THREE TIER SECURED ELECTRONIC VOTING MACHINE

[1] Chandrashekar C , [2] Akshay Nadig N R,[3] Kishan D G, [4] Deepthi M R, [5]Divyashree V

[1]Assistant Professor, Dept. of Electronics and Communication,
BNM Institute of Technology, Bengaluru, India.
[2,3,4,5]BE, Electronics and Communication,
BNM Institute of Technology, Bengaluru, India

Abstract: **Three Tier EVM is a voting machine that is used to make election process system more secure, faster, transparent and competent. All the problem like time delay for vote counting, security, proxy voting can be overcome through this project. The main idea behind this is to provide three levels of security using RFID card and biometric techniques such as Fingerprint face recognition. The fingerprint samples are extracted from stored database after the verification of RFID card. For giving additional security face recognition technique is added which captures an image of the voter and matches with the stored in the database. Due to these techniques this project provides a best way to avoid the forged voting. Once voting is done by the voter, status is updated for that particular person and the vote is registered.**

Keywords—EVM, RFID, Fingerprint module, EHD algorithm

I. INTRODUCTION

Throughout the history of mankind there has ever been a kind of competition among humans for power. In olden times, during sixth century BC Athenians used a process of or electing a person by raising their hands, but for some special person considered to be dangerous to the state, for that they took votes on clay ballots[1]. The process of voting is not a new idea rather it is as old as the history of mankind itself is. Throughout the history different methods and techniques of voting have been adopted. The design parameters of voting system should be chosen in such a way that all concerned parties acting as candidates as well as voters that are polling the votes must be satisfied with the announcement of results after elections have been conducted. Environment of voting and conducting elections basically depends upon the cultural values as well as political policies [2] [3].

II. LITERATURE REVIEW

In paper-based elections, voters cast their votes by simply depositing their ballots in sealed boxes distributed across the electoral circuits around a given country. When the election period ends, all these boxes are opened and votes are counted manually in presence of the certified officials. In this process, [4] there can be error in counting of votes or in some cases voters find ways to vote more than once. Sometimes votes are even manipulated to distort the results of an election in favor of certain candidates. In order to avoid these shortcomings, [4-7] the government of India came up with direct-recording electronic (DRE) voting system which are usually Electronic voting machine (EVM).

To make the system more stringent and robust, another layer of security is reinforced through the use of biometric fingerprint identification as every individual has unique fingerprints. Biometrics is the science and technology that deals with analyzing the biological information or data. Biometric logistics operates by procuring fingerprints from an individual, then decoction of a feature set from the acquired data, and comparing this feature set with reference to the template set stored in the database[7][8][14]. Arduinos have been used in the EVMs along with fingerprint sensors[15][16].

There has also been cryptographic research on electronic voting [9], and there are new approaches such as [10] currently the most viable solution for securing electronic voting machines is to introduce a “voter-verifiable audit trail” [11][12]. A verifiable audit trail does not, by itself, address voter privacy concerns, ballot stuffing, or numerous other attacks on elections. Some vendors have claimed “security through obscurity” as a defense, despite the security community’s universally held belief in the inadequacy of obscurity to provide meaningful protection. [10].The security of EVM can be increased by having many layers of verification process like Face recognition and fingerprint detection and web portal [13].

III. NEED FOR FURTHER DEVELOPMENT

- The authentication has to be extended in to second level(first level with VOTER ID) either by using thumb impression or by iris technology, so that one can avoid polling agents and casting vote by unauthorized voters.
- When the current EVM technology is innovated with networking capabilities, one can vote from anywhere in the world from any internet center provided with thumb impression/Iris device on the same day.
- Those network of Biometric EVM has to be developed for security as well as to get the result as fast as when the election gets over so that the Election day itself we get the result.
- The EVM software developed with minor modifications will favor the conduct of elections for both assembly and the parliament at the same time and it can also use for local body elections.
- The EVM has to be designed for addressing larger population so that we can conduct election for entire country without any day intervals.

Considering all these points we have developed an EVM which resolve all the problems mentioned above. We have also included networking in our project, which helps he voter to vote for their respective constituencies and the votes are updated immediately after casting the vote.

IV. METHODOLOGY

The proposed system is based on electronic voting machine with different levels of security. In first level the system is able to identify each voter by their RFID cards. Secondly it uses biometric fingerprint, whenever the system receives a fingerprint, it will match the fingerprint from the database. After the verification of fingerprint, it will go to third level of authentication by using face recognition. If the image of the voter is matched with the stored database it will allow the voter to vote. We have also given option for voter to select their constituency and vote to their respective candidates. Touchscreens will be used instead of push buttons in voting machines but for demo purpose we use PC to cast the vote. Fig 1 shows the block diagram of our proposed block diagram.

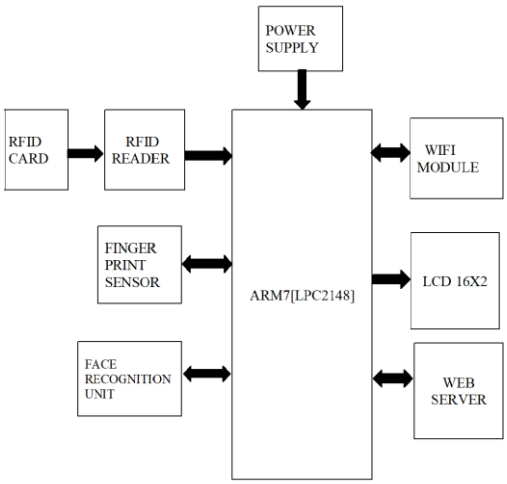

Fig.1. Block Diagram

4.1 ARM7 LPC2148

LPC2148(Fig.2) is the widely used IC from ARM7 family, it is preloaded with many peripherals making it more efficient and a reliable option for the beginners as well as high end application developers.

Fig. 2.ARM LPC 2148

4.2 RFID CARD AND READER

Radio frequency identification (RFID) technology is a wireless communication technology that enables users to uniquely identify tagged objects or people. In our project we use RFID(Fig.3) as a voter ID card, and used as first level of authentication.

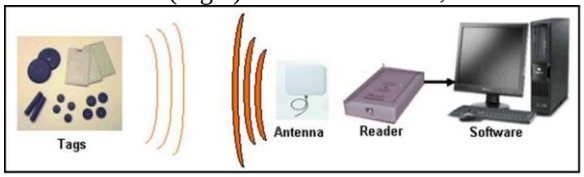

Fig. 3. Basic Building blocks of an RFID system

4.3 FINGERPRINT SENSOR

The Fingerprint scanner module used in this project is R305(Fig.4). The device is able to capture fingerprint, save it and match fingerprint with the database. The module has 4 external wires, two of them which communicate with the ARM7. Other two wires are biasing voltage and ground. We use fingerprint sensor as the second level of authentication. Only after the verification of fingerprint, the third authentication method i.e face recognition is carried out.

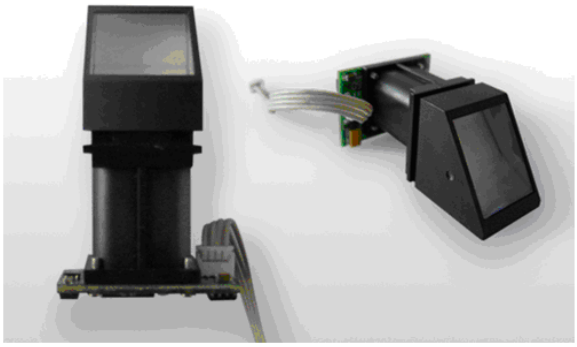

Fig. 4. Fingerprint Sensor

4.4 OTHER COMPONENTS

After the completion of three levels of security, a web page appears on the PC where the voters are allowed to vote. To send these data to the server we use Wi-Fi module(**ESP8266)** Fig.5.

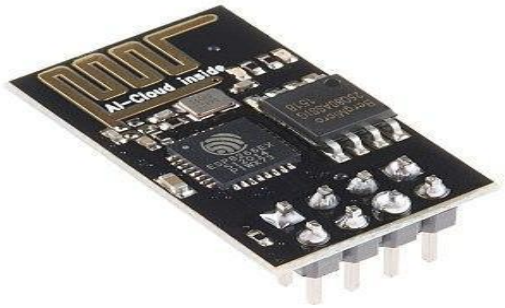

Fig. 5. Wi-Fi module ESP8266

We make use of 16x2 LCD to display the voter ID details and also the instruction in every level of security. Metal detector(Fig.6-Right) is used to detect any metals in the vicinity of the voting machine, the voting process will be stopped automatically if any metal is detected during voting. We have also used MQ3(Fig.6-Left) alcohol sensor to detect whether the voter has consumed alcohol or not, if yes an alert sound is given and voting process stops immediately.

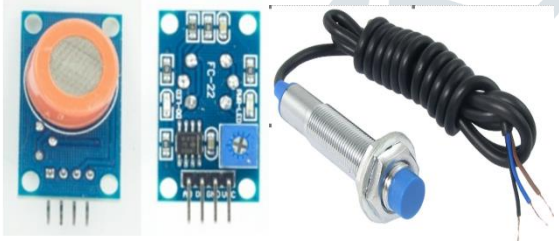

Fig.6. MQ3 Alcohol detector(Left) Metal detector(Right)

4.6. FACE RECOGNITION UNIT

Selecting a proper face recognition algorithm plays an important role in the efficiency of the system. In this project we use EHD(Edge Histogram Detection)[17]. The EHD basically represents the distribution of 5 types of edges in each local area called a sub-image. As shown in Fig.7, the sub-image is defined by dividing the image space into 4×4 non overlapping blocks.

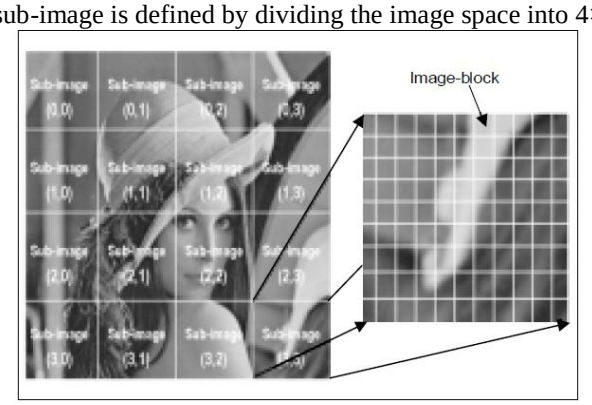

Fig. 7. Definition of sub-image and image-block.

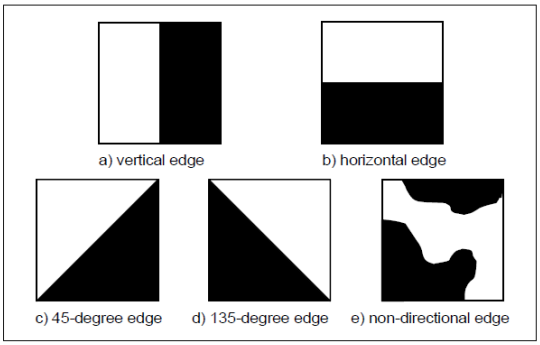

Fig. 8. Five types of edges.

To characterize the sub-image, we then generate a histogram of edge distribution for each sub-image. Edges in the sub-images are categorized into 5 types: vertical, horizontal, 45-degree diagonal, 135-degree diagonal, and non-directional edges (Fig.8).

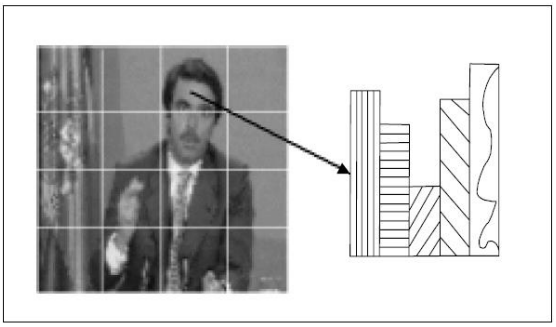

Fig. 9. Five types of edge bins for each sub-image.

Thus, the histogram for each sub-image represents the relative frequency of occurrence of the 5 types of edges in the corresponding sub-image. As a result, as shown in Fig. 9, each local histogram contains 5 bins. Each bin corresponds to one of 5 edge types. Since there are 16 sub-images in the image, a total of 5×16=80 histogram bins is required (Fig. 10).

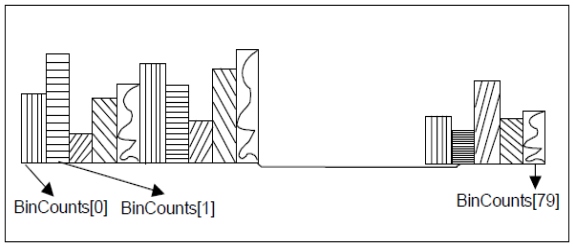

Fig. 10. 1-D array of 80 bins of EHD.

The Edge Histogram Descriptor describes edge distribution with a histogram based on local edge distribution in an image. We make use of global and semi-local edge histograms generated directly from the local histogram bins to increase the matching performance. Then, the global, semi global, and local histograms of images are combined to measure the image similarity and are compared with the MPEG-7 descriptor of the local-only histogram. Since we exploit the absolute location of the edge in the image as well as its global composition, the proposed matching method can retrieve semantically similar images. Fig. 11. Shows the flowchart of EHD algorithm.

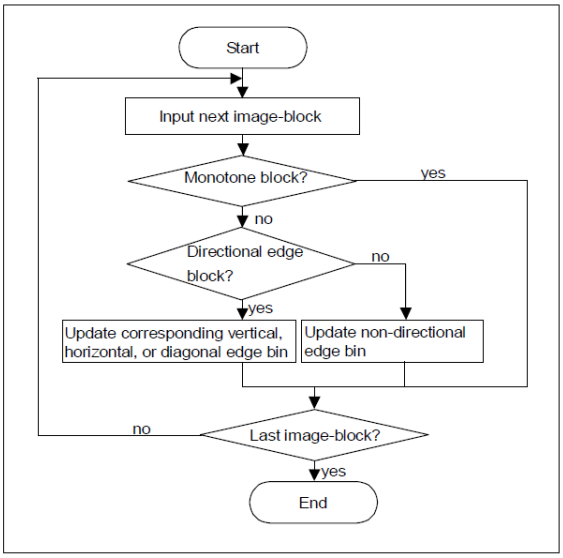

Fig. 11. Flowchart of EHD algorithm

A simple method to extract an edge feature in the image-block is to apply digital filters in the spatial domain. To this end, we first divide the image-block into four sub-blocks as (Fig. 12). Then, by assigning labels for four sub-blocks from 0 to 3, we can represent the average gray levels for four sub-blocks at (i,j)th image-block as a0(i,j), a1(i,j), a2(i,j), and a3(i,j), respectively.

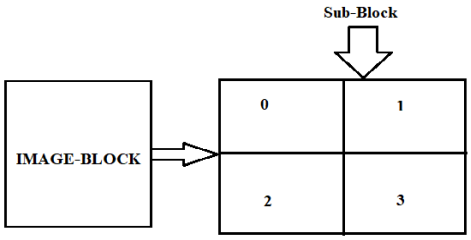

Fig. 12. sub-block and their labelling

Also, we can represent the filter coefficients for vertical, horizontal, 45-degree diagonal, 135-degree diagonal, and non-directional edges as fv(k), fh(k), fd-45(k), fd-135(k), and fnd(k), respectively, where k=0,…,3 represents the location of the sub-blocks. Now, the respective edge magnitudes mv(i,j), mh(i,j), md-45(i,j), md-135(i,j), and mnd(i,j) for the (i,j)th image-block can be obtained as follows:

$$m_v(i,j) = \left| \sum_{k=0}^{3} a_k(i,j) \times f_v(k) \right| \quad (1)$$

$$m_h(i,j) = \left| \sum_{k=0}^{3} a_k(i,j) \times f_h(k) \right| \quad (2)$$

$$m_{d-45}(i,j) = \left| \sum_{k=0}^{3} a_k(i,j) \times f_{d-45}(k) \right| \quad (3)$$

$$m_{d-135}(i,j) = \left| \sum_{k=0}^{3} a_k(i,j) \times f_{d-135}(k) \right| \quad (4)$$

$$m_{nd}(i,j) = \left| \sum_{k=0}^{3} a_k(i,j) \times f_{nd}(k) \right| \quad (5)$$

If the maximum value among 5 edge strengths obtained from (1) to (5) is greater than a threshold (Tedge) as in (6), then the image-block is considered to have the corresponding edge in it. Otherwise, the image-block contains no edge. Fig 13. shows the filter coefficients for different kind of edges.

$$\max\{m_v(i,j), m_h(i,j), m_{d-45}(i,j), m_{d-135}(i,j), m_{nd}(i,j)\} > T_{edge} \quad (6)$$

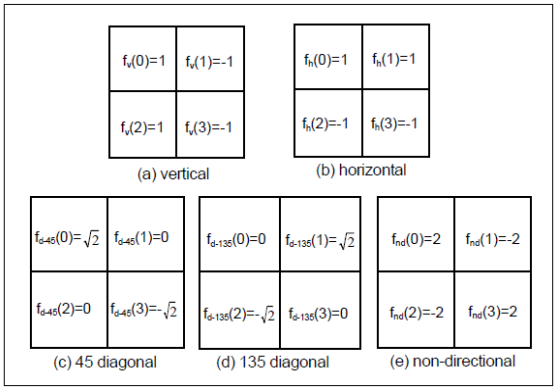

Fig. 13. Filter coefficients for edge detection.

4.7. WEB SERVER PART

After three level of authentication the voter is allowed to vote through the website. In that there are three possible operations.

1. **Registration**: Every voter has to register by giving their details like Name, ID and Constituency.
2. **Casting vote**: The voter logs in by entering their ID. Then the voter cast their vote to their respective constituency.
3. **Admin login**: Admin login is provided to check the results of the voting, and can also reset the voting list if necessary.

Fig. 14. shows the login webpage where the voting is done by entering voters ID.

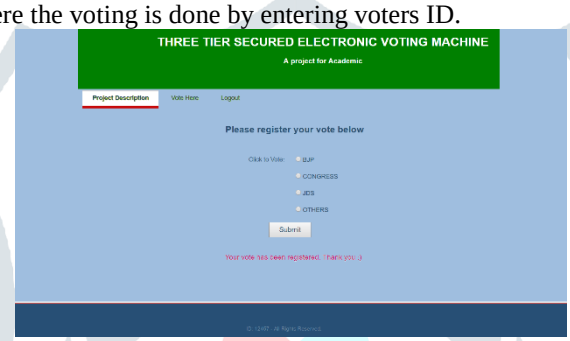

Fig. 14. Login webpage

V FLOW CHART

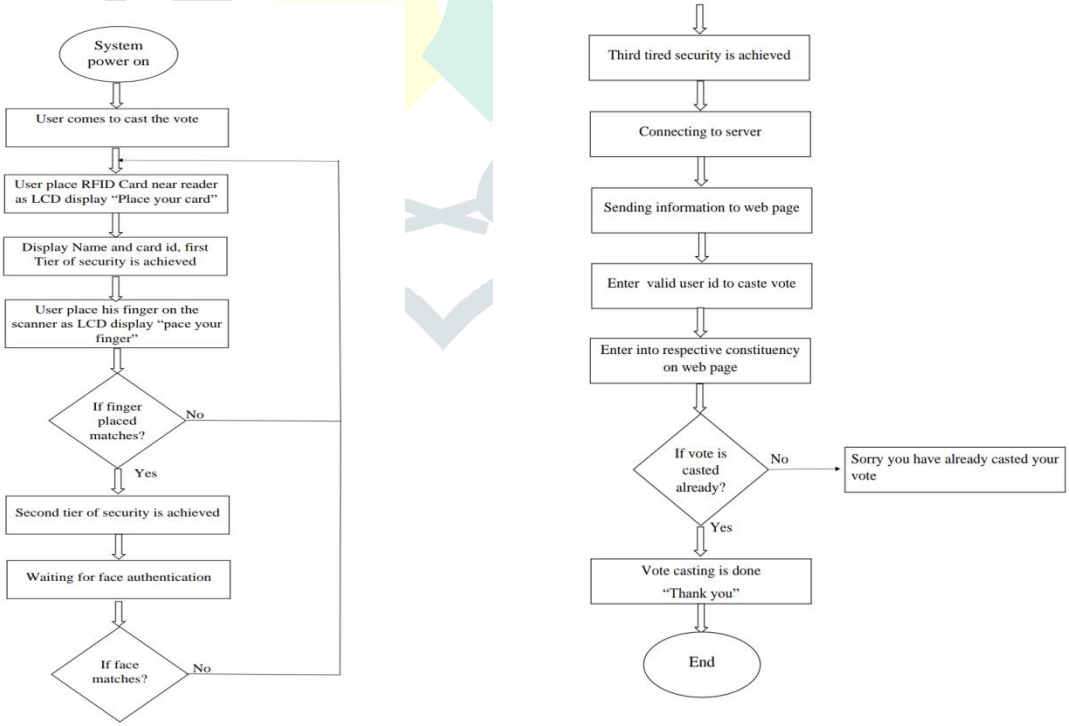

Fig. 15. Flowchart of the proposed system

Fig. 15 shows the detailed flowchart of our project, below is the brief procedure of the voting process. Voter place the RFID card on the reader, If it is valid card the voters information like Name and ID are displayed in LCD else it will display a message telling that card is not valid. For 2nd level of authentication the voters fingerprint are scanned and is matched with the stored database. Then for the third level of security the voters face is recognized using EHD algorithm. After completion of three levels of security the voter is allowed to cast his vote through a website which appears on the screen. Finally the voter can cast his vote to their respective constituencies If a person tries to vote for the second time an error message will be displayed on the screen telling that the voter has already registered his vote.

VI. CONCLUSIONS

The proposed method is to develop a secure voting system based on biometrics which tried to overcome all the drawback occurs in traditional or current voting system. The proposed system has many strong features like correctness, verifiability, convenience etc. For this system no requirement of an election officer, paper ballot or any electronic voting machine only the internet connection and Face scanners are required one can vote from anywhere securely. In this system no voter can vote twice because the voters Facial pattern will be linked to their Card. If any user tries to vote twice with some other person's RFID card, it will lead to a mismatch in the respective facial and finger Patterns stored in database storage which results in an error. This model satisfies the democracy, anonymity (privacy), reliability, accuracy and usability criterion. This model shows potential to re-engage all demographic age groups to participate in elections and cast their votes.

VII. FUTURE WORK

The performance of EVM can be increased by using Iris recognition. Confirmation messages can be sent to respective voter after casting their vote.

REFERENCES

[1] Chung-Huang Yang; Shih-Yi Tu; Pei-Hua Yen, "Implementation of an Electronic Voting System with Contactless IC Cards for Small-Scale Voting," Information Assurance and Security, 2009. IAS '09. Fifth International Conference on, vol.2, no., pp.122,125, 18-20 Aug. 2009

[2] Lambrinoudakis, C.; Kokolakis, S. Karyda, M.; Tsoumas, V.; Gritzalis, D.; Katsikas, S., "Electronic voting systems: security implications of the administrative workflow," Database and Expert Systems Applications, 2003. Proceedings. 14th International Workshop on , vol., no.,pp.467,471, 1-5 Sept. 2003

[3] Kohno, T.; Stubblefield, A.; Rubin A.D.; Wallach, D.S., "Analysis of an electronic voting system," Security and Privacy, 2004. Proceedings. 2004 IEEE Symposium on , vol.,on., pp.27,40, 9-12 May 2004

[4] Md. Asfaqul Alam, Md. Maminul Islam, Md. Nazmul Hassan, Md. SharifUddin Azad, " Raspberry Pi and image processing based Electronic Voting Machine (EVM)", International Journal of Scientific & Engineering Research, Vol.5, Issue 1,2014,pp.1506-1510.

[5] Deepak Rasaily"Jigmee Sherpa, Yashal Dorzee Lepcha, "Design of Electronic Voting Machine using Microcontroller", International Journal of Engineering Trends and Technology, ISSN: 2231,Vol-32 issue 5,2016,pp.277-278

[6] B. Divya Soundarya Sai, M. Sudhakar, "Biometric System Based Electronic Voting Machine Using Arm9 Microcontroller", IOSR Journal of Electronics and Communication Engineering (IOSR-JECE) e-ISSN: 2278- 2834,p-ISSN: 2278-8735.Vol.10, Issue 1,2015, pp.57-65.

[7] D. A. Kumar, U. S. Begum, "Electronic Voting Machine- A Review".

[8] R. Udupa, G. Garg and P. Sharma, "Fast and Accurate fingerprint Verification", International Conference on Audio- and Video-Based Biometric Person Authentication, pp. 192-97, 2001.

[9] Gritzalis D., [Editor]., "Secure Electronic Voting", Springer-Verlag, Berlin Germany, 2003.

[10] Chaum D., "Secret-ballot receipts: True voter-verifiable elections", IEEE Security and Privacy, 2(1):38-47, 2004.

[11] Dill D.L., Mercuri R., Neumann P.G., and Wallach D.S., "Frequently Asked Questions about DRE Voting Systems", Feb.2003.

[12] Mercuri, R., "Electronic Vote Tabulation Checks and balances", PhD thesis, University of Pennsylvania, Philadelphia, PA, Oct.2000.

[13] Anooshmitha Das, Manash Pratim Dutta, Subhasish Banarjee, "VOT-EL: Three Tier Secured State-Of-The-Art EVM Design Using Pragmatic Fingerprint Detection Annexed With NFC Enabled Voter -ID Card"

[14] Anandaraj S, Anish R, Devakumar P.V, "Secured Electronic Voting Machine using Biometric", IEEE Sponsored 2nd International Conference on Innovations in Information,Embedded and Communication systems (ICIIECS)2015

[15] Rahil Rezwan, Huzaifa Ahmed, M. R. N. Biplob, S. M. Shuvo, Md. Abdur Rahman,"Biometrically Secured Electronic Voting Machine", 2017 IEEE Region 10 Humanitarian Technology Conference (R10-HTC) 21 - 23 Dec 2017, Dhaka, Bangladesh

[16] V. Kiruthika Priya, V. Vimaladevi, B. Pandimeenal, T. Dhivya, "Arduino based Smart Electronic Voting Machine", International Conference on Trends in Electronics and Informatics ICEI 2017

[17] Neetesh Prajapati, Amit Kumar Nandanwar, G.S. Prajapati, "Edge Histogram Descriptor, Geometric Moment and Sobel Edge Detector Combined Features Based Object Recognition and Retrieval System", Neetesh Prajapati et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 7 (1) , 2016, 407-412, ISSN:0975-9646.