International Journal of Smart Sensor and Adhoc Network

Volume 2 | Issue 1 Article 13

October 2012

Mobile Voting using Global System for Mobile Communication (GSM) Technology and Authentication using Fingerprinting Biometrics and Wireless Networks

Sneha Pallav
Department Of Information Technology, Sri Sairam Engineering College, Chennai, India,
snehapallav@gmail.com

S. Dhanalakshmi
Department Of Information Technology, Sri Sairam Engineering College, Chennai, India,
dhanalakshmy2010@gmail.com

S. Aiswarya
Department Of Information Technology, Sri Sairam Engineering College, Chennai, India,
aiswaryabhumi@gmail.com

Mobile Voting using Global System for Mobile Communication (GSM) Technology and Authentication using Fingerprinting Biometrics and Wireless Networks

Sneha Pallav, S. Dhanalakshmi & S. Aiswarya

Department Of Information Technology, Sri Sairam Engineering College, Chennai, India
E-mail : snehapallav@gmail.com, dhanalakshmy2010@gmail.com, aiswaryabhumi@gmail.com

Abstract **-** India is world's largest democracy. Fundamental right to vote or simply voting in elections forms the basis of Indian democracy. In India all earlier elections a voter used to cast his vote by using ballot paper. This is a long, time-consuming process and very much prone to errors. This situation continued till election scene was completely changed by electronic voting machine. No more ballot paper, ballot boxes, stamping, etc. all this condensed into a simple box called ballot unit of the electronic voting machine. Cell phone based voting machine is capable of saving considerable printing stationery and transport of large volumes of electoral material. It is easy to transport, store, and maintain. It completely rules out the chance of invalid votes. Its use results in reduction of polling time, resulting in fewer problems in electoral preparations, law and order, candidates' expenditure, etc. and easy and accurate counting without any mischief at the counting centre.

Mobile technology has attained heights and the market trend is such that every citizen of India possesses a mobile handset at cheaper rates of services. Even NRIs who long to cast votes can avail this advanced technology without taking the pain of coming to Polling-booth with the help of their handy Mobile Equipment (ME). When such a Personal Digital Assistant (PDA) is available, why not using it for time-saving, cost- effective and secured method of voting??? The proposed paper is a collaboration of Computer Networking with biometrics. In this paper, an electronic voting scheme using GSM based Mobile technology is presented. By integrating an electronic voting scheme with the Mobile infrastructure, we are able to exploit existing Secure Mobile authentication mechanisms and provide enhanced voter authentication using Fingerprinting Technology (Biometrics) and mobility while maintaining voter privacy.

Keywords **-** *Mobile Equipment (ME); Personal Digital assistant (PDAs); Global system for Mobile communication (GSM); Fingerprinting Technology; voter privacy.*

I. INTRODUCTION

Elections in India are events involving political mobilization and organizational complexity on an amazing scale. In the 1996 election to Lok Sabha there were 1,269 candidates from 38 officially recognized national and state parties seeking election, 1,048 candidates from registered parties, not recognized and 10,635 independent candidates. A total number of 59, 25,72,288 people voted. The Election Commission employed almost 40, 00,000 people to run the election. A vast number if civilian police and security forces were deployed to ensure that the elections were carried out peacefully. The direct cost of organizing the election amounted to approximately Rs. 5,180 million. Since this was the case a decade and a half back, imagine the cost of organizing the elections at present? Lavish isn't it? [1]

Since, Voting is a vital part of the democratic process. As such, the efficiency, reliability, and security of the technologies involved are critical. Traditional voting technologies include hand-counted paper ballots. These paper-based systems can result in a number of problems, including:

- Unacceptable percentages of lost, stolen, or miscounted ballots
- Votes lost through unclear or invalid ballot marks
- Limited accommodations for people with disabilities

Today, the development and widespread use of information technologies is changing the way people view practical life situations , be it voting their preferred electoral candidates. This paper seeks to be panacea for issues affecting the genuinity of present

voting system by developing an assistive Technology of Mobile -voting systems which offers multiple advantages over traditional paper-based voting systems.

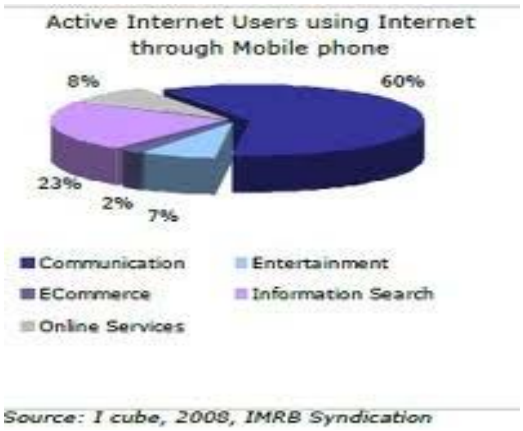

Fig. 1: use of internet through Mobiles phones [7]

II. RELATED WORKS

Voting machines are the total combination of mechanical, electromechanical, or electronic equipment (including software, firmware, and documentation required to program control, and support equipment), that is used to define ballots; to cast and count votes; to report or display election results; and to maintain and produce any audit trail information. The first voting machines were mechanical but it is increasingly more common to use electronic voting machines.

A voting system includes the practices and associated documentation used to identify system components and versions of such components; to test the system during its development and maintenance; to maintain records of system errors or defects; to determine specific changes made after initial certification; and to make available any materials to the voter (such as notices, instructions, forms, or paper ballots).

Traditionally, a voting machine has been defined by the mechanism the system uses to cast votes and further categorized by the location where the system tabulates the votes.

Voting machines have different levels of usability, security, efficiency and accuracy. Certain systems may be more or less accessible to all voters, or not accessible to those voters with certain types of disabilities. They can also have an effect on the public's ability to oversee election.

Vote recording technologies since early days include the following, viz..

- Document-based Ballot Voting Systems
- Manually-marked and Tabulated Paper Ballots
- Punched Card
- Optical Scan (Mark sense)
- Using Electronic Input Device

Fig. 2: Documented based Ballot voting machine.

The Votomatic vote recorder, a punched card voting machine originally developed in the mid of 1960s

Fig. 3. Punched Card

lever style voting machine on display at the National Museum of American History.

Electronic Voting Machines ("EVM") are being used in Indian General and State Elections to implement electronic voting in part from 1999 elections and in total since 2002 elections. The EVMs reduce the time in both casting a vote and declaring the results compared to the old paper ballot system.

Fig. 4. Electronic Voting Machine

III. PROPOSED ASSITIVE TECHNOLOGY

Use of the GSM security features, in particular the authentication The proposed system suggests the function along with fingerprint biometric scanner technology inbuilt in mobile phones, which will be customized in a cost-effective way, thus providing a more viable option compared to existing systems. It possesses the ability for the voters to cast vote even if they are not present in the polling booth, with high identification and secured measures, a unique feature of our concept.

A. Security Features in GSM

GSM is a digital wireless network standard widely used in European and Asian countries. It provides a common set of compatible services and capabilities to all GSM mobile users. The services and security features to subscribers are subscriber identity confidentiality, subscriber identity authentication, user data confidentiality on physical connections, connectionless user data confidentiality and signaling information element confidentiality. They are summarized as follows:

- Subscriber identity confidentiality is the property that the subscriber's real identity remains secret by protecting his International Mobile Subscriber Identity(IMSI), which is an internal subscriber identity used only by the network, and using only temporary identities for visited networks.
- Subscriber identity authentication is the property that ensures that the mobile subscriber who is accessing the network or using the service is the one claimed. This feature is to protect the network against unauthorized use.
- Data confidentiality is the property that the user information and signaling data is not disclosed to unauthorized individuals, entities or processes. This feature is to ensure the privacy of the user information.[5]

In our proposed GSM mobile voting scheme, communication between the mobile equipment and the GSM network uses standard GSM technology. Hence GSM security features apply. Among which, the subscriber identity authentication feature is particularly used in the protocol.

B. Basic Mobile Voting Scheme

In a mobile environment, the mobile device has limited computational abilities, so employing schemes with large computation is not practical. Therefore, we develop our mobile voting scheme based on a Fingerprint Technology. Every citizen above 18 years has the right to vote and hence obtaining their fingerprints and storing it in their Database along with their birth /death record becomes necessary. Once the user is connected to the service provider's GSM network, he can enter his password. The provider asks for security confirmation and the user sends his/her fingerprint (secured print in encrypted form and sent as sequence of data in encoded form)to the service provider. Service provider (GSM Network) verifies the fingerprint and checks for the validity of voting and sends a voter list (a mobile ballot paper)through SMS. User casts his/her vote and sends a message. Since mobile phones has connectivity with computer systems, it is easy to store and access at the service provider and results be published instantly. If an invalid password/choice , an error message will be given. We use a non-volatile memory for storing all data.EEPROM will preserve all information, in case of power failure.

IV. COMPONENTS USED IN THE PROPOSED WORK

A. Mobile Equipment/Voting Device (ME)

In electronic voting schemes, voters need to use dedicated voting devices to cast their votes electronically, for instance, Internet connected computers or DRE machines. In our scheme, the voting device corresponds to the GSM mobile equipment (ME), which consists of a GSM SIM card for connecting to the service provider (GSM Network) with an inbuilt Fingerprinting biometric scanner.

Our system is based on the following assumptions. We assume that the proposed Mobile Voting scheme is part of a voting system, and that voters can choose to vote through different methods, for example, the voting booth. If voters want to vote through Mobile, they have to be registered subscribers. This means that the voters have already registered their real names , addresses and their Fingerprint with their mobile operators by presenting their eligible credentials at the time of subscription. We assume that the Mobile operator is trusted to authenticate the mobile users for the purpose of voting and send the correct information to VS and CS. [3]

B. Authentication Center (AC)

AC is an entity within the GSM network. AC generates the authentication parameters and authenticates the mobile equipment.

C. Verification Server (VS)

VS belong to the voting authority, who organizes the voting event. It verifies the legitimacy of the voter and issues a voting token to the voter.

D. Collecting and Counting Server (CS)

CS is the server that collects and counts the votes to give the final result. CS's action need to be audited by all candidate parties.

E. Fingerprint Sensor

The FingerLoc sensor is a monolithic silicon chip comprising a sensing array and its associated circuitry, all covered by fairly thick (75 micrometer) proprietary coating. It can easily be embedded on the surface of the cell phone, where the robust coating will prevent it from the rigors of normal usage. Fingerloc key allows the advantage over other (optical) fingerprint sensors, is that it ignores the external fingerprint in a buried layer of living cells, where fingerprints are created, and where they are found in pristine condition. What it does is apply a low-voltage ac signal to the fingertip and then measure how the resulting electric field varies in amplitude over the fingertip surface. The signal is applied by means of a conductive epoxy ring surrounding the sensor area. It is defined and measured with respect to a reference plane within the chip. The electric field is set up between the reference plane and a thin layer of highly conductive saline liquid that resides at the interface of the living skin tissue and the dead skin. The saline layer has same shape as the living tissue- the shape of the fingerprint. Being highly conductive, it imposes its shape as a boundary condition on the field, thereby spatially modulating the field into an analog of the fingerprint. In the cell phone, a module from a special software suite analyzes the fingerprint pattern and extracts information from it, which it converts into a unique representation of the fingerprint owner's. To register a voter, that representation, called a template, is stored in nonvolatile memory and in storage of Service Provider for instance GSM Networks and VSNL for future use.[4]

What happens next depends on how the cell phone manufacturer and service provider have set things up. If the handset does not recognize the applicant, service will be denied. It gets more interesting when the system does recognize the fingerprint, because each user can have a stored profile, which personalizes the phone for him or her. The above explanation for FingerLoc sensor is being depicted in the next page diagram.

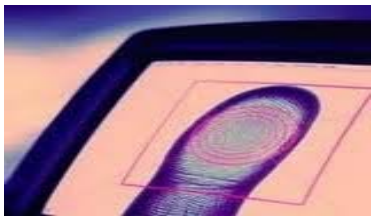

Fig. 5: Scanning Fingeprint

Fig. 6 : FingerLoc Sensor

F. Making of a FingerLoc Sensor

1. Saline Layer
2. Damaged external Fingerprint
3. Pixel sensor plate array
4. Excitation signal reference plane
5. Sense amplifier
6. Digital Circuitry
7. Analog Circuitry
8. Excitation generator
9. To conductive epoxy ring

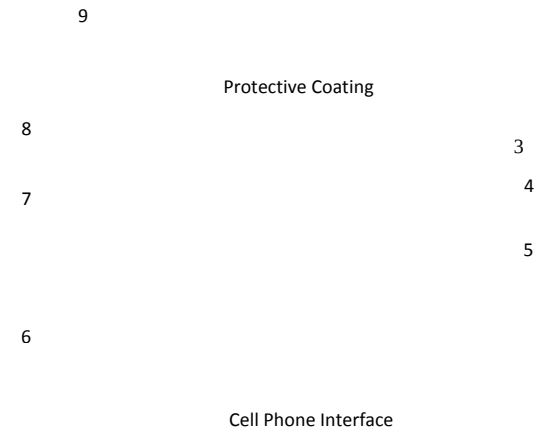

Fig. 7 : FingerLoc Sensor

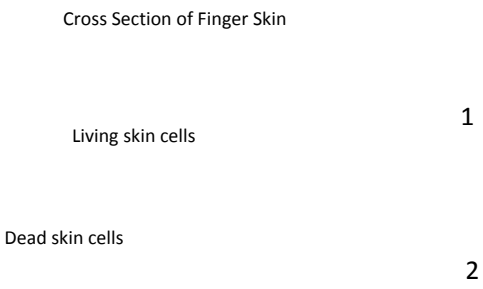

Fig. 8: Working Of Biometric Scanner

V. WORKING

Figure 9: A Mobile Equipment with GSM Sim Card and fingerprint Scanner.

Fig. 10: Connecting to the server

Fig. 11: Verification of Fingerprinting

Fig. 12: Access Denied if Not Valid

STEP 1:Start

STEP 2: Connect user to the server (GSM network to government service provider)

(Voter's Authentication Phase)

STEP 3: Get the password from the user.

STEP 4: Check for password's validity.

STEP 5: If authentic, he/she will be allowed to participate in the next steps of voting. This phase is default phase and it works automatically once user try to use the services of particular GSM service provider.

STEP 6: Send the voter's Fingerprint to AC.

STEP7: AC Compares the scanned fingerprint and the ID details from the Database.

(Voting Phase)

STEP 8: If Authenticated, the voter installs the application, fills in the ballot, and obtains a voting token from VS without revealing the vote.

STEP 9: The voter fills in the ballot, encrypts the ballot, and sends it to AC through Mobile.

STEP 10: AC authenticates the encrypted ballot and forwards the encrypted ballot Along with the verification (signature) to VS.

STEP 11: VS checks the authentication of AC and the eligibility of the voter, signs the encrypted ballot with its private key. Here VS generates one ID for this ballot with one asymmetric key. VS encrypt the ballot, ballot ID and public key of generated asymmetric key which is generated for this particular ballot and sends the verified encrypted ballot with added attributes back to the voter. VS also send the pair of ballot ID with the encrypted private key (using CS public key) to CS .

STEP 12: The voter checks the Fingerprint and retrieves (unblind) the VS- signed ballot, ballot ID and Public key from the message using the retrieving (unblinding) technique of the Fingerprinting scheme.

STEP 13: The voter sends the voting token along with ballot ID and the public key correspond to This particular ballot ID to AC, these four items ballot, ballot ID and Public key and fingerprint will be

Encrypted with CS's public key to avoid AC decrypting the ballot and compromising the privacy of the voter.

STEP14: Upon receiving the encrypted key and the voting token, CS keeps its safe till counting start as per the predefined schedule.

(Counting Phase)

STEP15: At the scheduled time of counting CS decrypt the ballot and checks whether the voting token is valid or not. If it is valid it will be counted else it will be rejected.

STEP16: Vote Casted Successfully

STEP 17: Thus, the vote is casted successfully

Algorithm 1: User-Friendly concept Casting a vote.

VI. ACKNOWLEGMENT

The instinsic purpose of any technology is to advance the quality of living. The main highlight of proposed technology is that it is the Most-secured voting ever and the time consumption is less. Cost-effective since there is no need of dedicated voting machine and the most important of all, be anywhere in the world, even if you are physically disabled you will still be able to participate in the voting process of your native country.

REFERENCES

[1] Elections in India http://en.wikipedia.org/ wiki/Elections_in_India.

[2] History of voting system –Google Search

[3] How does a GSM Technology Work? http://en.wikipedia.org/wiki/GSM

[4] FingerLoc Sensor -Google and other images

[5] J. D. Cohen and M. J. Fisher, "A robust and verifiable cryptographically secure election system," In Proc. 26th IEEE Symp. On Foundations of Comp. Science, pp 372-382, Portland, 1985.

[6] C. S. Park, K. Itoh, and K. Kurosawa, "Efficient anonymous channel and all/nothing election scheme," EROCRYPT 93, pp 248-259, Springer-Verlag, Lecture Notes in Computer Science No. 765, 1994.

[7] Wikipedia, "Pie charts for the usage of mobile phones in India".

[8] Suski, W.C., Temple, M.A., Mendenhall, M.J., Mills, R.F. "Using Spectral Fingerprints to Improve Wireless Network Security".

[9] Rajaveerappa, D.; Almarimi, A,"RSA/Shift Secured IFFT/FFT Based OFDM Wireless System".

[10] Shan Ao; Weiyin Ren; Shoulian Tang;"Analysis and Reflection on the Security of Biometrics System"'

❑❑❑