E-Voting – Secured NFC Voting

Pooja Dyta[1] Swapnil Junjare[2] Akshay Pandita[3] Prof. D.R. Ingle[4]
[1,2,3]Student [4]Assistant Professor
[1,2,3,4]Department of Computer Engineering
[1,2,3,4]Bharati Vidyapeeth College of Engineering, Navi Mumbai-400614

Abstract— Due to embedded systems, Evoting systems are becoming popular and widespread. Using homomorphic signature scheme, this paper implements the new Evoting system with the help of a Paillier cryptosystem and blind signature method. The embedded system is used as a voting machine and the RFID are used to perform the casting of votes according to government rules.

Key words: E-voting system, Paillier cryptosystem, RFID, Blind Signature, Embedded System, Security

I. INTRODUCTION

Due to the rise of mobile phones and their applications we can now use the phones themselves to make digital voting possible.. It is believed that voting via SMS and other means of social media and more digital ways is much more comfortable for most people and less cumbersome and likely to garner more response. The voting process also becomes more transparent and thus this paper has been made with an intent to tap into the potential of Evoting.

The general process of elections is quite tedious and this Electronic Voting System (EVS) has been introduced. The EVS system is secure , integrated , compatible, compact and faster than traditional voting system. It improves security to a huge extent and is much more comfortable from the point of view of large scale voting.

The main purpose of project is to use android based phones which contain NFC to help cast their votes. User uses NFC to verify their identity, after which the backend system verifies them and gives the identity authorization. The user can then place his/her embedded vote using the same NFC tag.

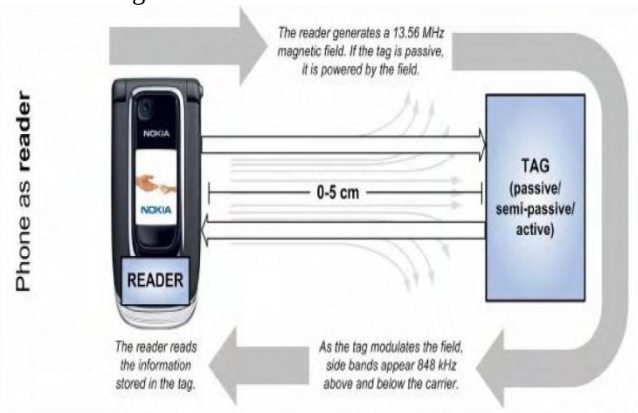

Fig. 1: Mobile phone acting as NFC Tag Reader

A. *Aims and Objectives:*

Our aim is to replace the current general voting system and bring in an era of Mobile voting using the NFC sensor found in most phones today.

It makes everything easier including reducing cost for physical ballot boxes and saves time and saves energy and makes the process much easier and digital and more secure.

II. NEAR FIELD COMMUNICATION (NFC):

Near field communication (NFC) is a set of ideas and technology that enables smartphones and other devices to establish radio communication with each other by touching them together or bringing them into proximity, typically a distance of 10 cm (3.9 in) or less. Each full NFC device can work in 3 modes: NFC target (acting like a credential), NFC initiator (as a reader) and NFC peer to peer. Most of the first business models like advertisement tags or other industrial applications have not been successful, always overtaken by another technology (2D barcodes, UHF tags, ...) The main advantage of NFC is that NFC devices are often cloud connected, "Connected" credentials can be provisioned over the air unlike a standard card (Hotel or visitor applications). All connected NFC enabled smartphones can be provisioned with dedicated apps, which gives any application a huge potential, like dedicated readers (as opposed to the traditional dedicated infrastructure of ticket), access control or payment readers. All NFC peers can connect a third party NFC device with a server for any action or reconfiguration.

Fig. 2: Samsung GALAXY Note

A. *NFC Tag:*

NFC (near field communication) is a wireless technology which allows for the transfer of data such as text or numbers between two NFC enabled devices. NFC tags, for example stickers or wristbands, contain small microchips with little aerials which can store a small amount of information for transfer to another NFC device, such as a mobile phone.

There's a whole set of different data types you can store on an NFC tag. The actual amount of data varies depending on the type of NFC tag used - different tags have different memory capacities. For example, you may choose to store a URL (web address) or a telephone number. A standard Ultralight NFC tag can store a URL of around 41 characters, whereas the newer NTAG203 nfc tag can store a URL of around 132 characters.

Usually, this information is stored in a specific data format (NDEF - NFC data exchange format) so that it can be reliably read by most devices and mobile phones.

1) Different kinds of NFC Tag.:

Fig. 3.2(a): Coin shaped NFC tags

Fig. 3.2(b): NFC tags in the form of key-chains, watches, etc

Fig. 3.2(c): NFC tags in the form of wristbands

III. EXISTING SYSTEM

The current system uses a 2 piece way of authentication i.e ballot boxes and voter id cards. This method is weak and not very effective in terms of security as you may have seen it has already been tampered with.

A. Methodology:

The voters will be equipped with a NFC enabled smart-phone. Google Android platform will be used to develop the mobile app. Google has provided many flexible APIs (Application Programming Interface) for NFC use. Using Googles IDE and software development kit we can implement NFC use in apps. A server will be developed to collect the votes and watch over the system. This system will be used to monitor voting activities. It will also be used later to tally the votes and display results.

B. Electronic Voting Security Requirements:

Security and accuracy are the first and foremost requirements for any voting system. Hence, EVS should satisfy at least the following security requirements which are described

1) Eligibility: Only pre authorized voters satisfying criteria can vote.
2) Uniqueness: you cannot vote more than once.
3) Privacy: No one can determine for whom one has voted even after the results.
4) Integrity: No one can copy and multiply anyone else's vote and no one can change anybody's vote without jeopardizing themselves.
5) Accuracy: Cryptography and blind signature is used for encrypting ballot and printing the receipt to make sure everyone has voted and everybody's vote has been counted.
6) Mix-net scheme will be used for encrypting receipt.
7) Using a Homomorphic method for hiding voter information and ballot content

IV. SIGNIFICANT SECURITY TOOLS

The cryptographic voting protocols are based on significant security tools. These tools are classified to

- Homomorphic encryption.
- Mix-net.
- Blind signature based on RSA. The following subsections describe briefly these tools

A. Homomorphic Cryptosystem Homomorphic Cryptosystem Is One Of The Efficient Security Tools For E-Voting System Due To Homomorphic Property [18].

It is an algebraic property that allows to apply mathematical operations on sets of encrypted ballots without need of decrypting them which improves privacy [18]. For example, in additive homomorphic encryption, the product of two ciphertexts is a third ciphertext that encrypts the sum of the two original plaintexts [2]. Paillier algorithm is one of the homomorphic cryptosystem which is widely used in most voting systems. It is a probabilistic asymmetric algorithm for public key cryptography, invented by Pascal Paillier in 1999 [2, 19]. A brief description of Paillier cryptosystem algorithm is described below [2].

1) Key Generation:

In this step both the public keys (n,g) and private keys (, μ) are generated .

- Choose two large prime numbers p and q where (gcd (pq, (p–1) (q–1)) =1)
- Compute n = p×q and = lcm (p---1, q---1) where, λ= (p --- 1)(q --- 1) / gcd ((p --- 1)(q --- 1))
- Select random integer g where, gcd [((g λ mod n2 --- 1) / n) , n] = 1
- Compute μ = (L(gλ mod n2))−1 mod n where, L(u) = (u-1) / n

2) Encryption:

- Select a random number r
- C (ciphertext) = gm rn mod n2 where, m is the plain message.

3) Decryption:

- m (plaintext) = L(c λ mod n2) . μ mod n.

To illustrate the homomorphic property consider two messages m1 and m2, the encryption of each message is E(m) = gm rn mod n2 . Consequently, the product of cipher texts E(m1) and E(m2) produces the cipher of addition of m1 and m2 messages as follows:

E(m1).E(m2) = (gm1 r1n)(gm2 r2n) mod n2 = (gm1+m2)(r1r2)n mod n2 = E(m1+m2)

B. Blind Signature based on RSA:

The blind signature technique allows a singer to sign documents without knowing what's inside. The security of this technique is achieved if the signers do not know the

content of the message to be signed. Moreover the signers should not know the signature message pair or for whom he signed this message [4]. This technique is first introduced by Chaum in 1983. Blind signature based on RSA is one of the techniques used in EVS. In this technique the registrar, who has the authority to sign, has a set (n, d, e) based on RSA key scheme. He chooses a random number k where $1< k \leq n$. The voter blinds his ballot m to get blind ballot B where

$$B = (mke) \bmod n \quad (1)$$

Where e is the public key

The blinded ballot B is signed by an authority person with a private key d to get signed ballot S where

$$S = Bd = (mke)d \bmod n = (mdk) \bmod n \quad (2)$$

The signed ballot is unblinded by dividing it over k

$$UB = S\ k–1 = md \bmod n \quad (3)$$

C. Mix- Net:

Mix-net technique is a way used to anonymize ballots by dissociating the encrypted message from its sender [11]. This technique mixes messages by sending them through a network of authorities. Then each authority shuffles the received messages before sending them to next one and keeping the permutation secret [20]. The mix-net has two types: decryption and reencryption. In decryption mix-net the messages are encrypted by all authorities' public keys and each authority partially decrypts the message. In reencryption mix-net the message is encrypted by a shared public key and reencrypted by each authority's private key [2,20].

V. Proposed E-Voting System

The proposed e-voting system adopts one Central Tabulation Facility (CTF) which collects all secret ballots from local committee servers that distributed among poll stations. Each server in each poll station is connected with a number of embedded systems named voting terminals which used to create voter's ballot. The proposed system utilizes both homomorphic cryptosystem which implemented using Paillier cryptosystem and blind signature based on RSA. The system is accomplished in five distinctive phases: authorizing, voting, authenticating, and tallying phases. The following subsections detail each phase.

A. Authorizing Phase:

Authorizing phase is the first phase in the proposed e --- voting system. It starts when a voter arrives at poll station with his national ID and RFID. The main role of this phase is to check the voter identity and eligibility. The voter identity is checked by an authority part that checks the voter national ID. Hence this part of the process is a human controlled process. The voter eligibility is confirmed by voter's passive RFID card which is prepared by the government before Election Day. The RFID card contains all information (constraints) required to check voter eligibility as shown in table I. The status of voter against each constraint is saved as a flag bit which equals to logic one if voter satisfy this constraint or logic zero if not. All these flags consumes one byte storage area. In addition, forty bytes are needed to store the voter's name. Since this system is proposed for any kind of election, a part of RFID memory is reserved to store the type of election. The proposed system suggests to serve eight different types of elections, each type needs 17-bit storage area as shown in table I. The first two bytes represent the date of election while the last bit is a flag bit which will be changed after a voter casts his vote. From the authority perspective this flag prevents voter from vote once again. The last field in RFID is validity field which concerns the RFID validity time. This field needs 2-bit which limits the validation time in four years.

The security of the RFID and its communication are beyond the scope of this paper.

B. Voting Phase:

After checking identity and eligibility of a voter, voting phase starts. In this phase, voting terminal displays an empty ballot, so the eligible voter selects his nominee and constructs his ballot. Subsequently, the voting terminal stores all ballots generated by voters in M×L tables where L is the number of nominees and M is a number of voter's ballots.

	Name of storage field in RFID	Size (bits)
	Voter name	40 bytes
Constrains of Eligibility	Nationality	1
	Age	1
	Criminal status	1
	Armed forces	1
	Quarintied status	1
	Mental illness	1
	Bankruptcy	1
	Status of requirement	1
	Name of storage field in RFID	**Size (bits)**
Type of Election	Presidential election	17
	Re-Presidential election	17
	People's Assembly elections	17
	Re-People's Assembly elections	17
	Shura Council elections	17
	Re- Shura Council elections	17
	Local people council election	17
	Re- local people council elections	17
	Validity (number of years)	2
	Total	466

Table 1: Data Stored in RFID

If a voter casts his vote his ballot will be constructed by storing a prime number representing vote YES in a cell intersects with the selected nominee while the rest L-1 cells have another prime number that represents vote NO as shown in table II. For a real time processing the number of rows M (ballots) is chosen to be small for example 5 rows or multiple of 5. The voting terminal encrypts each prime number in the ballot (row) using Paillier cryptosystem. Afterward the encrypted ballot is concatenated with a corresponding voter's information. The resulting tables are sent to the local committee. Based on the additive homomorphic property of Paillier cryptosystem the voting terminal multiplies all encrypted votes for each nominee (column) as shown in table

To prohibit any attempts to vote again, the RFID writer records the election date and set the flag in type of election field in voter's RFID to logic one. All these steps are repeated for the remaining ballots until the end of the Election Day.

	David	Jon	Carl	Arlond	Tom
Voter1	5	19	19	19	19
Voter2	5	19	19	19	19
Voter3	19	5	19	19	19
Voter4	19	5	19	19	19
Voter5	19	19	5	19	19

Table 2: Table 5*5 of Plain Ballots Prime No of Vote YES= 5 AND Vote No= 19

David	Jon	Carl	Arlond	Tom
E(5)	E(19)	E(19)	E(19)	E(19)
×E(5)	×E(19)	×E(19)	×E(19)	×E(19)
×E(19)	×E(5)	×E(19)	×E(19)	×E(19)
×E(19)	×E(5)	×E(19)	×E(19)	×E(19)
×E(19)	×E(19)	×E(5)	×E(19)	×E(19)
=ξ1	=ξ2	= ξ3	=ξ4	=ξ5

Table 3: Multiplied Votes for Each Nominee

C. *Authentication Phase:*

Authentication means, it should be possible for the receiver of a message to ascertain its origin; an intruder should not be able to masquerade as someone else [18]. In our system blind signature based on RSA is used for authentication. In this phase the voting terminal blinds the multiplied votes ξi using a public key e as depicted in equation

1) The blind votes are sent to the local committee server which signs them with a private key d as illustrated in equation
2) Consequently, the local committee blinds the received tables that contain the encrypted ballots and voter's information. Then all these blinded and signed data are sent to CTF.

D. *Tallying Phase:*

This phase starts when signed votes delivered to CTF which unblinds them as illustrated in equation 3.Afterwards CTF decrypts the resulting unblinded message. Due to the additive homomorphic property of the Paillier cryptosystem, the decryption results will be the addition of the prime numbers of votes YES and NO. To verify the idea table IV shows the decryption results for the example shown in table II.

David	Jon	Carl	Arlond	Tom
67	67	81	95	95

Table 4: Decryption Results for the example shown in table 2

At the end of Election Day CTF extracts the number of votes for each nominee to get the election results. Hence CTF calculates the number of vote YES by applying

$$n = (y - Nr_2) / (r_2 - r_2) \quad (4)$$

Where, n is the number of "Vote Yes" for each nominee.

1) Blind RSA Signatures[2]:235[edit]:

One of the simplest blind signature schemes is based on RSA signing. A traditional RSA signature is computed by raising the message *m* to the secret exponent *d* modulo the public modulus *N*. The blind version uses a random value *r*, such that *r* is relatively primeto *N* (i.e. $gcd(r, N) = 1$). *r* is raised to the public exponent *e* modulo *N*, and the resulting value $r^e \bmod N$ is used as a blinding factor. The author of the message computes the product of the message and blinding factor, i.e.

$$m' \equiv mr^e \pmod N$$

And sends the resulting value m' to the signing authority. Because *r* is a random value and the mapping $r \mapsto r^e \bmod N$ is a permutation it follows that $r^e \bmod N$ is random too. This implies that m' does not leak any information about *m*. The signing authority then calculates the blinded signature *s′* as:

$$s' \equiv (m')^d \pmod N.$$

s' is sent back to the author of the message, who can then remove the blinding factor to reveal *s*, the valid RSA signature of *m*:

$$s \equiv s' \cdot r^{-1} \pmod N$$

This works because RSA keys satisfy the equation $r^{ed} \equiv r \pmod N$ and thus

$$s \equiv s' \cdot r^{-1} \equiv (m')^d r^{-1} \equiv m^d r^{ed} r^{-1} \equiv m^d r r^{-1} \equiv m^d \pmod N,$$

Hence *s* is indeed the signature of *m*.

In practice, the property that signing one blinded message produces at most one valid signed messages is usually desired. This means one vote per signed ballot in elections, for example. This property does not hold for the simple scheme described above: the original message and the unblinded signature is valid, but so is the blinded message and the blind signature, and possibly other combinations given a clever attacker. A solution to this is to blind sign a cryptographic hash of the message, not the message itself.

VI. Security Analysis

In this section we analyze how strong the proposed e- voting system satisfies the security requirements.

A. *Eligibility:*

Using public key encryption algorithm, the government prepares a voters data using his NFC tag RFID and authorizes him and makes him, eligible to vote.

B. *Secrecy:*

Paillier cryptosystem with probabilistic encryption is used making it almost impossible for cryptoanalysts to decipher the messages. In addition the homomorphic property in Paillier allows CTF, in tallying phase, to count the encrypted votes with no need to decrypt them. In voting phase more secrecy is ensured by multiplying ballots and increasing number of virtual digital ballots making voters choice hard.

C. *Uniqueness:*

During voting a certain flag bit present in voters RFID gets marked as soon as he casts his vote so that the vote cannot be cast multiple times.

D. *Privacy:*

Blind signature using RSA is used in this part to ensure privacy of votes. It also unlinks the votes from voters RFID themselves after vote is cast to ensure that no one knows who one has voted for.

E. Accuracy:

Using the blind signature based on RSA can satisfy this requirement. All votes are blinded in voting phase then signed in the authentication phase. Therefore the CTF counts only the signed votes.

VII. CONCLUSION

In this paper, a new EVS is presented. It utilizes Pailier cryptosystem and blind signature based on RSA as security tools. It consists of CTF that communicates with multiple local committee servers that distributed among poll stations. Each server is connected with group of embedded systems acting as voting machines. The system satisfies the vital security requirements. Pailier cryptosystem provides the secrecy requirement because of its additive homomorphic property, which allows CTF to tally the secret votes without decrypting them. The blind signature based on RSA blinds the votes and voter identity to achieve privacy and accuracy security requirements. The eligibility and uniqueness requirements are accomplished by the data stored in voter's RFID.

REFERENCES

[1] K. Alam and S. Tamura, "Electronic voting using confirmation numbers systems," IEEE International Conference on System, Man and Cybernetics, SMC 2009, pp. 4535 – 4540, 2009., in press.
[2] M. J. Moayed, A. A. A. Ghani, and R. Mahmod, "A survey on cryptography algorithms in security of voting system approaches," International Conference on Computational Sciences and Its Applications, ICCSA '08, pp. 190 – 200, 2008., in press.
[3] B. Ondrisek, "E-Voting system security optimization," 42nd Hawaii International Conference on System Sciences, HICSS '09, pp. 1 – 8, 2009., in press.
[4] Gina Gallegos-García, Roberto Gómez-Cárdenas, and Gonzalo I. Duchén-Sánchez, "Identity based threshold cryptography and blind signatures for electronic voting," Journal WSEAS Transactions on Computers, vol. 9. Issue: 1, pp. 62-7.1, 2010., in press.
[5] Bruce Schnieer, "Applied Cryptography, Protocols, Algorthms, and Source Code in C," Wiley Computer Publishing, John Wiley & Sons, Inc. Second Edition, 1996.
[6] Byoungcheon Lee and Kwangjo Kim, "Receipt-free electronic voting scheme with a tamper-resistant randomizer," ICISC'02 Proceedings of the 5th international conference on Information security and cryptology, pp. 389-406, 2002.
[7] A. O. Santin, R. G. Costa, and C. A. Maziero, "A three-ballot-based secure electronic voting system," Security & Privacy IEEE, vol. 6. Issue: 3, pp. 14 – 21, 2008., in press.
[8] T. Rossler, H. Leitold, and R. Posch, "E-Voting: A scalable approach using XML and hardware security modules," The 2005 IEEE International Conference on e-Technology, e-Commerce and e-Service, pp. 480 – 485, 2005., in press.
[9] R. Anane, R. Freeland, and G. Theodoropoulos, "E-voting requirements and implementation," E-Commerce Technology and the 4th IEEE International Conference on Enterprise Computing, E-Commerce, and E-Services, pp. 382-392, 2007., in press.
[10] Kazue Sako, "Electronic voting scheme allowing open objection to the tally," IEICE transactions on fundamentals of electronics, communications and computer sciences, vol. E77-A. No.1, pp. 24-30, 1998., in press.
[11] Tatsuaki Okamoto. "Receipt-free electronic voting scheme for large scale election," Proceeding of the 5th International Workshop on Security Protocols, pp. 25 – 35, 1997. in press.
[12] Wakaha Ogata, Kaoru Kurosawa, Kazue Sako, and Kazunori Takatani, "Fault tolerant anonymous channel," Proceedings of the First International Conference on Information and Communication Security, Springer-Verlag, pp. 440–444, 1997.
[13] M. Abe and F. Hoshino, "Remarks on Mix-network based on permutation networks," Public Key Cryptography (PKC 2001), LNCS 1992 Springer Verlag, pp. 317-324, 2001., in press.
[14] Mads Johan Jurik, "Extensions to the Paillier Cryptosystem with Applications to Cryptological Protocols," A PhD dissertation, Faculty of Science of the University of Aarhus, Denmark, 2004.
[15] Josh Cohen Benaloh, "Verifiable Secret Ballot Elections," PhD dissertation, Yale University, New Haven, 1987.
[16] Kazue Sako and Joe Kilian, "Secure voting using partially compatible homomorphisms," Advances in Cryptology - CRYPTO'94, Springer- Verlag, pp. 411–424, 1994. in press.
[17] Ronald Cramer, Rosario Gennaro, and Berry Schoenmakers. "A secure and optimally efficient multi-authority election scheme," Advances in Cryptology - EUROCRYPT, pp. 103-118, 1997.
[18] Ben Adida, "Advances in Cryptographic Voting Systems," Doctor of Philosophy in Computer Science in the MASSACHUSETTS INSTITUTE OF TECHNOLOGY (MIT), 2006. , in press.
[19] Dario Catalano, Rosario Gennaro Nick, HowgraveGraham, and Phong Q. Nguyen, "Paillier's Cryptosystem Revisited," Proceeding CCS '01 Proceedings of the 8th ACM conference on Computer and Communications Security, pp. 206 – 214, USA, 2001.
[20] Martin Hirt and Kazue Sako, "Efficient receipt-free voting based on homomorphic encryption," In Proceedings of the Eurocrypt 2000, pp. 539-556, 2000., in press.

