	Biometric secured voting using mobile is developed.
3	Lavanya [8]	2011	Windows CE application	New technologies to maintain safe and secure voting are implemented.
4	Kumar, *et al.* [55]	2012	Biometric devices	Various types of EVM, issues, biometric

				used are studied.
5	Ankita *et al*. [9]	2013	RFID Biometrics	The limitation of maintaining a centralized voter database according to their constituency is resolved, and multilevel security is implemented through RFID biometric security during the election process.
6	Hussien, & Aboelnaga [10]	2013	Homomorphic System and Blind signature scheme with RFID	For security tools, a new voting system is implemented with Pallier cryptosystem and a blind signature scheme created on RSA.
7	Agarwal, & Pandey [11]	2013	Web-based and Fingerprint recognizer software	A person can vote from anywhere from their allotted constituency or their preferred location.
8	Matharu, *et al*. [12]	2014	Cloud-based ICT	It leverages ICT to combine the current Electronic Voting Machine system with the I-Voting system to increase voting percentages in India.
9	Ujir, *et al*. [13]	2014	3-D face recognition technology	For voting, modular approach human 3D faces recognition through neutral and 6 simple facial image expressions tests were conducted.
10	Mythili, *et al*. [14]	2014	Biometric devices	Voting is conducted using the SMS voting method.
11	Malladi, *et al*. [15]	2014	RESTful web services	Robust e-voting system developed using Micro ATM terminals avoids redundant votes by using OTP and Random Security Question (RSQ) dual-tiered authentication.
12	Adeshina, & Ojo [16]	2014	Online Web portal	E-voting systems focus solely on requirements, technical configurations, and implementation technologies to help choices from various aspects of registration and verification, by balloting and counting outcome.
13	Nikam, *et al*. [17]	2014	NFC with RFID	NFC tags attached mobile phones help users to get candidate information with security and allows people to cast vote anywhere.
14	Pomares, *et al*. [18]	2014	Online voting	A voting machine without the assistance of the user in the election process.
15	Shital & Pravin [19]	2015	Daughman algorithm to scan Iris detection.	The iris detection mechanism is used to scan every voter's iris and match against the same that is stored in the database to prevent dummy votes.
16	Dixit, *et al*. [20]	2015	GSM devises with cryptography techniques and Iris recognition	GSM devise with cryptography technique is used to maintain the number of voters and cast voting information are stored from time to time in the database. Offline

			techniques.	e-voting uses iris recognition to authenticate electors to cast votes.
17	Sudhakar & Sai [21]	2015	Fingerprint-based electronic voting machine using ARM9 microcontroller.	Fingerprint-based authentication to improve security by preventing fake voting and voting repetition
18	Grewal, *et al*. [22]	2015	Du-Vote is a new remote electronic voting protocol	In Du-Vote, trust is distributed between a simple hardware token that is given to the candidate, the voting machine, and a server executed by election authority persons.
19	Data, *et al*. [23]	2015	Paillier cryptosystem and blind signature method.	RSA-based Pailier cryptosystem and blind signature scheme for EVS is designed.
20	Nithya, *et al*. [24]	2015	Smart card and Iris recognition	The smart card reader is used to read a person's information and the iris recognition is used to further verify the user.
21	Madan Mohan & Srihari [25]	2015	RFID	A biometric voting method based on Aadhar card to prevent misconceptions.
22	Anandaraj, *et al*. [26]	2015	GSM module with fingerprint device	Fingerprint devise for authentication and GSM module for updating voting details in the database.
23	Naik [27]	2015	Atmega328 and Zigbee Module	A small-sized - smart wireless voting machine with authentication using Atmega328p is implemented.
24	Epstein [28]	2015	WiFi connectivity	WiFi connectivity helps polling officers to get polling summaries of all such WinVote machines placed at all booths.
25	Nithya, *et al*. [29]	2016	PIC 16F877A, Gsm Module, Cloud Storage.	It uses cloud-based IoT devices to get maximum benefits with minimal costs during the election.
26	Chakraborty, *et al*. [31]	2016	Fingerprint and Iris recognition	BVS is linked to a biometric fingerprint system that uses data stored in the database to recognize authenticated voters.
27	Hasan, *et al*. [32]	2016	Raspberry Pi 2, Arduino Uno, R3 microcontroller	Additional votes are prevented by using the photograph of the candidate with the details he casts.
28	Barnes, *et al*. [33]	2016	Blockchain	Digital voting with blockchain technology
29	Arooj & Riaz [34]	2016	Hash-based finger matching algorithm	A hybrid machine to verify the voter using hash base finger matching algorithm.
30	Dhinesh, *et al*. [35]	2016	ZigBee wireless technology	Zigbee, a wireless mesh network technology with low power and cost implements required communication during voting.
31	Bindia, & Aggarwal [36]	2016	An electronic signature, encryption	E-voting techniques like one-time password techniques, face recognition, and fingerprint recognition techniques.

			techniques, and hash functions	
32	Ayed [37]	2017	Blockchain technology	The new EVM could be used in local or national elections with a low cost.
33	Sarankumar, *et al*. [38]	2017	RS232 serial data transmission cable is used to connect the fingerprint module with Arduino.	Voter details are communicated using IoT to the database automatically.
34	Priya, *et al*. [56]	2017	Arduino and Finger Print Scanner	Arduino controls complete processes such as read button, increase vote value, generate results, and send vote and result to LCD.
35	Rezwan, *et al*. [57]	2017	Arduino and Finger Print Scanner	Arduino and Finger Print Scanner, capable of identifying every voter, counting votes, and preventing fake votes in Bangladesh.
36	Anik, *et al*. [39]	2017	Solar power based	Solar-powered EVM prototype that will perform all the tasks involved in voting.
37	Saravanan, *et al*. [58]	2017	Iris recognition	EVM is used with the IRIS recognition system, and AADHAR card database access is used for IRIS.
38	Selvarani, *et al*. [59]	2017	SMS using smartphone	Online voter registration, voting, and display of results using the SMS concept.
39	Baig, *et al*. [40]	2017	Smartphone App	The smartphone app allows users to cast the vote using mobile with complete security provided using OTP.
40	Deepika, *et al*. [41]	2017	IoT based	IoT will be used to communicate the votes cast to the database needed for ease of complete counting.
41	Bhuvanapriya, *et al*. [42]	2017	Smart device	Finger print-based application also offers the ability to vote online and 100% voting.
42	Kavitha, et al [60]	2018	Fingerprint, face and iris recognition	the voting system based on the Fingerprints and Iris verification is used.
43	Hjálmarsson, *et al*. [43]	2018	Blockchain-based	Blockchain-based technology that improves security and reduces the expense of holding a national election.
44	Khoury, *et al*. [44]	2018	Blockchain-based	Ethereum Blockchain-based decentralized voting platform.
45	Shaw, *et al*. [61]	2018	Arduino UNO	Arduino based Aadhar facilitated an EVM execution with Two-Tier fingerprint security.
46	Prabhakaran, *et al*. [62]	2018	Iris acknowledgment and thumb impression	voting framework with protection and security.
47	Kadam, *et al*. [63]	2018	ATMEGA 32 microcontroller.	Voting machine built with ATMEGA 32 microcontroller provides three-layered extra security.
48	Patil, *et al*. [45]	2018	Smartphone with cryptography	Next-generation online highly secure voting system.

			algorithms	
49	Shejwal, *et al*. [64]	2018	Blockchain	The usage of a blockchain in the delivery of e-voting databases will reduce the sources of database abuse cheating.
50	Sega, *et al*. [46]	2018	IoT	The vote count will be transferred to PC directly using the Internet of Things.
51	Abhirami, *et al* [47]	2018	Retina recognition using Fuzzy logic	Retina Based Voting Machine integrated with the RETINA recognition concept is designed.
52	Lakshmi & Kalpana [65]	2018	Arduino UNO	A secured electronic voting machine with a unique identification number (i.e. AADHAR number) has been introduced.
53	Yi [48]	2019	Blockchain	The blockchain-based voting system can be implemented to a range of networking applications directly.
54	Al-Rawy & Elçi [66]	2019	Blockchain	It provides availability, the immutability of results, and the privacy of ballots through double private Blockchain.
55	Jamkar, *et al.* [67]	2019	Arduino and Fingerprint module	An advanced framework, using the Arduino and Fingerprint module to eliminate abuse and defraud voting methods.
56	Sathya, *et al* [49]	2019	Blockchain-based Cloud computing	Cloud-based blockchain technologies can boost essential transparency and ballot information security.
57	Sadia, *et al* [68]	2019	Blockchain in association with Smart Contract.	The healthy election that is allowed by Smart Contract assistance
58	Salami, *et al* [69]	2019	A new programming language with OTP	Java programming language was used to encode the OTP algorithm into the current e-voting technique
59	Jagtap, *et al* [50]	2019	Raspberry Pi and TFT module	"Vote from Anywhere" system enables the voter to cast his vote from anywhere in India
60	Shanmugasundaram, *et al* [70]	2019	Blockchain	Integrating blockchain technology with biometric devices will make the electoral process more reliable and transparent
61	Mondal, & Chatterjee [51]	2019	Deep learning with face recognition	A secure and hassle-free face recognition based digital voting machine
62	Li, *et al* [71]	2020	IoT with Blockchain	Self- tallying systems in decentralized IoT based on Blockchain
63	Mansingh, *et al* [52]	2020	IoT	A new system of voting for improvising the security mechanisms using RFID and IoT is proposed.
64	Shakkeera, *et al* [53]	2020	Cloud-based technology using Blockchain	Ensures data integrity, and data confidentiality reduces extra storage and the overall electronic voting time consumption.

65	Mohan, *et al* [72]	2020	Arduino Uno	Improve protection by resolving bogus voting and fingerprint-based authentication.
66	Komatineni, & Lingala [54]	2020	Face recognition with Eigen face-based recognition algorithm and Minutiae based algorithm.	The two-factor Bio-metric authentication process with a full-pledged database as an input turns the regular voting system hooked on a robust and safer one.

5. IDENTIFIED RESEARCH AGENDA :

There is a very substantial amount of research on the use of new technologies in the voting system. System management viewpoints or strategies have been widely based but little attention has been paid to trustworthiness. However, research concentrate on the voting system and only the technical considerations have been taken into account. This study is being attempted to fill that gap. This research study is also unique as it has taken into account the full set of variables, the researchers' observations, the comparison of their explanations, and impressions of key technology
factors in voting, in a single sample. The following research agendas are identified.

1] What model would make an election system intelligent and intelligent to use new digital technology for the smart & informed voting process?
2] What new technology framework can be proposed to integrate an intelligent voting system with the best possible use of digital pedagogy and communication elements?
3] What Digital Technology can be proposed for election commission that reduces the software, hardware, and connectivity and storage complexities?
4] What Digital Platform can be proposed to link key stakeholders in one smart digital voting solution during the voting process?
5] What approaches to digital voting have progressed and will continue to advance about the technical context in the democratic voting process?
6] How an integrated automated voting system can be suggested for integrating all of the day's unaddressed voting system problems?.

6. RECOMMENDATION BASED ON THE STUDY :

Developing electronic voting systems is not only a security issue but also a basic concept in open elections to protect the legitimacy of the vote. There is currently no established technology capable of ensuring the privacy, confidentiality, and verifiability of a recorded ballot being information transmitted. Digital voting has many disadvantages and is inherently unsafe. There is space for unattended voting abuse as well as other security flaws like a possible [73] of service disruptions, malware encroachments, and privacy concerns. Online voting doesn't produce a trail on audit paper. Blockchain-based voting, which relies on a decentralized, distributed digital ledger, has not been proven secure and is vulnerable to so many of the security flaws inherent in electronic voting, such as the potential of hackers to alter ballots on a local voter's machine before the ballot is transmitted, and the failure of secret ballots. Several active projects aim to build secure hardware by introducing new CPU designs to improve immune hardware for software-based attacks [74]. Future systems based on stable hardware can provide additional security but the technology is still in initial stages. End-to-end demonstrable election software relies on cryptography to encrypt and secure votes so that electors can see that their vote has been legally registered, the vote has also been tabulated correctly and the final vote count meets the cast votes. End-to-end factual applications can be built into current election systems to strengthen the security of voter technology. New open-source

software packages, such as end-to-end verifiability services, including the software development kit for Microsoft's Election Guard, could boost security if implemented in upcoming elections [75].

7. CONCLUSION :

Across history, people have battled for both the right to vote and count for their votes. They not only want the vote, but they also want to progress opportunities and choices. Some of their ambitions are down to earth: work, health care, schooling, and improved living standards. Democracy is the means to make them come true. Free and fair elections are the foundation of every democracy – an election is a time when the power is completely in people's hands when they vote to shape their country's future. But elections too often do not meet the standards required to ensure that citizens can effectively hold their governments to account through the ballot box. Many of the political problems facing the world are the same for both rich and poor countries; promoting engagement where there is high disillusionment with politics; combating bribery and corruption; and ensuring that everybody's vote counts regardless of who they are or where they live. Solutions to universal problems such as poverty, injustice, sustainability in the world, or political unrest begin at the ballot box by encouraging people to vote successfully. We have seen many of these problems at first hand over a long international career, as well as the transformative role that legitimate elections can have in empowering people around the world. This paper sheds light on the models suggested by numbers of writers for integrating emerging technology to make the election foolproof. We also identified some research gaps and proposed some studies-based solutions. By utilizing the potential of emerging digital technologies, these will help future researchers to use and evolve some new ideas.

REFERENCES:

[1] International, I. (2017). The Use of New Technologies in Electoral Processes the Use of New Technologies in Electoral Processes. *Workshop report: Praia, Cabo Verde. 22-23.* http://creativecommons.org/licenses/by-nc-sa/3.0/

[2] Russell, M., & Zamfir, I. (2018). Digital technology in elections Efficiency versus credibility? *EPRS. European Parliamentary Research Service*, Retrieved from http://www.europarl.europa.eu/RegData/etudes/BRIE/2018/625178/EPRS_BRI(2018)625178_EN.pdf 20/06/2020

[3] Peralta, R. (2016). Electronic voting. Retrieved from https://www.britannica.com/topic/electronic-votingon 20/06/2020

[4] Bhuyan, Dip Jyoti (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

[5] Electoral system. (2020). Retrieved from https://en.wikipedia.org/wiki/Electoral_system on 20/06/2020

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

[7] Gentles, D., & Sankaranarayanan, S. (2011). Biometric secured mobile voting. In *2011 Second Asian Himalayas International Conference on Internet (AH-ICI)* (pp. 1-6). IEEE. DOI: https://doi.org/10.1109/AHICI.2011.6113931

[8] Lavanya, S. (2011). Trusted secure electronic voting machine. In International Conference on Nanoscience, Engineering and Technology (ICONSET 2011) (pp. 505-507). IEEE.
DOI: https://doi.org/10.1109/ICONSET.2011.6168014

[9] Ankita K, Shwetha B, & Siddhita C (2013). Biometric and RFID Secured Centralised Voting System International Journal of Computer Science and Information Technologies (IJCSIT), 4(2), 255 – 258.

[10] Hussien, H., & Aboelnaga, H. (2013). Design of a secured e-voting system. In *2013*

International Conference on Computer Applications Technology (ICCAT). 1-5. IEEE. DOI: https://doi.org/10.1109/ICCAT.2013.6521985

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

[12] Matharu, G. S., Mishra, A., & Chhikara, P. (2014). CIEVS: a cloud-based framework to modernize the Indian election voting system. In *2014 IEEE International Conference on Computational Intelligence and Computing Research*, 1-6. DOI: https://doi.org/10.1109/ICCIC.2014.7238454

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

[14] Mythili, K., Kanagavalli, K., & Shibi, B. (2014). An efficient method to avoid false voting using sms voting approach. *International Journal of Computer Science and Mobile Computing*, *3*(2), 804-810.

[15] Malladi, K., Sridharan, S., & Jay Prakash, L. T. (2014). Architecting a large-scale ubiquitous e-voting solution for conducting government elections. In *2014 International Conference on Advances in Electronics Computers and Communications*. 1-6. IEEE. ISBN: 978-1-4799-5496-4. DOI: https://doi.org/10.1109/ICAECC.2014.7002445

[16] Adeshina, S. A., & Ojo, A. (2014). Design imperatives for e-voting as a sociotechnical system. In *2014 11th International Conference on Electronics, Computer and Computation (ICECCO)*. 1-4. IEEE. ISBN: 978-1-4799-4106-3. DOI: https://doi.org/10.1109/ICECCO.2014.6997569

[17] Nikam, R., Rankhambe, M., Raikwar, D., & Kashyap, A. (2014). Secured E-Voting Using NFC Technology. *International Journal of Computer Science and Information Technologies (IJCSIT)*, *5*(6), 8325-8327.

[18] Pomares, J., Levin, I., Alvarez, R. M., Mirau, G. L., & Ovejero, T. (2014). From piloting to roll-out: voting experience and trust in the first full e-election in argentina. In *2014 6th International Conference on Electronic Voting: Verifying the Vote (EVOTE)*. 1-10. IEEE. ISBN: 978-3-2000-3697-0. DOI: https://doi.org/10.1109/EVOTE.2014.7001136

[19] Shital A, P., & Praveen G, K. (2015). IRIS Detection in Voting System. *International Journal for Research in Applied Science & Engineering Technology (IJRASET)*, *3*(8), 469–473.

[20] Dixit, P. V., Phalke, S., Ubale, R., Gavali, A.B, Prajkta, S., & Aparna, S. (2015). A Biometric-Secure E-Voting System for Election Process. *International Journal of Advanced Engineering and Global Technology*, *3*(3), 425–430.

[21] Sudhakar, M., & Sai, B. D. S. (2015). Biometric system based electronic voting machine using arm9 microcontroller. *IOSR Journal of Electronics and Communication Engineering (IOSR-JECE)*, *10*(1), 57-65.

[22] Grewal, G. S., Ryan, M. D., Chen, L., & Clarkson, M. R. (2015). Du-vote: Remote electronic voting with untrusted computers. In *2015 IEEE 28th Computer Security Foundations Symposium* (pp. 155-169). IEEE. DOI: https://doi.org/10.1109/CSF.2015.18

[23] Dyta, P., Junjare, S., Pandita, A., & Ingle, D. R. (2015). E-Voting – Secured NFC Voting. *IJSRD - International Journal for Scientific Research & Development*, *3*(1), 1032–1036.

[24] Nithya, M. J., Abinaya, G., Sankareswari, B., & Saravana, M. L. (2015). Iris recognition based voting system. In *International Conference on Science, Technology, Engineering and Management (ICON-STEM)* (Vol. 10, pp. 44-51).

[25] Madan Mohan Reddy, B., & Srihari, D. (2015). RFID Based Biometric Voting Machine Linked to Aadhaar For Safe and Secure Voting. *International Journal of Science, Engineering and Technology Research (IJSETR)*, *4*(4), 995–1001.

[26] Anandaraj, S., Anish, R., & Devakumar, P. V. (2015). Secured electronic voting machine using biometric. In *2015 International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS)*. 1-5. IEEE. DOI: https://doi.org/10.1109/ICIIECS.2015.7192976.

[27] Naik, D. V. (2015). Smart wireless authenticating voting machine. In *2015 International Conference on Communications and Signal Processing (ICCSP)* (pp. 0785-0788). IEEE.

DOI: https://doi.org/10.1109/ICCSP.2015.7322599.

[28] Epstein, J. (2015). Weakness in Depth: A Voting Machine's Demise. *IEEE Security & Privacy*, *13*(3), 55-58. DOI: https://doi.org/10.1109/MSP.2015.46

[29] Nithya, S., Ashwin, C., Karthikeyan, C., & Ajith kumar, M. (2016). Advanced Secure Voting System with IoT. International Journal Of Engineering and Computer Science, 5(3), 16033–16037. DOI: https://doi.org/10.18535/ijecs/v5i3.31

[30] Shrivastava, V., & Tere, G. (2016). An analysis of electronic voting machine for its effectiveness. *International Journal of Computing Experiments (IJCE)*, *1* (1), 8-12.

[31] Chakraborty, S., Mukherjee, S., Sadhukhan, B., & Yasmin, K. T. (2016). Biometric voting system using Aadhaar card in India. *International journal of Innovative research in Computer and Communication Engineering*, *4*(4). 5284-5291.DOI: https://doi.org/10.15680/IJIRCCE.2016. 0404222.

[32] Hasan, S. M., Rashid, M. T., Chowdhury, M. S. S., & Rhaman, M. K. (2016). Development of a credible and integrated electronic voting machine based on contactless IC cards, biometric fingerprint credentials and POS printer. In *2016 IEEE Canadian Conference on Electrical and Computer Engineering (CCECE)* .1-5. IEEE. ISBN: 978-1-4673-8721-7. DOI: https://doi.org/10.1109/CCECE.2016.7726821

[33] Barnes, A., Brake, C., & Perry, T. (2016). Digital Voting with the use of Blockchain Technology. *Team Plymouth Pioneers-Plymouth University*. (pp. 1-4). IEEE. ISBN: 978-1-5386-4273-3. DOI: https://doi.org/10.1109/I2CT.2018.8529497

[34] Arooj, A., & Riaz, M. (2016). Electronic voting with biometric verification Offline and Hybrid EVMS solution. In *2016 Sixth International Conference on Innovative Computing Technology (INTECH)* (pp. 332-337). IEEE. ISBN: 978-1-5090-2000-3. DOI: https://doi.org/10.1109/INTECH.2016.7845009

[35] Dhinesh, K. M., Santhosh, A., Aranganadhan, N. S., & Praveenkumar, D. (2016). Embedded system based voting machine system using wireless technology. *International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering*, *4*(2), 127-130. DOI: https://doi.org/10.17148/IJIREEICE.2016.4232

[36] Bindia, & Aggarwal, N. (2016). NEXT GENERATION HI-TECH E-VOTING TECHNIQUES IN INDIA. *International Journal of Science, Engineering and Technology Research (IJSETR)*, *5*(1), 228–233.

[37] Ayed, A. B. (2017). A conceptual secure blockchain-based electronic voting system. International Journal of Network Security & Its Applications, 9(3), 01-09.

[38] Sarankumar, V., Sasikumar, M., Ramprabu, K., Sathishkumar, A., & Gladwin Moses Stephen, S. (2017). AADHAR BASED ELECTRONIC VOTING SYSTEM USING BIOMETRIC AUTHENTICATION AND IOT. International Journal of Recent Trends in Engineering Research (IJRTER), Special issue, 203–208. DOI: https://doi.org/10.23883/IJRTER.CONF.20170331.040.ARAT.

[39] Anik, A. A., Jameel, R., Anik, A. F., & Akter, N. (2017). Design of a solar power Electronic Voting Machine. In 2017 International Conference on Networking, Systems and Security 127-131. IEEE. ISBN: 978-1-5090-3260-0. DOI: https://doi.org/10.1109/NSysS.2017.7885813

[40] Baig, J. T. H., Babu, R., & Adhikari, J. (2017). Secured E Voting via Smart Phone App. International Journal on Future Revolution in Computer Science & Communication Engineering, 2(12), 20-23.

[41] Deepika, J., Kalaiselvi, S., Mahalakshmi, S., & Shifani, S. A. (2017). Smart electronic voting system based on biometric identification-survey. In 2017 Third International Conference on Science Technology Engineering & Management (ICONSTEM). 939-942. IEEE. ISBN: 978-1-5090-4855-7. DOI: https://doi.org/10.1109/ICONSTEM.2017.8261341

[42] Bhuvanapriya, R., Sivapriya, P., & Kalaiselvi, V. K. G. (2017). Smart voting. In 2017 2nd International Conference on Computing and Communications Technologies (ICCCT) (pp. 143-147). IEEE. ISBN: 978-1-5090-6221-8. DOI: https://doi.org/10.1109/ICCCT2.2017.7972261

[43] Hjálmarsson, F. Þ., Hreiðarsson, G. K., Hamdaqa, M., & Hjálmtýsson, G. (2018). Blockchain-based e-voting system. In 2018 IEEE 11th International Conference on Cloud Computing (CLOUD) (pp. 983-986). ISBN: 978-1-5386-7235-8. IEEE. DOI: https://doi.org/10.1109/CLOUD.2018.00151

[44] Khoury, D., Kfoury, E. F., Kassem, A., & Harb, H. (2018). Decentralized voting platform based on ethereum blockchain. In 2018 IEEE International Multidisciplinary Conference on Engineering Technology (IMCET).1-6. IEEE. ISBN: 978-1-5386-4500-0. DOI: https://doi.org/10.1109/IMCET.2018.8603050

[45] Patil, S., Bansal, A., Raina, U., Pujari, V., & Kumar, R. (2018). E-Smart Voting System with Secure Data Identification Using Cryptography. In *2018 3rd International Conference for Convergence in Technology (I2CT)*.

[46] Snega, S., Saundarya, S., & Balraj, R. (2018). Highly secured electronic voting machine using Aadhaar in IOT platform. *International Journal of Electrical and Electronics Research*, *6*(2), 41-47.

[47] Abirami, P., Jothi, R. A., & Palanisamy, V. (2018). 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,

[48] Yi, H. (2019). Securing e-voting based on blockchain in P2P network. *EURASIP Journal on Wireless Communications and Networking*, *2019*(1), 1-9. DOI: https://doi.org/10.1186/s13638-019-1473-6

[49] Sathya, V., Sarkar, A., Paul, A., & Mishra, S. (2019). Block Chain Based Cloud Computing Model on EVM Transactions for Secure Voting. In *2019 3rd International Conference on Computing Methodologies and Communication (ICCMC)* (pp. 1075-1079). IEEE. ISBN: 978-1-5386-7808-4. DOI: https://doi.org/10.1109/ICCMC.2019.8819649

[50] Jagtap, A. M., Kesarkar, V., & Supekar, A. (2019). Electronic Voting System using Biometrics, Raspberry Pi and TFT module. In *2019 3rd International Conference on Trends in Electronics and Informatics (ICOEI)*. 977-982. IEEE.ISBN: 978-1-5386-9439-8. DOI: https://doi.org/10.1109/ICOEI.2019.8862671

[51] Mondal, I., & Chatterjee, S. (2019). Secure and Hassle-Free EVM Through Deep Learning Based Face Recognition. In *2019 International Conference on Machine Learning, Big Data, Cloud and Parallel Computing (COMITCon)* (pp. 109-113). IEEE. ISBN: 978-1-7281-0211-5. DOI: https://doi.org/10.1109/COMITCon.2019.8862263

[52] Mansingh, P. B., Titus, T. J., & Devi, V. S. (2020). A Secured Biometric Voting System Using RFID Linked with the Aadhar Database. In *2020 6th International Conference on Advanced*

Computing and Communication Systems (ICACCS) (pp. 1116-1119). IEEE. DOI: https://doi.org/10.1109/ICACCS48705.2020.9074281

[53] Shakkeera, L., Hem Prasanth, K, C., Sabareesh, Begum, Sumaiya., & Vali Sharmasth (2020). Cloud Database Security in E-Voting System using Blockchain Technology. International Journal of Recent Technology and Engineering (IJRTE), 8(5), 1361-1370. DOI: https://doi.org/10.35940/ijrte.E6292.018520

[54] Komatineni, S., & Lingala, G. (2020). Secured E-voting System Using Two-factor Biometric Authentication. In *2020 Fourth International Conference on Computing Methodologies and Communication (ICCMC)* (pp. 245-248). IEEE. ISBN: 978-1-7281-4889-2. DOI: https://doi.org/10.1109/ICCMC48092.2020.ICCMC-00046

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

[56] Priya, V. K., Vimaladevi, V., Pandimeenal, B., & Dhivya, T. (2017). Arduino based smart electronic voting machine. In 2017 International Conference on Trends in Electronics and Informatics (ICEI) (pp. 641-644). IEEE. ISBN: 978-1-5090-4257-9. DOI: https://doi.org/10.1109/ICOEI.2017.8300781

[57] Rezwan, R., Ahmed, H., Biplob, M. R. N., Shuvo, S. M., & Rahman, M. A. (2017). Biometrically secured electronic voting machine. In 2017 IEEE Region 10 Humanitarian Technology Conference (R10-HTC) (pp. 510-512). IEEE. DOI: https://doi.org/10.1109/R10-HTC.2017.8289010

[58] Saravanan, N., Pavithra, K., & Nandhini, C. (2017). Iris Based E-Voting System Using Aadhar Database. International Journal of Scientific & Engineering Research, *8*(4), 62–64.

[59] Selvarani, X. I., Shruthi, M., Geethanjali, R., Syamala, R., & Pavithra, S. (2017). Secure voting system through SMS and using smart phone application. In 2017 International Conference on Algorithms, Methodology, Models and Applications in Emerging Technologies (ICAMMAET) (pp. 1-3). IEEE. ISBN: 978-1-5090-3378-2. DOI: https://doi.org/10.1109/ICAMMAET.2017.8186724

[60] Kavitha, S. N., Shahila, K., & Kumar, S. P. (2018). Biometrics Secured Voting System with Finger Print, Face and Iris Verification. In 2018 Second International Conference on Computing Methodologies and Communication (ICCMC) (pp. 743-746). IEEE. ISBN: 978-1-5386-3452-3. DOI: https://doi.org/10.1109/ICCMC.2018.8487558

[61] Shaw, S. K., Poddar, S., Singh, V., & Dogra, S. (2018). Design and Implementation of Arduino Based Voting Machine. In 2018 IEEE Electron Devices Kolkata Conference (EDKCON). 450-454). IEEE. ISBN: 978-1-5386-6415-5. DOI: https://doi.org/10.1109/EDKCON.2018.8770474

[62] Prabhakaran, G., Dharshini priya, T., Janani, N., Deepan Raj, R., & Elavarasan, P. (2018). Electronic voting machine based on fingerprint and iris authentication. International Journal of Intellectual Advancements and Research in Engineering Computations, 6(1), 135–139.

[63] Kadam, S. S., Choudhary, R. N., Dandekar, S., Bardhan, D., & Vaidya, N. B. (2018). Electronic Voting Machine with Enhanced Security. In 2018 3rd International Conference on Communication and Electronics Systems (ICCES). 403-406. IEEE.ISBN: 978-1-5386-4765-3. DOI: https://doi.org/10.1109/CESYS.2018.8723921

[64] Shejwal, S., Gaikwad, A., Jadhav, M., Nanaware, N., & Shikalgar, N (2018). E-voting using blockchain technology. *International Journal of Research and Analytical Reviews (IJRAR)*, 5(4), 895-906.

[65] Lakshmi, C. J., & Kalpana, S. (2018). Secured and transparent voting system using biometrics. In 2018 2nd International Conference on Inventive Systems and Control (ICISC) (pp.

343-350). IEEE. ISBN: 978-1-5386-0807-4.DOI: https://doi.org/10.1109/ICISC.2018.8399092

[66] Al-Rawy, M., & Elçi, A. (2018, October). A design for blockchain-based digital voting system. In The 2018 International Conference on Digital Science. 397-407. Springer, DOI: https://doi.org/10.13140/RG.2.2.28347.67360

[67] Jamkar, A., Kulkarni, O., Salunke, A., & Pljonkin, A. (2019). Biometric Voting Machine Based on Fingerprint Scanner and Arduino. In 2019 *2nd International Conference on Intelligent Communication and Computational Techniques (ICCT)*, 322-326. IEEE. ISBN: 978-1-7281-1711-9. DOI: https://doi.org/10.1109/ICCT46177.2019.8969034

[68] Sadia, K., Masuduzzaman, M., Paul, R. K., & Islam, A. (2019). Blockchain Based Secured E-voting by Using the Assistance of Smart Contract. *Springer IETE International Conference on Blockchain Technology (IC-BCT 2019)*. https://arxiv.org/abs/1910.13635

[69] Salami, H. J., Adebayo, O. S., Isah, A. O., Lawal, K. H., & Alhassan, J. K. (2019). Development of a Secured E-Voting System with OTP as Second Order Authentication. *i-Manager's Journal on Software Engineering*, 13(3), 7-14. DOI: https://doi.org/10.26634/jse.13.3.15686

[70] Shanmugasundaram, G., Kalaimathy, A., Johnvee, M., & Pavithra, S. (2019). Perspective Analysis of Digital Voting Systems. In 2019 IEEE International Conference on System, Computation, Automation and Networking (ICSCAN).1-6. IEEE. ISBN: 978-1-7281-1525-2.DOI: https://doi.org/10.1109/ICSCAN.2019.8878849

[71] Li, Y., Susilo, W., Yang, G., Yu, Y., Liu, D., & Guizani, M. (2019). A blockchain-based self-tallying voting scheme in decentralized IoT. https://arxiv.org/abs/1902.03710.

[72] Mohan, M. Madhu, M. Prakash, M. Madhuseelan, and A. Kishore Kumar (2020). Design of Secured Biometric Voting Machine. *International Journal of Research in Engineering, Science and Management*, 3(3),199-201.

[73] Hacker Community to Take on DARPA Hardware Defenses at DEF CON 2019 (2019). Retrieved from https://www.darpa.mil/news-events/2019-08-01on 29/06/2020

[74] System Security Integrated Through Hardware and Firmware (SSITH) Proposers Day (2017). Retrieved from https://www.darpa.mil/news-events/ssith-proposers-day on 29/06/2020

[75] Appel, Andrew (2018), End-to-End Verifiable Elections," Freedom to Tinker, Retrieved from https://freedom-to-tinker.com/2018/11/05/end-to-end-verifiable-elections/ on 29/06/2020

****