OVERVIEW ON E-VOTING SYSTEM AND SECURITY CHALLENGES

[1]Seelam Sowjanya, [2]Dr.Barani Sundaram.

[1]*Assistant Professor, Department of Computer Science and Information Technology,
Defense University College of Engineering, Bishoftu, Ethiopia*

[2]*Department of Computer Science and Information Technology,
Defense University College of Engineering, Bishoftu, Ethiopia*

ABSTRACT:- *Now world expected to the electoral manner for focus on the use of latest technology in E-voting process. The current voting mechanism has many security problems, and it is challenging to prove even simple security aspects about them. A voting system that can elucidate and conventional has many considerations. Some of the major concerns for a government concerning electronic voting systems are to expand election activities and to depreciate the election expenses. Nevertheless, there is some opportunity of work in the electronic voting system regarding the authenticity of voters and to protect the computer-assisted voting machine from offenders. Biometrics is used widely for identification purposes. This chapter presents an analysis of different biometric techniques to find out which system is more stable for security improvement of an electronic voting system.*

KEYWORDS: biometric, Kiosk voting, Remote Internet voting, Poll-site Internet voting.

INTRODUCTION

The term 'Biometry' is independently associated with biological sciences, but now it is more commonly used in Information Technology for electronic authentication of users by their physical and behavioral attributes. Biometrics is a computerised method for recognising a form or authenticates a specific person based on a physiological or behavioural characteristic that can reliably differentiate between an authorised person and an unauthorised person. Examples of physical attributes are fingerprints, face, iris, and retina and hand geometry. Signature, voice and keystroke are the examples of behavioural characteristics on the other hand. Biometrics has better capability and reliability in comparison to traditional knowledge and token oriented techniques because biometric traits are unique and cannot comprise lost; moreover, a person to be identified need to be available physically during authentication. Anyone biometric technology cannot meet the requirements of all applications. All biometric systems have their advantages and drawbacks. Selection of appropriate biometric technology for an application depends on the differential capability of the technique as per the specified tolerance for the form in use. Biometrics is most commonly used the method in forensics applications like prison security and criminal identification. The biometric technology is robust acknowledged in civilian applications like e-banking, e-commerce and access control. Because of complex transactions through electronic means, e-banking and e-commerce are becoming one of the most related relationships of biometrics. With the advancement in biometric technology, the applications like credit card and smart card security, ATM security, check cashing and fund transfers, online transactions and web access are increasingly use biometrics for authentication. Biometrics is becoming popular because of the following reasons: i. It is most definitive and real-time tool available today. ii. It can easily merge with other tools to have better security. iii. Easier to use verification solutions. iv. It guarantees to acknowledge the person. v. It occurs based on physical and behavioural features of individuals. vi. It is authentic and accurate vii. Less expensive

LITERATURE SURVEY

A. Fujioka et al. [1992] authors presented a mathematical framework for a secure election that involves an administrator, a counter and the voter connected by an anonymous channel. Practically focused projects build on the blind voting protocol.
Lorrie F. Cranor et al. [1997] the use of unseeing signatures to certify that only enrolled citizens can vote and that mainly registered voter votes only once, and at the same time maintain the privacy of voter's is implemented. It allows voters to validate separately that their votes were counted correctly and anonymously challenge the results, should their votes be miscounted.
Ronald L. Rivest [2001] addresses some issues like the "secure platform problem" and the impossibility of giving a receipt to the voter. He also contributes some personal verdicts on a host of issues including the striking dissimilarity between e-commerce and e-voting. The dangers of opponents performing automated, wide-scale attacks while voting from home, the

need for extreme simplicity of voting devices, the importance of audit-trails, support concerning disabled voters, security problems of absentee ballots, etc.

[Hanady Hussien et al. [2013] "Design of secured E-voting systems." can desire with the widespread use of computers and embedded systems. Security is the essential problem should denote in such systems. This paper proposes a new e-voting system that fulfils the security requirements of e-voting. It signifies on the homomorphic property and blind signature plan. The suggested system implies executed on an embedded system which serves as a voting machine. The system employees RFID to store all conditions that comply with the rule of the government to check voter eligibility.

Steven J.Anderson et al. [2013] "Robust Tri-Model Automatic Speech Recognition for Consumer Applications." Investment automatic speech recognition (ASR) started to appear in the late 1980"s and can project a more tangible means of sustaining user inputs than methods such as typing on keyboards or touchscreens. Aforementioned is an especially important consideration for small consumer devices such as smartphones. In many practical circumstances, however, presentation of ASR can be significant. Compromised due to ambient noise and variable illumination circumstances. Prior research has shown that adding visual signals to standard ASR can mitigate the effects of ambient noise. ASR using adaptations of established techniques such as MT, DCT and MFCC.

Firas I. Hazzaa, Seifedine Khadr [2016] This paper deals with the design and development of a "Web-Based Voting System Using Fingerprint Design and Implementation", to provide high performance with high security to the voting system also we use web technology to make the voting system more practical. The new design has proposed an election for a university for selecting the president of the university. The proposed EVS allows the voters to scan their fingerprint, which is already followed by a previously saved image within a database. Developed Web-based Voting System using Fingerprint Recognition. This system has implemented an efficient way to cast votes, free of fraud, and make the system more trustable, economical and fast. We have used Minutiae-based fingerprint identification and matching with high accuracy.

PROBLEM STATEMENT

A voting system that can happen verified correctly has various concerns. The underlying reasons for a government to use electronic systems are to increase election activities and to reduce the election expenses. Still, there is the unusual scope of work in the electronic voting system regarding checking the authenticity of voters and securing electronic voting machine from miscreants. Biometrics is used to verify the identity of a person based on a physiological or behavioural behaviour. It can distinguish between a valid and invalid person. Biometrics features are distinct and cannot comprise lost. Moreover, since individual needs to be established should be available physically during the verification process, biometrics proved to be more reliable and more capable than traditional knowledge-based and token-based techniques. Electronic Voting Machine is a simple device used to store votes in place of ballot papers which were used earlier in the conventional voting system. It is a straightforward electronic machine that can be handled easily by the officials on election duty as well as by the voters. Being an autonomous and standalone machine, no one can interfere with its programming and manipulate the results. Advantages of EVM over the traditional ballot paper/ box system are:

It completely removes the possibility of vote casting by an unauthorised voter leading to the unpleasant situation like disputes and election petitions.

It addresses the procedure of counting the votes faster than the traditional system.

It minimizes to a comprehensive scope the quantity of paper used thus saving a large number of trees making the procedure eco-friendly.

It depreciates the cost of printing.

TYPES OF BIOMETRICS

Face Recognition His facial image can recognize a person. In this technique, the key feature from the centre position of a face image is overwhelmed with the help of a camera. Critical elements obtained from the centre portion of face do not change over the time. Visible light systems ignore the exterior features such as facial expressions and hair while capturing the image from the camera. Facial images can transpire stewarded by various methods like principal component analysis, neural networks and multi-resolution analysis. Some face recognition systems do not allow any movement during image capture stage, although many systems use a real-time process to locate the face automatically. Significant benefits of this technique included the acceptable by most of the user is described in [5].

Voice Recognition Voice recognition is alternative to speech recognition. It uses the acoustic features of speech which is shifting among the persons. Application sections of the voice recognition system are: Fixed Text, Text-Dependent, Text Independent, Conversational Voice verification system mostly uses the text-dependent method involving selection of one or more voice passwords. In case of concern of imposters, a text-prompt method comprises for voice verification. Degraded

performance may result in a change in behavioural features of voice and response if a different telephone has implied for enrollment and confirmation. Voice changes due to ageing need to be approached by recognition systems [4].

Iris Recognition Iris recognition is an analysis of the iris of eyes, which is a coloured ring of tissue surrounds the pupil of the eye. It is based on visible features. The digital template is recognized with the help of elements and their locations. It is considered to one of the safest and accurate biometric technology as it can match one pattern with the large set of data successfully with extremely high speed without compromising the accuracy of the match. This system can be used successfully in the presence of eyeglasses and contact lenses. This system has been experimented to work with people from different genetic groups [4].

Fingerprints Recognition with the fingerprint is an remarkably useful biometric technology as finger impressions of the individuals are distinct and have long been recognized as a leading and accurate identification method. Finger print based biometrics is extensively used for authentication and identification of a person. Authentication: in authentication 1:1 correspondence is founded by matching the persons claimed identity to his/her biometric and one or more other confidence technologies like password or PIN. Identification: in identification 1: Many conformities are confirmed by matching a person from complete database enrolled. Fingerprint systems can further be functioned in identification mode. Several countries check fingerprints for new persons to social services benefits to ensure beneficiary do not fraudulently obtain benefits under fake persons [6].

TYPES OF E-VOTING

Poll-site Internet voting: It advises the guarantee of higher compensation and effectiveness in that voter could cast their votes from any poll site, and the tallying manner would be fast and straightforward. More importantly, since election magistrates would control the voting principles and the physical circumstances, managing the safety risks of such systems is reasonable.
Kiosk voting: Voting machines would be located away from regular polling places, in such suitable public places as malls, libraries, colleges or schools just like ATM. The voting platforms would noiseless be under the supervision and full control of election officials. The corporeal circumstances could be mitigated by the election officials as per need to address security and privacy concerns and prevent any outside interference or coercion.
Remote Internet voting: It aims to maximize the portion of voting by optimizing the preference and access of the voters to enable them to cast their votes from internet access with no restriction on geographical location. The concept of remote internet voting is beautiful and offers significant benefits by taking the advantages of ICT in the electoral process provided security issues has to imply adequately pleaded during framework design and implementation.

CONCLUSION

In this paper, studied overview of various biometric techniques is presented. It also includes the comparative study of different biometric methods by advantages and disadvantages and implications of error rates. Based on the benefits and impact of error rates, it is concluded that fingerprint biometrics is the best choice for E-voting system.

REFERENCES

1. A.Fujioka et al. 1992 "A Practical Secret Voting Scheme for Large Scale Elections", Advances in Cryptology – AUSCRYPT.
2. Lorrie F. Cranor et al. 1997 "Sensus: A Security-Conscious Electronic Polling System for the Internet", in the proceedings of the Hawai International Conference on System Sciences, Wailea, Hawai, USA.
3. Ronald L. Rivest 2001, "Electronic Voting", Technical Report, Laboratory for Computer Science, Massachusetts Institute of Technology.
4. Salil Prabhakar, 2001, "Fingerprint classification and matching with filterbank", PhD Thesis, University of Michigan State.
5. George Chellin Chandran et.al, 2003, "Performance Analysis of Multimodal Biometric System Authentication",, VOL.9 No.3.
6. Robert Carrigan et.al 2005, "Automated fingerprint identification systems", Technical Report by Computer world honours case study.
7 .Hanady Hussien, Hussien Aboelnaga, "Design of secured E-voting-voting system." Electronic and Communication Department. AAST, Cairo, Egypt 2013 IEEE.
8. Steven J. Anderson et.al 2013," Robust Tri-Modal Automatic Speech Recognition for Consumer Applications." Vol. 59, No. 2.
9. Firas I. Hazzaa et.al ,"Web-Based Voting System Using Fingerprint Design and Implementation", ISSN: 2231-4946.