RFID AND FINGERPRINT BASED EVOTING

V.Imran
B.Tech, Department of CSE, Narayana Engineering College, Gudur.

N.Kesava Rao
Asso. Professor, Department of CSE, Narayana Engineering College, Gudur.

P.Dileep
B.Tech, Department of CSE, Narayana Engineering College, Gudur.

M.Praveen Kumar
B.Tech, Department of CSE, Narayana Engineering College, Gudur.

Abstract

Providing preventive measures is one of the challenging matters in the modern world, either it is a bank or institutions or home or real estates and the preventive measures are most important. Among the several field, providing the preventive measures for the system voting are the tedious and expensive one. In order to provide the inexpensive solutions to the above, the Fingerprint Based Electronic voting machine project is developed. This provides the security by means of fingerprints which is stored already in the data base. Then the fingerprint which is stored in the data base is checked. Only if both the persons and the voter's fingerprint are the same then the voting machine is enabled. This fingerprint matching is done with the help of sensors. This is done using a Microcontroller processor. The Microcontroller processes the signal and then enables the buzzer. Nowadays with the rise in population the need for checking the validity of the voters has become problem. With the microcontroller based fingerprint technique the task looks much simpler and also the accuracy is high. So this system provides cost effective as well as reliable security for the users. The main idea is to develop a microcontroller based application which can work as Intelligent Electronic Voting Machine. It has got two units, one for the control unit and the other is the ballet unit. It has a "RESULT" button that will be display the number of votes to respective candidate at the end of the poll. The ballet unit consists of various buttons, so that the user can elect any one of them and the next trail of same user is being avoided. At the end of polling system the recorded information stored in the control unit is displayed and sent to the computer. The control unit is completely designed by the micro controller and it has got flexibility to increase the number of members for taken part in election. This application must be used by any one and provides security with accurate result.

Keywords*--*RFID,RFID-TID, Fingerprint, cryptanalysis, Mutual Authentication.

I. INTRODUCTION

The right of people to vote for our government voice is at the sum of the commonwealth that each one will enjoy. Historically, great drive and care has been taken to make sure that election s are conducted during a fair behaviour specified the prospect who should win the election supported the vote count actually does. within the past changes to the election process have proceeded deliberately and judiciously, often entailing lengthy debates over even the second of particular . With the rapid extension of the online and also the validation of the data superhighway mesh, the promotion of an information oriented social club has demanded the looks of recent information inspection and repair that deserve attention. Voters needn't visit the canvass to vote and might vote at any place where they'll use the web. However, through Internet Ballot has these vantage, its safety must be guaranteed for practical use. The present organization meets the wants of electronic voting, it's the disadvantage of not having the ability to stop purchasing votes .Manual voting of the people could be a difficult one. so as to observe these fact automatically, this microcontroller based system is proposed to develop. This project uses image scanner, keyboard, liquid display so the RFID card, pin no: and ovule imprint is stored within the database. When the ballot or keeps his moulding within the scanner the system searches for the matches which is already Fed. If it matches, the PC shows the main points of elector's identity like pic, residential address etc. Then the PC sends the information which is connected serially to the microcontroller with one bleep doorbell sense experience and valid right to vote r is displayed, at the identical meter within the LCD "please enquiry your vote" message is additionally displayed. When voter press the button a

double beep sound is heard which indicates the vote is completed. After the vote is finished, the LCD displays a message stating, "Your vote is registered". If suppose an invalid voter or already voted person comes for voting crusader Booth and when his moulding impression is scanned, the PC sends never-ending beep sound to the controller and necessary steps are taken by the govt. Electronic ballot scheme s may offer advantages compared to other balloting techniques. An electronic voting organization will be involved in anyone of variety of measure within the apparatus, distributing, voting, collecting and counting of ballots, thus may or might not introduce advantages into any of those steps. Another important aspect to contemplate is to make sure that e-voting doesn't leash to the exclusion of certain groups, for instance the socially disadvantaged or mass with disabilities. Furthermore, it takes meter to develop a sturdy and secure system and also the necessary research and exploitation time must be allocated before any e-voting system is finally introduced. Online Election System could be a legal system by which any elector can use his/her voting rights from anywhere within the country, we offer a detail description of the functional and carrying into action characteristic of Online Election System.

SOCIAL ISSUES

Ultimately, the case for online voting does not depend on technical foul potential. Elections are political events and proposed changes must be evaluated on the basis of democratic and administrative criteria, including the levels of public access to the internet voting will become democratically acceptable only when most eligible voters have easy access to the internet, possibly via digital Goggle box.

II. RELATED WORKS

1. First Level of Security

To achieve security to the core, sometimes of losing the wag or letting out the peg issue to unauthorized person, the finger mark of the cardboard holder as drug exploiter 's is give n as input . The authorized exploiter should give his / her fingerprint at the time of adjustment. On every occasion the user uses the cardboard, they need to show their card and provides their pin numeral and fingerprint. Unless and until, this proves to be valid, they'll not be allowed for the subsequent process i.e. voting process of the user are visiting be blocked at this phase if fingerprint and number doesn't match with the audio recording within the backend information infrastructure. The fingerprint isn't stored in and of itself in database instead it's strongly encrypted. the primary fingerprint look-alike has been split into four look-alike s which many persona s are embedded on the primary split image which lands up in an exceedingly pseudo image[1]. This fake image is encrypted and stored in database. Hence, even when the hacker hacks the database and tries to induce the fingerprint, the hacker will end up with fake image, because the database contains the encrypted type of fake persona embedded on the primary image.

a.Original finger print

b. Fingerprint will be split into Four Parts

c. Fake fingerprintd. Fake images are embedded on the original image

FIG. 1 FINGER PRINT EMBEDDING

2. Second Level Of Security

Each RFID tag contains a singular identification, often called Tag Identification (TID). The reader is employed to question the tag's TID and forward it to the rear end database. Once the tag is found to be valid, the rear end database will research its voter's information for further processing. The cardboard holder is allowed to provide a PIN together with the exposure of RFID card [2]. The PIN could be a fourdigit number which can be stored as 16 bit value. The TID is additionally a 16bit value but it'll be in Manchester code format. These two values which are the user's input unique to every card holder is safely stored in database as encrypted form.The encryption performed could be a strong encryption scheme i.e. the primary 8 little bit of RFID TID is concatenated with first 8bit of PIN then an encryption scheme is applied to encrypt the concatenated bits, say X encryption scheme. Secondly the following 8 {bit of little bit of} RFID TID is concatenated with the following 8 bit of PIN then a distinct encryption scheme is performed say 'Y' to encrypt them.

16 bitManchestercode

----------First 8 bit----------	----------second 8 bit--------

RFID TID

----------First 8 bit----------	----------second 8 bit----------

16 bit value

PIN **NUMB**

Concatenated string 16 bit

-----First 8 bit of RFID TID------	-------First 8 bit of pin numb-----

COLUMN 1

("X" Encryption is performed)

Concatenated string 16 bit

--Second 8 bit of RFID TID------	-------Second 8 bit of pin numb-

COLUMN 2

(“Y” Encryption is performed)

FIG. 2 ENCRYPTION OF RFID-TID AND PIN

Thus the RFID TID and number are visiting be saved as two columns of encrypted string in database. By this, one are ready to do strong integrity of data and even it's safer from hackers. Even when the database is hacked, the hacker cannot hack neither the amount nor the RFID TID. It is also tedious to understand the encryption scheme and also the concatenated pin and TID[3].RFID (Radio Frequency Identification) is shown in figures 3&4 belongs the family of Automatic Identification and Data Capture (AIDC) technologies and it's fast and reliable means of identifying objects. There are two main components: The Interrogator (RFID Reader) which transmits and receives the signal and thus the Transponder (tag) that's attached to the thing. An RFID tag consists of a miniscule microchip and antenna. RFID tags is also passive or active and are available in wide selection of shapes and sizes. Communication between the RFID [3] Reader and tags occurs wirelessly and doesn't require a line of sight between the devices. An RFID Reader can read through most anythingwith the exceptionof conductive materials like water and metal. The RFID Reader emits a coffee power radiation field which is utilized to power up the tag so to die any information thatcontained on the chip. Passive tags are generally smaller, lighter and expensive than those who are active and should applied to things within the cruel environments, are maintenance free and may last for years.

FIG. 3 RFID READER-125Khz/LF

SPECIFICATION OF RFID

Dimensions (LXBXH) mm	30 x 30 x 10
Frequency	125 kHz
Reading Distance	>= 50 mm
Interface	UART, Wiegand26
Antenna	Built-in and External
Supply Voltage	+5 V
Operating temperature	−10°C to +50°C (-14°F to +122°F)
Tag Types	Unique, TK5530
Output Format	ASCII or Wiegand26
Housing	Plastic with 10x pin out
Color	Black

III. EXISTING SYSTEMS

The existing elections were done in traditional way, using ballot, ink and tallying the votes afterward, voting machines, etc., but this system prevents the election from being more accurate, consumes more time to publish the result.

Drawbacks In Existing System

Problems encounter the standard elections are as follows:

1. It requires human participation, in tallying the votes that produces the elections time consuming and at risk of human error.
2. The voter find the event boring resulting to atiny low number of voters.
3. Deceitful election mechanism.
4. Constant spending funds for the elections staff each year.
5. Voter ID, slips, required to poll the vote.
6. Voting is completed only within the concerned ballots.
7. Lack of evidence and fraud resistance (duplicate votes and forged modified votes) are supported. So, the proposed electronic legal system must be addressed these problems.

IV. SYSTEM DESIGN

The following diagram shows the general view of the voting terminal's architectural design:

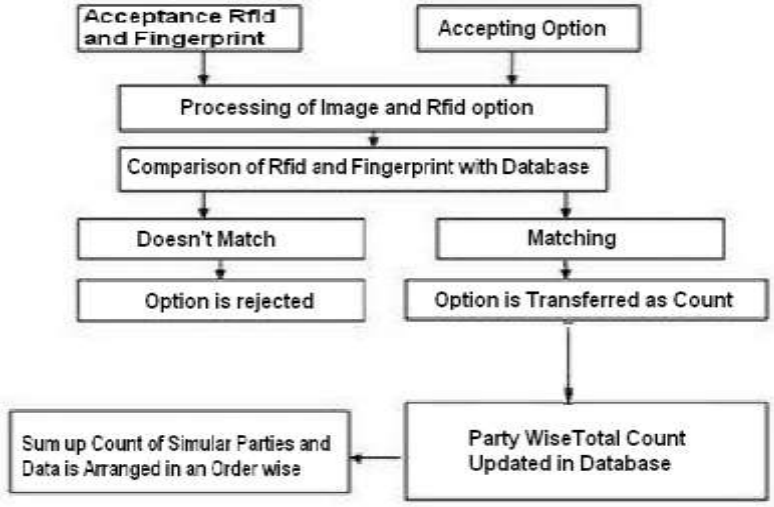

FIG. 4.1 INPUT AND OUTPUT DESIGN

When the voter involves poll, the RFID, finger print, and therefore the password are verified, then the processing of the RFID and finger print image are done by comparing with the database[5]. If it matches, the method is carried further, else rejected. During this paper, the issues of the present system are analyzed and thus suggested a way to stop buying vote and also looks at options for using new technologies in voting, that specialize in the pros and cons of internet voting and therefore the implications of such a radical change within the way that elections are conducted.

1. PROPOSED SYSTEM

These days, the explosive growth of internet use is accelerating the establishment of internet voting, which is more convenient and creates a higher turnout than the existing voting systems. Many internet electronic voting systems have been suggested, but they have the disadvantage of not having sufficient means of preventing attempts to doing fake votes and in terms of security. To overcome this disadvantage, a practical internet electronic voting system that provides two level of security is proposed. In the first level, the user's fingerprint along with username and password is given as input. If it is found to be valid, then the second level is reached. Now the user is expected to show the RFID card and must enter the pin number to perform voting. The user is allowed to vote only when the RFID Tag Identification (TID) and pin voter's id is found to be valid. In this phase, the voters, with along their personal data, and also provide the fingerprint[6]. The official in process, gives high associating RFID card and with biometric voter registration, for electronic voting later use. In the starting phase, which is based on a streamlined electoral process, candidates are set to choose, and the criteria by which biometric references to candidates will be split to stay in individual of the deployed electronic voting machines[4]. These references divided the database into fragments, encrypted, packed and signed electronically to be stored on USB storage devices that can have its own security system fingerprint and to add additional insurance to the operation of the transported data.

Merits:

COUNTERMEASURES:

A. Physical Layer Security

•The most crucial protection mechanism against relay attacks is to shield the voting station from electromagnetic radiation.

•Secure from jamming, zapping and selective denial of service attacks from being carried out from a distance.

B. Single-Write Ballots

•The voting station is to be including some sort of irreversible "commitment" or ballot cancellation process.

•RFID smartcard can be read and but not written to again.

IMPLEMENTATION WITH RESULTS

Implementation is that the stage of the project when the theoretical design is clothed into a working system. Thus it will be considered to be the foremost it's constraints on implementation, designing of methods to attain change over and evaluation of changeover methods. Implementation is that the process of converting a replacement system design into operation. It's the phase that focuses critical stage in achieving a successful new system and in giving the user, confidence that the new system will work and be effective. The implementation stage involves careful planning, investigation of the present system and on user training, site preparation and file conversion for installing a candidate system. The important factor that ought to be considered here is that the conversion mustn't disrupt the functioning of the organization

FIG. 1.0 a Home Page for E-Voting

FIG. 1.0 b Login Page for E-Voting

FIG. 1.2 c Login Page for Admin Details

		
FIG. 1.2 d Login Page for User Details	**FIG. 1.2 e The RFID already exists**	**FIG. 1.2 f The User details are successfully saved**

		
FIG. 1.2 g Shows the User Information	**FIG. 1.2 h Shows the Registration for a New Party**	**FIG. 1.2 h Shows the Registration for a New Party**
		
FIG. 1.2 j User Voting Login Page	**FIG. 1.2 k User Voter is added successfully**	**FIG. 1.2 l Shows the Page for Election Result**

CONCLUSION

In this paper a secure e-Vote organization supported biometric fingermark method is developed. With the implementation of this method one can get eliminate all the standard electoral system problems and that they will have an saint election unconscious process containing all properties of a system like accuracy, loving democracy, verifiability, gadget , flexibility, mobility and fixity. This can be a system during which might is in system's help instead of man being. Previously existing technical security flaws were also eliminated. This brings us one pace

closer to our target of creating electronic voting feasible at networked polling stations within the short terminus and using any terminals with none technical, legal or organization problems within the medium to future. Thus a model for electronic voting is presented wherein fingerprint is embedded as biometry for voter identification. The time to come back work will focus on implementation of fast and accurate fingerprint recognition and other related technical aspects within the system.

REFERENCES

[1]Bilal.Z., A.Masood, and F. Kausar. Security analysis of ultra-lightweight cryptographic protocol for low-cost RFID tags: Gossamer protocol. in Network-Based Information Systems, 2009. NBIS'09. International Conference on. 2009. IEEE.

[2]Wang, K.-H., et al., On the security of a new ultra-lightweight authentication protocol in IoT environment for RFID tags. The Journal of Supercomputing, 2018. 74(1): p. 65-70.

[3] Peris-Lopez, P., et al. M2AP: A minimalist mutual-authentication protocol for low-cost RFID tags. in International Conference on Ubiquitous Intelligence and Computing. 2006. Springer.

[4] K. Finkenzeller. RFID Handbook: Fundamentals and Applications in Contactless Smart Cards and Identification. John Wiley& Sons, 2003.

[5] Advances in Machine Learning Techniques for Penaeid Shrimp Disease Detection: A Survey.P.Venkateswara Rao,A.RamMohoan Reddy, V.Sucharita International Journal of Engineering and Applied Sciences (IJEAS) ISSN: 2394-3661, Volume-3, Issue-8, August 2016

[6]Voting System using UIDAI, International Conference on Electronics and Communication Systems.Sathya.G,Jeevanantham.C, Sangeetha.K, Venmathi.V, Ramya.P, "Bio Metric Authentication System Based On Aadhar Card (2017)",International Journal of Pure and Applied Mathematics (IJPAM),Volume 117, No. 9, pg. 7-11, DOI: 10.12732/ijpam.v117i9.2