Evoting system using multifactor authentication with NFC chip

First V. S. Mundhe, Second S. Patodkar, Third B. Jadhav, Fourth D. Singh Chandel

Abstract- Election system making use of electronic voting machine becoming more common now a days, however online voting still not conducted in India.. In this paper we propose an E-voting procedure which by using NFC chip provides voters an enhanced way to audit and cast their votes more securely. This paper provides the solution for encrypting the vote by offering a portable identification(login/password) system that will give an access to cryptographic keys actually used in voting procedure. In order to achieve the goal this paper has propose the creation in computationally optimal way, of a cryptographically secure key store to be used for voting procedure. As for secure it give proof that the voter has taken one and only one set.

***Index Terms*—NFC chip ,security, cryptography**

I.INTRODUCTION

Election is an important social activity and on which to much research has been conducted to find an enhanced and efficient method that would replace the traditional voting procedure. In past two decades, various types evoting system has evolved to make the election process more easy and efficient for voters, political parties, candidates and election administration different types of voting scheme has been implemented with varying success rate. Even some of the Scheme worked well ,prototypes in the other have been not accepted because of issues related to the technical reliability, security and privacy. Though some of them succeeded because they have meet the specific requirement of particular country.

The development of electronic model should be based on the electoral process and the specific need of other affected parties as well as voters. In developing countries the even though electronic machines has been introduce for the voting but on-line voting is not allowed. Thus the challenge is to create a successful framework on which en evoting can be effectively executed in the developing countries. While choosing India as a case study, a framework should be developed to specify in details the functional requirements that

must be monitored to fit into the constitutional election principles of Indian voting laws. The framework should also be provide the guidelines for design an e-voting scheme to be applicable for direct deployment.

The framework should also consider the digital divides in the India as a main factor that would affect the public acceptance of an e-voting scheme. Therefore among the functional requirements that would be critical is scheme simplicity and familiarity in terms of voters participation ,and their ability to learn and interact with a new voting Procedure. This familiarity comes from the traditional voting process.

This conventional election method asks the voters to fill the paper form if he/she fulfills the age criteria and get the voterID. At the time of election voter has to reach to the local polling booth an give his vote to any one of the candidate and ink is applied on his first finger so that he cannot apply again.

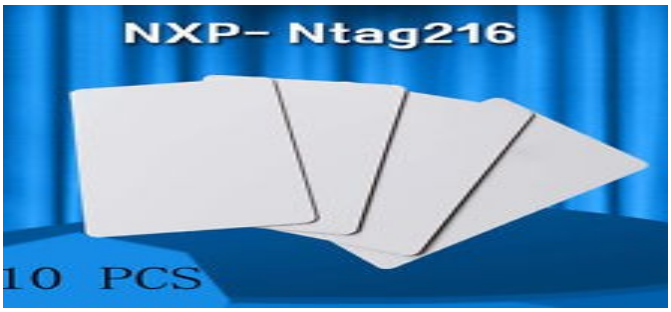
Other voter related issue also include the voter might not be able to reach to local polling booths he might at the far location from his local place. In that case the vote might get lost to avoid this e-voting provides the way to give vote from any location across the country. Some of the more voter related requirements such as convenience, must eliminate all physical restrictions and decrease the number of voters having to learn too complex techniques in order to vote.

Critical requirement related to the security of the e-voting systems have to be considered to provide vote security in the term of vote fraud ,vote for others, duplicate vote and voter coercion. An voting scheme must protect the privacy of the voter at the time of casting the vote . An evoting scheme should not have assumption and requirements that may be difficult to implement on a large scale. This in turn satisfies practically and scalability properties .Voters should be able to verify that their votes are correctly counted for in the final tally. Voters should not be able to be modified .Another desirable property is the voters mobility; that the voter need not be restricted to a certain geographical region to cast his vote.

II. RELATED WORK

A.NFC

NFC stands for near field communication as its name suggest it is used for the communication within short range between two compatible devices. This requires at least two devices one for sending the signal and another for receiving the signal. A range of devices can use the NFC standard can be considered as the passive or active depending on their way of working. The passive devices having tags another small devices can able to sends the information other HFC devices without using their own power source. However they cannot process the information sent from other source, and can't connect to other passive components. They often takes forms of the interactive signs on the wall or advertisement.



Fig[1].NFC chip

Active devices can able to send data receive data with each other or can able to communicate with each other or with passive devices. Smartphone is the most common implementation of the NFC active devices .Fig[1] shows how NFC looks .

NFC technology is pretty common these days and features in most high end smartphone. As well as phone to hone communication, small little NFC tag can be used to store and transfer information. These tag can store wide range of information , from short line of text , such as web address or contact details to link the apps in the google store. It's a quick and efficient way to quickly push he information to your phone and these little tag can replace bar and QI codes, and could even be used instead of Bluetooth in some cases.

B. Working Of NFC Tag

NFC tags are passive devices, which means they operate without power supply of their own and are reliant on the active devices to come into range before they are activated. The Trade-off here is that these devices can't do any processing of their own, instead they are used to transfer information to an active devices, such as smartphone.

In order to power these NFC tag electromagnetic induction is used to create current in the passive devices. In these coils of wires are used to produce electromagnetic waves, which can be then picked up and turn back into current by another coil of wire. This is very similar to the techniques used for wireless charging technologies, albeit much less powerful. The active devices such as smartphone, are responsible for generating the magnetic field. These is done by the simple coil of wire, which produces the magnetic field perpendicular to the flow of the alternating current in the wire. The strength of the magnetic field can be adjusted by varying the number of turns in the coil of wire, or increasing the current flowing through the wire. However increasing current will requires more energy , and very high power requirement would not desirable to use in the mobile technologies. Hence why NFC operate over just a few inches, rather than many meters.NFC tag communicate using the ISO 14443 type A and B wireless standards, which is the international standard for contact-less smartcards use on many transportation system. This is why NFC devices can be used with existing contact-less technologies, such as card payment point.

C. Security Using NFC Chip

NFC chips are very tiny read-only chips that can appear in the informational poster and identification document, such as corporate budges or passports. NFC also can be used to connect to secure networks without having to enter into the complex authorization code. User can tap an NFC to wireless router and after the NFC chip confirm your identity, tablet is cleared to connect to the much faster WiFi signals so that you can get to the work. NFC is fundamentally secure by virtue of its extremely short range. In order to snag your NFC signal, a hacker would need to be very close to you. Uncomfortably close, which some difficult.

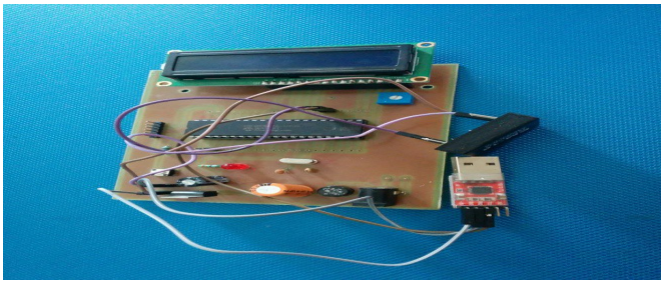
Security experts stress that NFC doesn't come loaded with built-in hardware-driven security measures. NFC is just a platform establishing communication between two devices. But NFC's short range, in sense, serve as a safeguard against hackers. In order to grab NFC signal from thin air(called eavesdropping), an attacker would have to accomplish few critical things. First he did have to be close enough. Well, the NFC functions on the device only go into active mode when you want hem to. NFC signals are extremely sensitive to the in terms of directions. So sensitive that if you turn on your device just slightly, it won't be able to read NFC tag. For a hacker to illicitly grab your signal he did have to somehow maneuver a hacking device's antenna into precisely rightly angle.

III. ARDUINO AND NFC INTERFACING

Near field communication are protocols that electronic devices use to communicate and transfer data between each other. Near field communication devices have to be very near to each other, usually between 10cm, but the range can vary depending on the device that is transmitting and the size of the tag. NFC tags require no power input whatsoever. They use magnetic induction between two between two small loop antennas. The tags these days carry between 96 and 4,096 bytes of information.

It is important that the NFC Tags are rewritable, otherwise this won't work. Fig[2] show actual practical implementation of interfacing.

To test whether what we wrote on the tags was successful, we can test with the Arduino or with an NFC-enabled phone. Most smartphones running Android should be able to read NFC tags, and I will be testing with a Nexus 5. Unfortunately for iPhone users, the only iPhones that supports NFC are the iPhone 6 and the 6s, but they do not support NFC tag reading so just use the Arduino to test out what your tag has written on them. iPhones only us their NFC capability for apple pay, therefore you cannot use them to read tags or anything else. Once we have all the part together, we need to install two libraries that will make the reading and writing on tags possible. The libraries are don / NDEF and Seeedstudio's, the one we will be mainly using is don's since Seeedstudio's library is used if you have the Seeedstudio NFC shield. We will install it as a library just in case. You have to download and install both libraries u-sing Arduino's "Add .zip Library" under Sketch >> Include Library. Make sure to install both libraries separately and under the default Arduino directory otherwise you will have compiling errors. Start the IDE and you should have a new sketch file. Save your new file under any name that you chose, like "Read NFC Tag." The first files that you will have will be the header files and they will be the following. They will go before the void setup().



Fig[2].Arduino circuit for NFC interfacing.

IV.VOTING PROCESS

1.Pre-Election Phase:

voter has to go at the remote polling booth and register himself with the personal phone number and the e-mail address. In the similar manner candidate Registration will be done.

2.Election Phase:

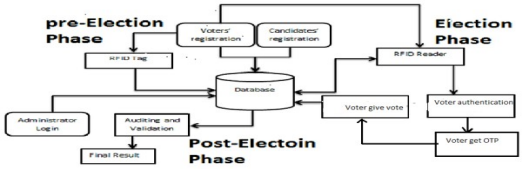
On the election day voter have to scan the NFC chip and he will get one private key as a OTP .voter will have to use same private key as a password while login.

After login one web portal with the different parties name with respective symbols will be generate.

voter has to choose one of it and click on vote button. The app will be close for 24 hours

3.Post-Election Phase:

vote of different parties will be calculated and result will be generated.



Fig[3].e-voting system architecture

Fig[3] given above shows the complete voting process. The scheme satisfies eligibility and authentication properties ; only voters satisfying the voter's requirements are listed in the registration database and only voters are listed in the database are allowed to vote. The scheme satisfies uniqueness and non-reusability; no voter should be able to vote more than once, No one can change or duplicate someone else's vote. This can be done by sealing the encrypted digital representation of the vote in digital envelop signed with the polling station public key. Secure audit logs should be implemented on the remote database server where the digitally signed envelops are stored to prevent undetected tampering or deletion which will in turn satisfy the integrity property.

The privacy property is satisfied through the use of voting booths present at the polling stations. Convenience property is satisfied since the voter would cast the vote with minimal equ-ipment and skills without having to learn too complex techni-ques in order to vote. Voter should able to possess a general understanding of the whole process thus satisfying transparency property. After voting, the voter is not involved in any other post vote process satisfying walk away property.

The incoercibility property is conditionally satisfied since the voting receipt prevent the voter from proving to other how he voted. The scheme satisfies the flexibility property and can be used for several types of election such as

approval voting. The scheme has no special requirement that limit its implementation and use therefore it should be affordable in terms of hardware and maintenance. This intern satisfies cost effectiveness property.

Verifiability Participation property ensures that it is possible

To find out whether particular voter has participated in the election by checking database.

Efficiency property focuses on avoiding too many steps to reach to the goal of the voting process. The use if the e-voting scheme avoided the use of the too complex techniques such as anonymous channels to provide scheme simplicity through the use of public key cryptography, which in turn increases its efficiency relative to other schemes that use anonymous channels. Scheme implementation will further verify the efficiency property.

V. FUTURE WORK

The e-voting using NFC chip scheme should be expanded to accommodate all aspect of a full e-voting experience to form a fully functional electronic voting system. The e-voting using NFC should be implemented using finger print security to provide more security. A full mathematical model of the key security properties of the scheme and its resistance to well-known security attacks is the subject of ongoing research.

I. VI. CONCLUSION

This paper described a protocol allowing a portable e-voting system. To carry it out, users only need to remember a previously issued login/password pair. This will lower the bar for users partaking in online voting, as they will no longer need any special devices to take part in the process. Considering the substantial growth experimented by the global network of digital certificates, this paper propose a mechanism whereby a user is able to use a certificate specially crafted for each votation. The issued keys allow them to keep their anonymity all through the voting process using NFC tag. The protocol uses a secrets store and oblivious transfer to carry out the key exchange. To optimize their implementation, we have optimized the computation of the keys involved in the process of e-voting. The described protocol is limited in that for each new voting process its public key must be distributed anew. However, it does not happen so with each user's login and password.

REFERENCES

[1] R. L. Rivest, A. Shamir, and Y. Tauman, "How to leak a secret," in Proceedings of the 7th International Conference on the Theory and Application of Cryptology and Information Security: Advances in Cryptology, ser. ASIACRYPT '01.London, UK: Springer-Verlag, 2001, pp. 552–565. [Online].Available: http://dl.acm.org/citation.cfm?id=647097.717015

[2] S. S. Xia, Z., "A new receipt-free e-voiting scheme based on blind signature," inWorkshop on Trustworthy Elections, ser. WOTE 2006, Cambridge, UK, 2006, pp. 14–28.

[3] I. Damgard, M. Jurik, and J. B. Nielsen, "A generalization of pailliers public-key system with applications to electronic voting,"Inf.Secur., vol. 9, no. 6, pp. 371–385, Dec. 2010. [Online]. Available:http://dx.doi.org/10.1007/s10207-010-0119-9

[4] B. Lee and K. Kim, "Receipt-free electronic voting scheme with a tamper-resistant randomizer," inProceedings of the 5th international conference on Information security and cryptology, ser. ICISC'02. Berlin, Heidelberg: Springer-Verlag, 2003, pp. 389–406. [Online].Available: http://dl.acm.org/citation.cfm?id=1765361.1765396

[5] I. Rayand N. Narasimhamurthi, "An anonymous electronic votingprotocol for voting over the Internet,"Proc.Third International Workshop on Advanced Issues of E-Commerce and We-Based Information Systems (WECWIS 2001),San Jose, CA, USA2001pp.188190.

[6] H.Pan .E. Hou, and N.Ansari, E-NOTE: "An E-voting system that ensures voter confidentiality and voting accuracy,"Proc.2012 IEEE International Conference onCommunicationsOttawa, Canada, June 1015 2012pp.825,829.

[7]EAC, "Voluntary Voting System Guidelines 1.1 - Volume 1," The U.S. Election Assistance Commission, Tech. Rep., 2009. [Online]. Available: http://www.eac.gov/assets/1/workflowstaging/Page/124.PDF

[8] W. Pieters, "Combatting Electoral Traces: The Dutch Tempest Discussion and Beyond," inE-Voting and Identity, ser. Lecture Notes in Computer Science, P. Y. Ryan and B. Schoenmakers, Eds. Springer Berlin / Heidelberg, 2009, vol. 5767, pp. 172–190.

[9] Recommendation Rec(2004)11 and explanatory memorandum - Legal, operational and technical standards for e-voting, Council of Europe,2004.

[10] V. Hartmann, N. Meissner, and D. Richter, "Online VotingSystems for Non-parliamentary Elections - Catalogue ofRequirements," Physikalisc Technische Bundesanstalt Braunscheigund Berlin, Laborbericht PTB-8.5-2004-1, 2004. [Online]. Available:http://ib.ptb.de/8/85/LB8520041AnfKat.pdf

[11]M. Volkamer, "Requirements for electronic voting machines," in Eval-uation of Electronic Voting, ser. Lecture Notes in Business Information Processing, W. van der Aalst, J. Mylopoulos, N. M. Sadeh, M. J. Shaw,and C. Szyperski, Eds. Springer Berlin / Heidelberg, 2009, vol. 30,ch. 5, pp. 73–91.

[12] K. Gandolfi, C. Mourtel, and F. Olivier, "Electromagnetic Analysis: Concrete Results," inProceedings of the Third International Workshopon Cryptographic Hardware and Embedded Systems (CHES), ser. CHES'01. London, UK: Springer-Verlag, 2001, pp. 251–261.

[14] M. Kuhn, "Electromagnetic Eavesdropping Risks of Flat-Panel Displays," inPrivacy Enhancing Technologies, ser. Lecture Notes in Computer Science, D. Martin and A. Serjantov, Eds. Springer Berlin /Heidelberg, 2005, vol. 3424, pp. 88–107

[15] T. Okamoto, "An electronic voting scheme," in Proc. IFIP'96, 1996, pp. 21,30.

[16] J. Cohen and M. Fisher, “A robust and verifiable cryptographically secure election scheme,” in Proc. 26th IEEE Symp. Found. Comput. Sci. (FOCS’85), 1985, pp. 372-382

[17] M. Hirt and K. Sako, “Efficient receipt-free voting based on homomorphic encryption,” in Proc. Adv. EUROCRYPT’00, 2000, vol. 1807, LNCS, pp. 539–556.

[18] C. A. Neff, “A verifiable secret shuffle and its application to e-voting,”in Proc. 8th ACM Conf. Comput. Commun. Security (CSS’01), 2001,pp. 116-125

[19] B. Randell and P. Y. A. Ryan, “Voting technologies and trust,” IEEESecurity Privacy, vol. 4, no. 5, pp. 50–56, Sep./Oct. 2006.

[20] Araújo, Roberto. "Improving the Farnel, Threeballot, and Randell-Ryan Voting Schemes." IACR Cryptology ePrint Archive 2008 (2008): 82.

.