International Journal of Scientific and Technical Advancements
IJSTA
ISSN: 2454-1532

Developing a Cost Efficient Wireless Voting System

Parveen Sharma, Mayukh Banathia
Chandigarh Engineering College, Landrah, India

***Abstract*—** In the era of technology, where majority of decisions are based on voting mechanisms, a cost efficient wireless voting system thus becomes need of the hour. In the present day, voting mechanism used is highly unsecured, and moreover, the security is being compromised. The present electronic voting machine cannot determine the eligibility of a person thus giving entire control to the voting in-charge officer and thus leading to an expensive voting mechanism. One more risk with the present voting machine is that anybody can increase the vote count, since the count is present in the machine itself. With this objective the author proposes a framework to provide inexpensive solutions to the above, thereby introducing voting mechanism using biometric system i.e. finger print scanning etc. to authenticate the user and ensure no repeated voting and enhance the accuracy and speed of the process. The proposed system can be also be implemented in different institutions thereby giving the institution a provision of using wired/wireless networks and act as an edge over the present day voting systems.

I. INTRODUCTION

In democratic societies, voting is an important tool to collect and react people's opinions. Traditionally, voting is conducted in centralized or distributed places called voting booths. Voters go to voting booths and cast their votes under the supervision of authorized parties. The votes are then counted manually once the election has finished. With the rapid development of computer technology and cryptographic methods, electronic voting systems can be employed that replace the traditional ones and most importantly are error prone human component [1]. There is great demand for remote voting procedures that are easy, transparent, and, most importantly, secure. In this paper, we endeavour to improve mobility and address security problems of remote voting procedures and systems. We present an electronic voting scheme using biometric mechanism.

II. BIOMETRIC STUDY

The biometric is the study of physical or behavioural characteristics used for the identification of a person [2]. These characteristics of a person include the features like fingerprints, face, hand geometry, voice, and iris biometric features. These biometrics features can be used for authentication purpose in computer based security systems. A biometric system contains mainly an image capturing module, a feature extraction module and a pattern matching module as shown in Fig. 1.

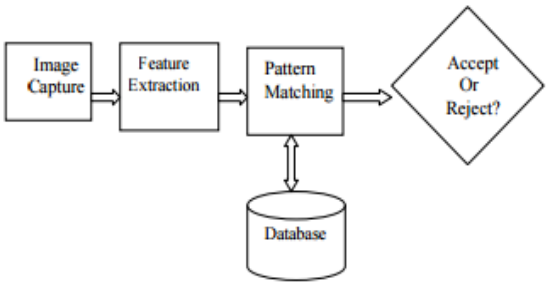

Fig. 1. Biometric System [3].

An image capturing module acquires the raw biometric data of a person using a sensor. Utilizing suitable algorithm/s feature extraction module improves the quality of the captured image. Database module stores the biometric template information of enrolled Persons. Pattern matching module compares the extracted features with the stored templates, which in-turn generates match score [4].

Thus biometric-based authentication method is most secure system. For many applications the system uses the password as well as biometrics for authentication. The biometric characteristics have been used in different applications. According to the requirement of the application suitable biometric can be selected. In this paper, we have concentrated on finger print biometrics to secure wireless voting system.

III. FINGERPRINT BIOMETRIC

Fingerprint is the oldest and easily available traits of biometrics, it shows an infallible means of personal identification. Accuracy is matched by use of fingerprint technique. It has been shown to be very high as compare to other existing biometric traits [5]. Unlike face and voice patterns, fingerprints are persistent with age and can't be easily changed. A fingerprint is defined by a set of ridge lines and they run parallel and sometimes terminates and sometimes intersects. The points are known as Minutiae where the ridge lines are terminated [6].

Fig. 2. Fingerprint image.

Fingerprint Identification Module: Fingerprint processing includes two parts: fingerprint enrolment and fingerprint matching (the matching can be 1:1 or 1:N).When enrolling, user needs to enter the finger two times. The system will process the two time finger images, generate a template of the finger based on processing results and store the template. When matching, user enters the finger through optical sensor and system will generate a template of the finger and compare it with templates of the finger library. For 1:1 matching,

Parveen Sharma and Mayukh Banathia, "Developing a cost efficient wireless voting system," *International Journal of Scientific and Technical Advancements*, Volume 2, Issue 4, pp. 133-134, 2016.

system will compare the live finger with specific template designated in the Module; for 1:N matching, or searching, system will search the whole finger library for the matching finger. In both circumstances, system will return the matching result, success or failure [7].

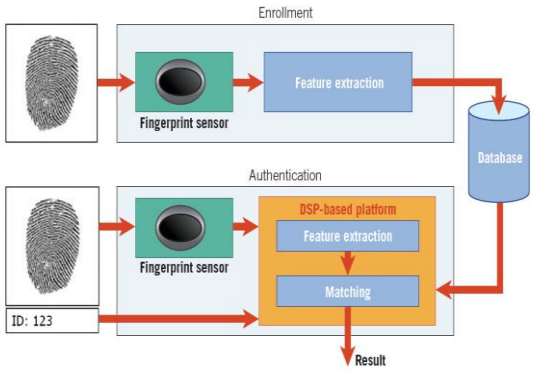

Fig. 3. Finger print process system.

IV. Proposed System

In the wireless e-voting machine, the votes being casted will be stored in another remote secured server. An electronic system will be used to enable the voter to vote and this vote will be transferred to the remote secured system by converting it into the radio waves. Unlike the previous systems, our system is capable of checking the legibility of the person who comes to voting initially through entering his unique identification number and in the later stages by using biometric system. Even if the machine gets damaged the count of voting will not be lost and we can vote from anywhere. The electronic device which converts the input digital signals to micro waves. Micro waves will then be transmitted routers connected to the server. These waves shall consist of UID routed to remoter server. The remote server will transmit Positive or negative acknowledgement to the client side, a positive acknowledgement shall be accompanied by a ballot paper. Micro waves containing the selected vote will then be transmitted back to remote server. Acknowledged vote shall finally be stored in the server.

V. Major Issues in the Implementation

1. Security: In the process of transmission, there may be problems like signals being trapped by an attacker. As the votes will be saved in the remote server, Attackers can crack the security levels of the database and can fiddle with the results of the voting, change the count of the votes polled. To avoid these type of problems, we can adopt secured and complex encryption algorithms at the sending side and the respective decryption algorithms at the receiving side. For this we shall be using an encryption algorithm, called UID algorithm.

2. Efficiency: In case more than one person casts his vote at the same time from various places, the efficiency can be maintained by reducing the data size. A compression algorithm can be used to overcome this problem. This will decrease the data transfer. Compression methods like jpeg, gif, png etc. may be used. We may also use distributed computing. Using distributed operating system with multiple servers is more effective than using single server.

VI. Conclusion

This project can be used for voting since it overcomes all the draw backs of ordinary voting machine and also provides additional security. Its main advantage is that since fingerprints of every person is unique and hence this system completely reduces the chance of invalid votes. The system can be manufactured simply as well as cheap and casting vote shall become easier by the process of voting from any place initially within the organisation.

References

[1] Mrs. S. M. Shinde, Mrs. Priti Subramanium, "Biometric GSM voting system," *International Journal of Technical Research and Applications*, volume 1, issue 4, pp.103-107, 2013

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

[3] R. Subban and D. P. Mankame, "A Study of Biometric Approach Using Fingerprint Recognition", *Lecture Notes on Software Engineering*, vol. 1, no. 2, May 2013.

[4] Y. J. Wang and K. N. Plataniotis, "An analysis of random projection for changeable and privacy-preserving biometric verification," *IEEE Transactions on Systems, MAN and Cybernetics PART B: CYBERNETICS*, vol. 40, no. 5, 2010.

[5] A. K. Jain, P. Flynn, and A. A. Ross; *Handbook of Biometrics*; Springer, Secaucus, NJ, USA, 2007.

[6] D. Maio and D. Maltoni, "A structural approach to fingerprint classification," *in 13th International Conference on Pattern Recognition*, 1996.

[7] S. Agrawal, P. Majhi, and V. Yadav, "Fingerprint Recognition Based Electronic Voting Machine," *National Conference on Synergetic Trends in engineering and Technology (STET-2014) International Journal of Engineering and Technical Research*, ISSN: 2321-0869, Special Issue.

Parveen Sharma and Mayukh Banathia, "Developing a cost efficient wireless voting system," *International Journal of Scientific and Technical Advancements*, Volume 2, Issue 4, pp. 133-134, 2016.