ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 9, September 2016

A Survey on Secure eVoting platform for QoE Evaluation

Aishwarya D. Jagtap

Student of BE(Comp), All India Shri Shivaji Memorial Society's, College of Engineering, Pune, India

ABSTRACT: The internet usage is increasing day-by-day. This makes the use of internet for voting necessary as it provides ease and availability. In order to make the voting system secure, the ring signatures are used. The linkability feature of ring signatures proves to be a boon in giving security and is useful tool for information gathering in QoE evaluation. It also makes possible to link different ballots without the loss of anonymity and helps to check the changes in opinion of the user. The 'linking tag' parameter of signatures is generated to identify multiple votes sent by a single voter that adds as a characteristic in e-cognocracy and QoE evaluation.

KEYWORDS: linking tag, ring signature, secure eVoting, QoE.

I. INTRODUCTION

In the mid of last century different mechanical methods like punch cards, methods for optical reading of votes and later Direct Recording Electronic (DRE) [1] that avoided the need of counting votes. Further, Internet made possible to have different kinds of eVoting that did not require voters at the polling stations. Internet eVoting includes the polls found in websites. To provide security there were also systems that required the user to register before voting. There were also systems that required identifying the user in the platform only then could the voter cast the voting. It included open-ended or close-ended questions. With the increasing popularity of Internet, different methods have been implemented to know the user's opinion. The surveys are very popular in the Internet which is done mostly in online newspapers, social networks, forums. They are used for informative purpose and gathering opinion of the reader about a topic. In real voting process the information should me hidden to maintain anonymity.

The different voting systems proposed before did not satisfy the secure eVoting requirements [2]. Hence, various e-voting systems were developed that used the suitable protocols: blind signatures [3] mix-nets [4], homomorphic encryption [5,6] and ring signatures [7] that provide anonymity by using cryptography, net servers that prevents link formation between the voter and the ballot.

In order to look for trends in ballot and tracking the changes in the opinion of user there is a need to link the ballots. When the ballots are linked there are chances of losing the anonymity and/or the link breakage. To satisfy the use of *linkable spontaneous ring* (LSR) signatures [8] a system is described [9]. The parameter of 'linking tag' allows linking throughout the different rounds of voting. But it is not possible to link across different votings.

This mechanism is an emergent democratic system, e-cognocracy [10], which uses ICT for achieving an active participation of citizens in the decision-making process of the government. e-Cognocracy also requires tracing the users' opinions and the creation of different groups of voters carrying different weights. As the system is based on LSR signatures, it can establish a relation among voters and their ballots. This is a very powerful mechanism to perform secure polls with high quality information sources within a marketing environment [11]

Keeping in mind the current situation of the Internet popularity, there is a need of e-voting system that provides the advantage [12] of voting from offices, home, work places with the help of smartphones, tablets. These can provide facilities that allows the user outside municipality to vote, increase the participation of youth as they are familiar with the Internet technologies, avoids long queues and ultimately saves time and temporary restrictions can be relaxed.

In order to implement a system compliant to the specific requirements of the protocol described in [9], it is necessary to develop both the administrator of the system software (server) and the user's program (client). We chose a web browser and android system as the tool to perform the voting. The only usefulness about the eVoting process will be when the system asks the password protecting users private key. Besides, using web browser as the way to collect QoE information is very useful as it allows introducing multimedia content within the poll and provides an integrated eVoting environment as described in [11].

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 9, September 2016

The whole system discussed [13] is free and open source software(FOSS). There are five elements that form the basis of the model. They are: Firstly, the *user administration module* that keeps the track of the users' management, registration and data modification; loading of certificates and coordination with accepted Certification Authorities (CAs). Second, the *voting administration module* manages the different voting processes stored in the server. This module keeps the census of users which can participate in the voting, the number of rounds, the duration of the voting process, the ballot box, etc. Third, the *connection and verification module* connects the voter and the administration module, selecting the voting to be accessed by the user, and verifying the conditions, so as to permit or deny the access. Fourth, the *client module* which is to be utilized at the user's device (smartphone and web pages). It is in charge of the cryptographic calculus required for the emission of the vote, and for its sending, through the connection module, to the "electronic ballot box".Fifth, the key generation module that performs the key and certificate calculations required to identify the user. The remaining of the article is organized as follows: In this Section II we discuss the work related to the electronic voting systems and the different protocols in which secure eVoting systems are based. In Section III we analyse in detail the proposed protocol in [13], describing each of its blocks. In Section IV signature and information management for QoE Evaluation is discussed. The paper ends with the conclusions and the future work lines in Section V.

II. SECURE EVOTING SYSTEMS

A. WORK RELATED TO EVOTING SYSTEMS

In the first case, an eVoting system has been employed in Estonia since 2005, for both local and national elections. The use of this system has increased his penetration [14], which supposed 24 percent of the total votes cast in the elections in 2011. In Switzerland [15], eVoting has been used for more than ten years. At the beginning, the number of citizens able to use the system was limited to 20 percent in a canton, and to 10 percent in the whole country. Nowadays, the penetration rate is 30 percent in a single canton. The experience with eVoting in Norway [16] started during the local government elections in 2011 and 2013, and it was also used in the parliamentary elections [17].

In [18] an implementation which enables the participation by means of a web browser or SMS, using a login/password user identification is defined. In [19] an eVoting system was developed, based in mobile devices, using the SIM of the used phones by means of symmetric keys and an SMS-based system.

In [20] the cloud-based system was implemented allows cost reduction and increases flexibility at the same time but lacked security. For the system to be secure it should have basic properties and some advance requirements. The basic requirements include privacy, completeness, soundness, reusability, eligibility, fairness as discussed in [2]. The advance requirements are Robustness; Universal verifiability; Receipt-freeness; Incoercibility where robustness includes that if some module fails the whole system is not affected. Receipt free ensures that the voter should not carry any receipts and lastly incoercibility assures that n person is forced to cast a vote under pressure of third parties.

B. DIFFERENT EVOTING SYSTEMS

Depending upon the cryptography and security the eVoting systems can be classified as:

-*Blind signatures* [23]: In a blind signature process, each voter sends to an authority its ballot obfuscated in such a way that its content cannot be known. This authority then verifies that the voter is eligible to vote and signs the obfuscated ballot. When the voter gets back his ballot signed by the authority, undoes the obfuscation and sends it to the ballot box together with the authority's signature. Finally, the ballot box checks the ballot and the signature and, if everything is correct, adds the vote to the tally.

-*Mix-nets* [24]: these eVoting systems use secure servers (known as mixes), that receive as an input a set of votes, and generate as an output the same set of votes, but disordered. Two different methods for cyphering the voting information can be employed: the information can go cyphered through the whole set of mixes to traverse (known as cascade or series of mixes), or a re-encryption system can be used, as proposed in [25].

-*Homomorphic encryption* [26]: It is used for voting based on referendums. Homomorphic cyphering is limited to basic operations as addition and subtraction hence, adequate for referendums.

- *Ring signatures* [7] is advancement of group signatures [21]. Ring signatures do not require manger that can deploy the anonymity, thus be spontaneous (i.e. no previous preparation is required). Later, ring signatures which allow linking together different votes of the same user were developed [22]. The weak point of these signatures was its length, which increased linearly with the number of members of the ring. In [8] this problem is overcome and a constant length signature can be obtained with any number of members of the ring.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 9, September 2016

III. PROPOSED ALGORITHM

The eVoting system we are analysing in this paper is based on ring signatures protocol, and in the security descriptions presented in [9]. In addition, to the five blocks mentioned earlier the user needs to incorporate the signature module into the device that is in charge of the cryptographic operations associated to the signature of the vote. The *key generation module* and the *client module* are at the user's side. The first one develops the tasks related to user's voting setup (calculate the private key, create the Certificate Signing Request and the PKCS12 [27], which will be used later by the client module). In the server we can find three modules: *user administration*, *voting administration module connection and verification module*. The modules are explained in [13]. Since as discussed above we need FOSS the different programming languages like Java, MySQL, Firefox, etc. has been used.

A. SERVER

Two servers were used for testing: one for Firefox browser, to be used in netbooks, laptops and desktops, and second specific application for Android smartphones and tablets. Two different profiles have been created for accessing the server, one related to user management and the other for voting management. The user management creates and manages the users' profiles. In addition, they will manage the keys employed when signing the votes to be sent to the ballot box. Thus, even if a single eVoting server is shared, and the ballot boxes corresponding to different voting processes are stored in it, only the administrator of each voting will be able to know the final result. The second group to be managed corresponds to the potential voters included in the platform, i.e. a record including all the eligible users, according to the criteria defined by each voting administrator.

The administrator should introduce name of the voting or query, questions to answer, security parameters, number of rounds and the census of the users who may participate. The administrator will also be able to define different groups, each of them with a different weight if necessary. The question will be edited in HTML, and the only requirement from the platform is that a *getBallot()* function exists, able to take the vote in a string. This string will be signed by the user so as to grant the security of the process as described in [13]

B. PROTOCOL FOR INTERACTION

1) The information about the user (name, identification …) is first uploaded in the database.
2) The user key is generated and to create the public certificate in the PKCS12 file some communications are performed.
3) As soon as the administrator of a voting uploads the parameters to the platform, census with the participants is also uploaded. The voting administrator needs to connect to the user administration module in order to verify the users registered in the platform are in the census the once that are not registered cannot participate in the voting process.
4) When the voting platform is ready the user is connected to the server. The user needs to download the parameters, perform the voting, perform the evaluation and sign the vote with public key of ballot box and send the vote to the server along with the signature
5) Once the server has received the vote and its signature, it verifies the signature and, if correct, sends it to the ballot box.

The ballot box has been included in the same server. It is implemented as a database table, only accessible to the connection and verification module, and stores already verified votes and their attached signatures. Once the voting has finished, the voting administrators verifies the signature again, decipher the votes and proceed with the final accounting.

C. CLIENT

As stated before there are two types of client on which the eVoting can be implemented. For laptops, desktops and PC's Firefox client and for smart phones and tablets Android Client.

Firefox client

The client part has been developed as an extension to the browser. The extension performs all the cryptographic operations providing security to the platform. Once the extension is installed the user will have to send the location and his private key that is stored in PKCS12. The user needs to create new key each time he participates in the survey or voting process or evaluation and send the key along with the signature to the server.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 9, September 2016

D. ANDROID CLIENT

The android client has same functionalities as that of the Firefox client with only difference that once the app is downloaded there is no need of selecting the server address. It is possible that the same terminal can be used by more than one person the app will ask to select the user for adding and will display a username and ask for correctness if correct he will have to introduce the public key and vote. Once the validity is checked the vote will be ciphered with public key of the ballot box and then signed with the users' private key.

IV. SIGNATURE AND INFORMATION MANAGEMENT FOR QOE EVALUATION

As we are making use of ring signatures, the usres' participation list cannot be revealed publically but the list of voter that have voted can be published. If there are duplicate votes the extra recounts can be done later weighting partial tallies to obtain the final result. The linking tag feature is like a boon as it helps in keeping track of the users' opinion and also helps in QoE.

QoE management has three basic steps [28]: understanding and modeling QoE; monitoring and estimating QoE and adapting and controlling QoE. In the first one mean opinion scores (MOS) is necessary based on the evaluation of responses perceived by the user. The value that represents the mean opinion is calculated based on the first step. As QoE and QoS are related [29,30] to the platform discussed here we can ask the users for QoE Evaluation based on the same features. The feature of linkability has provided to be a boon as the user can honestly give opinion without losing anonymity. In future votings, these users will have a higher weight and so it will be possible to obtain a better QoE estimation. Besides, through the analysis of the results, it is possible to make observations, QoE variations along time and with different QoS parameters. This allows the poll administrator to perform a more detailed analysis of the voters' opinions and to feedback the polls with more specific information for each of the groups with similar features.

V. CONCLUSION

The system discussed above satisfies all the characteristics of eVoting system and does not have any flaws. The implementation is of the system includes free and verifiable softwares. It has many features that makes it important for QoE and provides linking of ballot and anonymity at the same time along with analyzing of the QoE evaluation. Moreover, the platform is also suitable for e-Cognocracy. As a future scope more users can be added for testing i.e. to check the scalability of the system and also make the eVoting platform available for iOS and also provide more features for mobile apps.

REFERENCES

[1] T. Kohno, A. Stubblefield, A.D. Rubin and D.S. Wallach: "Analysis of an electronic voting system". In: IEEE Symposium on Security and Privacy. IEEE Computer Society Press, Los Alamitos (2004)
[2] B. Lee and K. Kim: "Receipt-free electronic voting scheme with a tamper-resistant randomizer". In Proceedings of the 5th international conference on Information security and cryptology (ICISC'02), pp. 389 - 406.
[3] Z. Xia and S. Schneider: "A New Receipt-Free E-Voting Scheme Based on Blind Signature" In: WOTE: Workshop on Trustworthy Elections, 2006, pp. 14 – 28
[4] M. Jakobsson, A. Juels, and R. L. Rivest: "Making mix nets robust for electronic voting by randomized partial checking". In Proceedings of the 11th USENIX Security Symposium (USENIX '02), 2002, pp 339 – 353.
[5] A. Acquisti: "Receipt-free homomorphic elections and write-in ballots." Cryptology ePrint Archive, Report 2004/105 (2004)
[6] I. Damgård, M. Jurik: "A Generalisation, a Simplification and Some Applications of Paillier's Probabilistic Public-Key System". In: PKC 2001. LNCS, (vol. 1992), 2001, pp. 119–136
[7] 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 (ASIACRYPT '01), 2001 , pp. 552-565.
[8] P. P. Tsang and V. K. Wei: "Short linkable ring signatures for e-voting, e-cash and attestation". In Proceedings of the First international conference on Information Security Practice and Experience (ISPEC'05), 2005, pp. 48 - 60. DOI=10.1007/978-3-540-31979-5_5
[9] J.L. Salazar, J. Piles, J. Ruiz and J.M. Moreno-Jiménez: "Security approaches in e-cognocracy". Computer Standards and Interfaces, 32 (5–6), 2010, pp. 256–265.
[10] J.L. Salazar, J. Piles, J. Ruiz and J.M.Moreno-Jiménez: "E-cognocracy and its voting process", Computer Standards and Interfaces, 2008, pp 124–131.
[11] Tornos, J.L, Salazar, J.L. and Piles, J. J. "An eVoting platform for QoE evaluation", IEEE International Symposium on Integrated Network Management (IM 2013). Ghent, Belgium, May 2013.
[12] Schaupp, L.C. and Carter, L. "E-voting: from apathy to adoption" Journal of Enterprise Information Management, 18 (5/6) (2005), pp. 586–601
[13] J.L.Tornos, J.L. Salazar, J.J.Piles, J. Saldana, L. CasadesusJ. Ruiz-Mas y J. Fernandez- Navajas "An eVoting system based on Ring Signatures" Dept. of Communication and Electronics Engineering, University of Zaragoza(Spain)

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 9, September 2016

DOI:10.5296/npa.v6i2.5390
[14] Madise, U. and Vinkel, P. "Constitutionality of Remote Internet Voting: The Estonian Perspective". Juridica Internationa XVIII. pp. 4-16 (2011).
[15] Gerlach, J. and Gasser, U. (2009): Three Case Studies from Switzerland: E-Voting. March 2009, Berkman Center Research Publication No. 2009-03.1.
[16] Stenerud, I.S.G, and Christian B. "When Reality Comes Knocking: Norwegian Experiences with Verifiable Electronic Voting." 5th International Workshop on Electronic Voting, EVOTE 2012, Bregenz, Austria, pp. 21–33 (2012)
[17] 2013 elections http://www.regjeringen.no/en/dep/kmd/prosjekter/e-vote-trial/about-thee-vote-project.html?id=597724 (accessed 18.06.2014).
[18] Qadah, G.Z. and Taha,R. "Electronic voting systems: requirements, design, and implementation" Computer Standards & Interfaces, 29 (3) (2007), pp. 376–386
[19] Ullah, M., Umar, A.I., Amin, N.; Nizamuddin, "An efficient and secure mobile phone voting system," Digital Information Management (ICDIM), 2013 Eighth International Conference on , vol., no., pp.332,336, 10-12 Sept. 2013. http://dx.doi.org/10.1109/ICDIM.2013.6693989.
[20] Zissis, D., Lekkas, D. "Securing e-Government and e-Voting with an open cloud computing architecture", Government Information Quarterly, Volume 28, Issue 2, April 2011, Pages 239-251, ISSN 0740-624X, http://dx.doi.org/10.1016/j.giq.2010.05.010.
[21] D. Chaum and E. Van Heyst: "Group signatures". In Proceedings of the 10th annual international conference on Theory and application of cryptographic techniques (EUROCRYPT'91), 1991, pp. 257 – 265
[22] J. Liu, V. Wei, D. Wong: "Linkable spontaneous anonymous group signature for ad hoc groups", in:, ACISP 2004. LNCS, (3108), 2004, pp. 325–335
[23] Chaum, D. "Blind signatures for untraceable payments". In Advances in Cryptology – Crypto '82, pages 199–203. Plenum Press, 1983.
[24] Chaum, D.L. "Untraceable electronic mail, return addresses, and digital pseudonyms". Commun. ACM,24(2):84–90, 1981
[25] Boneh, D. and Golle, P. "Almost entirely correct mixing with applications to voting" In ACM Conference on Computer and Communications Security , 2002 , pp. 68-77 .
[26] Johnson, R., Molnar, D., Song, D., Wagner, D. "Homomorphic signature schemes". In: Preneel, B. (ed.) CT-RSA 2002. LNCS, vol. 2271, pp. 244–262. Springer, Heidelberg (2002).
[27] PKCS #12: Personal Information Exchange Syntax Standard. http://www.emc.com/emcplus/rsa-labs/standards-initiatives/pkcs12-personal-information-exchange-syntaxstandard.htm (accessed 18.06.2014)
[28] T. Hobfeld, R. Schatz, M. Varela and C. Timmerer: "Challenges of QoE management for cloud applications," Communications Magazine, IEEE , vol.50, no.4, pp.28-36, April 2012 doi: 10.1109/MCOM.2012.6178831
[29] H. J. Kim, D. H. Lee, J. M. Lee, K. H. Lee, W. Lyu and S. G. Choi: "The QoE Evaluation Method through the QoS-QoE Correlation Model," Networked Computing and Advanced Information Management, 2008. NCM '08. Fourth International Conference on , vol.2, no., pp.719-725, 2-4 Sept. 2008 doi: 10.1109/NCM.2008.202
[30] H. J. Kim and S. G. Choi: "A study on a QoS/QoE correlation model for QoE evaluation on IPTV service" Advanced Communication Technology (ICACT), 2010 The 12th International Conference on , vol.2, no., pp.1377-1382, 7-10 Feb. 2010

BIOGRAPHY

Aishwarya Deepak Jagtap is a student at the All India Shri Shivaji Memorial Society's, College of Engineering, Pune,. She is pursuing the Bachelors degree for Engineering (B.E Comp) in Pune, India under Savitribai Phule Pune University.