Biometric and RFID Secured Centralised Voting System

Ankita Kadbe, Shweta Balgujar, Siddhita Chimote

Department of Computer Technology,
Yeshwantrao Chavan College of Engineering,
Nagpur, India.

Abstract **- Election and Voting is a routine part of our lives. In current voting system a person not in his constituency cannot vote. This paper removes this limitation by maintaining a centralized database of voters according to their consistency .A dynamic user interface provides list of candidates according to the constituency of voters. The voter can hence select candidate of his choice. The centralized database can also be updated online by having each polling station maintain their local database and update the centralized database after completion of election process. This paper also aims to provide RFID and biometric security. A RFID card will be provided to each voter. RFID card has a unique 12 byte code which can be read by RFID reader. A person can also use his fingerprint for unique identification. A five digit password will also be provided which again adds a level of security.**

Keywords **- Authentication, Biometric Recognition, Central database, hamming distance, RFID (radio frequency identification)**

I. Introduction

Radio-frequency identification (RFID) is an automatic identification method, relying on storing and remotely retrieving data using devices called RFID tags or transponders. A voter is provided with RFID card which has unique 12 byte code embedded in it. When the card is brought in the vicinity of RFID card reader, the reader detects 12 byte embedded code. A voter can also identify himself uniquely by fingerprint recognition process. A static central database containing details of voters according to their constituency is maintained. The database also maintains the candidates along with their constituency. At the time of login it is checked whether the voter is registered or not. The voter is allowed to proceed only if he is registered. After login a voting form appears before the voter. The voting form displays list of candidates according to the constituency of voter. The voter selects the candidate of his choice. The count of votes for that candidate is maintained. Once the user votes the application is exited so that the user cannot change his vote. After the voter has voted the Boolean status for that voter is marked true so that the same voter cannot vote for the second time. Only administrator has right to access the database. The administrator enters into database all the required information by various master forms created in application. At polling stations local database is maintained containing list of candidates and their vote counts. After the completion of election process centralized database is updated from every local database at polling stations.

A. RFID Systems

Only RFID reader and tag are of little use. The real power to RFID comes when they are used with backend. The backend stores the information about the product and also when the particular RFID tag was scanned. The backend consists of an application and a database. The RFID reader reads the unique RFID number from card and passes it to the backend. As stated in [3], the general RFID system has a following structure:

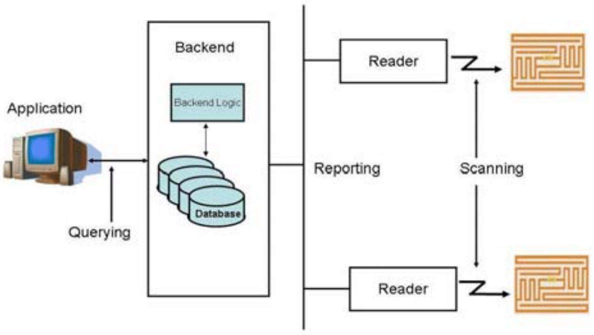


Fig1. A simple RFID system

B. Biometric Recognition

As stated in [21] biometrics (or biometric authentication) refers to the identification of humans by their characteristics or traits. Biometrics is used in computer science as a form of identification and access control. The system performs a one-to-one comparison of a captured biometric with a specific template stored in a biometric database in order to verify the individual is the person they claim to be. As stated in [22] fingerprint identification is well known because of uniqueness and consistency. In the application we are using hamming distance algorithm.

II. Previous work

A. The Israeli e-Voting Scheme

Reference [20] shows this voting scheme aims to save paper and manpower, makes forgery difficult and makes counting process transparent. To cast their votes, the voters use a computer terminal to write their choice into a contactless smartcard, and then physically deposit this smartcard into a ballot box. The voting committee "manually" counts the votes. This probably means they take the S-cards and feed them into another counting machine C. Machine A electronically counts the votes chosen there. The results are compared.

1) Problems with Israeli System: As stated in [20] following problems exist with Israeli system:

1. The dependency on machines becomes even more acute One depends on software and also on smart cards .Smart cards were designed to protect their content from outsiders, checking what is on a smart card is even harder.

2. Smart cards make forgery for an insider much easier and hard to detect.

3. In case of a mismatch there is no way to determine whether forgery took place.

Also in recent years, electronic voting systems have largely replaced traditional hand-counted paper ballots in most states and counties. These systems can be divided into two large categories:

B. Computer-counted

Mark-sense and punch card systems still rely on a paper ballot. The voter either physically modifies the ballot or marks specific regions with a machine readable carbon-based ink. Ballots are collected as normal and then tallies are computed using a computer to read the ballots.

C. DREs

Instead of marking a printed sheet, voters are presented a computer monitor displaying the ballot choices. They make their selection using either a touch-screen interface or with simple buttons. The vote is recorded on the machine's internal storage and then transferred to a central repository for tabulation.

None of the above systems are useful when the voter is not present in constituency leading to precious vote loss. Our paper overcomes this limitation by maintaining a central database and a dynamic user interface. A voter can not only vote from outside his constituency but also from any polling station in his constituency. This avoids a chaos at polling station. Bulk manufacturing of rfid's is far cheaper than smart cards. This makes the application cost effective.

III. METHODOLOGY

The Project mainly consists of four modules:

A. The Input Module

The input module consists of the devices that are used to accept user input. The RFID reader module reads RFID cards, as soon as they are brought in its proximity. As such, the user only needs to bring his RFID based Voter Id card close to the RFID reader, and the system will detect and read the RFID tag's unique 12 byte ID. The detected ID is then sent to the Authentication Module for Authentication. Also voter can use his fingerprint for authentication. Hamming distance algorithm is used for biometric recognition. The algorithm implementation is still in progress.

B. Authentication Module

The Authentication Module authenticates the user, in two phases viz.

1) RFID Voter Card or biometric authentication phase: The system connects to the central database, and checks whether the RFID ID code or fingerprint is registered, i.e. whether the user is a registered voter or not. If the user is not a registered voter, the system allows no further processing. If the user is validated, i.e. found to be a registered user, then phase 2 commences.

2) Secret Pin Authentication Phase: In this phase of authentication, the user is requested to input his secret PIN, which is a 5 digit numerical pin only known to the voter. Once the user inputs the pin, it is validated against the PIN stored in the central database. Once the user successfully clears the authentication phase, the voting module takes over.

C. Vote Registration Module

The Voting Module displays the user the list of various candidates in his constituency. The user can then select the candidate he wishes to vote for. A confirmation is asked for once the user selects a candidate. If the user does not select a candidate within the stipulated time period, a timeout occurs and current voting session terminates. Once the vote is casted, the vote count for the particular candidate is updated i.e. incremented in the Central Database. Also, the Central Database is updated to mark the selected user as 'voted', so as to maintain the record that he has casted a vote. However, the voted candidate information is not recorded.

*D. Central Databas*e

The Central Database is a combination of a server system and multiple databases and which are connected on a network with the various Polling stations .The central database contains:

a) The Database of Registered voters and their constituency and voted status.

b) The Database of all constituencies and Election Candidates and the database of Vote Count for Each Candidate.

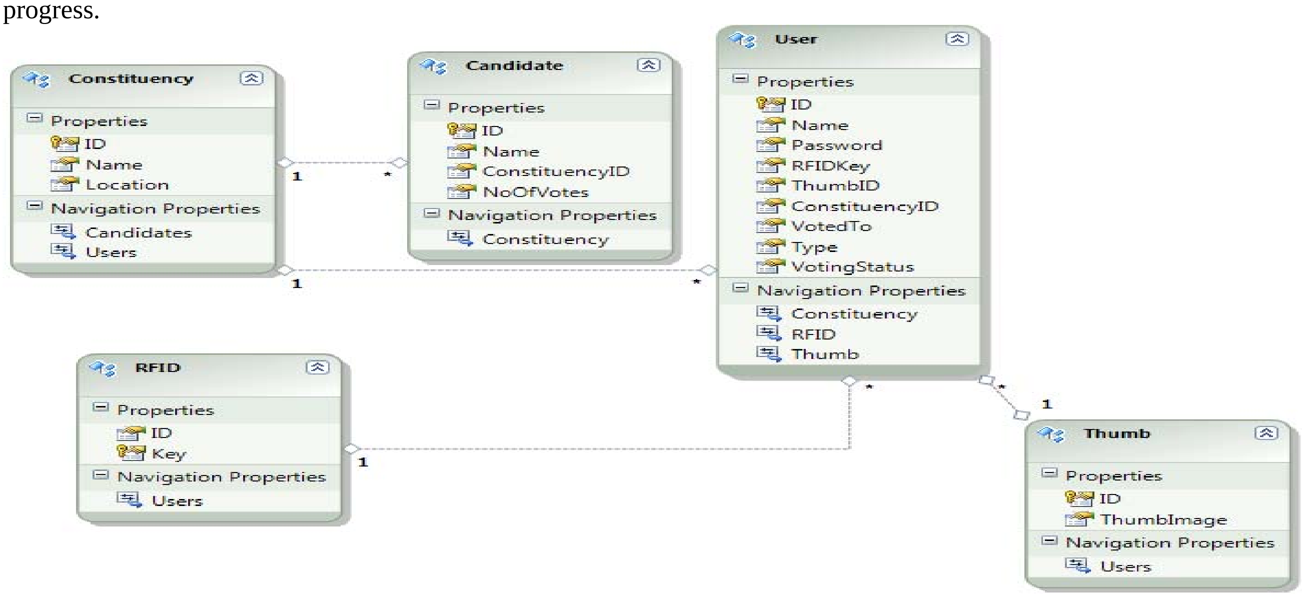


Fig2. Class diagram for biometric and rfid secured centralized voting system

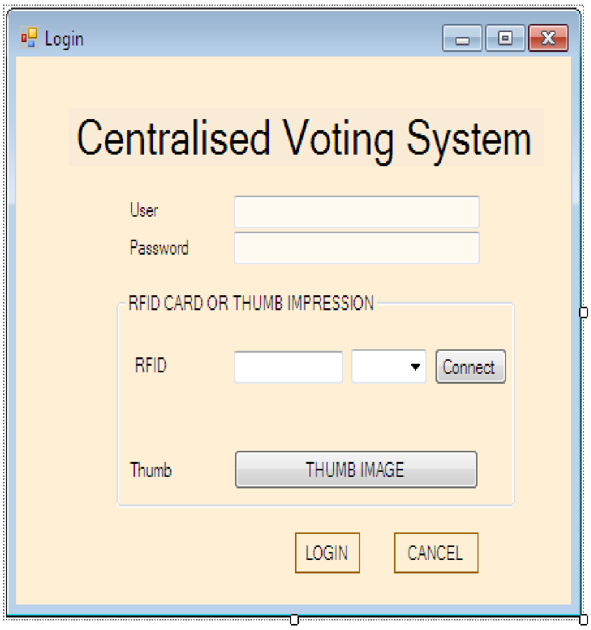


Fig3. Login form

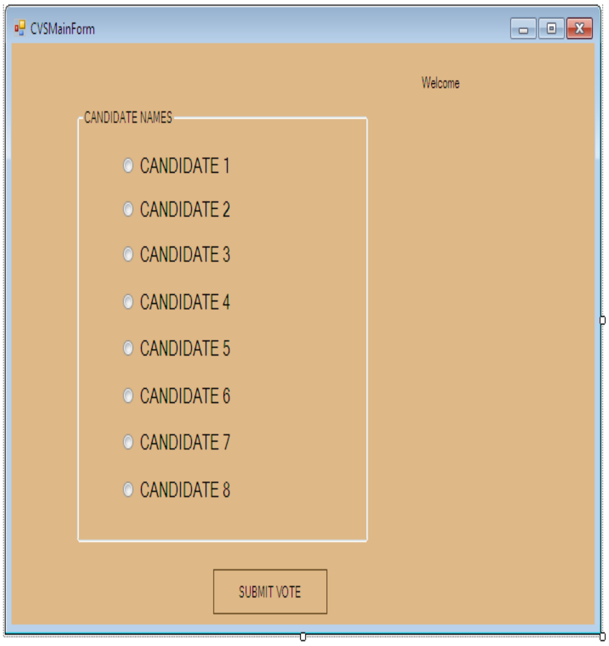
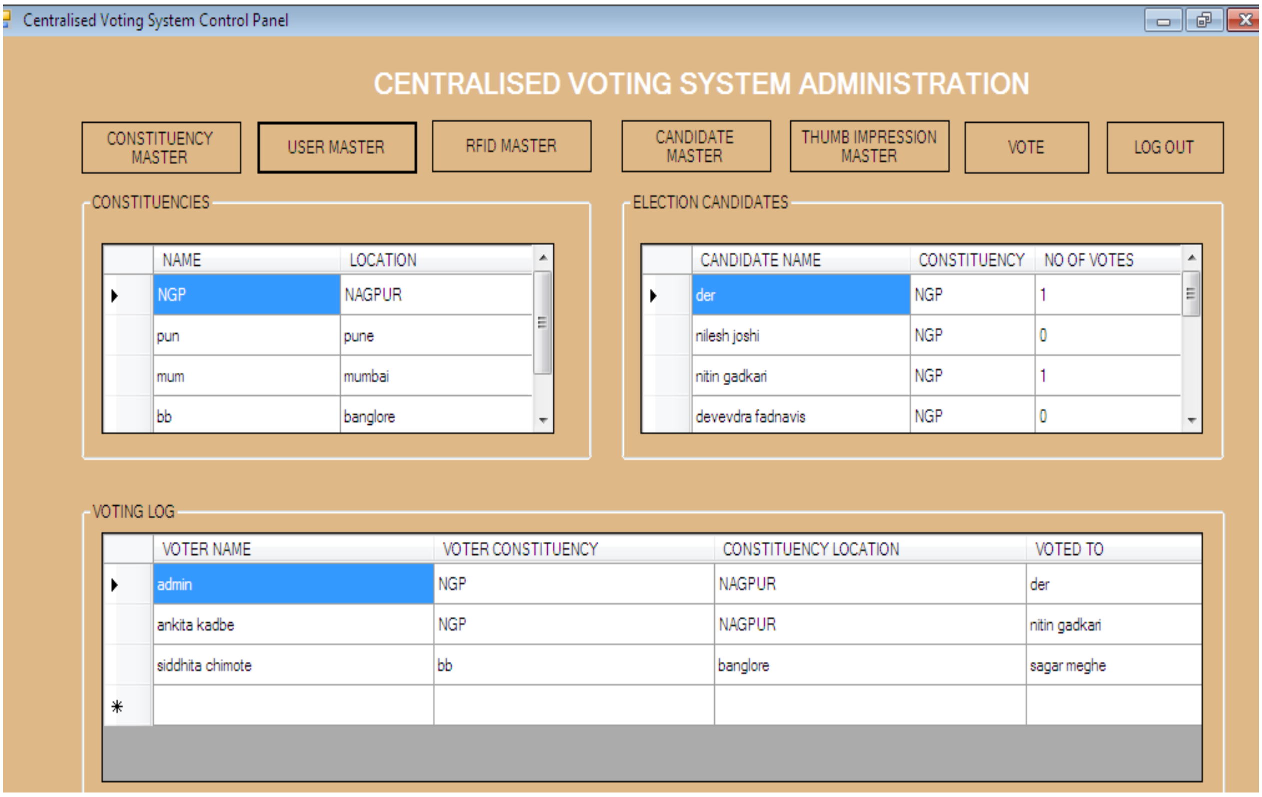


Fig4. Voting form



CONSTITUENCIES

NAME	LOCATION
NGP	NAGPUR
pun	pune
mum	mumbai
bb	banglore

ELECTION CANDIDATES

CANDIDATE NAME	CONSTITUENCY	NO OF VOTES
der	NGP	1
nilesh joshi	NGP	0
nitin gadkari	NGP	1
devevdra fadnavis	NGP	0

VOTING LOG

VOTER NAME	VOTER CONSTITUENCY	CONSTITUENCY LOCATION	VOTED TO
admin	NGP	NAGPUR	der
ankita kadbe	NGP	NAGPUR	nitin gadkari
siddhita chimote	bb	banglore	sagar meghe

Fig 5. main screen screenshot

IV. Conclusion

The designers of the voting system chose rfid for cost and reliability reason. Central database in the proposed system guarantees that a voter can vote for his constituency candidates from any place in the country. This prevents loss of valuable vote and reduces chaos at polling centers. Biometric recognition further improves security of the system.

References

[1] CCC-TV lightning talk's day 1. Online, 2005.

[2] Common Criteria Recognition Agreement. Common criteria for information technology security evaluation part 2: Security functional components. Online, July 2009.

[3] Christoph Jechlitchek. A survey paper on radio frequency identification and trends.

[4] B.Dolev .Laying the groundwork for electronic elections in Israel. Invited Talk, CPIIS IDC/TAU Workshop on Electronic Voting, May 2009.

[5] S. Drimer and S. J. Murdoch. Keep your enemies close: distance bounding against smartcard relay attacks. In *Proceedings of 16th USENIX Security Symposium*, pages 1–16, Boston, MA, 2007. USENIX Association.

[6] EMVCo contactless communication protocol specification V2.0.1 Online, July 2009.

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

[8] Government of Israel, Ministry of the Interior. Public tender 16-2008 for the establishment and operation of a computerized election system. Online, August 2008.

[9] Government of Israel, Prime Minister's Office. Decisions of the ministerial committee on legislation. Online, August 2009.

[10] G. Hancke. A Practical Relay Attack on ISO 14443 Proximity Cards. Manuscript, February 2005.

[11] G.Hancke, K. Mayes, and K. Markantonakis. Confidence in smart token proximity: Relay attacks revisited. *Computers Security*, In Press, Accepted Manuscript:–, 2009.

[12] G. P. Hancke. Practical attacks on proximity identification Systems (short paper). In *SP '06: Proceedings of the 2006 IEEE Symposium on Security and Privacy*, pages 328–333, Oakland, CA, 2006. IEEE Computer Society.

[13] M. Hutter, J.-M. Schmidt, and T. Plos. Rfid and its vulnerability to faults. In *CHES '08: Proceeding sof the 10th international workshop on Cryptographic Hardware and Embedded Systems*, pages 363–379, Berlin, Heidelberg, 2008. Springer-Verlag.

[14] International Organization for Standardization, Geneva. *ISO/IEC 14443-2 Identification cards – Contactless integrated Circuit cards – Proximity cards – Part 2: Radio frequency Power and signal interface*, 2001.

[15] A. Juels, R. L. Rivest, and M. Szydlo. The blocker tag: selective blocking of rfid tags for consumer privacy. In *CCS '03: Proceedings of the 10th ACM conference on Computer and communications security*, pages 103–111. ACM Press, 2003.

[16] Z. Kfir and A. Wool. Picking virtual pockets using relay attacks on contactless smartcards. In *International Conference on Security and Privacy for Emerging Areas in Communications Networks*, pages 47–58, Los Alamitos, CA, USA, 2005. IEEE Computer Society.

[17] I. Kirschenbaum and A. Wool. How to build a low-cost, extended-range RFID skimmer. In *Proceedings of the 15th USENIX Security Symposium*, Vancouver, B.C., Canada, 2006. USENIX Association.

[18] T. "Minime" and C. "Mahajivana". RFID zapper. 22nd Chaos Communication Congress, December 2005.

[19] N3ldan. Cheap/free capacitor bank and charger. Online,October 2006.

[20] Yossef Oren and Avishai Wool. RFID based electronic voting: what could possibly go wrong?

[21] Maheswari M A.P, Ancy S Eben Praisy and Devanesam. Biometric identification system for fusion of iris and fingerprint.

[21] Chris Roberts Biometric Technologies- fingerprint**.**