# DESIGN A SECURE ELECTRONIC VOTING SYSTEM USING FINGERPRINT TECHNIQUE

**Sanjay Kumar[1], Manpreet Singh[2]**

**[1]Computer Science & Engineering Department, Maharishi Markandeshwar University Mullana, Ambala, Haryana-133203, India**

**[2]Computer Science & Engineering Department, Maharishi Markandeshwar University , Ambala, Haryana-133203, India**

**Abstract**

Fingerprint biometric is the most widely deployed publicized biometrics for identification. This is largely due to its easy and cost effective integration in existing and upcoming technologies. The integration of biometric with electronic voting machine undoubtedly requires less manpower, save much time of voters and personnel, eliminate rigging, ensure accuracy, transparency and fast results in election. In this paper, a framework for electronic voting machine based on biometric verification is proposed and implemented. The proposed framework ensures secured identification and authentication processes for the voters and candidates through the use of fingerprint biometrics.

***Keywords:*** *EVM, Fingerprint, Biometric, Fingerprint module.*

## 1. Introduction

### 1.1 Traditional Voting Process:

Traditional voting process can be divided into different phases [10]:

1. *Authentication:* In this phase, voter authenticates himself or herself by showing his or her voting card, this step is public and verified by the presiding officer. At the end of authentication process, presiding officer give a ballot paper to voter to cast his or her vote.
2. *Vote:* The vote takes place in a protected booth where voter cannot be seen by any person. The voter cast their vote by writing it with a pen on the paper ballot, folds the ballot paper and put into the ballot box where all the votes are mixed.
3. *Vote counting:* At the end of voting time, the presiding officer collect the ballot box containing all ballot papers and submit it to the counting centre. After that with the help of members of the election committee nominated by election commission of India, the ballot boxes are opened and votes are counted and the results are then announced.
4. *Verification:* Various types of verification process are used, most procedure are public and verified by the representative of candidates of competing parties. Recount is also possible if there is any fraud or error.

Conventional voting systems are not efficient due to long period of preparation, bogus voting, include papers, punch cards, mechanical levers, optical-scan machines [1]. These systems are not efficient as they are conducted manually and therefore very often are not accurate. As a consequence, it is obligatory to carry the available voting through an electronic system.

### 1.2 Requirement of E-Voting:

The requirement in traditional voting process is also applicable for e-voting and some of them are mentioned below [12].

1. *Fairness:* No person can learn the voting outcomes before the tally.
2. *Eligibility:* Only eligible voters are allowed to cast their vote.
3. *Uniqueness:* No voter is allowed to cast their vote more than once.
4. *Privacy:* No person can access the information about the voters vote.
5. *Accuracy:* All the valid votes should be counted correctly.
6. *Efficiency:* The counting of votes can be performed within a minimum amount of time [2].

### 1.3 Biometric Authentication:

Fingerprint matching is one of the most popular and reliable biometric techniques used in automatic personal identification. There are two main stages during the use of fingerprints authentication: fingerprint verification and fingerprint identification. While the goal of fingerprint verification is to verify the identity of a person, the goal of fingerprint

identification is to establish the identity of a person [13].

In a traditional biometric recognition system, the biometric template is usually stored on a central server during enrolment. The candidate biometric template captured by the biometric device is sent to the server where the processing and matching steps are performed [6].

The objective of voting is to allow voters to exercise their right to express their choices regarding specific issues, pieces of legislation, citizen initiatives, constitutional amendments, recalls and/or to choose their government and political representatives [11]. Technology is being used more and more as a tool to assist voters to cast their votes. To allow the exercise of this right, almost all voting systems around the world include the following steps:

- Voter identification and authentication
- Voting and recording of votes cast
- Vote counting
- Publication of election results

Voter identification is required during two phases of the electoral process: first for voter registration in order to establish the right to vote and afterwards, at voting time, to allow a citizen to exercise their right to vote by verifying if the person satisfies all the requirements needed to vote (authentication) [14].

The field of biometrics was formed and has since expanded on to many types of physical identification. Still, the human fingerprint remains a very common identifier and the biometric method of choice among law enforcement [8]. These concepts of human identification have lead to the development of fingerprint scanners that serve to quickly identify individuals and assign access privileges. Finger printing recognition, the electronic methods of recording and recognizing an individual finger print, advanced substantially during the last decade of the 21th century [15]. Today, identification can be achieved in a few seconds with reasonable accuracy. As a result, the use of automated fingerprint identification systems (AFIS) that record, store, search, match and identify finger prints is rapidly expanding. AFIS can be integrated with a microcontroller and other peripherals to form an embedded system which is a comprehensive electronic voting machine with fingerprint print identification system.

## 2. Existing E-Voting System

The category “electronic voting” is potentially broad, referring to several distinct possible stages of electronic usage during the course of an election.

A. *Electronic voting:* Electronic voting refers to any system where a voter casts his or her ballot using an electronic system, rather than a paper. Once recorded, an electronic vote is stored digitally and transferred from each electronic voting machine to a counting system [16].

B. *Electronic vote counting:* Electronic vote counting refers to the system that is used to tabulate ballots and award seats. It would be possible to vote using a non-electronic medium and then convert these votes to an electronic system and award seats through an electronic vote counting system [3].

Electronic Voting Machine is a simple electronic device used to record votes in place of ballot papers and boxes which were used earlier in conventional voting system [4]. It is a simple machine that can be operated easily by both the polling personnel and the voters. Being a standalone machine without any network connectivity, nobody can interfere with its programming and manipulate the result. Keeping the erratic power supply position in many places in the country, the machines have been made to run on batteries. It has mainly two units: Control unit and Ballot unit. The Control Unit is the main unit which stores all data and controls the functioning of EVM. The program which controls the functioning of the control unit is burnt into a micro chip on a “one time programmable basis”. Once burnt it cannot be read, copied out or altered. The EVMs use dynamic coding to enhance security of data transmitted from ballot unit to control unit. The new EVMs have also got real time clock and date-time stamping facility which enables them to record the exact time and date whenever a key is pressed. After the voting is completed and the close button is pressed, the machine does not accept any data or record any vote. Through the press of “total” button, the control unit can display the number of votes recorded till that time which can be cross checked with the register of voters. The display system of the control unit shows the total number of votes polled in a polling station and the candidate-wise votes polled in the machine when the ‘result’ button is pressed by the counting staff in the presence of counting agents at the counting centre. The control unit can also detect any physical tampering made with the connecting cable and indicate the same in the display unit [16].

The security of an EVM can be significantly improved by using biometric authentication system. The main reasons for augmenting a biometric authentication with electronic voting system is that biometrics are traits of a person which can be hardly copied or shared thereby it becomes very difficult to forge the identity of a person [5]. The major biometric-based technologies include finger-scanning, hand geometry, facial recognition, iris scanning, retinal scanning, finger geometry, voice recognition and dynamic signature verification.

In [6], a scheme for a dynamic voter registration, enrolment and voting in an online biometric electronic voting system is proposed. An indexing technique for facilitating the search of a matching identity to an input fingerprint is incorporated. In [7],

a web based secure e-voting system with fingerprint authentication is implemented. A public voting system based on biometric fingerprint method to make the election process transparent and efficient is implemented [8]. In [9], the challenges existing in the conventional electoral system of India are analyzed with the aim of addressing fraudulent electoral prices by the use of biometric authentication based Electronic Voting System.

This research work deals with the design and development of fingerprint recognition based Electronic Voting System. The proposed system also takes into account the essential voting requirements in terms of privacy, uniqueness, completeness, efficiency and fairness.

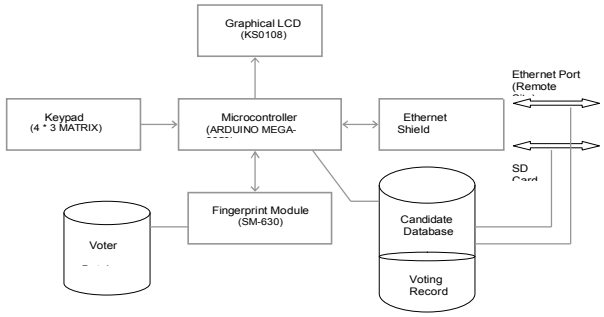


**Figure 1:** Block Diagram of Proposed Secure E-Voting System

## 3. System Framework

The system framework for secure voting comprises of a key pad, graphical LCD, microcontroller, finger print module and system interface as shown in Fig 1.

**Arduino Mega 2560** is a microcontroller board having a number of facilities for communicating with a computer or other devices. It can be programmed for serial communication on any of the Mega 2560's digital pins. **SM630** fingerprint verification module consists of optical fingerprint sensor, high performance Digital Signal Processor and Flash memory. It boasts of functions such as fingerprint login, deletion, verification, upload and fingerprint download etc. The voter information is stored in fingerprint module, whereas, the candidate database along with voting record is kept in microcontroller flash memory and remote site through Ethernet port. At the lowest level, keyboards are organized in a matrix of rows and columns. The microcontroller accesses both rows and column through ports; therefore, with a port of microcontroller, a 4 x 3 matrix of keys can be connected. The graphical LCD has a display format of 128x64 dots and yellow-green color backlight. It makes the use of **KS0108** controller to execute
its internal operations.

## 4. Working of Proposed Secure Electronic Voting System

The main phases of a voting system are registration, authentication, accessibility, casting and counting. The implementation of all these phases in the proposed system is elaborated in following steps:

//variables used are:
candidate [100] – candidate database
candidate_tot = 0 – total number of registered candidates
voter_tot = 0 – total number of registered voters
voted = 0 – total number of votes
SECURITY_PIN – stores security pin //

**Step 1:** Display Welcome Screen
**Step 2:** Security Check. If password is correct go to step 3 else repeat 2
**Step 3:** Detect memory card. If memory card found go to step 4 else display No Memory card Detected
**Step 4:** Display main menu options
**Step 5:** Candidate Zone
**Step 6:** Voter Zone
**Step 7:** Vote Now
**Step 8:** Result
**Step 9:** Change Pin
**Step 10:** Exit
**Step 11:** If Keypad input is 1 than go to step 12
**Step 12:** If Keypad input is 2 than go to step 41
**Step 13:** If Keypad input is 3 than go to step 59
**Step 14:** If Keypad input is 4 than go to step 73
**Step 15:** If Keypad input is 5 than go to step 80
**Step 16:** If Keypad input is 6 than go to step 85
**Step 17:** If Keypad input is greater than 6 then print Invalid option. Please try again. Go to step 4
**Step 18:** Display candidate zone options
**Step 19:** New Registration
**Step 20:** Modify Candidate
**Step 21:** Empty Database
**Step 22:** Back to Main Menu
**Step 23:** Exit
**Step 24:** If Keypad input is 1 than go to step 19
**Step 25:** If Keypad input is 2 than go to step 25
**Step 26:** If Keypad input is 3 than go to step 37
**Step 27:** If Keypad input is 4 than go to step 4
**Step 28:** If Keypad input is 5 than go to step 85
**Step 29:** If Keypad input is greater than 5 then display Invalid option. Please try again. Go to step 12
**Step 30:** Enter Candidate code using keypad

**Step 31:** If candidate code exists in candidate database display Already registered. Go to step 12
**Step 32:** candidate_tot++
**Step 33:** candidate[candidate_tot] = New candidate's code and display Candidate has been registered.
**Step 34:** Store candidate information in memory card, EEPROM and remote system. Go to step 12
**Step 35:** If list is candidate database is empty then display List is empty. Go to step 12
**Step 36:** Display option for modification.
**Step 37:** Change Code
**Step 38:** Delete Candidate
**Step 39:** If Keypad input is 1 than go to step 29
**Step 40:** If Keypad input is 2 than go to step 34
**Step 41:** If Keypad input is greater than 2 then print Invalid option. Please try again. Go to step 25
**Step 42:** Enter candidate code for modification using keypad
**Step 43:** Enter new code for candidate
**Step 44:** If code already exists in candidate database then display Already registered. Go to step 12
**Step 45:** Replace old code with new one and display Information has been updated.
**Step 46:** Updated information in memory card, EEPROM and remote system. Go to step 12
**Step 47:** Delete candidate code form database and display Candidate removed.
**Step 48:** Remove candidate information from memory card, EEPROM and remote system.
**Step 49:** candidate_tot--. Go to step 12
**Step 50:** Security Check. If password is correct go to step 38 else repeat 37
**Step 51:** candidate_tot = 0
**Step 52:** Delete complete database and display Database Clear.
**Step 53:** Update candidate information in memory card, EEPROM and remote system. Go to step 12
**Step 54:** Display voter zone options
**Step 55:** Register voter
**Step 56:** Delete Voter
**Step 57:** Empty Database
**Step 58:** Back to Main Menu
**Step 59:** Exit
**Step 60:** If Keypad input is 1 than go to step 48
**Step 61:** If Keypad input is 2 than go to step 52
**Step 62:** If Keypad input is 3 than go to step 56
**Step 63:** If Keypad input is 4 than go to step 4
**Step 64:** If Keypad input is 5 than go to step 85
**Step 65:** If Keypad input is greater than 5 then print Invalid option. Please try again. Go to step 41
**Step 66:** Input voter thumb print using fingerprint module
**Step 67:** If fingerprint matches in database then print Already registered. Go to step 41
**Step 68:** Add fingerprint in voter database.
**Step 69:** voter_tot++. Go to step 41
**Step 70:** Input voter thumb print using fingerprint module
**Step 71:** If fingerprint doesn't matches in database then print Doesn't exist. Go to step 41
**Step 72:** Delete fingerprint from voter database.
**Step 73:** voter_tot--. Go to step 41
**Step 74:** Security Check. If password is correct go to step 57 else repeat 56
**Step 75:** Delete complete database and display Database Clear.
**Step 76:** voter_tot= 0. Go to step 41
**Step 77:** Display vote now options
**Step 78:** Vote
**Step 79:** Back to Main Menu
**Step 80:** If Keypad input is 1 than go to step 63
**Step 81:** If Keypad input is 2 than go to step 71
**Step 82:** If Keypad input is greater than 2 then display Invalid option. Please try again. Go to step 59
**Step 83:** Input voter thumb print using fingerprint module
**Step 84:** If fingerprint doesn't matches in database then display You are Not Eligible. Go to step 59
**Step 85:** Enter candidate code using keypad
**Step 86:** If candidate code doesn't matches in database display invalid candidate code. Go to step 59
**Step 87:** Votes++. Increase the vote of selected candidate by 1.
**Step 88:** Update voted database in memory card, EEPROM and remote system.
**Step 89:** Delete fingerprint from voter's database.
**Step 90:** Display successfully voted. Go to step 59
**Step 91:** Security Check. If password is correct go to step 4 else repeat 71
**Step 92:** Display Winner of election's code with votes
**Step 93:** Display Result section's options

**Step 94:** Full list
**Step 95:** Main menu
**Step 96:** Exit
**Step 97:** If Keypad input is 1 than go to step 78
**Step 98:** If Keypad input is 2 than go to step 4
**Step 99:** If Keypad input is 3 than go to step 85
**Step 100:** If Keypad input is greater than 3 then print Invalid option. Please try again.
**Step 101:** Display whole list of candidates and their respective votes. Go to step 12
**Step 102:** Security Check. If password is correct go to step 80 else repeat 79
**Step 103:** Enter new security pin.
**Step 104:** Confirm security pin.
**Step 105:** If value of step 80 and step 81 matches then go to step 84
**Step 106:** If value of step 80 and step 81 matches print Pin not matched. Go to step 12
**Step 107:** SECURITY_PIN = new security pin. Go to step 12
**Step 108:** Display Thank you for using EVM. Exit.

The interaction among the various entities in the proposed framework is shown in Figure 2.

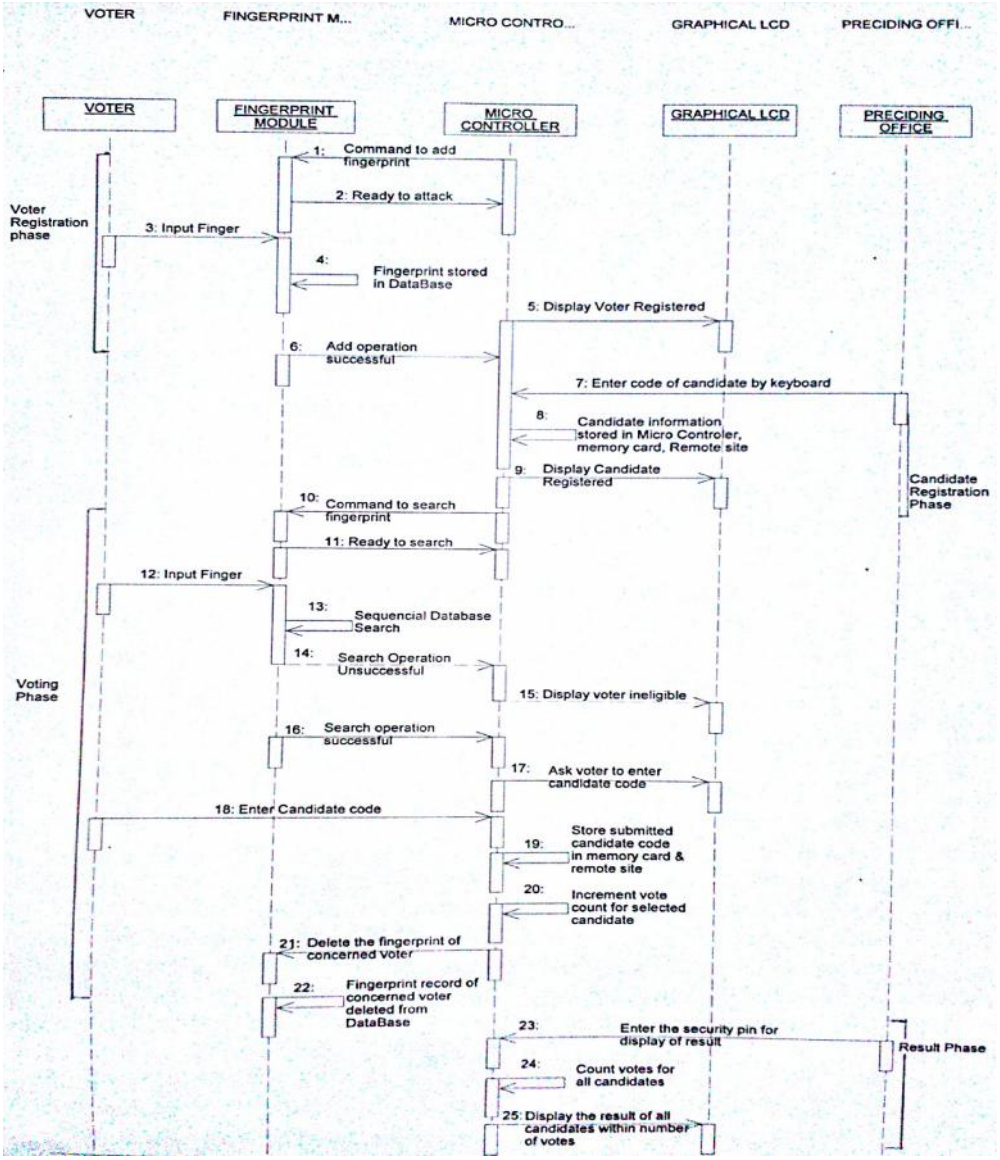


**Figure 2:** Sequence Diagram showing the Control flow in Proposed System

## 5. System Implementation & Discussion

This proposed framework has been successfully simulated on Arduino 1.0.3 platform. The steps involved in the implementation of the proposed secure electronic voting system are highlighted from Figure 3 to Figure 12.

**Figure 3:** Secure Electronic Voting System Implementation


**Figure 4:** Candidate Information Zone


**Figure 5:** Voter Information Zone

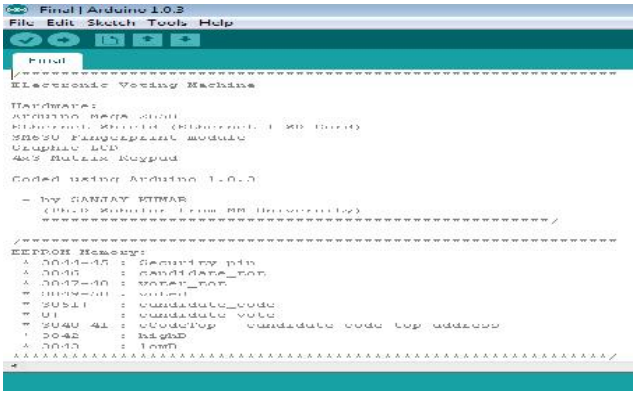


**Figure 6:** Coding for Proposed System on ARDUINO 1.0.3 Platform


**Figure 7:** Functionalities Available in Proposed System


**Figure 8:** Voter Registration Phase

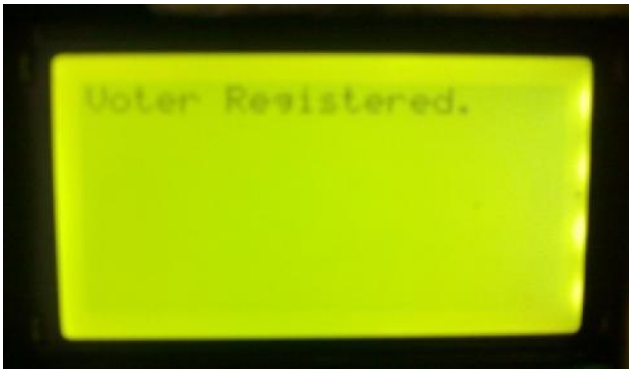


**Figure 9:** Result of Voter's Authentication through Fingerprint Matching

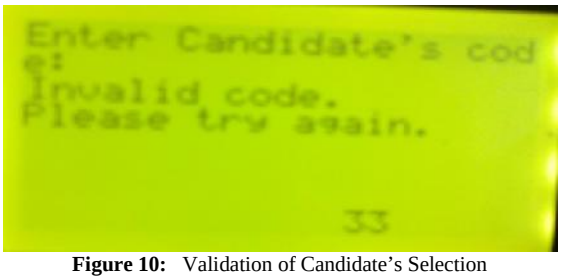


**Figure 10:** Validation of Candidate's Selection


**Figure 11:** Information of Winning Candidate

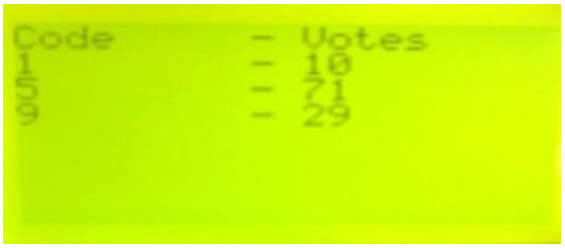


**Figure 12:** Voting Result Summary

Some of the salient features of the proposed system are as follow:

- Voters during voting cannot perform the tempering as he is not authorized to scroll any other screen.
- A voter cannot do bogus voting as his fingerprint must match the previously stored data. After voting, the voter's fingerprint record is deleted from the database thereby not allowing him to cast voting more than once.
- The candidate information and voting records are stored at three different places: SD card, EEPROM of microcontroller and remote site through Ethernet port, thereby, improving the availability and reliability of system.
- The replication of voting information at multiple locations reduces the risk of biasing during vote counting.
- The existing Electronic Voting Machine comprises of two separate components: Ballot unit and Control unit; however in the developed system all functionalities are embedded in one module making it as compact and concise.
- The design of currently used voting machines depends on the number of candidates within a constituency; however this is not a constraint for proposed system and the same model of machine can be used anywhere during voting.

## 6. Conclusion

Electronic voting system is emerging as significant alternative to the conventional systems in the delivery of reliable and trusted elections. In this paper, a framework for electronic voting system based on fingerprint biometric is proposed and implemented with the objective of eliminating bogus voting and vote repetition, less election expenditure, more transparency and fast results.

## REFERENCES

[1]. M. Byrne, K. Greene, and S. Everett, "Usability of Voting Systems: Baseline Data for Paper, Punch Cards, and Lever Machines," ACM International Conference on Human Factors in Computing Systems, pp. 171–180, 2007.

[2]. Sussane Caarls, " E-voting Handbook: Key Steps in the Implementation of E-enabled Elections", Council of Europe, 2010.

[3]. Santin, R. Costa and C. Maziero, " A Three-Ballot-Based Secure Electronic Voting System", IEEE Transaction on Security & Privacy, Vol. 6(3), pp. 14-21, 2008.

[4]. Kumar, " Electronic voting machine- A review", IEEE International Conference on Pattern Recognition, Informatics and Medical Engineering (PRIME), pp. 44-48, 2012.

[5]. Jain and D. Maltoni, "Handbook of Fingerprint Recognition," Springer-Verlag, New York, USA, 2003.

[6]. O. Iloanusi and C. Osuagwu, "Framework for a dynamic Fingerprint Indexing Biometric-based Voting System", African Journal of Computing & ICTs, pp. 55-63, Vol. 5(4), 2012.

[7]. Altun and M. Bilgin, "Web baesd secure e-voting system with fingerprint authentication", Scintific Research and Essays, pp. 2494-2500, Vol. 6(12), 2011.

[8]. K. Memon, D. Kumar and S. Usman, "Next Generation A secure E-Voting System Based On Biometric Fingerprint Method", International Conference on Information and Intelligent Computing (IPCSIT), pp. 26-32, 2011.

[9]. S. Yadav and A. Singh, "A Biometric Traits based Authentication system for Indian Voting System", International Journal of Computer Applications, pp. 28-32, Vol. 65(15), 2013.

[10]. S. Kumar and M. Singh, "Security Enhancement of E-Voting System", Global Journal of Computer Science and Technology, Volume 12 Issue 5 Version 1.0 March 2012.

[11]. R. Udupa, G. Garg and P. Sharma, "Fast and accurate fingerprint verification", International Conference on Audio- and Video-Based Biometric Person Authentication, pp. 192–197, 2001.

[12]. R. Haenni, E. Dubuis, and U. Ultes-Nitsche, “Research on e-voting technologies." Bern University of Applied Sciences, Technical Report 5, 2008.
[13]. M. Min and Y. Thein, “Intelligent Fingerprint Recognition System by using geometry approach”, International Conference on the Current Trends in Information Technology (CTIT), pp. 1-5, 2009.
[14]. M. Khan, “Fingerprint biometric-based self-authentication and deniable authentication schemes for the electronic world." IETE Technical Review, vol. 26(3), pp. 191, 2009.
[15]. L. O'Gorman, “An overview of fingerprint verification technologies."Information Security Technical Report 3.1, pp. 21-32, 1998.
[16]. S. Kumar and E. Walia, “Analysis of Electronic Voting system in Various Countries”, International Journal on Computer Science and Engineering, vol. 3(5), 1825-1830, 2011.