# A NOVEL COGNIZANCE OF RETICULATED CONTEMPORANEOUS THERMIONIC BALLOTING SYSTEMATIZATION WITH IOT

**K.Parvateesam**[1]
Assistant professor, Dept. of ECE,
Aditya College of Engineering and Technology,
Kakinada, AP, India[1]

**P.Satya Sruthi**[2]
Assistant professor, Dept. of CSE,
Aditya College of Engineering and Technology,
Kakinada, AP, India[2]

***Abstract*:** The Election polling system is not a new concept. It is the right of people to choose leader who works for their bright futures. In this connection so many proposals are invented. The most traditional way of the voting system is based on papers. It requires lot of paper work. The man power is also largely required for it. It is a time taking process also. In this present situation conducting polling process with large number of working people is difficult task. Due to increase in the COVID-19 cases the entire world is under Lock-Down. In this pandemic situation every body is under self quarantine. So in this situation it is better to develop new schemes and new procedures. The concept behind this problem is the proposes new scheme of this paper. It is possible to conduct elections without large gathering of people at one place or the large working crew. So in this connection a framework related to IoT can solve the problem with desired functionality. By designing simple hardware system with modules like finger print scanner sensor, Arduino module, WiFi module, power supply along with dashboard display. This approach can greatly reduce the paper work and large working crew. In place of finger print scanner it is possible to use iris scanner also to increase security and genuine results. So in this connection the objective is to reduce paper work and working crew but here also people need to go for polling centre for voting. To avoid large gathering of people it is required to design a frame work so that every one can cast their vote from home. The possibilities are around IoT protocols. It is possible to cast their vote through mobile phone with the help of secure IoT frame work. So that no need to go to polling station and results will be displayed at that time of instant. To access this feature every can login with finger print scanning or iris scanner. So it avoids fraud while voting. Hence it easy to conduct polling process without any disturbances. So this process is simple, secure, efficient, accurate and fast than compared to traditional voting process.

***Index Terms*-Reticulate,Thermionic Balloting, Real Time, Systematization and IoT-protocols.**

## I.INTRODUCTION

Voting is an important key factor in democratic society. It is traditionally old activity but it is a powerful tool to elect powerful leaders for the society and for the bright future of the people. The electronic voting is the one of the most popular method to solve current problems like wastage of paper and ecosystem related to trees. These are inter related parameters. These scenario is explained by author [15] (A. D. Rubin and D. R. Jefferson (2008)) [15] to over come the problems in old voting process due to so many advantages includes confidentiality, automation, more economic, less burden etc. Different kinds of voting process are including ballot papers. But requires more paper and it is the main drawback of this paper. The word ballot (Y. Chung and Z. Wu(2012)) [19] is used in polling process within any organization like companies, industries, institutes. The main drawback of this type is it uses heavy paper for the entire process, takes much time, especially not suitable for blind peoples, takes more time to declare results due to manual counting process so that more man power required for counting and also to provide security. So it is a time consuming process. Another one is lever voting machines. In this approach the voter have to pull the lever to desired person and then the corresponding counter will be incremented. Then finally the chief have to count the counter value for results conclusion. The main disadvantage of this process is based on time factor it is a time consuming process, re-verification is hectic because of manual process and time taking, requires more crew so more money required for maintenance including security. The next one is punched cards. In this process a small ATM card sized device will be used for counting votes. Here voters have to make a hole beside their desired candidate name and then that card should put into ballot box. The card is then tested under the device to check punching candidate details. The disadvantage here is the Candidate to be elected as leader details such as names are not available in the machine, less confidential polling may happen, less secured. The new one is Electronic Voting Machines (N. Paul and A. S. Tanenbaum(2009)) [17] was designed to replace old voting schemes. Due to enhanced security features (M. Bishop and S. Peisert(2012)) [18], automatic counting, economic etc. The concept of security is a dependent factor on Internet of Things(IoT). More security features can be enhanced by using this concept. At polling stations it is possible to monitor the situations with the help of IoT devices (A. K. Gupta and R. Johari (2019)) [20]. The design attributes like power consumption also very less for these type of IoT devices (S. K. Vishwakarma, P. Upadhyaya, B. Kumari and A. K. Mishra(2019)) [21]. The more secured features are explained in (J. M. AlJa'am, M. Alkhelaifi, A. Al-Khinji and M. Al-Sayrafi (2009)) [8] network based electronic voting schemes. Here the entire process is based on real time online network and voter can cast vote from any location from home, office or from any where. By using encryption process of user data which is including vote and digital sign. All these details will be sent to server and compared at server end. If matching is done that data will be displayed. If mis matched then that corresponding data from particular user will be denied. The voter can cast vote from any where in the world through mobile phone. Once server received data from user it is decoded with suitable public keys and data will be recorded

for future references. The data which is from user will be compared with data base available in the EC office server. The system uses iris and thumb print also required to include to increase security and to get more reliable genuine results in the polling process.

## II.METHODOLOGY

**2.1 Proposed Approach:** In this technique the main process is depending on design of frame work with IoT protocols. According to it everyone can cast their vote through a simple URL which is under Government maintenance. The next requirement is the portal itself contains database of all users thumbprints and iris scanning images. So in the mobile every user have to download application frame work through the URL provided by Government to mobile phones. So that the entire process of polling is simple and smooth. In this regard the preliminary work to be done by EC is to verify all data is available or not. If any new data need to update that should be performed before the commencement of the polling process. This entire process works based on different section. They are Data base section of voters, Updating data base for new users, User name and password allocation, Cross verification at supervisory level, IoT gate way connection establishment, maintaining URLs and framework up gradation policies.

**2.1.1 Transmitter side :**

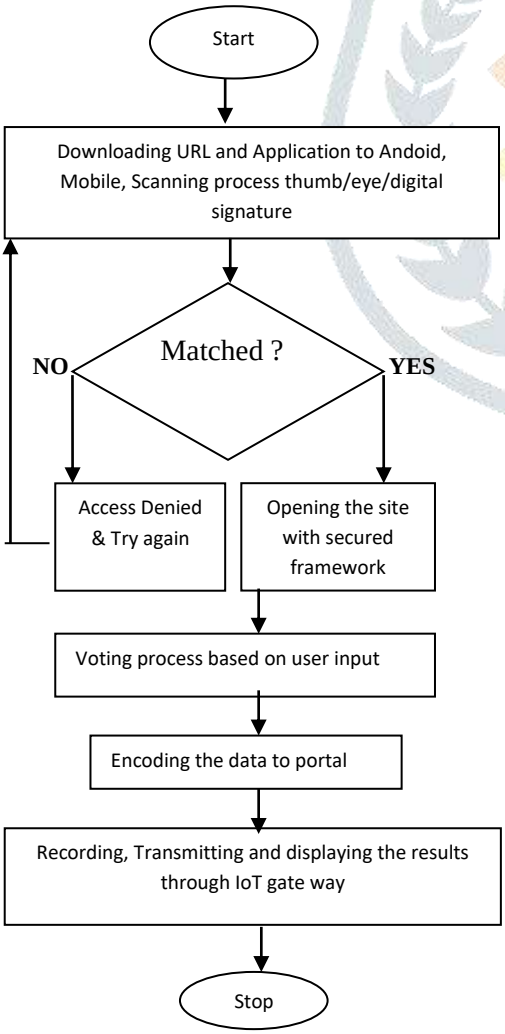


**Fig 1: Flowchart for Transmitter**

**2.1.2 Receiver side :**

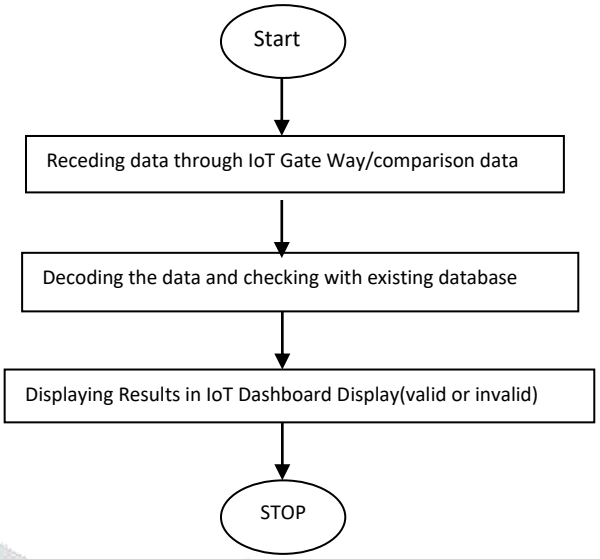


**Fig 2: Flowchart for Receiver**

## III.SYSTEM IMPLEMENTATION

So many implementations are proposed but the main objective is to achieve desired output with accurate and efficient manner. The author[26] explained the working of gateway and server. The first figure describes data reporting from client side and figure 2 describes command sending through the same gateway[26].

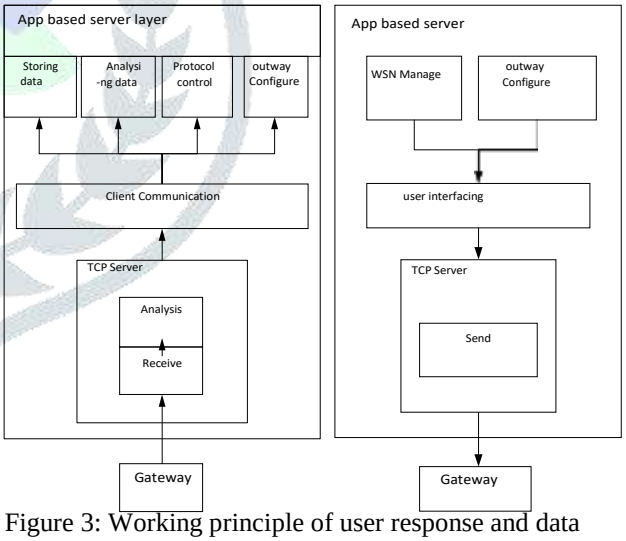


Figure 3: Working principle of user response and data between gateway and server. (a)Data receiving (b)data transmitting [26]

The author [25] described the three ballot polling mechanism in which three candidates can get different votes based on probability. Finally there are Eighteen a two candidate multi ballot can be completed based on probability estimation [25]

Table I: Example for Multi-ballot system [25]

| Voters | Recon. | TP $(k=1)$ | TP $(k=5)$ |
|---|---|---|---|
| 100 | 7 | 2 | 2 |
| 1000 | 11 | 4 | 3 |
| 10000 | 15 | 6 | 5 |

The author[12] explained the voting process with iris scanning. The following figure shows that how iris scanner collects data and process it[12]. When the device captures the image a DSP processor in the module will analyze the data in it and process it. Then it will generate a random mathematical number in digital with is stored in the database. The data base already contains voters data. So if it is matched then it is valid otherwise invalid. In this way all users data will be captures and stored for record in patterns formats.

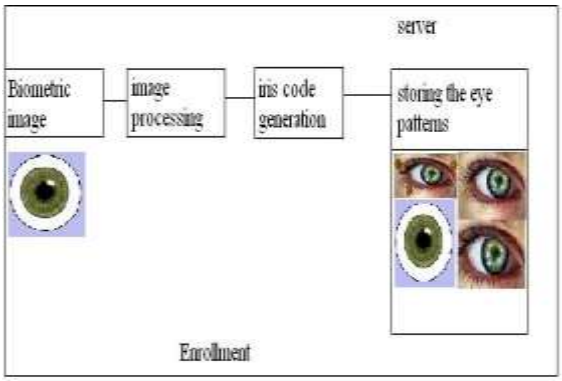


Fig 4: Enrollment process through iris scanner [12].

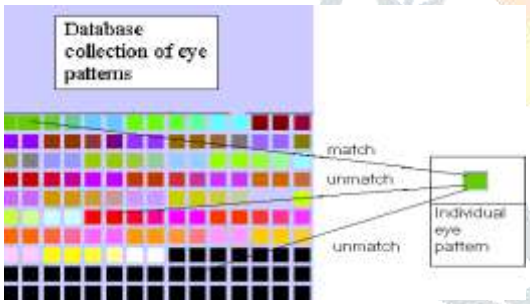


Fig 5: Biometric Data Analysis[12]

**3.1 The algorithm[12] for this will be :**

Step1 : captures the image
Step2: Compares with data base.
Step3: If matched then proceed to next section
Step4: If mismatched then access denied.
Step5: stop

**3.2 User client machine:**

PC2 server

PC3 user1 PC1 PC4 user 2 password key

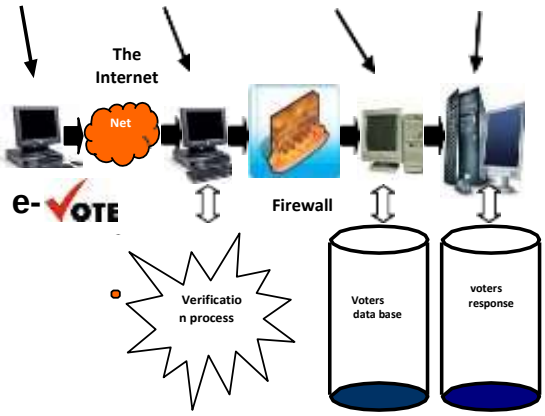


Fig.6: Verification of the e-voting application [8]

The above figure illustrates the concept of e-voting process. It requires systems with servers like user client machine, main server, and all these will be compared with data base. All these are connected with secure network [8]. Hence by examining all the methods it is clear that the e-voting process must have the following algorithm which provides high security.

**3.3 Proposed Algorithm:**

Step1: start
Step2 : scan the iris and finger print
Step 3: Match with data base
Step4: If matched next section else denied
Step5: If matched them casting vote with personal key and digital signature.
Step6: encryption of user response and digital signature
Step7: User data transmission to server
Step8: If both encrypted data is matched then vote can be considered else rejected.
Step9 :Displaying data on the dash board recorded in data base and Stop.

The expected results from the above discussions are showing below. The design contains Receiver side and Transmitter side. Transmitter contains hardware module along with finger print sensor. Receiving side it is usually window updates data regarding voter from transmitter. The figures shows how columns are updated when user gave input. The registration process is also very easy and simple. Cost is also very less and maintenance also easy.

## IV.CONCLUSION

The paper is completely based on software approach and it is possible to get good result in this Lock-Down situation for Election Commission. Every voter can cast their vote through this IoT framework and it provides more security by means of finger print scanning and iris scanner mechanisms. It will work efficiently with real time frame work application through URLs and software applications. The front end uses a dash board there the user can register into polling portal and the user can cast vote to desired people. It is required to maintain data related to Leaders by using symbols or photos for identification purpose of the voter.

## V. FUTURE IMPLEMENTATIONS

This proposed schemes and techniques can be improved with dedicated modules specially designed for voting process, so every voter can cast their vote from the device at any where in the world with any condition and also can monitor results with the feature thumb scanning/iris authentic access. As of now we are suffering with CORONA Pandemic situation. So in this regard we have to maintain social distancing. So this process can avoid problems occurred due to large gathering of people to voting stations to cast their vote. The results are also possible to see in online any time with proper keys. The same will be send to user mobile as a SMS like acknowledgement. The important thing here is that every one have to get clear awareness about voting procedure through mobile. Once it is successfully completed then it is easy to conduct polls with additional security features.

## REFERENCES


[1] D. Chaum et al., "Scantegrity II: End-to-End Verifiability by Voters of Optical Scan Elections Through Confirmation Codes," in IEEE Transactions on Information Forensics and Security, vol. 4, no. 4, pp. 611-627, Dec. 2009.

[2] J. P. Conti, "Amazon voters tally up," in Engineering & Technology, vol. 5, no. 6, pp. 58-61, April 24-14 May 2010.

[3] L. F. Cranor and R. K. Cytron, "Sensus: a security-conscious electronic polling system for the Internet," Proceedings of the Thirtieth Hawaii International Conference on System Sciences, Wailea, HI, USA, 1997, pp. 561-570 vol.3.

[4] T. Kohno, A. Stubblefield, A. D. Rubin and D. S. Wallach, "Analysis of an electronic voting system," IEEE Symposium on Security and Privacy, 2004. Proceedings. 2004, Berkeley, CA, USA, 2004, pp. 27-40.

[5] D. Foster, L. Stapleton and H. Fu, "Secure Remote Electronic Voting," 2006 IEEE International Conference on Electro/Information Technology, East Lansing, MI, 2006, pp. 591-596.

[6] M. Zygula, W. Zabierowski and A. Napieralski, "Integration of Internet Systems for Mobile Devices. Poll System," 2007 9th International Conference - The Experience of Designing and Applications of CAD Systems in Microelectronics, Lviv-Polyana, 2007, pp. 469-473.

[7] B. Kang, "Cryptanalysis on an E-voting Scheme over Computer Network," 2008 International Conference on Computer Science and Software Engineering, Hubei, 2008, pp. 826-829.

[8] J. M. AlJa'am, M. Alkhelaifi, A. Al-Khinji and M. Al-Sayrafi, "Towards an electronic voting system for the state of Qatar," 2009 International Conference on Advances in Computational Tools for Engineering Applications, Zouk Mosbeh, 2009, pp. 569-572.

[9] Abdolreza Rasouli Kenari, Javad Hosseinkhani, Mahboubeh Shamsi and Majid Harouni, "A robust and high speed E-voting algorithm using elgammel cryptosystem," 2010 The 2nd International Conference on Computer and Automation Engineering (ICCAE), Singapore, 2010, pp. 812-816.

[10] L. Kyrillidis, S. Cobourne, K. Mayes, S. Dong and K. Markantonakis, "Distributed e-voting using the Smart Card Web Server," 2012 7th International Conference on Risks and Security of Internet and Systems (CRiSIS), Cork, 2012, pp.1-8.

[11] I. Katakis, N. Tsapatsoulis, V. Triga, C. Tziouvas and F. Mendez, "Clustering Online Poll Data: Towards a Voting Assistance System," 2012 Seventh International Workshop on Semantic and Social Media Adaptation and Personalization, Luxembourg, 2012, pp. 54-59.

[12] S. Bhargavi, N. Bhavithra Devi, B. R. Priya, B. Yamuna and E. K. Vellingiri Raj, "Election voting system using mobile m-voting," 2013 International Conference on Optical Imaging Sensor and Security (ICOSS), Coimbatore, 2013, pp. 1-6.

[13] S. M. Ali et al., "Micro-controller based smart electronic voting machine system," IEEE International Conference on Electro/Information Technology, Milwaukee, WI, 2014, pp. 438-442.

[14] Anandaraj S, Anish R and Devakumar P.V, "Secured electronic voting machine using biometric," 2015 International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS), Coimbatore, 2015, pp. 1-5.

[15]. A. D. Rubin and D. R. Jefferson, "New Research Results for Electronic Voting," in IEEE Security & Privacy, vol. 6, no. 3, pp. 12-13, May- June 2008.

[16]. A. O. Santin, R. G. Costa and C. A. Maziero, "A Three-Ballot-Based Secure Electronic Voting System," in IEEE Security & Privacy, vol. 6, no. 3, pp. 14-21, May-June 2008.

[17]. N. Paul and A. S. Tanenbaum, "Trustworthy Voting: From Machine to System," in Computer, vol. 42, no. 5, pp. 23-29, May 2009.

[18]. M. Bishop and S. Peisert, "Security and Elections," in IEEE Security & Privacy, vol. 10, no. 5, pp. 64-67, Sept.-Oct. 2012.

[19]. Y. Chung and Z. Wu, "Casting Ballots over Internet Connection Against Bribery and Coercion," in The Computer Journal, vol. 55, no. 10, pp.1169-1179, Oct. 2012.

[20]. A. K. Gupta and R. Johari, "IOT based Electrical Device Surveillance and Control System," 2019 4th International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU), Ghaziabad, India, 2019, pp. 1-5.

[21]. S. K. Vishwakarma, P. Upadhyaya, B. Kumari and A. K. Mishra, "Smart Energy Efficient Home Automation System Using IoT," 2019 4th International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU), Ghaziabad, India, 2019, pp. 1-4.

[22] A. Vakaloudis and C. O'Leary, "A framework for rapid integration of IoT Systems with industrial environments," 2019 IEEE 5th World Forum on Internet of Things (WF-IoT), Limerick, Ireland, 2019, pp. 601-605.

[23] S. Chaudhary, R. Johari, R. Bhatia, K. Gupta and A. Bhatnagar, "CRAIoT: Concept, Review and Application(s) of IoT," 2019 4th International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU), Ghaziabad, India, 2019, pp. 1-4.

[24] T. Yokotani and Y. Sasaki, "Transfer protocols of tiny data blocks in IoT and their performance evaluation," 2016 IEEE 3rd World Forum on Internet of Things (WF-IoT), Reston, VA, 2016, pp. 54-57.

[25] K. Henry, D. R. Stinson and J. Sui, "The Effectiveness of Receipt-Based Attacks on ThreeBallot," in IEEE Transactions on Information Forensics and Security, vol. 4, no. 4, pp. 699-707, Dec. 2009.

[26] Q. Zhu, R. Wang, Q. Chen, Y. Liu and W. Qin, "IOT Gateway: BridgingWireless Sensor Networks into Internet of Things," 2010 IEEE/IFIP International Conference on Embedded and Ubiquitous Computing, Hong Kong, 2010, pp. 347-352.

[27] B. Kang "Cryptanalysis On An E-Voting Scheme Over Computer Network," 2008 International Conference On Computer Science And Software Engineering, Hubei, 2008, Pp. 826-829.