



# ADVANCED VOTING MACHINE (AVM)

Fousiya C I<sup>1</sup>, Hajera M P<sup>2</sup>, Krishna veni P Anil<sup>3</sup>, Shabna Hasheeb<sup>4</sup>

Department of Computer Science Engineering, KMEA Engineering College, Edathala, India

**ABSTRACT** - Before 2004 there was a paper based voting system called the Ballot Paper System. With the growth of technology, we have moved in to the electronic voting machine system, called the EVM. But now a days EVM are not safe, because of the hardware malpractice which includes virus, hacking as well as physical tampering. To overcome such situations we are proposing a new system called the Advanced Voting Machine (AVM). Initially the voters are enrolled using the biometric fingerprint. After the verification of fingerprint the voters can cast their vote. There by we can avoid the fake votes. The candidate details are already stored so the voters can easily choose the candidate. At the time of voting, camera will be activated and it will capture the image of the corresponding voter symbol and it will be stored in the database. These images will be processed to identify the symbols using the image comparison techniques, and based on that counting take place. After casting the vote a token will be generated to the voters in the encrypted form to their mobile phones. After voting token generated in mobile phones to the voters, through this token voters get the details of the voting like candidate name, party name and symbol of the party etc in which we can assure that vote will be given for the right person. Otherwise we can claim on it.

## I. INTRODUCTION

Elections were a defining feature of democratic government. Political electoral systems were organized by governments. Vote counting accuracy has become a well-known issue in the election process. Digital image processing techniques can be used in the analysis of printed election ballots. The paper ballots can provide independent auditing capabilities to elections, however they do not guarantee fast and trustful elections. The National Institute of Standards and Technology (NIST) observes in a draft report on Voluntary Voting Systems Guidelines for 2007 that the use of paper to provide independent auditing in elections is practical, but that there are undeniably open technical issues that can and should be addressed.

In developing countries like Bangladesh, the way of election is ballot paper based system which is very much time consuming. By ballot paper based system there is transparency at vote casting time as well as at counting time.

Although Bangladesh introduce EVM in parliamentary election but this system also do not ensure security. Considering these problems, a new system of voting is proposed based on electronic voting machine (EVM).

The additional feature of this system is biometric security which will be realized by the fingerprints of the voters. The fingerprint voting project demands the user to enroll Fingerprint at the polling booth. The system reads the data from the Fingerprint and verifies the data which is already stored in the database. If the given details match with the database data, the system gives the permission to the person to cast their vote. If the given Fingerprint does not match with the stored data in the database, the system display the error message and the security authorities can take the further action. The main objective of this project is to design a system that asks to user to show his/her Fingerprint as an identity proof. In voting systems, the system should be easy to authenticate and verify, it also have high accuracy rate and reliability. The system also be cost effective and unique. In an advanced voting system is introduced where adhaar card was used to verify the voter.

Digital identity is the key representation of user most crucial subject for information security. The password based authentication is weak solution. User select static password which is easy to guess, relevant information or common for all authentication process. Further, Security Token based runtime interaction can elaborate the strength of authentication control. For strong authentication Security tokens can be used. For strong authentication token will be passed to the mobile phones. Hashing algorithm is used to generate token for authentication. Thereafter to implement mobile token on different prospective, explore various authentication mechanisms. The generation of token by apply hash function with value generated after voting and a timestamp. And the token is in an encrypted form will given to each voters to their mobile phones. This token can be scanned and they get the details of voting which time, date and vote given to which candidate.

The object counting technique are being faster and advanced nowadays. Several techniques are discovered and still developing. It implements to detect a real-life object using a simple webcam. The image captured by the webcam is compared with similar type of image in database to detect the type of image. The data being compared is binary string, a unique attribute is compared which has been acquired by the feature extraction method. The experiments conducted in accordance with proposed methods which are suitable for realtime system. These images will be processed and identify the symbols and basis on that counting is take place. The counting will be incremented to the corresponding candidate.

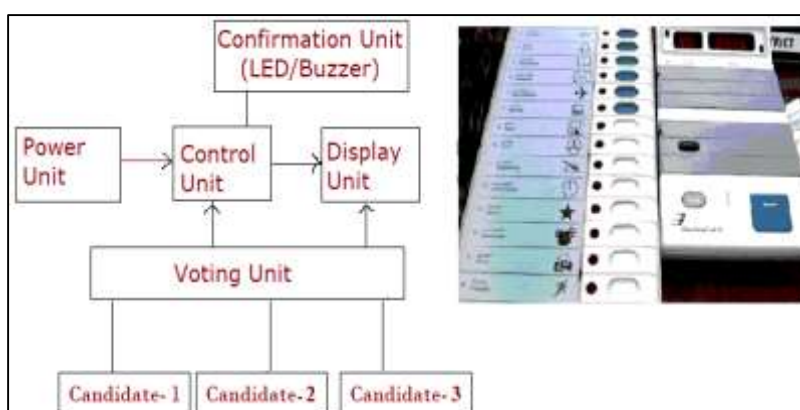


Fig 1.1 Existed System

## II. LITERATURE REVIEW

Anandaraj S [1] said that it implements a simple and secured method of casting vote by using biometric information. As per technology increases, so many changes were introduced in the field of voting. The changes aim at increasing the flexibility, security, reliability, scalability of the model and provide less time consumption to announce the result. Nowadays, the voting procedure was held by manually operating machines and even through SMS also. This electronic voting machine is a unique and new concept which saves a lot of time and avoids the false voting by a false person and it make more user friendly. In this system, the user has to use his fingerprint to cast the authenticated vote.

Md. T. Akhtar, S. T. Razi , K. N. Jaman , A. Azimusshan , Md. A. Sohel are said that it implements to detect a real-life object using a simple webcam. The image captured by the webcam is compared with similar type of image in database to detect the type of image. The data being compared is binary string, a unique attribute is compared which has been acquired by the feature extraction method. This technology can be used in face recognition system, defence system, production line or removal of defective product. Here using MATLAB to develop the technique. The experiments conducted in accordance with proposed methods which are suitable for realtime system[2].

Young Sil Lee, Hyo Taek Lim, HoonJae Lee [3] The ID and password is the best standard method among authentication process on the internet, and it is performed more easily and successfully .Anyway, it is a vulnerable method against attacks such as eavesdropping or replay attack. To overcome this problem, OTP technique is used. The most popular OTP is HOTP algorithm, based on one-way hash function SHA-1. It is a cornerstone of enterprise for Open Authentication (OATH), it was issued as an information IETF RFC 4226 in December 2005. As recent researches show the weakness of the hash function, to overcome this we need a new algorithm to replace them. Here, we propose a method of creating one time password key using Ping Pong-128 stream cipher. Ping Pong is bit based stream cipher and it is draft with both security and efficiency to satisfy the need for lightweight algorithm. And also use random digit, to safe from attacks to generate a variable with the digit of the OTP.

Jivnesh Sandhan, Amit Mitra proposes system to count the objects using a single frame from a surveillance camera. It focus on the area where individual object detectors fail, mostly due to clutter, occlusion or variations in view due to perspective transform. For handling the counting problem, firstly the object density is estimated by using ridge regression. Objects counts are then estimated by integrating the density over the region of focus coupled with single hot feature encoding and image perspective correction. Performance of the proposed method is shown in a typical counting application such as people counting in a crowd and vehicle counting at the traffic signal [4].

Parekh Tanvi [5] the enrichment of Internet, business solutions, online services, government portals, social networking sites, information portals are replacing the traditional way of working and the communication.

Authentication helps to establish proof of identity. It is the way to prove that, the user accessing their account in authenticate way. Most of the solutions comprise personal details, operational credits, certified information or services, which requisite digital identification for making proof of authenticity. The three universally recognized philosophy are used for digital identification: what we know, what we have and universal identity. To extend authentication strength and make more flexible and strong, recent work has been done on the virtual identification approach. These virtual tokens not only help to reduce extra cost but also overcome the problem of remembrance and keeping the token.

Mohammed Khasawneh<sup>1</sup> proposed system is capable of handling electronic ballots with multiple choices at the same time, e.g., presidential, municipal, parliamentary. The system is used for integrity of an election process in terms of the functional and non-functional requirements. The functional requirements of the design of the system is secured identification and authentication processes for the voter through the use of biometrics. The system ensures that no votes in favor of a given candidate are lost, due to improper tallying of the voting counts. The most important thing in the proposed system is importance for the correctness, robustness, coherence, consistency, and security [6].

Himanshu Agarwal [7] Online voting system is contemplated as an interesting topic in information security research. Online voting system is a way that helps public to select their representatives and express their preferences for how they will be governed. This system will increase the level of security and also the trust of voters. The problems of Maoist affected places for the voting has been addressed in while describe the genesis of Maoist violence and showed that public needs a more secure way of casting their vote. Online voting system definition given in states that Online voting systems offer advantages compared to other voting processes. An Online voting system may be involved in any one of a number of steps in the setup, voting, collecting, distributing and counting of ballots. The question of who gets to count your vote was addressed in while in the voting security has been analysed.

A. Piratheepan [8] Fingerprint Voting System was implemented by using Arduino technology. All voter's information was stored in the database server of the system. The voter should fill a registration form by user id and password. This information will be checked by the server. Because all the information about the voter would be already stored in the database so it can easily know there is anything wrong, in that cases the system does not allow to cast the vote. This system is very time consuming. Fingerprint is an important identity of the user for the authentication. this system has simple architecture, and gets the responses very quickly manner.

### III. PROPOSED METHOD

The architecture of the proposed system is the voters first have a fingerprint enrollment. To avoid fake votes. The voters fingerprint details are stored in a database. The candidate details are already stored in the device. So the

voters can easily choose the candidate. After casting the vote a token will be generated to the voters in the encrypted form to each voters to the mobile phones. Through this token voters get the details of the voting like candidate name, party name and symbol of the party . By using this we can assure that vote is given for the right person. Otherwise we can claim on it.

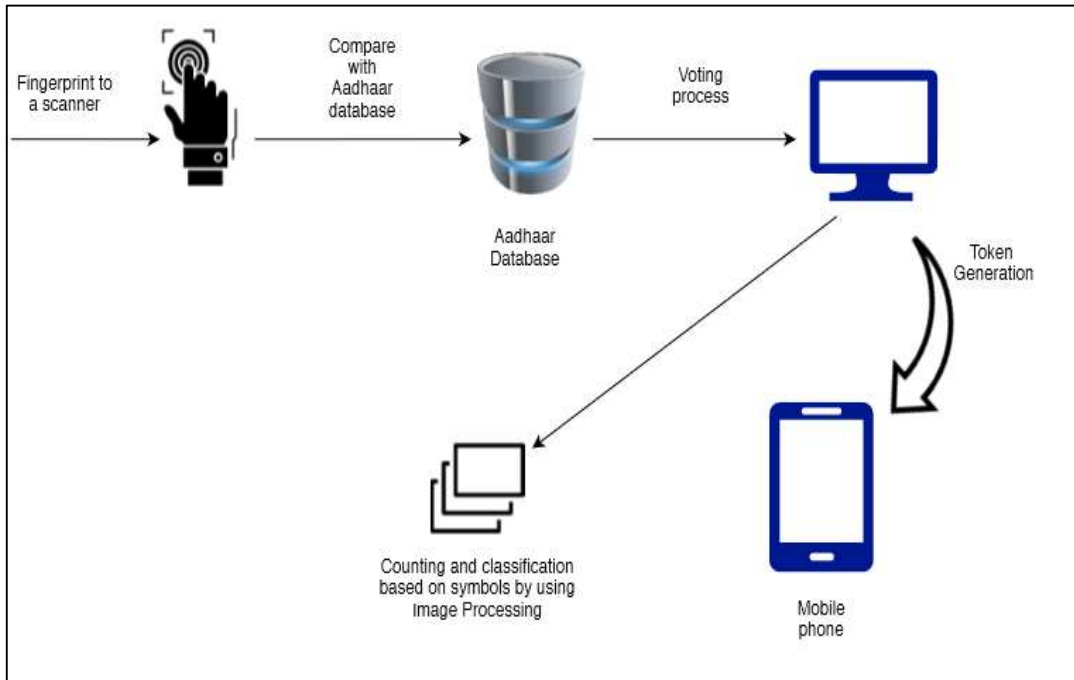


Fig 3.1 Proposed System

## SYSTEM DESCRIPTION

This system basically includes:

1. Fingerprint voting system
2. Encrypted code generation
3. Classification and counting

## FINGERPRINT VOTING SYSTEM

A fingerprint will be given as input to a scanner. The system checks your fingerprint with Aadhar database's fingerprint and also checks whether you are eligible or not. Then if you are eligible then you can vote otherwise it shows "Fingerprint is not matched" because you are not eligible. Then we can choose the candidate from that list. Cast the vote through the system. Then your vote is successfully registered.

This system satisfies the following requirements,

1. Illegal Voting will totally remove because of Fingerprint (a biometric trait which is unique to each individual).
2. Aadhar's database permits only eligible voters to vote and, it also ensures that eligible voters vote only once.
3. It maintains privacy means authority; ballot officer or anyone else can not link any ballot to the voter.
4. The major benefit of this system is to increase the voting percentage.
5. Quick results are possible.

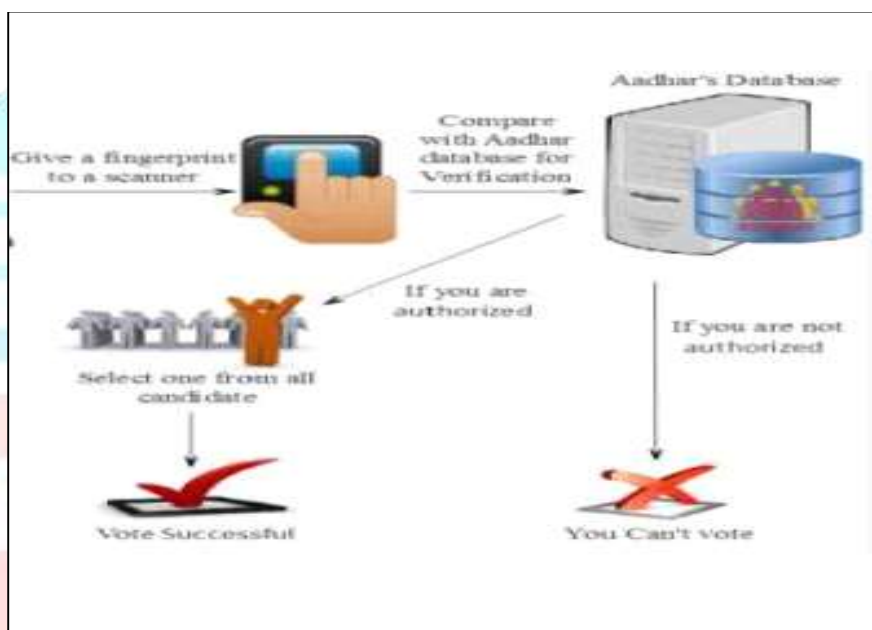


Fig 3.2 Fingerprint matching

## ENCRYPTED TOKEN GENERATION

The generation of token by using the appropriate data of each voters on the database. And the token is in an encrypted form will given to each voters to their mobile phones. This token can be decrypt and voters get the details of voting like candidate name, party name and symbol of the party. This token is generated for the security assurance of our vote. Now a days, the voters does not know how much secure their vote. So to keep the belief of voters we have to secure their valuable votes. For that we are generating a token for each voters. For the generation of the token we are using hash function algorithm to secure the vote. This will be in the encrypted form and send to the corresponding mobiles of voters.

This is one of the important part of the voting that different and very secure tokens are given to the voters. The information they get from the token they can assure that their vote is given for the right person and there is no mismatch. Otherwise voter can claim on it.

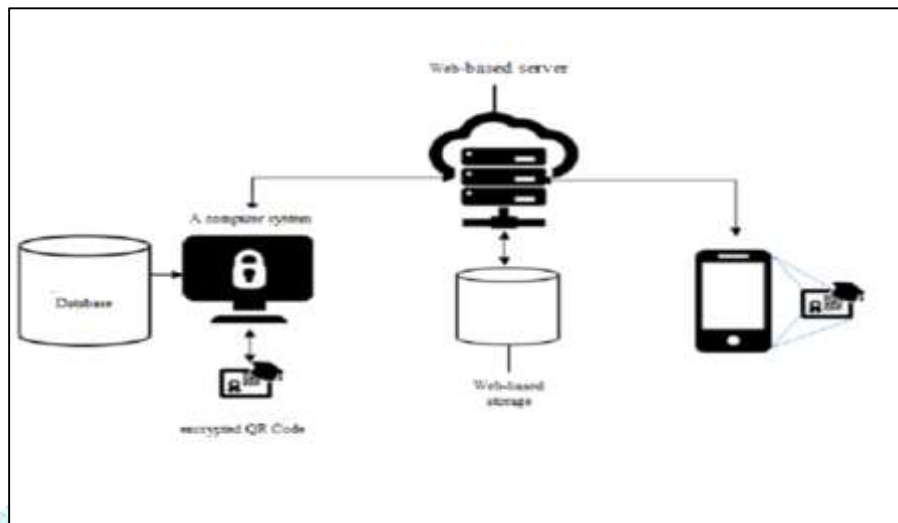


Fig 3.3 Token Generation

### CLASSIFICATION AND COUNTING

Counting is the one of the important part of this system. We need to get the accurate and correct number of votes. So we are using a camera in this system. Candidate details are already stored in the database, through this the voters can easily choose the candidates. At the time of voting the activated camera will capture the images of voting. The images that are captured by the camera will be processed and identify the symbols on it .Through this the counting will be take place and vote is incremented and stored.

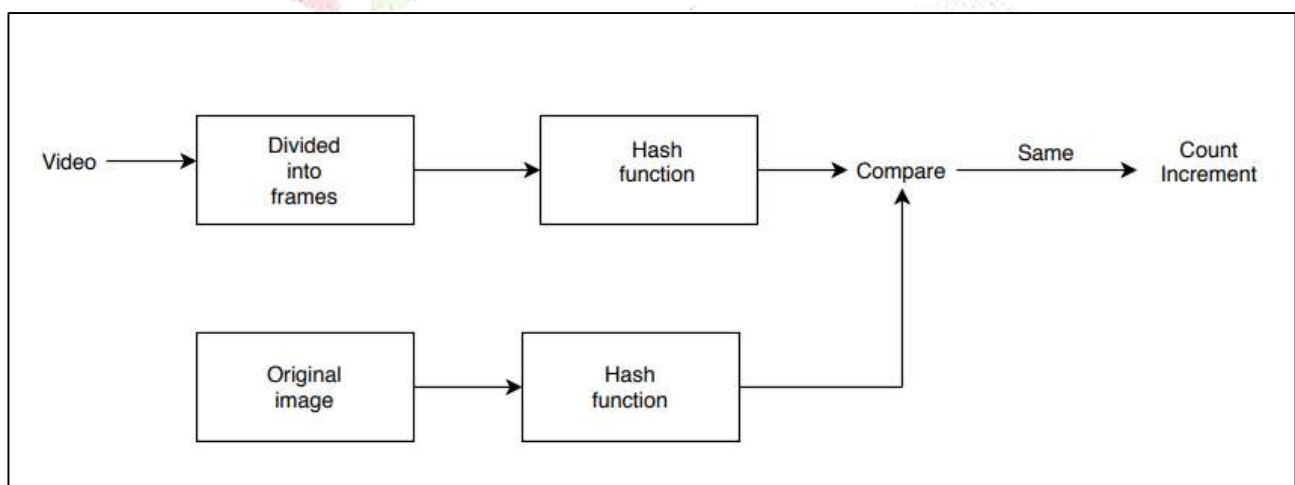


Fig 3.4 Counting and Classification

#### IV. RESULT

First voter place their finger on fingerprint module to scan, and compare the fingerprint with already stored in the voter's database. After the verification of fingerprint the voters can cast their vote. The candidate details are already stored so the voters can easily choose the candidate. The detection of symbol using a simple webcam. The image captured by the webcam is compared with similar type of image in database to detect the type of image. The data being compared is binary string, a unique attribute is compared which has been acquired by the feature extraction method. After casting the vote a token will be generated to the voters in the encrypted form to their mobile phones. Through this token voters get the details of the voting candidate name, party name and symbol of the party in which we can assure that vote will be given for the right person. Otherwise voter's can claim on it.

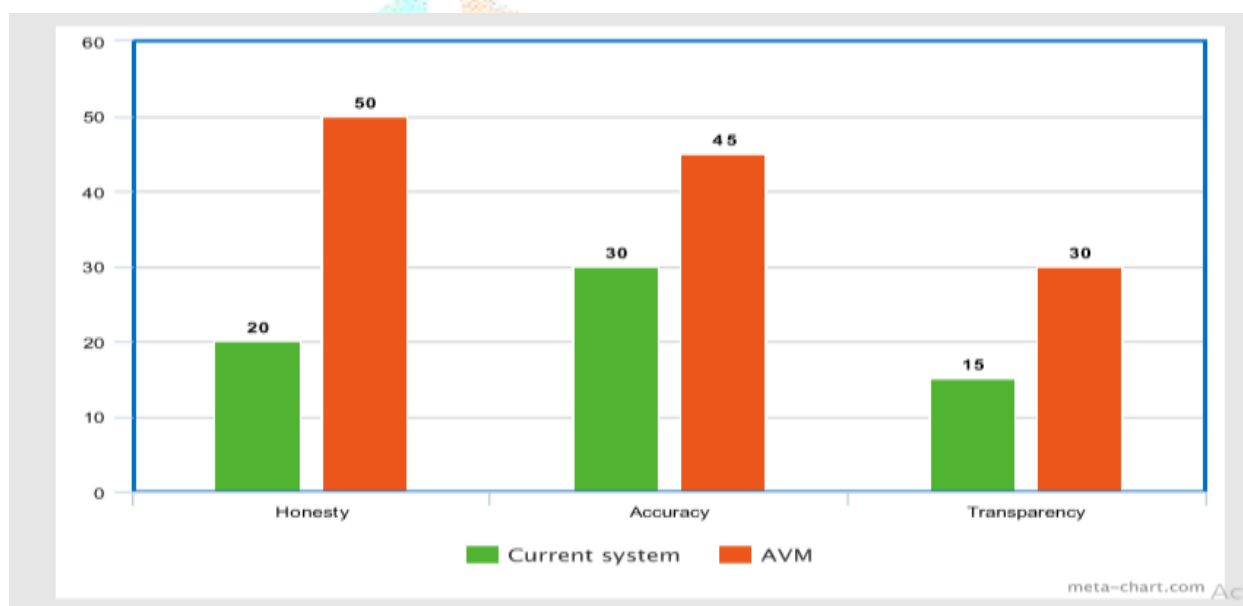


Fig 4.1 Graph

The graph shows that difference between the current system and the AVM. Honesty, Accuracy, Transparency are the parameters are used to find the difference between the both systems. From this graph shows that the AVM is much better than the current system in terms of the parameters. Honesty, Accuracy, Transparency are the must need factors of a voting system. But in the current system we cannot say that the machine is much trustable. So from this we can clearly say that AVM is better in terms of security.

#### V. CONCLUSION

This system overcomes most of the problems faced by the EVM. This will surely ensure a safer voting method which is very much what is required for a healthy growth of a developing nation. The proposed Fingerprint based voting system which is better and faster than previous systems. The new system prevents access to illegal voters, provides ease of use, transparency and maintains integrity of the voting process. The system also prevents multiple



votes by the same person and checks eligibility of the voter. This will give correct counting of votes. Due to the token generation each voter can verify their votes after voting.

## REFERENCES

- [1]Anandaraj S, Anish R , Devakumar P.V "*Secured Electronic Voting Machine using Biometric*" 2015 International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS).
- [2]Md. T. Akhtar , S. T. Razi , K. N. Jaman, A. Azimusshan , Md. A. Sohel , "*Fast and Real Life Object Detection System Using Simple Webcam*" International Journal of Scientific Research in Research Paper. Computer Science and Engineering Vol.6, Issue.4, pp.18-23, August (2018) .
- [3] Young Sil Lee, Hyo Taek Lim, HoonJae Lee "*A Study on Efficient OTP Generation using Stream Cipher with Random Digit*" 2010 The 12<sup>th</sup> International Conference on Advanced Communication Technology (ICACT).
- [4]Jivnesh Sandhan, Amit Mitra “ *Object Counting in a Single Surveillance Image*” 2017 Twenty-third Conference on Communication (NCC).
- [5]Parekh Tanvi SIMS, Gawshinde Sonal SSSIST, Sharma Mayank Kumar IET-DAVV "*Token Based Authentication using Mobile Phone*" 2011 International Conference on Communication Systems and Network Technologies.
- [6]Mohammed Khasawneh<sup>1</sup>, Mohammad Malkawi, Omar Al-Jarrah<sup>2</sup>, Laith Barakat<sup>2</sup>, Thayer S. Hayajneh<sup>3</sup>, Munzer S. Ebaid<sup>4</sup> "*A Biometric-Secure e-Voting System for Election Processes*" Proceeding of the 5th International Symposium on Mechatronics and its Applications (ISMA08), Amman, Jordan, May 27-29, 2008.
- [7]Himanshu Agarwal, G.N.Pandey "*Online Voting System for India Based on AADHAAR ID*" 2013 Eleventh International Conference on ICT and Knowledge Engineering.
- [8]A. Piratheepan, S. Sasikaran, P. Thanushkanth, S. Tharsika, 1 1 1 1 M. Nathiya, C. Sivakaran, N. Thiruchchelvan and K. Thiruthanigesan "*Fingerprint Voting System Using Arduino*" Middle-East Journal of Scientific Research 25 (8): 1793-1802, 2017 ISSN 1990-9233