International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 3 Issue: 7 4586 - 4594

Automatic Voting Machine – An Advanced Model for Secured Biometrics Based Voting System

Soumadip Sen[1]
Department of Computer Science & Engineering
University Institute of Technology
The University of Burdwan
West Bengal, India
soumadip.95@gmail.com

Sankhadip Sen[2]
Department of Computer Science & Engineering
Regent Education & Research Foundation
West Bengal University of Technology (WBUT)
West Bengal, India
sankhadip.rerf@gmail.com

***Abstract*—**India, which is now considered as the world's largest democracy has been praised in the whole world for its democratic principles of "Sovereign, Socialist, Secular, Democratic, Republic". It is now the second largest populous country in the world. Although the country has a rich technical and scientific infrastructure yet the voting and election procedures do not reflect it. In this paper we are going to propose a concept or idea about how the voting processes and equipments can be designed for a "free, fair and secure" polling in the upcoming days. Researchers have proved various problems related to the present voting technique in India which is through Electronic Voting Machines (EVM) [2]. Our proposed model of the equipment for voting will overcome those problems making elections & voting fair, convenient and reliable to every citizen. This proposed model will assure complete transparency and will definitely gain the trust and integrity of the voters. Biometric authentication and identity proof are given much priority while proposing the concept since biometric authentication is a type of system that relies on the unique biological characteristics (such as finger prints, retina scan, etc.) of individuals to verify identity for secure access to electronic systems.

Keywords- *Automatic Voting Machines(AVM), Biometric Fingerprint Authentication, Centralized Voting,Smart Voter Card (SVC)*

*****

I. INTRODUCTION

Though we are living in the 21st century, era of science and technology yet our voting procedure and system does not show it. India is the largest democratic country where Right to vote and Adult Franchise are considered as the major pillars of democracy. So the people of India have complete power to elect the deserving candidate and form the government. As a result election and voting systems are given much importance in India. In spite of that, there are no easy or well accessible processes for the people to cast their votes. After the abolition of paper ballot voting system for its high time consuming and several related drawbacks, the use of EVM or Electronic Voting Machines became popular in India, for its easy access and less time consuming features. Yet the process is not at all efficient and secure because of its various drawbacks [2]. Therefore a country like, India, adorned with blessings of science and highly modern technologies should employ much secure, easy and relax voting techniques. Massive projects and researches are going on to discover advanced voting systems. In majority of the cases authentication checking and reliability are the basic concern. Here we have discussed the various drawbacks related to the present voting scenario which can be solved by advanced technology. In this paper we have actually introduced a concept of centralized voting system guided by biometric fingerprint authentication technology.

II. PRESENT VOTING SCENARIO IN INDIA

Now the election seems to be a great messy proceeding. On or before election days transport system totally ceases and maximum surface transport vehicles are taken off the road for election purpose. Moreover official works in a majority of public sectors are suspended during election months. Officers and staffs from public sectors are appointed on election duties. As a result the public sectors have to face a complete disorder and the employees, customers related to it also suffer a lot.
Schools, colleges and other related institutions are taken as polling stations or DCRCs (Distribution Centre cum Receiving Centers) for distribution and collection of voting equipments, related documents & applications, to the polling officers. For these, the official works, classes are suspended and the students have to face various problems.

 ISSN: 2321-8169
4586 - 4594

On a particular election day, the election booths become heavily crowded. People have to stand in the scorching sunlight for hours just to cast "a vote". Aged people and senior citizens have to face the same problems. Pregnant women and women with kids face great difficulty for the lack of various facilities; as a result a great percentage of these women do not come to the booths to cast their votes.

Fig 1: Old & aged person standing in a long vote queue waiting for her turn.

III. PROBLEMS WITH EVM

1. Do not guarantee transparency: A voter could not check what happened to his/her vote i.e., whether it has been properly recorded in the system database or not.
2. Since the EVMs move through different hands therefore they are susceptible to manipulations by fraudulent.
3. Inefficient process of identity checking: Here valid voters are just checked by polling officers by their photos on the voter card therefore more or less similar looking persons can give the vote on behalf of another.
4. Since the structure and composition of the EVM is very simple so substituting a Look-Alike fake EVM with the real one can be done easily.
5. Susceptible to manipulations: by attaching additional hardware to the control unit's circuit board, an attacker could directly read and write the EEPROM chips that record the votes.
6. Natural Hazards: high temperature, humidity and adverse climatic conditions can damage the EVM chips and internal circuitry. Moreover attack by vermin, rats, fungus or mechanical danger can generate malfunctions.
7. Small chips attached to the EVMs that can be controlled by fraudulent through radio waves or infrared can alter or manipulate the functioning of the machine leading to alter the vote results-research proved by Hari Prasad, Rop Gonggrijp, and J. Alex Halderman in "Security Analysis of India's Electronic Voting Machines" [2].

IV. ADVANCEMENT THAT CAN BE MADE IN THE FIELD OF VOTING

So in this modern era of technology we can have ATM like touch screen Machines which can be called as AVM (or Automatic Voting Machine) to cast our votes. For this thing we must have the voter cards in the form of smart cards i.e. Smart Voter Card (SVC) containing all the informations of Aadhaar Card[16] (or Unique Identification Card). The Unique Identification Authority of India (UIDAI) [16,17] is a central government agency of India. It is attached to the erstwhile Planning Commission of India, now NITI Aayog (National Institution for Transforming India). Its objective is to collect the biometric and demographic data (Name, address, DoB, age, address, mobile no., email id) of residents to issue a 12-digit unique identify number called Aadhaar to each citizen. It is mandatory for all citizens of India to enroll him/her in this world's largest national identification number project. So by tagging the 12-digit unique identity number with the Smart Voter Card the system can access the fingerprint and details of every citizen (from the UIDAI database) for voting purpose. By doing this, there will be no need to enroll all the citizens again for obtaining their fingerprint and details.

Fig 2: Casting vote on touch screen.

If we watch properly around us, everything is becoming centralized and online, starting from booking of railway tickets, flight tickets, online payment of money, buying of garments and useful daily accessories to admission in schools and colleges through e-counseling process, transfer of money worldwide via national and international credit and debit cards. Now a days ATMs can also print bank statements, pass books, dispense postage stamps, transfer or deposits checks. Even in Delhi(capital of India) the Delhi Jal*(Water)* Board (DJB)[7] has launched a massive program – "Sarvajal*"(i.e. Water to all)* [9,10] to make water ATM's

 ISSN: 2321-8169
4586 - 4594

allover Delhi, in which a sort of prepaid smart card (called water cards) is used to get the desired and particular quantity of drinking water from the water ATMs. *So, "why the Voting system should be so much back-dated and primitive in India?"*

V. ACCESSIBILITY OF AVM

Automatic Voting Machines (AVMs) should be made in such a way that it should have multiple language options, easy to access, strong and durable and above all it should have the capacity to detect and prevent any illegal proceedings so, that tampering with the machine can be completely prevented. The name of the candidates with their corresponding party symbol or logo along with the NOTA[12](or None Of The Above) option can be made to display on the AVM touch screen. The voters will just have to press or touch the screen over the name

Fig 3: An imagined model of Automatic Voting Machine (AVM) with Touch Screen and Smart Voter Card

of the candidate or NOTA, he desires to vote. As a step for security checking about the authentication of the voter, his finger prints will serve as the best as it is unique to all.

First of all the voter will have to enter the AVM counter, then he will have to place the voter card(that can be made as a smart card which will contain complete information about the voter along with his/her fingerprints) over a scanner through which the machine will be fetched with the voter's complete details and information. Then the machine will direct the voter to place his fingers on a finger print scanner for authentication. After that the machine will perform a checking between the two templates of the fingerprint, one taken from the live-scan and the other stored previously in the system database. Now, if the two templates match then only the said person will be eligible to cast his/her vote. As a result of this process one person cannot cast the vote of another person. Then as said above the voter will have to press or touch his desired candidate's name or NOTA option over the screen to cast the vote. At last, as a sense to win the trust and belief of the voter the AVM screen will display a confirmation message stating the name of the candidate (along with the corresponding party

Fig 4: Candidates' name stood up in the election can be made to display on the AVM screen.

symbol or logo) or NOTA as voted by the said voter. If they want to do any changes in their vote they can press the cancel button to reenter their choice. If not, the voter can press the 'yes' button to confirm their vote. After the voting is confirmed an assurance message will be displayed stating the name of the candidate along with his party symbol or NOTA as voted by the said voter, then the thank you message will be displayed on the screen. After this the machine will be ready for next use. In our opinion this message at the last will serve as a great significance as the voter will be completely assured that their vote has been properly casted against their desired candidate. There will be no discrepancy as the whole setup would be guided, secured and controlled under the complete supervision of the Election Commission of India.

In case of EVM no such assurance is offered to the voter related to the casting of the vote. Therefore, if the idea is implemented in case of AVM, then this sort of message displayed at last, will assure the voters that their vote has been properly casted against their desired candidate, thus wining the trust and integrity of the voters.

VI. SECURITY ASPECTS THAT CAN BE IMPLEMENTED IN AVM

For security purpose CCTV, surveillance cameras and spy cameras can be installed outside the AVM counters. Again, to enter into the AVM counter the voter has to enter his/her voter card (that can be made as a sort of smart card) into a card slot outside the AVM counter. Now, if the card is valid

 ISSN: 2321-8169
4586 - 4594

then a green light will glow(otherwise: red) and the counter door will automatically open allowing the voter to enter into the AVM counter; these security strategies will ensure that only one person (or voter) can enter the AVM counter at a time. Moreover on the voting day special cops and reserved forces should be made ready to control law and order. Proper monitoring teams will be present to tackle any problems. Above all the software should be programmed in such a way that any eligible candidate can cast his/her vote from any AVM within or outside their proper constituency. Thereby the candidates can cast their votes from any place within India through any voting AVM. As the process will be completely centralized so, there will be no burden on the voter to come to their own constituency howsoever to cast their votes. This will also help to reduce the crowd and rush during votes in a particular counter. Even the time of voting can also be increased from 6 AM in the morning to 12 AM midnight (which is usually 7 AM in the morning to 6 PM in the evening) as everything will be processed and submitted online through automatic system. After the voting time is over, the process will be closed automatically and the machine will not accept any voter card. So, after the scheduled time no one will be able to cast any vote even though being an eligible voter.

VII. OUR PROPOSED AVM MODEL AND FRAMEWORK

The external appearance of AVM should be somewhat like the modern day ATMs. It should have the following important units.

1. *Display Unit / Touch Screen* – the visual display unit or touch screen will display the names of the candidates stood up in the election from the concerned constituency of the voter along with their corresponding party symbol. Moreover after voting the assurance message will also be displayed on this screen which will assure the voter that his/her vote has been properly casted and recorded in the system data base.

2. *Keyboard* – Voters can press the touch screen over the name of the candidate they desire to vote or they can also press the serial number of the candidate on the keyboards to cast their votes (both options can be implemented for convenience).

3. *Card Slot* – the voter will have to swipe his/her voter card which can be made as a smart card containing encrypted informations of both the traditional voter card and the Aadhaar Card. As the voter card will be in the form of a smart card, so it will obviously contain an embedded integrated circuit that can be either a secure microcontroller or equivalent intelligence with internal memory or a memory chip alone. As a result of swiping the voter card, in the card reader/card slot the computer will be fetched with the complete details of the voter including his/her finger prints from the System Data Base.

4. *Biometric Finger Print Scanner* – a finger print scanner should be present in the AVM to check the authentication of the voter i.e. a voter can cast his/her vote if and only if the finger print stored in the system database matches with the finger print of the voter scanned through the biometric scanner.

The AVM counters will be like simple work stations or terminals. One server is required for each assembly (situated in the district town) and this should be connected to all terminals throughout the villages/towns. As per the population of the concerned constituency or assembly AVM counters can be constructed. As the process will be completely centralized so

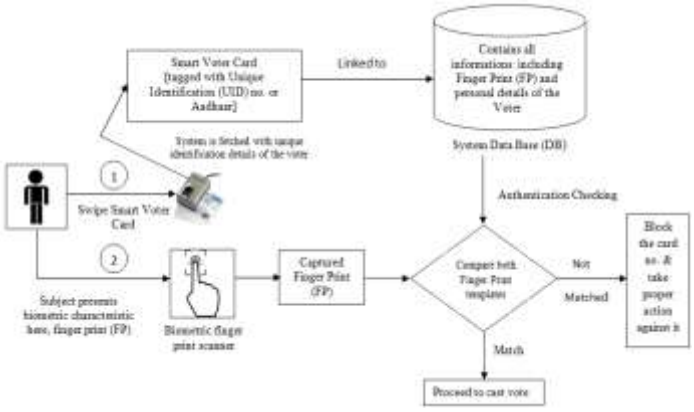

Fig 5: Work-flow diagram of our proposed model with systemic authentication using fingerprint verification system

there will be no hard-and-fast rule that voters will have to cast their votes only from their concerned constituency. That is, voter of one constituency may cast his/her vote from another constituency because on inserting the smart voter card on any AVM the system will show the candidate list for the concerned constituency to which the voter actually belongs. Therefore, after voting the system will automatically store the information to the appropriate block in the system database.

 ISSN: 2321-8169
4586 - 4594

VIII. BIOMETRIC FINGERPRINT AUTHENTICATION SYSTEM

Why fingerprints?

The cost of a fingerprint based biometric system is relatively low in comparison to other biometric based authentication systems like iris recognition, face readers, retina scanning, voice recognitions or hand geometry. At present, there are mainly nine different biometric techniques that are either widely used or under investigation, including face recognition, fingerprint verification, hand geometry detection, hand vein detection, iris recognition, retinal pattern, signature, voice print, and facial thermograms.
Although to a certain extent each of these techniques, has been used in practical systems and has the potential to become a valid biometric technique yet many of them are not acceptable in a court of law as indisputable proof of identity.

Despite the fact that wide-spread experiments have been conducted on automatic face recognition, it has not yet been proven that: (a) face can be used reliably to establish/verify identity and (b) a biometric system using only face recognition can be easily fooled. For example, without any other information about the people in Fig.6, it will be extremely difficult for both a human and a face-recognition system to conclude that the different faces shown in Fig.6 are disguised versions of the same person.

Moreover, voice recognition systems are highly susceptible to noise and misuse. Interactive Voice Response Based Voting System is under research but one of its major drawbacks is that, as the voters are going to give their votes through telephones (mobile or landline), therefore it cannot be known

Fig 6: Multiple personalities: all of the people in this image are the same person. (From The New York Times Magazine, Sept. 1, 1996, sect. 6, pp. 48–49. Reproduced with permission of Robert Trachtenberg.) [18]

whether the voters are giving the vote as per their will(or choice) or forcefully under the pressure of some individual or political organizations. Since no monitoring system is present around the voter so this system can lead to havoc misuse.

To overcome these problems we have to use a simple, easy accessible, accurate and financially balanced authentication system for voting. So far, the only legally acceptable, readily automated, and mature biometric technique is the automatic fingerprint authentication technique, which has been used and accepted in forensics since the early 1970's. Although signatures are also legally acceptable biometrics, but they rank a distant second to fingerprint due to issues involved with accuracy, forgery, and behavioral variability. Moreover

Biometric Identifier	Universality	Distinctiveness	Permanence	Collectability	Performance	Acceptability	Circumvention
DNA	H	H	H	L	H	L	L
Ear	M	M	H	M	M	H	M
Face	H	L	M	H	L	H	H
Facial thermogram	H	H	L	H	M	H	L
Fingerprint	M	H	H	M	H	M	M
Gait	M	L	L	H	L	H	M
Hand geometry	M	M	M	H	M	M	M
Hand vein	M	M	M	M	M	M	L
Iris	H	H	H	M	H	L	L
Keystroke	L	L	L	M	L	M	M
Odor	H	H	H	L	L	M	L
Plamprint	M	H	H	M	H	M	M
Retina	H	H	M	L	H	L	L
Signature	L	L	L	H	L	H	H
Voice	M	L	L	M	L	H	H

Fig 7: Comparison of various biometric technologies based on the research done by A. K. Jain et.al. in "An Introduction to Biometric Recognition" ©IEEE, Jan 2004 . In the chart, High - **H**, Medium - **M**, and Low – **L**

statistics have shown that the matching accuracy using the system of fingerprints is the highest among all the biometrics based authentication systems.

Concept

A biometric fingerprint authentication system is essentially a pattern recognition system that operates by acquiring biometric data (here, fingerprint) from an individual, extracting a feature set from the acquired data, and comparing this feature set against the template set stored in the system database. In [3] Jain et al. have proposed a concept that depending on the application context, a biometric system may operate either in verification mode or identification mode.
• In the verification mode, the system validates a person's identity by comparing the captured biometric data (here, fingerprint) with the template(s) stored in the system database. In such a system, an individual who desires to be recognized claims an identity, usually via a personal identification number (PIN), a user name, or a smart card [here, it will be through a

ISSN: 2321-8169
4586 - 4594

Smart Voter Card tagged with Aadhaar or Unique Identification (UID) number], and the system conducts a one-to-one comparison to determine whether the claim is true or not (e.g., "Does this fingerprint belong to Mr. X?"). Identity verification is generally used for positive recognition, where the aim is to prevent multiple people or fraudulent from using the same identity [3].

• In the identification mode, the system recognizes an individual (or person) by searching the templates of all the users in the database for a match. Therefore, the system conducts a one-to-many comparison to establish an individual's identity (or fails if the subject/individual is not enrolled in the system database) without the subject having to claim an identity (e.g., "Whose biometric data is this?") [3].

Here we will use the verification mode to determine whether the voter is authenticated or not.

IX. UNIQUE CHARACTERISTICS OR FEATURES OF FINGERPRINTS

Each and every individual has a different or unique fingerprint. Even twins also share unique fingerprints. A fingerprint is made of a number of ridges and valleys on the surface of the finger. Ridges are the upper skin layer segments of the finger and valleys are the lower segments. The ridges form so-called minutiae points. Minutiae and patterns are very important in the analysis of fingerprints since no two fingers can have these things to be identical.

Patterns

The three vital patterns of fingerprint ridges are the arch, loop, and whorl [19, 20]:

- Arch: The ridges enter from one side of the finger, rise in the center forming an arc/curve, and then exit on the other side of the finger.
- Loop: The ridges enter (come in) from one side of a finger, form a curve, and then exit (go out) on that same side.
- Whorl: Ridges form circularly aligned around a central point on the finger.

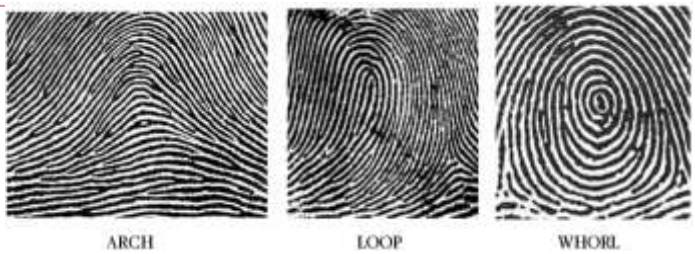

Fig 8: Different fingerprint patterns- arch, loop, and whorl

Minutiae features

The major minutiae features of fingerprint ridges are ridge ending, bifurcation, and short ridge (or dot) [19, 20]:

- The ridge ending is the point at which a ridge terminates.
- Bifurcations are points at which a single ridge splits into two ridges.
- Short ridges (or dots) are ridges which are significantly shorter than the average ridge length on the fingerprint.

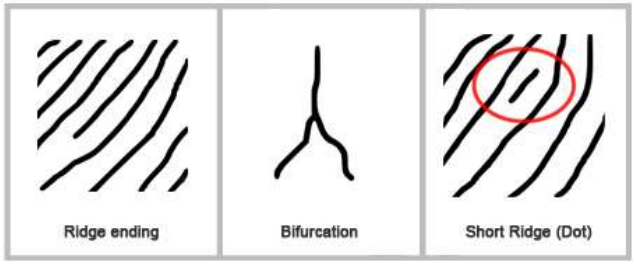

Fig 9: Types of Fingerprint Minutiae such as ridge ending, bifurcations, short ridges (or dots) respectively.

X. DESIGN OF A FINGERPRINT-VERIFICATION SYSTEM

First of all fingerprints are scanned through a fingerprint sensor/scanner, which is an electronic device used to capture a digital image of the fingerprint pattern. The captured image is called a live scan taken by the optical frustrated total internal reflection (FTIR) concept. When a finger is placed on one side of a glass platen (prism), ridges of the finger are in contact with the platen while the valleys of the finger are not. The imaging system essentially consists of a combination of a light emitting diode (LED) light source and a charge-couple device (CCD) placed on the other side of the glass platen. The laser light source illuminates the glass at a definite angle, and the camera is placed in such a way that it can capture the laser light reflected from the glass platen. The light that is incident on the platen at the glass surface touched by the ridges is randomly scattered, while the light incident at the glass surface corresponding to valleys suffers total internal reflection, resulting in a corresponding fingerprint image on the imaging plane of the CCD [18].

 ISSN: 2321-8169
4586 - 4594

This live scan is digitally processed to create a biometric

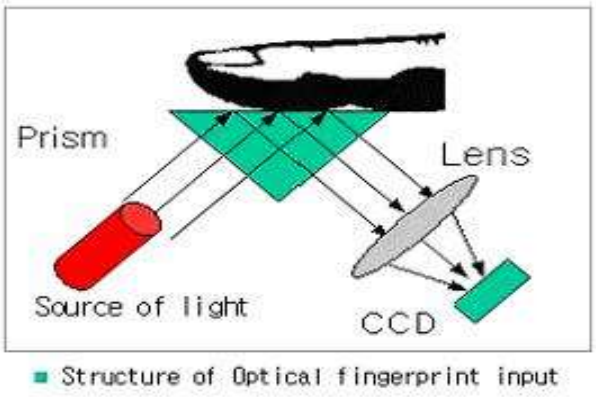

Fig 10: Internal structure of an optical fingerprint scanner

template (based on a collection of extracted features) which is stored in a database and used for matching. Presently fingerprint scanning can be done through different fingerprint sensor technologies such as Optical sensors, Ultrasonic sensors, Capacitance sensors, passive capacitance sensor, and Active capacitance sensors.

A fingerprint scanner system has two basic jobs -- it needs to get an image of our finger, and it needs to determine whether the pattern of ridges, valleys and minutia points in this image (live scan), matches the pattern of ridges, valleys and minutia points in pre-scanned images stored in the system database. By the two representations the matching module determines whether the prints are impressions of the same finger. The matching phase typically finds a metric of the similarity between two fingerprint representations. The matching stage also defines a threshold to decide whether a given pair of representations is of the same finger (mated pair) or not. Based on this matching technique access is granted otherwise rejected.

Only specific characteristics (such as pattern of ridges, valleys and minutia features) which are unique to every fingerprint are filtered and saved as an encrypted biometric key or mathematical representation.

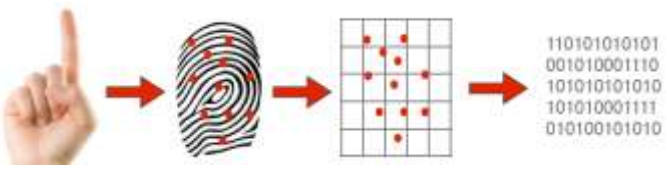

Fig 11: Biometric fingerprint encryption

No image of a fingerprint is ever saved, only a series of numbers (a binary code), which is used for verification. Therefore, algorithm cannot be reconverted to an image, so no one can duplicate our fingerprints.

XI. ADVANTAGES

1. AVMs will contribute to a faster vote casting, effortless counting and delivery of the election results.
2. They standardize the counting of ballots, improve counting accuracy and allow the results to be prepared in less time compared to a manual balloting system.
3. AVM will completely strikeout the errors in the vote casting and counting process by decreasing the chances of invalid vote.
4. The system is highly user friendly: With the advancement in online systems now almost all individuals use ATM for banking so this AVM system (which is much similar to ATM) will be easily understood by them.
5. Tamper-free & assures authentication: The system will be completely centralized and valid voters will be checked through biometric (unique) characteristics such as finger prints therefore not a single invalid vote could be casted.
6. Since the system will be completely centralized so workload can be reduced drastically.
7. It is impossible to tamper with the software or hardware and as the database will be centralized so results cannot be manipulated.
8. Gaining transparency, trust and integrity of the voters: After casting the vote, the AVM screen will display the name and symbol of the party voted by the said voter. This message will allow the voters to verify that their vote has been properly casted or recorded in the system database.
9. The system cannot be fooled easily with fake fingerprints because of the presence of different methods to detect the liveness of finger scan as (i)Temperature sensing (ii) Detection of pulsation on finger trip (iii) Pulse oximetry (iv) Electrical conductivity [14]

(v)Analysis of textural features (vi) Sweat pores detection [15].

The wide spread setup and infrastructure of ATMs all over the world have proved that ATM type machines are not vulnerable to manipulations so if AVMs are setup on that same infrastructure (for voting purpose) then they too will not be susceptible to manipulations after all AVM will be just like a "voting ATM" with an added biometric fingerprint authentication system for checking the authenticity of the voters.

XII. CONCLUSION

We believe that at the time of creation of anything bigger, first comes imagination which will help us to frame an outline of our goal. Then the imagination should be implemented properly and efficiently to achieve the desired goal. We have just presented an idea or concept that how our voting systems can be made in the recent future for "free and fair" voting, with faster, secure, easy accessible and reliable voting techniques. The application of biometric fingerprint authentication system will enhance the authenticity of a voter thereby leading to a fair election. The system proposed, when put into proper functioning will revolutionize the world of voting. We know that for these things highly efficient technology, system and application software, a large database and proper infrastructure is required. But a country like India adorned with the blessings of Science & Technology can easily implement such a process. We have complete faith and belief in our government, the Election Commission of India and our day to day upgrading technology. We are also sure that in the upcoming days our technology is going to build something like this or much better and convenient from this.

XIII. REFERENCES

[1] Electronic Voting Machines-Scribd. https://www.scribd.com/doc/236412542/Electronic-Voting-Machines.

[2] Hari K. Prasad, J. Alex Halderman, Rop Gonggrijp – '*Security Analysis of India's Electronic Voting Machines*'. https://indiaevm.org/evm_tr2010-jul29.pdf

[3] Anil K. Jain, Fellow, IEEE, Arun Ross, and Salil Prabhakar, "An Introduction to Biometric Recognition", IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS FOR VIDEO TECHNOLOGY, VOL. 14, NO. 1,pp.4-20, JANUARY 2004

[4] S. Prabhakar, S. Pankanti, and A. K. Jain, "Biometric recognition: Security and privacy concerns",IEEE Security PrivacyMag.,vol.1,no. 2, pp. 33–42, 2003.

[5] D. Maio, D. Maltoni, R. Cappelli, J. L. Wayman, and A. K. Jain, "FVC2002: Fingerprint verification competition," in Proc. Int. Conf. Pattern Recognition (ICPR), Quebec City, QC, Canada, Aug. 2002, pp. 744–747.

[6] Mr. Ratnakar anandrao kharade, Mr. M.S. Kumbhar / International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622, "An Identity-Authentication System Using Fingerprints", www.ijera.com Vol. 2, Issue 6, November- December 2012, pp.303-311

[7] Delhi Jal Board, Govt. of NCT of Delhi.http://www.delhi.gov.in

[8] ATMs as voting machines: An idea whose time hasn't come---- by Jay MacDonald http://www.creditcards.com/credit-card-news/atm-voting-machines-1273.php#ixzz31EtIJy6S

[9] Sarvajal: http://www.sarvajal.com/#sarvajal

[10] Sarvajal project provides clean and safe drinking water, it uses prepaid Water Cards to get water in the Water ATMs http://businesstoday.intoday.in/story/innovation-drinking-water-supply-sarvajal-waterlife/1/186622.html

[11] The Association of the Bar of the City Of New York -- *REPORT OF THE ELECTION LAW COMMITTEE: SUBCOMMITTEE ON NEW VOTING TECHNOLOGY* http://www.nycbar.org/pdf/report/New%20Voting%20Technology%20Report.pdf

[12] THE ECONOMIC TIMES POLITICS AND ELECTION: *FROM ELECTION TO SELECTION:* regarding NOTA –a landmark verdict by the *Supreme Court* http://eci.nic.in/archive/press/current/PN_28062002.htm

[13] ELECTION COMMISION OF INDIA ----- No. ECI/PN/24/2002 "Subject: *Supreme Court's order dated 2nd May, 2002 relating to right to information of electors regarding criminal antecedents, assets and liabilities and educational qualifications of candidates – implementation of the order.*" http://eci.nic.in/archive/press/current/PN_28062002.htm

[14] Utilizing Characteristic Electrical Properties of the Epidermal Skin Layers to Detect Fake Fingers in Biometric Fingerprint Systems—A Pilot Study, 16 April 2007.

[15] Memon, S.; Manivannan, N.; Boulgouris, A.; Balachandran, W. Fingerprint Sensors: Liveness Detection and Hardware Solutions. In Sensors and Biosensors, MEMS Technologies and its Applications; Yurish, S., Ed.; Volume 2, pp. 121–148.)

[16] Aadhaar Card (The Unique Identification Authority of India).http://uidai.gov.in/

[17] Unique identification card or Aadhaar Card. https://en.wikipedia.org/wiki/Unique_Identification_Authority_of_India

[18] Anil K. Jain, Fellow, IEEE, Lin Hong, Sharath Pankanti, Associate Member, IEEE, and Ruud Bolle, Fellow, IEEE,

"An Identity-Authentication System using Fingerprints", proceedings of the IEEE, Vol. 85, no. 9, September 1997, pp.1365-1388.

[19] Fingerprint recognition or fingerprint authentication – Source Wikipedia. https://en.wikipedia.org/wiki/Fingerprint_recognition

[20] Dr. Prateek Rastogi (Associate Professor, Deptt. of Forensic Medicine & Toxicology, Kasturba Medical College, Mangalore)and Ms. Keerthi R Pillai, "A study of fingerprints in relation to gender and blood group ", Journal of Indian Academy of Forensic Medicine, J Indian Acad Forensic Med, 32(1) , ISSN 0971-0973, pp.11-14. http://medind.nic.in/jal/t10/i1/jalt10i1p11.pdf