The next generation voting system - flexible, scalable and adaptable

Kavita Vemuri* & Class of Product Development(spring 2009)
. * Senior Research Scientist, International institute of Information Technology,
Hyderabad Andhra Pradesh, India
kvemuri@iiit.ac.in

Author: In the US worked in companies like Rational (now IBM), Comverse Networks Systems, Galactic Industries (now ThermoGalactic) and at the Corporate Materials Research labs of 3M, Austin, Texas. In India was heading the Technology Development Center (TNTDPC) of CII at Chennai/Tamil Nadu and currently heading the Center for Innovation & Entrepreneurship at IIIT-H and also teaches product development.

Fiber optic devices, control systems, telecom voice messaging applications and new product development have been areas of work/experience.
Co-inventor of 2 US patents in ‘dispersion compensation’ in fiber optic communication networks.

Education: MSc/MPhil (HCU) – Physics, MS ECE from UMASS

Co-authors: Product Development Class of Spring 2009
The students of the class worked on the idea as their final semester project, designing some of the architectures and also spent a lot of time understand the Indian voters. Many of them even volunteered at polling booths. Their enthusiasm and bright thoughts have made this paper possible. They are the implementers and future ME-Voters.

The next generation voting system - flexible, scalable and adaptable

Kavita Vemuri* & Class of Product Development(spring 2009)
. * Senior Research Scientist, International institute of Information Technology,
Hyderabad Andhra Pradesh, India
kvemuri@iiit.ac.in

Abstract:
We are proposing an integrated architecture that can augment the existing Electronic Voting machines and also introduce other electronic voting systems. The integrated product is designed to enable voting from any system that can support text messages like: mobile phones, internet /web and also bank ATM's. Voting systems require the following fundamental features: verification of the voter, security of the ballot, faster counting, tamper free systems and finally ability to scale up in terms of data and network expansion, which will be technically very strong at the backend but with a user friendly front end. Algorithms for data routing, text parsing, robust databases, integrations with telecom service providers, Indian languages & speech recognition tools can also be incorporated into the product if required.

The design process has taken into account the need to deploy e- voting system in phases – covering urban people who are technology-savvy, migrant voters – that is people who are registered to vote in one constituency but have temporarily moved to another state or area.

The goal is to 'make a system that gives a citizen no excuse for not voting'

Key words: Voting system, SMS routers, mobile phones, internet, distributed databases ,local area networks or ATMs.

1 Introduction

The greatest democratic exercise in India is the elections, a vital expression of people's power to shape the future of the country. The election machinery gears up to enable a free and fair election, give the right to vote without interference or intimidation and an assurance that every vote counts. Though there is a perception of chaos & complexity, the Indian elections are by and large peaceful considering the magnitude of the exercise. Major credit for fewer instances of booth capturing and intimidation goes to the election commission office and also to the alert media. In the past few years, active citizen groups have contributed immensely in terms of information diffusion and call for more participation in the electoral process. With adequate and streamlined processes in place, it is still a challenge getting people to exercise their fundamental duty – to be part of the process and this is reflected in the voter turnout percentages across the democratic countries.

The proposed concept is to enable a voter who wants to vote and is away from a polling station or constituency, or wants to vote from place of work or home (for the elderly).

There is a lot of debate in city dwellers on the importance of their vote as their problems are solved not by the state or central governments but by economy and market forces. This argument is a flawed as the educated or informed population can make the right choice for leaders who can help the less-fortunate, a vote is necessary not for oneself but take it as a moral duty to elect leaders who will help the uneducated

Modernization of the voting process was initiated with the introduction of the electronic voting or e-voting The first paper to introduce the idea of a mix-net based on blind signatures, was by Chaum[2], which is a mechanism that allows a party to get a message digitally signed by another party without revealing any information about the message to the signer. If such a system, the service provider can be the signatory but will not have access to the actual content of the message. Chaum also was the first to introduce electronic voting protocol in 1981 [3].

India has been among the first countries to introduce electronic voting machines or EVMs as they are referred too. The present version of the EVMs in India are standalone devices not connected through a landline or over the wireless, so the basic function is to record and store the vote accurately. EVMs help speed up the counting process. The transition from EVMs is logically the internet but for the low penetration and connectivity issues. With three decades of internet the technology is quite evolved for internet based voting and with the right selection of security software, network configuration and firewalls it is still quite safe for internet voting, a strong example is online banking. Because of the inherited security vulnerabilities of the Internet and computerized systems in general, Internet voting incurs a wide range of criticism. However, to date many pilot projects in different countries and research groups have been carried out. The Secure Electronic Registration and Voting Experiment (SERVE), an Internet-based voting system built by Accenture and its subcontractors for the U.S. Department of Defense's Federal Voting Assistance Program (FVAP), is the most well-known of this kind. The perception of an unsafe network, fueled by secure networks being compromised has been detrimental to wide acceptance of internet based voting for national elections

Estonia voted on the internet for its 2008 elections, though only ~2% of the 70% eligible internet users actually used the option[4] but the government has announced that 2011 national elections will be via mobile phones. Britain has also conducted county elections with cellular phone. India's electronic voting entry has been with EVMs, which have been widely accepted and also perceived to be more secure than paper ballot.

There is no system that can guarantee total protection from disrupters, but the risk can be mitigated by a right balance between technology and human cognition. It is not an easy task to balance security and usability, auditing and secrecy or cost and return on investment. One of the hall mark analysis on this was done by Peter Neuman[1]

1.0 Motivation

1.1 Cost

The national and assembly elections costs the Indian exchequer approximately Rs 1300 crores(or 13 billion rupees), which does not include costs incurred for mobilization of security forces and man-hours of election officers. The 1967 elections cost around 1.79 crores , 597 crores in 1996 and a steep jump to 1300 crores in 2004 (Figure 1). The numbers in Figure 1 is the cost incurred by the election commission for Lok Sabha and does include state elections, which is estimated to be another 700 crores of rupees. This additional amount is spent by various central and state government agencies for purposes like photo ID cards, Electronic voting machines (EVMs) and costs for setting up polling booths.

The total cost of the 2009 Lok Sabha elections, which includes spending by the various political parties in addition to the election commission budget, is predicted to be more than the US election, which was Rs 8000 crores compared to India's Rs 10,000 crores.

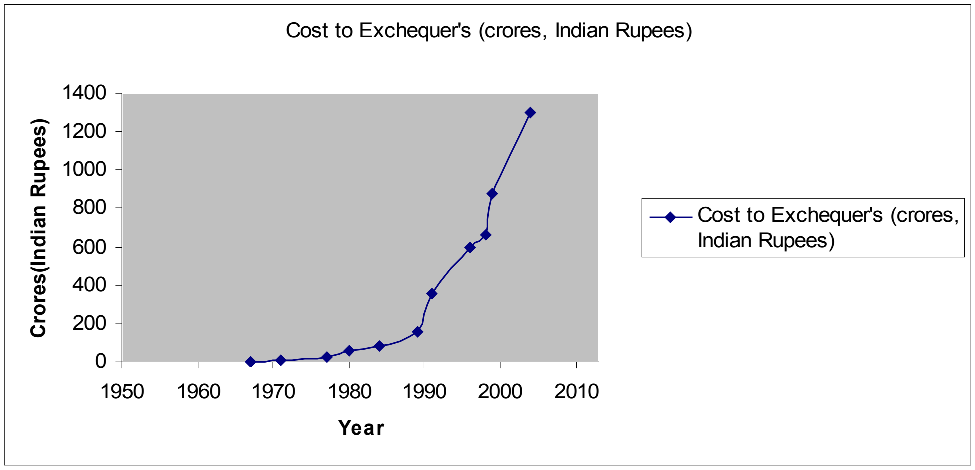


Figure 1: Cost of elections in India

The EVMs have reduced considerably the quantity of ballot paper, for example the 1999 polls used 7,700 metric tones of printing ballot paper and the 1996 saw a use of 8,800 metric tonnes. Hence it is estimated that with over 13.6 lakh EVMs deployed in the 2009 elections, there will be a significant drop in the quantity of paper that will be used and tangible cost and environmental savings.

1.2 Voter turnout

The country has seen approximately 58.85% voter turnout from 1952 (Fig 2) , whereas the cost for conducting polls has seen a steep increase, Fig 1. This increase in costs is significant even if one considers the rise in population and also the number of candidates that get fielded from each constituency. A further difference of 7% between the rural and urban voter turnout was recorded for the 2004 elections, of a total 58% turnout, the rural turnout was higher by 7% to urban, or in other words approximately 3 crores fewer urban population voted. The lower urban voting numbers is a matter of great concern for a democratic country as it might also translate to fewer informed voters exercising their franchise leading to a debate on the value of a vote.

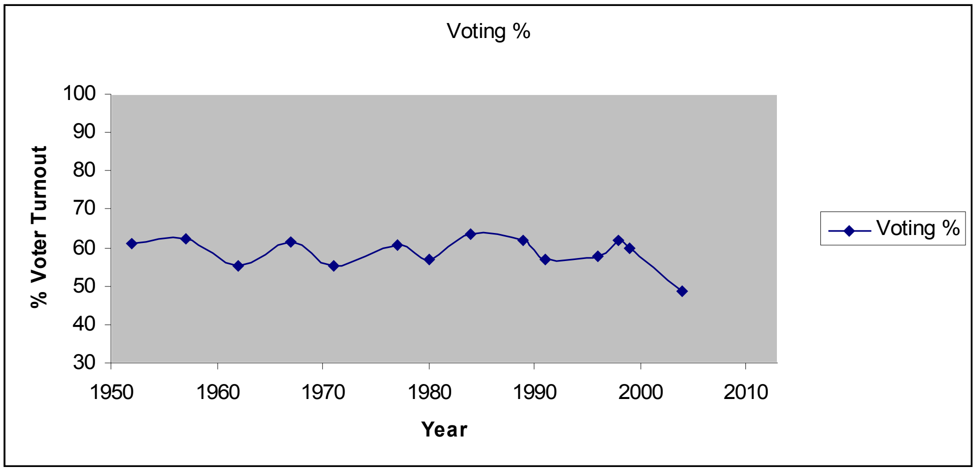


Figure 2: Voter turnout

This leads one to look at the underlying issues for lower urban turn out, and one reason has been unwillingness to stand in the queue at the polling booths. In order to encourage voting in cities, employers give either give the day or time off. While this shows a commitment of the employer to the democratic process, it still is not making the voter go to the booth.
The general apathy across population can also be contributed to cynicism towards the political system in the urban areas and intimidation, distance, geographical barriers like rivers and lakes in rural areas.

1.3 Ballot security & accuracy

For the 2009 polls there are 8,28,804 polling stations in the country, an increase of 1,41,402 from the last 2004 elections. Except for 12,901 new polling stations which have around 300 voters on the list, the rest have 1500 each. Each constituency fields an average of 14 candidates for the Lok Sabha elections. If on an average 50% of the population gets to poll, the number will be 61 crore votes to record and count. Currently the EVMs can hold upto 3900 votes and display 64 candidates, but this data is stored in the machine is only downloaded onto computers when the counting starts or when the machines reach the control rooms. Till the counting begins the ballot boxes and the EVMs are in secure locations and under 24 hour guard. The EVMs output is electronically counted and tallied whereas the ballot papers are manually counted which can potentially lead to inaccuracy and hence re-counts.

2.0 System Overview

Our work aims to introduce systems that can potentially increase the number of voters, ensure ballot security and reduce the cost of elections (as EVMs vs. ballot paper). Importantly, we have strived to come up with a solution that is easy to implement, scalable with minimal changes to the present wireless network backbone. Hence we propose an electronic voting, coined ME-Vote, using the personal mobile phone for India as the penetration levels is far greater, 391.9 million as of 2009 March, than internet access or even for solutions over landline telephone.

The ME-Vote election process involves four distinct stages;

- Registration: In the registration stage the election authorities determine who is eligible to vote by mobile phone, maintain proper lists of the registered voters linked to their constituency and provide them with identification that will enable them to vote.
- Validation: On Election Day, the systems authenticate the voter to cast a vote
- Casting: During this stage, voters cast the vote using secure Short message service (SMS) of mobile phones.
- Counting: the vote is counted as it comes in and the final tally is published and made available to the world after the complete count is accounted for.

The ME-voting system uses mobile network to ensure the smooth and secure transfer of data between the 4 stages and a technical solution which is a balance between control and anonymity that is, having a fool-proof method of authenticating the voter but separating out the vote with the voter. A mobile phone based voting transaction consists of four main components, ie the user, the mobile phone, the service provider and the election office. The flow chart in figure [3], depicts the registration process by the user to vote by mobile phone, here we assume that the issuance of the voter ID or the national ID has been done with due diligence.

2.1: Registration

The voter sends a request via SMS (short message service) from his/her mobile to a dedicated number given by the election office. The SMS message will have the voter ID or nationalID, Name, date of birth and constituency. Upon receiving this information, the Election office (EC) office verifies the same with the data in their servers when the ID was issued and also with the service provider based on the mobile number from which the call is received. If the data verifies, a username/password is sent to the voter. The password will be a randomly generated alpha-numeric character and the username a combination of the name and the last 4 digits of the ID number. Three chances are given for registration, after which the voter has to physically register at the election office. The system is also deigned to allow only 3 eligible ID'ed voters to register with one SIM number.

Another method for a voter to register is by a personal visit to the election office where all the identification papers will be checked and the pin number is issued on a scratch card. In the event bio-metric systems are introduced, fingerprint can also be collected at this stage. This will increase the workload of the election office, but does add to the authentification process.

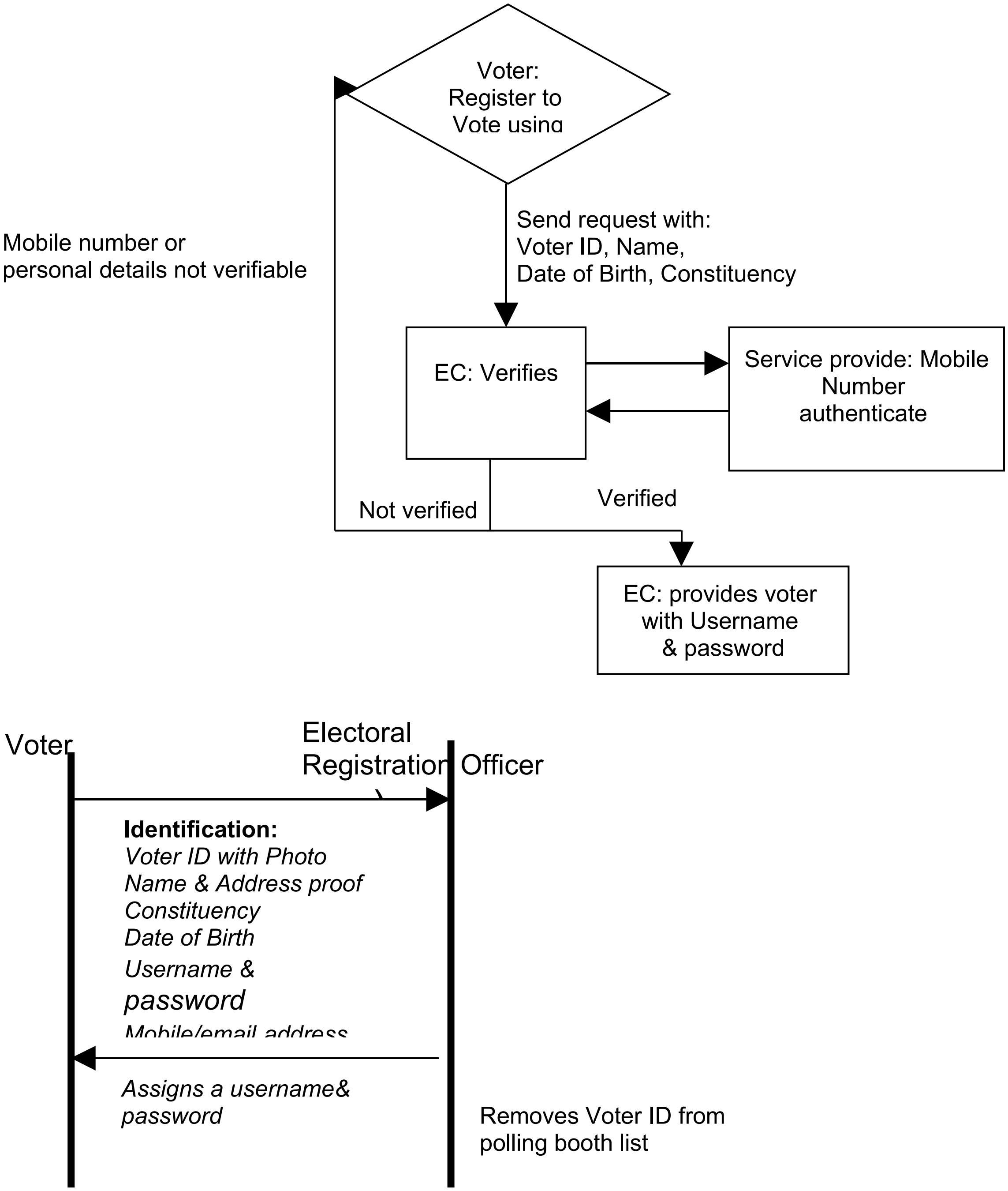
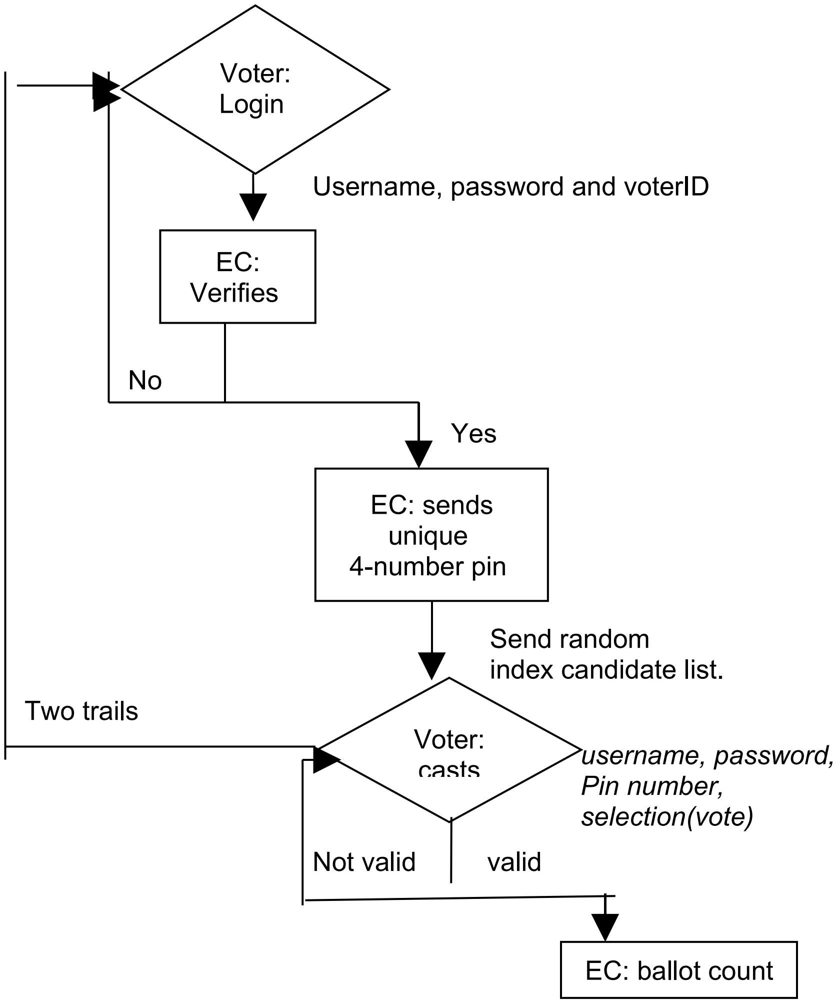

Voter: Register to Vote usinq
Send request with: Voter ID, Name, Date of Birth, Constituency
Mobile number or personal details not verifiable
EC: Verifies
Service provide: Mobile Number authenticate
Not verified
Verified
EC: provides voter with Username & password
Voter
Electoral Registration Officer
Identification:
Voter ID with Photo
Name & Address proof
Constituency
Date of Birth
Username & password
Mobile/email address
Assigns a username& password
Removes Voter ID from polling booth list

Figure [3] : Registration to vote by mobile phone, flow and state diagram

2.2 Casting the vote

On the day of the voting/election, voter initiates a connection to the EC SMS servers with the VoterID/national ID and the username, the EC server prompts for the password after verifying the VoterID and username. A 4-digit pin number is generated and this is automatically stored on the phone and not on the SIM card. The EC server generates a random and uniquely indexed candidates (the politicians standing for election) list for voter's constituency. Every unique and random indexed generated list (list 1: party 1 index 001, party 2 index 005. list 2: party 1 index 005 and party 2 index 001) is linked in the database to the 4- digit pin-number given by the election office. The random indexing makes it difficult for eavesdroppers to collect and change the vote on a mass scale unless the entire network is compromised. At this point the voter is ready and casts the vote tagged to the pin number. Two or three trails are given to each user and all trials start at the login stage.



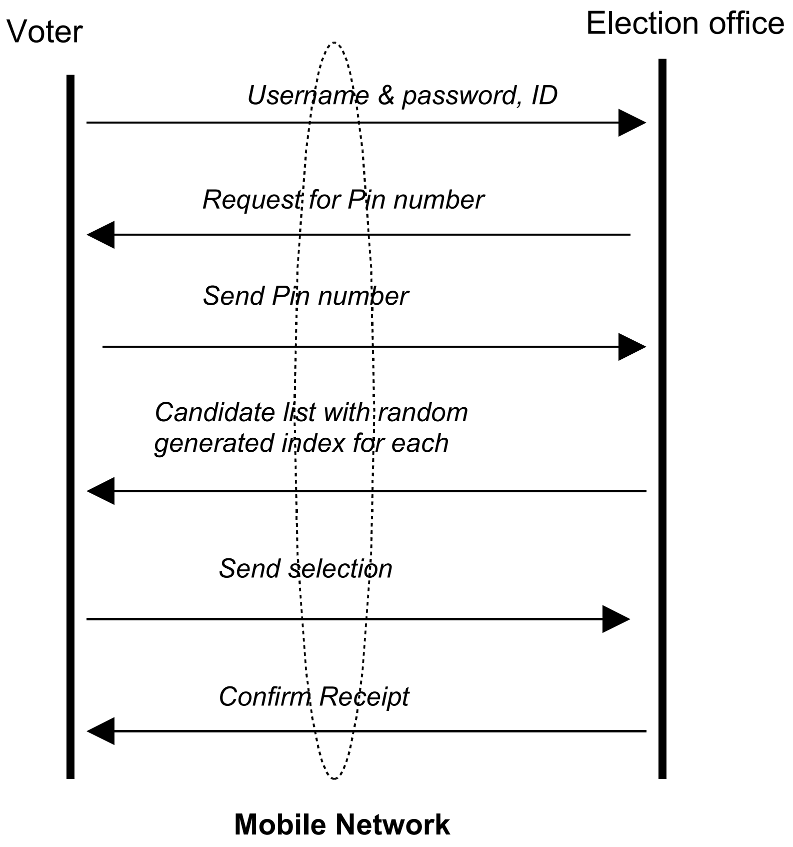


Figure 4: ballot casting process – flow & state diagram.

<u>3.0 The Modular architecture</u>

3.1 The mobile service network

The wireless network that is currently deployed by most service providers is considered in our design [figure 4]. In the current setup the SMS message that originates from the voter passes through the base station switch (BTS) and base station controller (BSC), to the Mobile switching center (MSC), Home Location Register (HLR) to a SMS router. The network elements that enable the flow of information (figure 3 & 4) is shown in figure 5.

The SMS router has been a recent introduction in networks to address the 'Denial of service attacks' or message flooding which potentially overwhelms the SMS centers (SMSCs) and shuts access. The SMS router will be configured with intelligent algorithms to route messages to the end servers based on the content of the SMSs. Additionally the router is programmed to split the data based on certain rules and stream this data to different servers installed at the election office. The forking of ballot data to a separate server is to ensure the voter's right to confidentiality. Another security feature introduced is using different SMS classes , like the CLASS0, where the candidate selection flashes on the voter's mobile phone screen for a few seconds and class1 SMS where the return message from the ballot database contains the ballot cast flag or evidence (similar to the mark on the figure after voting) in the device instead of the SIM card of the voter's mobile phone.

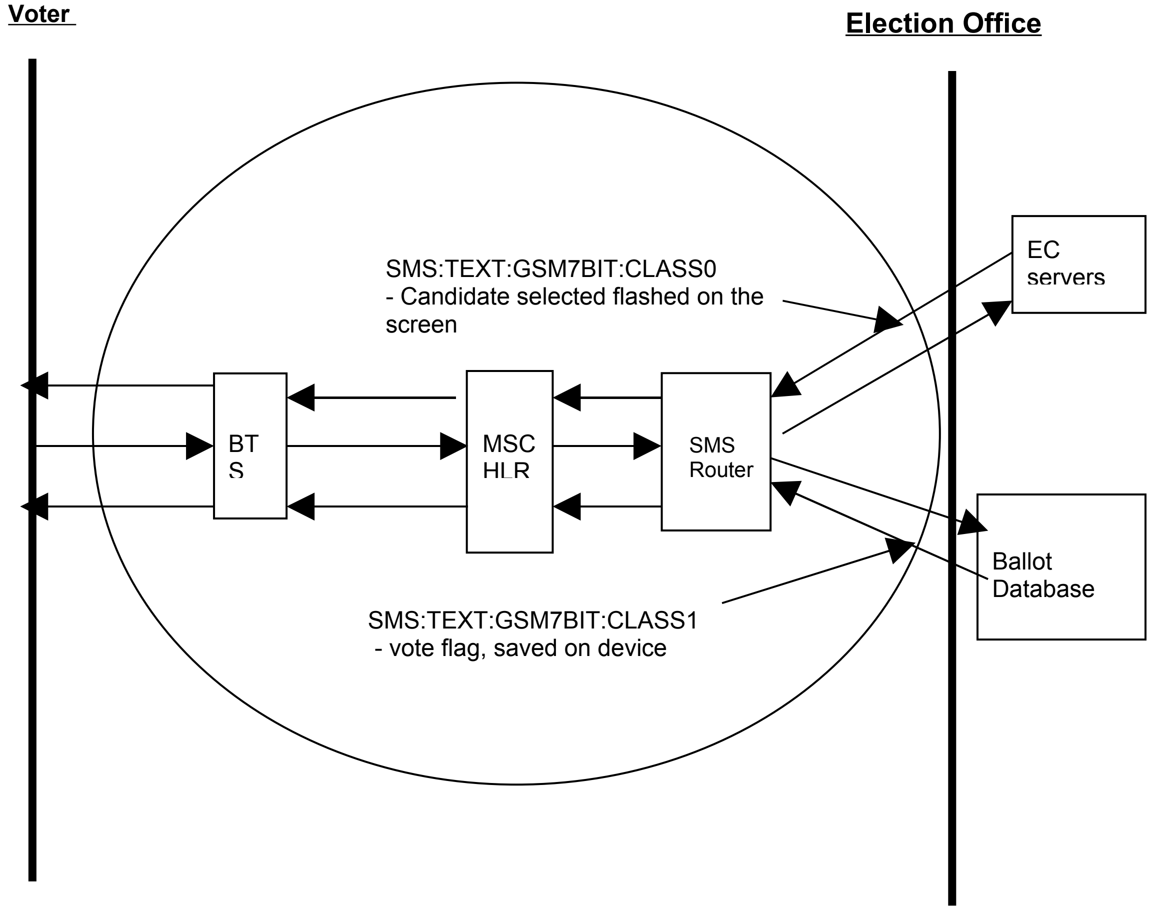


Figure 6: Wireless or cellular network architecture for ME-Vote

3.2: System Configuration at the Election Office

The main features of the architecture at the election office(s) are: distributed data management, data redundancy and scalability. As shown in figure 6, the SMS routers at the service provider end route the messages to and from the servers managed by the election office. Intelligent identification and message parsing algorithms will be deployed on the routers. To ensure that at no point the voterID is linked with actual selection, the vote is routed to another bank of servers. In the event of any re-count or clarification the 'broker' acts as the bridge between the two networks and can link to each of the networks by a unique ID number. The servers can be distributed geographically (within city) to protect from physical attacks or any natural hazards.

The servers (s1,s2…) (figure 7) will manage the databases and also generate the SMS messages and maintain two-way communication with the router and the ballot servers (b1,b2,b3…) will only receive the vote from the router. The router will parse the SMS message which contains the vote and route the message sans the voterID to the ballot server and the rest of the message is sent to the Me-Vote servers. The Me-server than activates a flag on the corresponding VoterID to indicate that the person has exercised the franchise. A confirmation message is sent to the voter, after the vote is logged in. At this juncture, the debate is still one whether the confirmation SMS message should also indicate the choice.

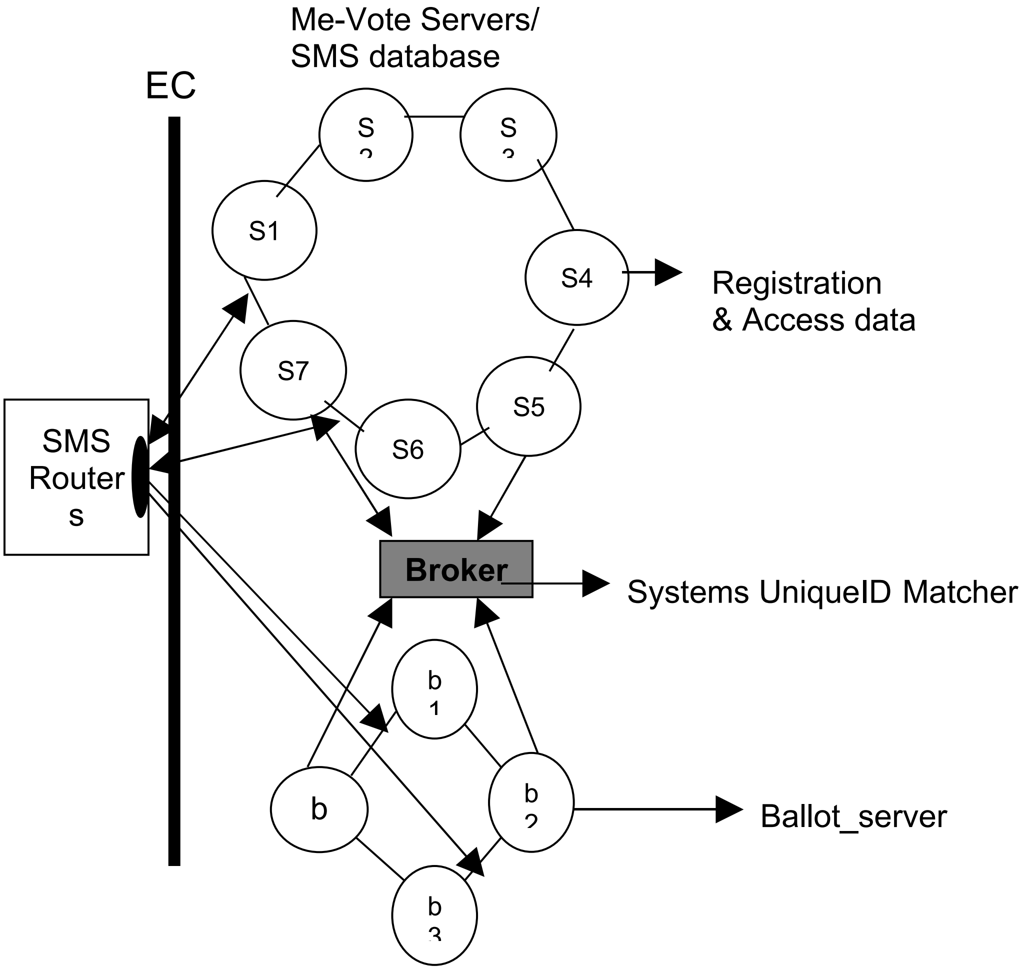


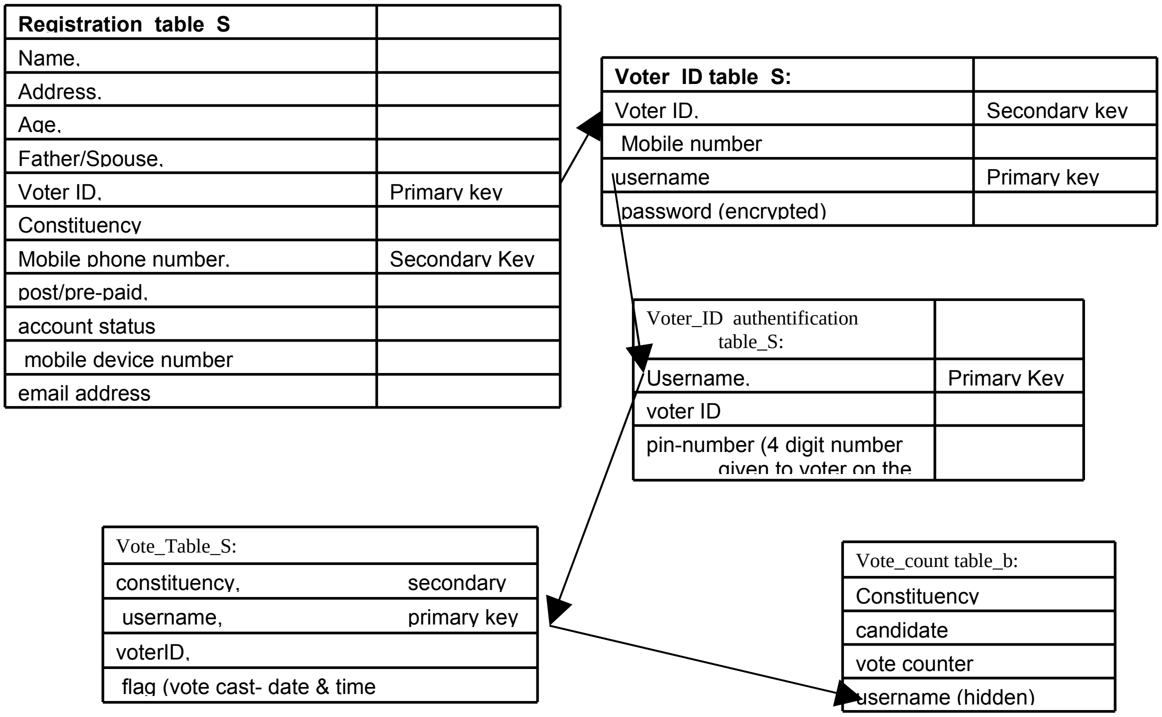
Figure 7: The system architecture at the election office

3.3 Database Schema

The database is designed to be lean and the tables are uniquely linked, that is using different primary keys instead of one primary key for querying. Intrusions into any one of the tables does not give access to information on the primary key used in linked table and hence data cannot be retrieved. The tables are structured simply and a sample scheme is shown below in figure 8. The query routines will be slightly more complex than a routine relational database query for data.

As the databases are centrally managed, fields can be added and removed without the necessity of any changes at the service providers network.

The mobile number collected from the voter is verified by the service provider and additional fields like mobile phone account status, type of connection and even the mobile (machine) number are tabled. In the registration phase, the service provider plays a crucial role and the credibility of the provider as a stake holder is assumed. The storage space and processing power of the servers can be scaled up as required, for example if mobile phone have biometric capture and transmit capability, the data size will increase substantially.



Registration table S	
Name,	
Address,	
Age,	
Father/Spouse,	
Voter ID,	Primary key
Constituency	
Mobile phone number,	Secondary Key
post/pre-paid,	
account status	
mobile device number	
email address	

Voter ID table S:	
Voter ID.	Secondary key
Mobile number	
username	Primary key
password (encrypted)	

Voter_ID authentification table_S:	
Username.	Primary Key
voter ID	
pin-number (4 digit number given to voter on the	

Vote_Table_S:	
constituency,	secondary
username,	primary key
voterID,	
flag (vote cast- date & time	

Vote_count table_b:
Constituency
candidate
vote counter
username (hidden)

Figure 8 : Sample database scheme

3.4 Secure communication

A high-profile and critical event like elections where power and money is at stake is sure to attract mischief or disruption by enemies of democracy from within or outside the country. Some of the know disruptions are Distributed Denial of Service (DDos) and network outages due to high-volume traffic/time. A vulnerable spot in the proposed network is the path between the mobile phone and the base station center and again between the SMS routers and the servers at the election office. A break at the latter will disrupt traffic but does not allow for any fraud, like changing the vote, as the data is parsed and distributed. A intruder tuned continuously for long periods of time to the open waves between base station and mobile phones can potentially impersonate the voter. This will require access to the pin-number, which is not electronically recorded if the voter registers at the election office personally. Additional checks and balances are introduced by the controlled randomness of the data generation for candidate list and window for voting.

Intelligent routing algorithms introduced in the SMS routers play a crucial role in blocking spoofing messages by screening the incoming messages and verifying the identity of the sender by location. This is done by a routing algorithm that queries the originating subscriber details from the HLR before the message is submitted for delivery.

The architecture & planning has considered many possible methods to increase the security while at the same time not compromising on the ease of use to the voter. Much of the complexity is moved to the back-end. An element of surprise is planned to catch the hackers or disrupters unawares, for example: time-intervals allocated for a randomly selected set of mobile registrants – instead of an open long time window common to all, sets of subscribers are individually invited to vote during a certain time interval. A fraud detection system using complex event processing built on Apama platform (Progress Software) will be plugged in to check for outliers and aberrations to normal polling trends. The Apama engine can be programmed with rules that election commission tend to use to detect fraud.

And as final check, a voter who has successfully voted using the mobile network will have his/her name removed or flagged on the voter-list, which will atke care of double-voting.

Conclusion

As discussed in this paper, the proposed voting protocol using anonymous code lists, distributed servers, and fraud detection engines can provide the basis for a secure implementation of an e-voting solution over mobile channels. We conclude with some underlying design principles and best practices for a secure electronic voting architecture.

- A pragmatic approach focusing on standard situations is recommended. Usually, e-voting is an additional channel, which is not mandatory to use, but one that can penetrate deeper in India if voters perceive it as safe.
- The voter experience should be intuitive and ensure value for vote.
- The m-voting protocol must rely on a minimum amount of short messages,
- Technology intervention should be balanced with complexity and hence maintenance.
- The voter's cognition and perception should be heightened for acceptance to mobile voting.

Acknowledgments

I would like to thank Prof's Srinathan Kannan, Kamal Karlapalem, and Ramesh Loganathan for their valuable inputs and marathon discussions.

References:

[1] Peter G. Neumann, September 1993, Security Criteria for Electronic Voting http://www.csl.sri.com/users/neumann/ncs93.html

[3] D. Chaum: 1983, Blind signatures for Untraceable Payments In Advances of Cryptology - Crypto ‘82, pgs. 199-203. Plenum Press,.

[3] D. Chaum: 1981, Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms. Communications of the ACM, 24(2), pgs. 84-88,

[4] Ülle Madise,e-voting in Estonia experience, http://www.vvk.ee/engindex.html

[5] Satbir Silas & K.N. Kumaru, 2004,Elections in India. A MONUMENTAL EXERCISE, India Perspectives.

[6] Voutsis, Nico; Zimmermann, Frank: Anonymous Code Lists for Secure Electronic Voting over Insecure Mobile Channels, in: Mobile Government – An Emerging Direction in E-Government, ed. Ibrahim Kushchu, IGI Publishing – Hershey – New York

Websites:

[1] Statistics on India Elections, http://www.indian-elections.com/india-statistics.html

[2] The Estonia e-voting government site, http://www.vvk.ee/?lang=en –