International Journal of Scientific Research and Engineering Development-– Volume 2 Issue 6, Nov- Dec 2019

Available at www.ijsred.com

RESEARCH ARTICLE OPEN ACCESS

Secure Verifiable Mobile Voting Based On Kerberos Mechanism

Abdullahi Yahya Imam

(Department of Information Technology, Bayero University, Kano, Nigeria)

Email:ayimam.it@buk.edu.ng

----------**********----------

Abstract:

Recent technological breakthroughs make the use of mobile smartphones in our daily lives so ubiquitous. Democratic systems mostly depend on elections to provide teeming electorates the right to vote for their leaders or to express their views in referendums. In literature, several electronic voting systems from standalone to mobile were proposed. However, a valid and usable electronic voting system supposes to meet some requirements among which vote verifiability is a challenge to many of the current systems. Thus, this paper proposes a mobile phone e-voting system based on Kerberos authentication mechanism which achieves vote verifiability using a cryptographic tag each voter produces independently. The proposed system uses secure symmetric key cryptography to fit the most used mobile devices' performance.

Keywords —electronic voting, verifiability, cryptographic tag,Kerberos authentication, two–factor authentication.

----------**********----------

I. INTRODUCTION

The advent of smartphones made mobile voting a research area. Nowadays people use smartphones in their daily activities such as mobile banking, online shopping and many more. Thus, mobile voting should also not be an exception. Recently, several works propose different mobile phone voting schemes. Unlike traditional voting system, known as paper-based, electronic voting provides platform where electronic devices are used to carry out the tasks. It is not vague that paper-based schemes could have less performance and accuracy than electronic voting system. Certainly, electronic voting protocol has some additional requirements compared to traditional paper–based schemes. An ideal voting protocol of secure electronic voting has the following requirements [1]:

(a) Only authenticated and authorized voters can cast vote in an election.
(b) The system does not allow anyone to cast vote more than once.
(c) Neither voting authority nor election participant can determine for whom anyone else voted.
(d) There is no way someone's vote can be duplicated.
(e) Any change to voter's choice can be detected.
(f) Every voter can make sure that his vote has been taken into account in the final tabulation.
(g) Everyone knows who voted and who didn't.

In addition to these, mobile voting also needs internet connection. Thus it is prone to more security challenges than standalone ones. If implemented successfully, mobile votingsystem would provide more flexibility and mobility compared to a standalone electronic system which requires the presence of the voter at the voting

booth. It also allows a voter to cast his vote from his convenient location as long as the Internet service is available therein. Among the above mentioned requirements, vote verifiability—every voter can make sure that his vote has been taken into account in the final tabulation and everyone knows who voted and who did not vote—happens to be a challenge to many electronic voting systems. Popoveniuc et al. [2] describes end–to–end verifiable election as one which meets the following performance requirements.

a) The representation of the voter's choices on the ballot agrees with the representation that will be read by the rest of the election system.
b) Cast ballots do not contain over-votes or negative votes.
c) The ballot the voter cast is the one that was received and saved by the voting system.
d) No ballots are included in the final tally that could not have been checked by at least one voter.

In order to achieve some of the stated requirements, there are some proposed schemes that enable the voter to retrieve his vote from voting authority to ensure it is recorded as voted. But such schemes could be vulnerable to buying and selling of votes as the buyer can ensure that the seller votes as promised. To mitigate such scenario, some receipt-free schemes were proposed which make it impossible for a voter to reveal the way he voted [1].

This work proposes a mobile phone voting scheme that enables vote verifiability as well as eliminating buying and selling ofthe votes. Thus, this scheme is in between the above two mentioned schemes. It uses some of Kerberos authentication mechanisms along with a cryptographic tag.

The remainder of this paper is organized as follows. Section 2 provides literature review of the related works. Section 3 states the design goals, while section 4 explains the proposed model and design. Section 5 gives justification of the design goals of the proposed model. Section 6 draws conclusions.

II. LITERATURE REVIEW OF THE RELATED WORKS

This section reviews some related works from standalone electronic voting to fully mobile phone voting systems. In literature, several attempts were put in place to achieve deployable electronic voting systems. Chaum proposed the verifiable electronic voting scheme using blind signature [3]. Recently, [4] came up with a way based on blind signature and Kerberos mechanism to provide a lightweight scheme by removal of the Certificate Authority and the use of symmetric key algorithms throughout the system. Blind signature schemes can provide secrecy and individually verifiable (every voter can make sure that his vote has been taken into account in the final tabulation) but does not support universal verifiability (everyone knows who voted and who didn't).

Kazue and Joe [5] present a receipt-free scheme that facilitates both individual and universal verifiable voting protocol. The scheme is based on the mix-type voting technique that uses collection of servers to shuffle the encrypted votes till the relationship between the voter and vote is hidden. Such scheme is categorized as inefficient for large scale voting as it incurs high computational overhead.

In 2013 Estonian local municipal elections and the 2014 European Parliament elections a scheme known as Verifiable Internet Voting in Estonia was used [6]. The scheme allows the voters to check the cast-as-intended and recorded-as-cast properties of their vote by using a mobile device. The voter retrieves the encrypted vote from the voting server then applies some cryptographic calculations to verify. This provides individual verifiability only. Moreover, it requires the voter to use two different devices-one for voting and the other for verification processes- and yet it is vulnerable to buying and selling of votes as the buyer can make the voter to prove what he voted for.

Besides the aforementioned, there are some proposed mobile voting schemes in the literature [7], [8], [9] and [10]. Based on my survey, most of them do not concentrate on vote verifiability rather

than authentication and confidentiality.

III. DESIGN GOALS

From the literature survey, existing mobile voting schemes mostly do not provide solution to vote verifiability. As discussed, they mostly propose solutions to authentication and authorization alone. Considering its importance in achieving free and fair election, this work suggests a mobile voting scheme that meets the following requirements:

1. Efficient use of secure symmetric cryptographic algorithms to suit most mobile devices performance.
2. Only authenticated and authorized voters can vote.
3. No one can determine for whom anyone else voted.
4. Every voter can make sure that his vote has been taken into account in the final tabulation.
5. Everyone knows who voted and who didn't.
6. Cast ballots do not contain over-votes or negative votes.

IV. PROPOSED SYSTEM MODEL AND DESIGN

This section describes the model of the proposed voting system with detailed explanation of how it works. The scheme is mainly made of the following phases: two-level voter authentication, secure cryptographic tag generation and vote, vote tabulation and verifiability. Fig.1 contains the architectural design of the proposed system.

Voter Authentication Server (*VAS*) has the database of registered voters before the Election Day. The database maintains Voter Card Number VCN which identifies a voter, registered mobile phone and secure password of each voter.

VAS follows these steps to determine an eligible voter in the election period:

a. A prospective voter (V) sends his plaintext *VCN* to V*AS* which decides eligible of the voter.
b. *VAS* sends identity authentication SMS to only eligible voter's registered phone number.
c. The voter uses his password, generates symmetric key Kp to encrypt the identity authentication code received and sends it via Internet to *VAS*.
d. *VAS* generates similar symmetric key Kp from corresponding voter's password in its database and decrypts the identity authentication code.
e. *VAS* then generates a unique symmetric voting key Kv, encrypts it with Kp and sends to a successfully authenticated voter.
f. It also sends the copy of that Kv to Voting Box Server *VBS*.

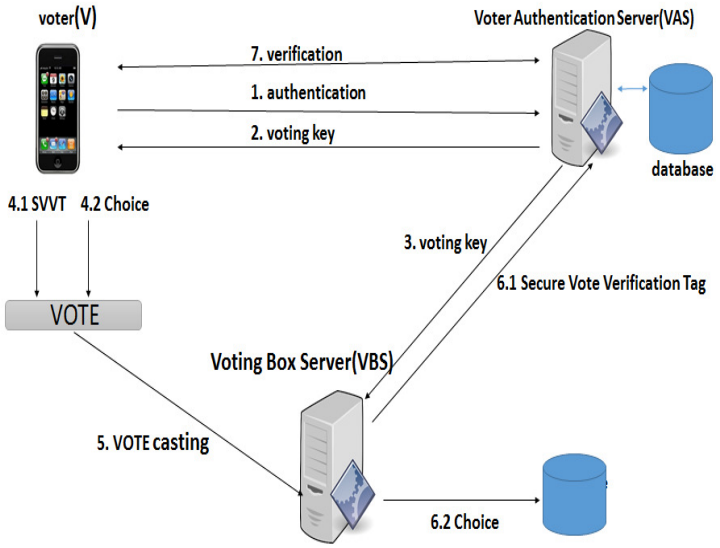

Fig.1 Architecture of the proposed system

4.1 Voter Two-Level Authentication Phase

4.2 Generating Secure Vote Verification Tag and VOTE Phase

The ability of each and every voter to securely produce a unique and easily identifiable tag that does not reveal confidential information about the candidate he elected is the substantial stage to achieve vote verifiability in our scheme. In the election, every voter generates such tag and attaches to his chosen candidate. We termed this tag as *SVVT (*Secure Vote Verification Tag). Each voter

prepares SVVT and casts his vote using the following *VOTE Preparation:*

$$Generate\ Random\ Number, R \quad (1)$$

$$PreTag = E(Kv)\{R\} \quad (2)$$

$$SVVT = Hash(PreSVVT) \quad (3)$$

$$VOTE = E(Kv)\{Choice \,||\, SVVT\} \quad (4)$$

Algorithm:

Description of the above algorithm:

a. *Random Number Generation:* voter generates random number *R*.
b. *Pre-SVVT:* voter uses his given Kv to encrypt *R*.
c. *SVVT: voter takes the SHA-2 of the Pre-SVVT.*
d. *VOTE:* voter combines the copy of his *SVVT* to the candidate and encrypts with Kv. He then sends it to *VBS.*

4.3 Vote Tabulation and Verifiability Phase

Once VBS receives a *VOTE* from a voter, it applies the corresponding Kv it receives from VAS to decrypt that vote. It then tallies the valid vote as follows:

$$VOTE = D(Kv)\{Choice \,||\, SVVT\}$$

a. VBS takes the choice into tabulation and sends the SVVT to VAS via secure channel.
b. VAS then marks voter as voted and records the SVVT for the respective voter. It also sends the SVVT copy to the voter to verify.
c. When the election time is over, VAS announces publically the voters with their respective SVVT and voting status (either voted or not voted).
d. On the other hand, VBS also independently announces the candidates with their respective tallies.
e. Individuals and publics can use the two independent releases from VAS and VBS to validate the election result.

V. JUSTIFICATION OF OUR STATED DESIGN GOALS

This section discusses the justification and analysis of our design goals. The syste implemented in Java programming for Android platforms.Following are the design goals along with their corresponding validations.

a. ***Efficient use of Symmetric Cryptographic Algorithms to Suit Most Mobile Devices:***

Using algorithms that can perform efficiently is of paramount importance to our proposed system. Basically, Kerberos release from MIT uses Data Encryption Standard (DES) algorithm. Due to short key length and some other security challenges, Nowadays DES is considered as less secure. SinceI incorporate some of Kerberos authentication mechanisms into the work and at the same it wants achieve high security, I use Advanced Encryption Standard (AES-128) algorithms rather than DES. However, to determine the performance overhead that AES128 can incur compared to DES, I implemented and tested the work using both the DES and AES128 algorithms. Table 1 contains the results of the measurements.The test was performed on some of the commonly used android devices.

Table 1 Sampled Devices and Measurements

Device Model	Processor	RAM	Android OS Version	DES: Vote Preparation Time (in Micro second)	AES-128: Vote Preparation Time (in Micro second)
Samsung GT-S531F	1.2 GHz Quad Core	1GB	5.1.1	2546	3690
Samsung SM-G360H	1.1GHz	1GB	4.4	3070	3787
HTC Desire 626	1.7 GHz Octa-core	2GB	4.4.2	2912	3575
Samsung SGH-I747	1.5GHz Advanced dual Core	2GB	4.4	2872	3377

We recorded the *VOTE Preparation Algorithm* running time on the devices whose specifications are as in Table 1.

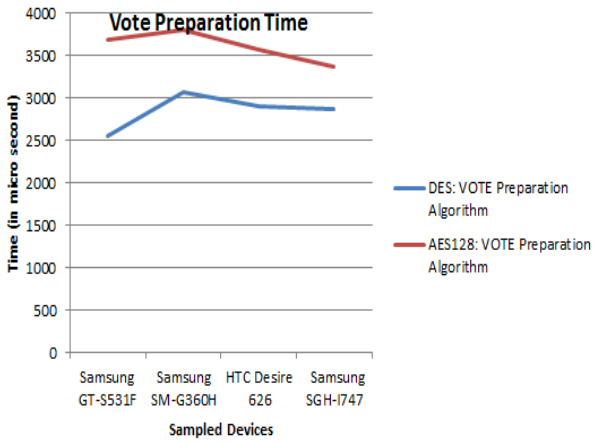

Fig.2 Performances graph for DES & AES-128

Based on this result, it is clear that the performance overhead incurred by AES128 is more affordable compared to basicDES.Thus, the proposed system can perform well on commonly used Android smartphones.

b. ***Only Authorized Voters Can Vote:***each voter authenticates himself with V*AS* before getting the voting key which serves as a ticket to cast vote in *VBS*. Sending authentication code to voter's mobile phone along with using his/her password for encrypting furthercommunications between V*AS* and a voter proves that only the outright owner of the phone and the password can authenticate successfully.

c. ***No One Can Determine For Whom Anyone Else Voted:***the separation of the voting system into V*AS* and *VBS* enables each entity to maintain some specific information that helps accomplish this goal. V*AS* maintains the voters' database and acts as voting-key generator as well. It does not have access to the votes throughout the election. Meanwhile, the *VBS* which receives encrypted votes from voters does not have access to the voters' database residing in *AS*. Thus, it does not know detailed identity of the voter. It only knows the voting key that can decrypts the received vote.

d. ***Every Voter Can Make Sure That His Vote Has Been Taken Into Account In The Final Tabulation:*** a voter prepares *VOTE* and sends to *VBS* which decrypts and separates it into *choice* and S*VVT*. It then tallies the valid voter's choice.

e. ***Everyone Knows Who Voted And Who Didn't:***from the information V*AS* releases, voters can compare the list of the voter with tallies from VBS. Every voter must find his exact SVVT in VAS list. Everyone can check the list from V*AS* to determine who voted. If need arises, anyone can ask the voters to submit their S*VVT* to verify no one is missing from the list.

f. ***Cast Ballots Do Not Contain Over-Votes Or Negative Votes:***the independent results from VBS must follow the result VAS releases. An inconsistency in the two separate information leads to invalid result.

VI. CONCLUSION

This paper describes a verifiable mobile voting system that incorporates some of Kerberos authentication mechanisms. It explains how to achieve secure voter authentication using some of Kerberos mechanisms which employ two-factor authentication. This work achieves its main target, both individual and public vote verifiability, using a cryptographic tag that does not reveal information about the voter's choice rather than enabling him to track his vote. Finally, majority of currently used android devices can also support the proposed system with less performance overhead.

REFERENCES

[1] S. Bruice, *Applied Cryptography: Protocols, Algorithms, and Source Code in C (2nd ed.).* (Sharda OffPress, Delhi:Wiley), (2001). p.121.

[2] S. Popoveniuc, J. Kelsey, A. Regenscheid and P. Vora, "Performance requirements for end-to-end verifiable elections", In Proceedings of the 2010 international conference on Electronic voting technology/workshop on trustworthy elections, (EVT/WOTE'10, 2010). p.1-16.

[3] D. Chaum, "Untraceable electronic mail, return addresses, and digital pseudonyms" (Communications of the ACM, 1981), pp. 84-88.

[4] Z. Hongyu, Y. Qianzi and Z. Junxing, "A lightweight electronic voting scheme based on blind signature and Kerberos mechanism", IEEE 2015, pp. 210-214.

[5] S. Kazue and K. Joe, "Receipt-Free Mix-Type Voting Scheme --A practical solution to the implementation of a voting booth", Advances in Cryptology—EUROCRYPT '95 Proceedings, (Springer-Verlag, 1995), pp. 393-403.

[6] H. Ven and W. Jan, "Verifiable Internet Voting in Estonia", Proceedings of 2014 International Conference on Electronic Voting EVOTE 2014, (E-Voting.CC GmbH, 2014), pp. 1-7.

[7] P. Deniel and A. S. Dan, "A Hybrid Mobile Biometric-Based E-Voting System",Proc. of the 9th International Symposium on Advanced Topics in Electrical Engineering, May 7-9, 2015, (Bucharest, Romania, IEEE, 2015), pp. 37-42.

[8] K. Adel, G. Yasmin, S. Dima, M. Dalya and Shastry P.V.S, "M-Vote: A Reliable and Highly Secure Mobile Voting System",Proc. of 2013 Palestinian International Conference on Information and Communication Technology, (IEEE, 2013), pp. 90-98.

[9] K. A. Hussein , S. I. Mohammad and M. D. Omar, "Secure Internet Voting System based on Public Key Kerberos" , Proceedings of IJCSI International Journal of Computer Science Issues, (Vol. 9, Issue 2, No 3, 2012), pp. 428-434.

[10] U. Mohib, I. U. Arif, Noor ul Amin and Nizamuddin, "An Efficient and Secure Mobile Phone Voting System", (IEEE, 2013), pp. 332-336.

