iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 5 **Issue:** IV **Month of publication:** April 2017

DOI: http://doi.org/10.22214/ijraset.2017.4033

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Survey Paper on Online Election System

Yamini Jangde[1], Farheen Sheikh[2], Ankita Chandekar[3]
[1,2,3]B. E Sixth Sem CSE, Smt. Rajshree Mulak College of Engineering, RTMN University

Abstract- An electronic voting (e-voting) system is a voting system in which the election data is recorded, stored and processed primarily as digital information. There are two types of election: On-Line and Offline. In online election system we can vote via Internet, and in offline election system we vote by using a voting machine or an electronic polling booth.
Online Election System: Authentication of Voters, Security of voting process, Securing voted data are the main challenge of e-voting. This paper deals with design, build and test an online voting system that facilitates user, candidate, election commission officer to participate in online voting. Its design is very simple, ease of use and also reliable.
Offline Election System: In many proposals the security of the system relies mainly on the black box voting machine but security of data privacy of the voters and the accuracy of the vote are also main aspects that have to be taken into consideration while building secure e-voting system. It ensures that vote casting cannot be altered by unauthorized person. The voter authentication in online election process can be done by formal registration through administrators and by entering One time password.
Keywords— Online e-voting

I. INTRODUCTION

The voting scheme have evolved from counting hands in early days to system that include paper, punch card, mechanical lever and optical- scan machines. These drawbacks are overcome by Online Election System.
Online Election System is a voting system by which any voter can use his/her voting rights from anywhere in the country. We provide a detail description of the functional and performance characteristics of Online Election System. Voters can cast their votes from anywhere in the country without visiting to voting booths, in highly secured way. That makes voting is a fearless of violence and that increase the percentage of voting.
Online Election System are simple, attractive and easy to use. It reduces manual efforts and bulk of information can be handled easily. But out of all these features there are some disadvantage with this system are there can be software failure issue, insecure access of internet and also voter should be familiar with internet.
The administrator's effort is much reduced by checking the election status of all the localities individually forms a place and it is easy for whom to announce the election result.
Security is a heart of e-voting process. Therefore the necessity of designing a secure e-voting system is very important. Usually, mechanisms that ensure the security and privacy of an election can be time-consuming, expensive for election administrators, and inconvenient for voters.
Online Election System as the name implies, is the voting process held over electronic media. i.e. computer. In general , such Online election voting system should satisfy such requirements as follows

A. Accuracy
B. Simplicity
C. Democracy
D. Verifiability
E. Privacy
F. Security

The voter authentication in online e-voting process can be done by formal registration through administrators and by entering OTP Certificate. In Offline e-voting process authentication can be done using facial recognition, fingerprint sensing and RFID (smart cards) which enables the electronic ballot reset for allowing voters to cast their votes.

II. ELECTRONIC VOTING SYSTEMS

E-voting is referred as "electronic voting" and it defined as any voting process where an electronic means is used for votes casting and results counting. E-voting is an election system that allows a voter to record their ballots in the electrically secured method. An electronic voting system is a voting system in which the election data is recorded, stored and processed primarily as digital

©IJRASET: All Rights are Reserved

information. A number of electronic voting systems are used in large applications like optical scanners which read manually marked ballots to entirely electronic touch screen voting systems. Specialized voting systems like DRE (direct recording electronic) voting systems, RFID, national IDs, the Internet, cellular systems and computer networks are also used in voting processes.

A. *Securities of the E-Voting Systems*

The main goal of a secure online election is to ensure the privacy of the voters and the accuracy of the votes.
A secure online election system are satisfies on the following requirements:

1) *Eligibility:* only votes of legitimate voters shall be taken into account
2) *Anonymity:* votes are set secret.
3) *Un-Reusability:* each voter is allowed to cast one vote.
4) *Accuracy:* cast ballot cannot be altered. Therefore, it must neither be possible to delete ballots nor to add ballots, once the election has been closed.
5) *Vote and Go:* once a voter has casted their vote, no further action prior to the end of the election
6) *Fairness:* partial tabulation is impossible.
7) *Public Verifiability:* anyone should be able to readily check the validity of the whole voting process.

B. *Issues of Present Voting System*

The several studies have been studied by using computer technology to improve elections. These studies caution against the risk of moving too quickly to adopt online voting system, because of the software engineering challenges ,network vulnerabilities and the challenges of auditing. There are some issues present in voting system:

1) *Accuracy:* It is not possible for a vote to be changed, eliminated the invalid vote cannot be counted from the
2) Finally tally
3) *Availability:* The system works properly as long as the poll stands and any voter can have access to it from the beginning to the end of the poll.
4) *Democracy:* It permits only who is eligible for voting to vote and it ensures that eligible voters vote only once.
5) *Privacy:* Neither authority nor anyone else can link any ballot to the voter.
6) *Verifiability:* Independently verification of that all votes have been counted correctly.
7) *Resistance:* No electoral entity (any server participating in the election) or group of entities, running the election can work in a conspiracy to introduce votes or to prevent voters from voting.
8) *Resume Ability:* The system allows any voter to interrupt the voting process to resume it or restart it while the poll stands.

The existing elections were done in traditional way, using ballot, ink and tallying the votes later. But the proposed system prevents the election from being accurate. Problems encountered during the usual elections are as follows

a) It requires human participation, in tallying the votes that makes the elections time consuming and prone to human error.
b) Deceitful election mechanism.
c) The voter finds the event boring resulting to a small number of voters.
d) Constant spending funds for the elections staff are provided.

So, the proposed electronic voting system has to be addressed with these problems.

C. *Proposed System of Online E-Voting*

"Online voting system" is an online voting technique. It is based on the other online services like "online reservation system". In this system people who have citizenship of India and whose age is above 18 years of any sex can give his\her vote online without going to any polling booth. There is a database which is maintained by the election commission of India in which all the names of voter with complete information is stored.in "online voting system" a voter can use his\her voting right online without any difficulty. He\she has to fill a registration form to register himself\herself. All the entries is checked by the database which has already all information about the voter. If all the entries are correct then a user id and password is given to the voter, by using that id and password he\she can use his\her vote. If conditions are wrong then that entry will be discarded.

III. OFFLINE E-VOTING SYSTEMS

A. *Fingerprint Recognition*

©IJRASET: All Rights are Reserved

In fingerprint authentication refers to the automated method of verifying a match between two human fingerprints. Fingerprints are one of many forms of the biometrics used to identify the individuals and then the identification is done. There are many ways to deal with verification of fingerprints. A fingerprint looks at the patterns found on a fingertip. Some emulate the traditional police method of matching pattern; others use straight minutiae matching devices and still others are a bit more unique, including things like moiré fringe patterns and ultrasonic. A greater variety of fingerprint devices are available than for any other biometric. Fingerprint verification may be a good choice for in e-voting systems. It is not surprising that the workstation access application area seems to be based almost exclusively on fingerprints, due to the relatively small size, low cost, and ease of integration of fingerprint authentication devices that will be implemented.

B. Facial Recognition

Iris recognition systems have same as any other biometric modality. After capturing an image of the eye, the iris is located and segmented to extract its features, these features are then compared to a previously stored template .This section describes each of these blocks in detail, providing information on the approaches found in previous publications.

The two different strategies are followed in offline biometric authentication systems: 1) The token performs the verification tasks and supplies the result, avoiding external access to the user's personal template. And 2)The token provides the biometric template. This paper recommends the second strategy for security and privacy motivations. Thus, different architecture approaches to build personal tokens will be described. These tokens are designed as tamper-proof devices, maintaining not only internal data security, but also a secure communications channel with the external world

1) *Iris Acquisition:* The iris biometrics systems do not use laser-scans to capture the image of the human eye. Currently, most of the work performed in this area has been dedicated for improving the user-system interaction by the developing cameras where the focusing system is automatic, such that the users are not required to remain steady at a fixed point in front of the camera. Instead, an infrared photo or video camera is used at a set distance to capture the high quality image of the iris. Working in the infrared range provides many advantages when compared to the visible range: crypts, iris ridges, and nerves are more evident the border between the iris and the pupil is more pronounced and users are not exposed to annoying flashes.
2) *Iris Segmentation:* The main purpose of this process is to locate the iris on the image and isolate it from the rest of the eye image for further processing. Some another important tasks that are also performed in this iris segmentation block include image quality enhancement, noise reduction, and emphasis of the ridges of the iris. Several proposals have been made by different authors for iris location and segmentation, whereas most consider iris detections finding two circumferences that model the iris boundaries. Daugman has proposed an integro differential operator, which works by examining the difference in the pixel levels between circles drawn in the image..
3) *Feature Extraction:* The normalization method varies from changes to the polar coordinate system, as Daugman proposed, to only considering a virtual line drawn around the pupil, known as the iris signature. This normalization becomes necessary when considering that the pupil varies in size for different light intensities. The majority of these begin with a normalization of the segmented iris image. In the feature extraction block, different authors have presented a wide variety of proposals. After normalization, the phase information by applying different Gabor filters was studied by Daugman. This was followed by the codification of this information in terms of the quadrant where the phase belongs however, Wildes, performs the extraction using Laplacian or Gaussian filters by obtaining several images of different scales for posterior comparison .
4) *Matching:* The Hamming distance is described by the following equation: where are the component of the template and sample vector, vector length and respectively, which are XOR in the equation. Selection of the threshold level usually depends on the final application. Although some authors have studied other matching algorithms the most employed matching algorithm has been the Hamming distance, as was initially proposed by Daugman . If the distance obtained is below a predefined threshold level, the studied sample is considered to belong to the user whose template is being studied.

©IJRASET: All Rights are Reserved

Volume 5 Issue IV, April 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

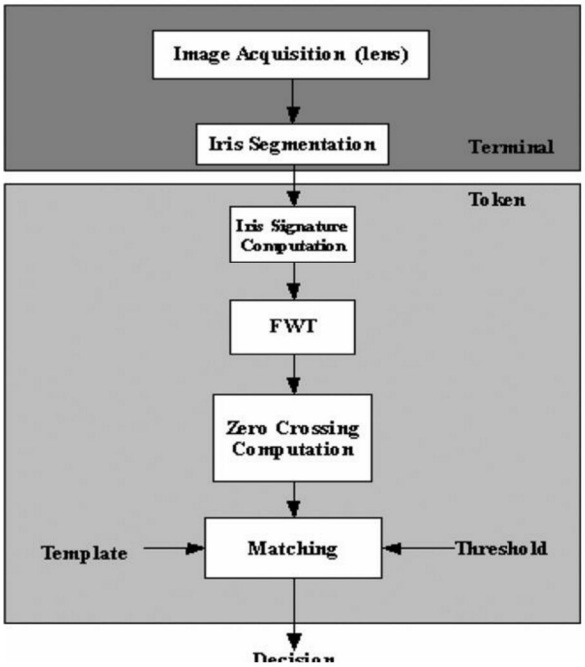


Fig.3.Terminal and platform functionalities.

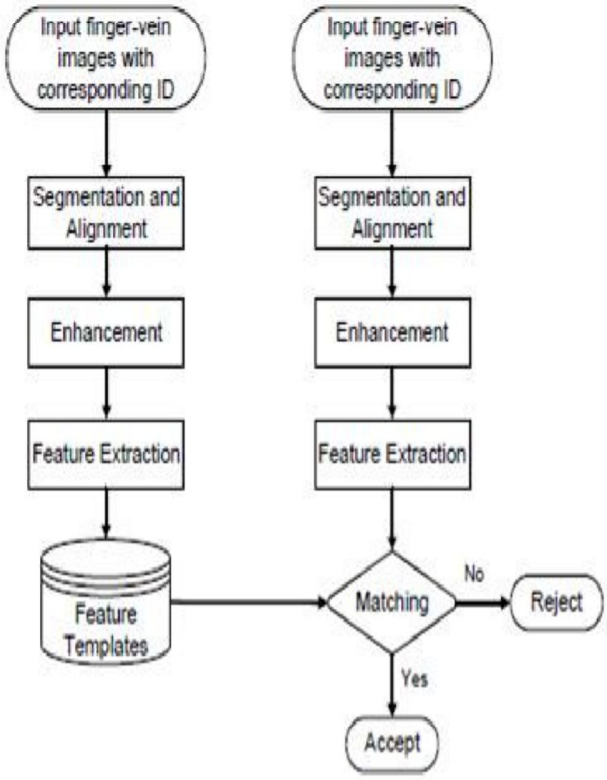


Fig.4.The flow-chart of the proposed recognition algorithm

C. Finger Vein

The proposed finger-vein recognition algorithm contains two stages: the verification stage and the enrollment stage. Both stages start with finger-vein image pre-processing, which includes detection of the region of interest (ROI), alignment, image segmentation and enhancement. For the verification stage, the input finger-vein image is matched with the corresponding template after its features are extracted. For the enrollment stage, after the pre-processing and the feature extraction step, the finger-vein template database is built. Fig. 4 shows the flow chart of the proposed algorithm. Some different methods may have been proposed for finger-vein matching. Considering the computation practicability, complexity, efficiency, however, we propose a novel method based on the fractal theory.

Finger vein has three hardware modules: DSP main board, image acquisition module and human machine. The structure diagram of the system is shown in Fig.4. The DSP main board including the DSP chip, memory (flash), and communication port is used to execute the finger vein recognition algorithm and communicate with the peripheral device. The image acquisition module is used to collect finger-vein images. The human machine communication module (LED or keyboard) is used to display recognition results and receive inputs from users.

IV. CONCLUSION AND FUTURE ENHANCEMENT

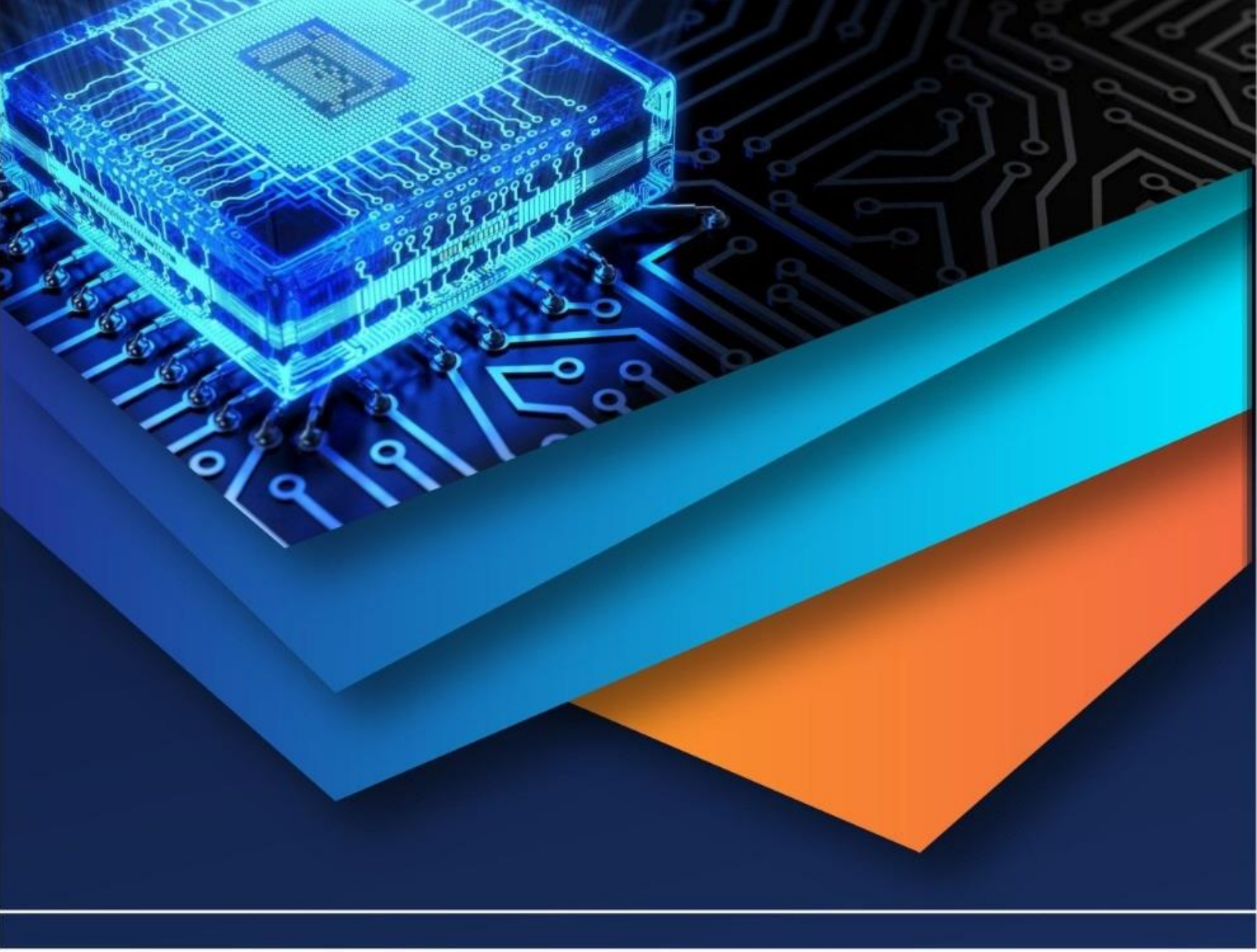
Online Voting systems enables a voter to cast his/her vote through internet without going to voting booth and additionally registering himself/herself for voting in advance, proxy vote or double voting is not possible, highly secure, fast to access, highly efficient and flexible, easy to maintain all information of voting. The use of online voting has the capability to reduce unwanted human errors. In addition to its reliability, online voting can handle multiple modalities and provide better scalability for large elections. Online election is also an excellent mechanism that does not require geographical proximity of the voters. Future enhancements focused to design a system which can be easy to use and will provide security and privacy of votes on acceptable level by concentrating the authentication and processing section. In that case of online election system some authentication parameters like facial recognization and in offline election system some authentication parameters like, Finger Vein and iris matching detection can be done.

©IJRASET: All Rights are Reserved

REFERENCES

[1] Tai-Pang Wu, , Sai-Kit, Yeung, Jiaya Jia, Chi-Keung Tang, And Ge´ Rard Medioni Closed-Form Solution To Tensor Voting: Theory applications Transactions On Pattern Analysis And Machine Intelligence, Vol34, No. 8, August 2012
[2] Scott Wolchok, Eric Wustrow, Dawn Isabel, and J. Alex HaldermanAttacking the Washington, D.C. Internet Voting System In Proc. 16th Conference on Financial Cryptography & Data Security, Feb. 2012
[3] S.W. Ambler, process Patterns: Building Large Scale System Using Object Technology, Cambridge University Press,1998.
[4] M. Andrews and J. A. Whittaker, How to Break Web Software : Functional and Security Testing of Web Applications and Web Servers. Addiso Wesley, 2006.
[5] Ali Fawzi Najm Al-Shammari, Sergio Tessaris " Vote Verification through Open Standard: A Roadmap", 978-1- 4577-0953-1/11IEEE2011
[6] Amir Omidi and Mohammad Abdollahi Azgomi, "An Architecture for E-Voting System Based on Dependable Web Services" 978-1-4244-5700-7-10,2009 IEEE.

©IJRASET: All Rights are Reserved



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)