I-voting System using JCJ Protocol

Ashwinkumar Panchal[1], Shailesh Indrale[2], Nitin Jadhav[3], Nandkishor Karlekar[4]

[1,2,3]*B.E Final year student, Sinhgad Institute of Technology, Lonavala, Maharashtra, India*
[4]*professor, Sinhgad Institute of Technology, Lonavala, Maharashtra, India*

***Abstract*: In this paper, The JCJ protocol is used to implement I-voting systems architecture. This system provides security to Internet-voting using different security algorithms (like MD9). In this system there are three types of users that are Administrator, Nominator, voters. Each user has different rights to access the I-voting system. The whole I-voting system is controlled by administrator module. They has to verify voters and nominators application and depend upon verification result decides to accept or reject application of that particular user. For verification of voters and nominator the UID and OTP are used. After registration nominator and voter can check election schedule. On the date of election voter has to vote and can see result on the date of result which is scheduled by administrator.**

***Keywords*: I-voting, OTP(One Time Password), UID(Unique Identification Number).**

I. INTRODUCTION

Many governments are like to introduce latest technology into their voting system. I-voting is system which is for online voting. Security is very important in online voting. Alireza Toroghi Haghighat, Mohammad Sadeq Dousti, and Rasool Jalili proposed an efficient and provably-secure, coercion-resistance e-voting protocol which is focus on security and functional properties, such as correctness, verifiability, receipt-freeness, scalability, and robustness [1].

Remote electronic elections may provide many benefits to democratic societies. They may increase elections turnouts, afford convenience to the voters, and

reduce costs, for instance[9]. But there is risk of using I-voting system one can discourage its use in major political elections. Another big problem is opponent can perform coercion or vote-selling and that may be difficult to identify which is valid vote or which is invalid.

Juels, Catalano, and Jakobsson [2] introduced a more correct requirement for remote elections called coercion-resistance. This coercion-resistance take cares of receipt-freeness requirement as well as attacks (like vote-selling). By coercion-resistance adversary may get details of voter like credentials of voter and can cast vote as he/she wants to cast. To overcome the drawbacks of remote election JCJ introduced the first scheme that fulfills it. The scheme basically reduces coercive attacks by allowing the voter to deceive adversaries about her vote intention [9]. It, though, requires a quadratic work factor (in number of votes) to compute the voting results and hence it is impractical for large scale elections. Particularly, the scheme relies on an inefficient blind comparison mechanism to determine the results [9].

In this I-voting system first administrator module is configured according to type of voting then registration of voter and nominator is involved. Voter and nominator have to send all detail information about themselves to administrator. Then administrator verify the applications of voter and nominator using OTP and UID if result is true then accept otherwise administrator has authority to reject the application. If application of voter and nominator is accepted by administrator then the account for that particular user is created.

The user ID for each user is created and it is unique and encrypted using cryptography and saved in database which is located at server side. On the time of log-in to account of any user the credentials are encrypted and matched with saved credentials, If result is true then home page for that particular user is displayed otherwise can't log-in message will be displayed.

In registration phase the verification of valid application is very important task in online voting system. For verifying the valid user we have to use UID and OTP mechanism to conform that the current user is valid for the registration. In voting phase the voter can vote for the candidate as per his/her choice. But voter allowed to vote for only one time second time it can't be accepted by system.

A. Fundamental Concepts On (Domain)

The protocol underlying this paper was published in 2009 by Juels, Catalano, and Jakobsson [2], often referred to as the JCJ protocol. The scheme of Juels, Catalano, and Jakobsson [2] relies essentially on a method of indirect identification through anonymous credentials to overcome coercive attacks [9]. Especially, when the voter have a valid credential (like alphanumeric string) in a secure way and uses it when he wants to cast his vote. Opponent may try to do coercion then he may go through some fake credentials and had over it to coercer. After the voting, a blind comparison mechanism distinguishes the valid credentials and the fake ones to identify the valid votes and invalid votes; conversely, an adversary has no other way to perform this distinction action.

In a registration phase free of adversaries and a bulletin board communication model. Also, it requires the following cryptographic tools: non-interactive zero-knowledge proofs, a probabilistic threshold public-key cryptosystem, and universally verifiable mix nets [9].

B. Contributions

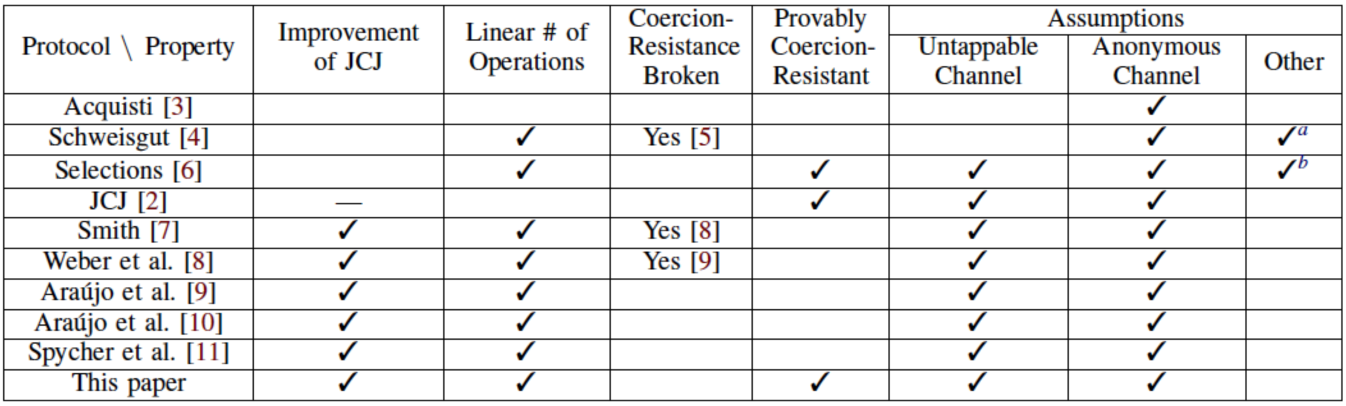
An efficient and provably secure coercion-resistance E-voting protocol is remote voting system. But there is no mechanism to verify and validate the voter and candidate so we are providing the verification phase in which voter and nominator are checked that they were valid or invalid.

For security purpose we are getting all the details about voter and candidate (like UID, security question etc.) and we are providing voter ID for each user which is used for log-in purpose, and we encrypt the voter Id and password (both are alphanumeric) and store in database of server, when user try to log-in we check that they have entered correct credentials or not.

II. LITERATURE SURVEY

Literature survey is the most important step in software development process. Before developing the tool it is necessary to determine the time factor, economy n company strength. Once these things r satisfied, ten next steps are to determine which operating system and language can be used for developing the tool. Once the programmers start building the tool the programmers need lot of external support. This support can be obtained from senior programmers, from book or from websites. Before building the system the above consideration are taken into account for developing the proposed system. We are considering all the existing systems and protocols of e-voting and using some the features to develop our system which will became god and secured example of online-voting system.

There are many e-voting protocols have been proposed by different authors which has different mechanism and assumptions. Following table 1 shows difference between these protocols. Many of these protocols are just little improvement in JCJ [2] protocol. We can take an example of Acquisti [3], Clark and Hengartner [6], Scheisgut [4], they proposed coercion-resistance e-voting protocols, which are mostly similar to JCJ [2] protocol. Smith [7], Weber et al. [8], Araujo et al. [9], [10], and Spycher et al. [11] proposed improved versions of the JCJ protocol. Acquisti [3] proposed a coercion-resistant e-voting protocol that allows write-in ballots (i.e., candidates are not predefined, and voters can vote for anyone they prefer) [1]. His protocol is similar to the preliminary version of the JCJ protocol [12], in that both rely on a number of authorities to issue the credentials of voters, and both tally election results by making a blind comparison between the list of encrypted votes and the list of encrypted credentials. A main difference is that Acquisti's protocol allows voters to encrypt a combination of their votes together with their credential shares [1].



Protocol \ Property	Improvement of JCJ	Linear # of Operations	Coercion-Resistance Broken	Provably Coercion-Resistant	Assumptions		
					Untappable Channel	Anonymous Channel	Other
Acquisti [3]						✓	
Schweisgut [4]		✓	Yes [5]			✓	✓[a]
Selections [6]		✓		✓	✓	✓	✓[b]
JCJ [2]	—			✓	✓	✓	
Smith [7]	✓	✓	Yes [8]		✓	✓	
Weber et al. [8]	✓	✓	Yes [9]		✓	✓	
Araújo et al. [9]	✓	✓			✓	✓	
Araújo et al. [10]	✓	✓			✓	✓	
Spycher et al. [11]	✓	✓			✓	✓	
This paper	✓	✓		✓	✓	✓	

Table 1: Literature Survey

Schweisgut [4] proposed a coercion-resistant e-voting protocol that works in linear fashion. In this protocol, each voter may have two credentials, which are stored on the tamper-resistant hardware. One of the credentials is the valid credential of the voter, while the other one is his fake credential. Araujo et al. [5] explained the attacks on Schweisgut [4] protocol that allows an opponent to check whether a voter submitted to coercion. Another proposed coercion-resistant e-voting protocol, known as Selections [6]. It shares several similarities with the JCJ protocol. Selection protocols consist of eliminating votes with invalid zero-knowledge proofs, eliminating duplicate votes, applying votes to a verifiable mix-net, and checking the validity of the asserted passwords. While similar to the JCJ protocol, the Selections [6] protocol needs anonymous and untappable channel, with addition to that it uses some other physical assumptions as well. For instance, the Selections protocol assumes that a voter cannot recall and he will shred his preparation sheet. That said, the Selections protocol has several properties, such as linear overhead, revocation of voters, and password-based authentication [6].

Smith [7] proposed a similar of the JCJ protocol to reduce the inefficiency problem of the JCJ. However, Smith's protocol is ambiguous in some aspects, and his new comparison method (that is the alternative of the PET method of the JCJ) may get fail in some special cases, and cause unexpected election results [8].

Weber et al. [8] proposed another similar of the JCJ protocol with O(n) operations, which is based on the Smith's ideas [7]. They proposed a new method of comparison, which is based on Pedersen's distributed key generation [13].

Araujo et al. [9], [10] proposed two other e-voting protocols which are basically based on the JCJ protocol, with O(n) operations. They described that the use of approaches based on group signatures. While variant to the JCJ protocol, The voters obtain their credentials (like user ID, Password) at the registration phase, There is no public voter roll at the registration phase. Spycher et al. [11] declared that protocols based on this approach have an inherent weakness.

Based on JCJ protocol Spycher et al. [11] proposed another e-voting protocol. His proposed e-voting protocol can removed duplicate votes using the linear-time method of Smith [7] and Weber et al. [8]. Particularly, to check credentials of each and every voter in linear-time, each voter should show the voter roll entry with which the vote's credential is to be matched. Spycher et al. [11] did not provide a proof for coercion-resistance.

The Table 1 compares all the aforementioned protocols with each other. The proposed protocol of Alireza Toroghi Haghighat, Mohammad Sadeq Dousti, and Rasool Jalili has several aspects. As is shown in the above table, Their protocol achieves the O(n) bound, does not rely on assumptions such as tamper-proof hardware or voter behavior,

And most importantly includes a detailed proof for the achieving the coercion-resistance property.

III. PRPOSED SYSTEM

I-voting system architecture is shown in following diagram. To understand working of the system you have to know what types of users in the system.

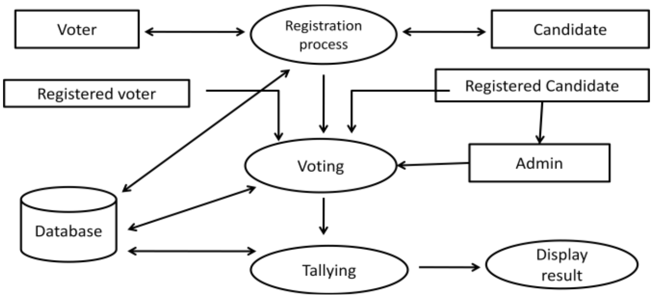


Fig 1: System Architecture

First of all administrator is configured then the nominator and voter can request to the administrator for registration in I-voting system by submitting application form. Then Administrator has to check that application form and validate the candidate and voter. If the verification process completed successfully then he has to accept request of voter and candidate otherwise he have to reject the application. Verification is done by using unique identification number and one time password. The application form contains lot of information like name, address, Contact details, Aadhar Id, election Id etc. of the applicant. There are two major advantages of this proposed system that are it will save our valuable time and provide reliable I-voting.

IV. IMPLEMENTATION

Implementation is the stage of the project when the theoretical design is turned out into a working system. Thus it can be considered to be the most critical stage in achieving a successful new system and in giving the user, confidence that the new system will work and be effective.

The implementation stage involves careful planning, investigation of the existing system and it's constraints on implementation, designing of methods to achieve changeover and evaluation of changeover methods.

A. Interaction Model

1. Client-driven interventions

Client-driven interventions are the means to protect customers from unreliable services. For example, services that miss deadlines or do not respond at all for a longer time are replaced by other more reliable services in future discovery operations.

2. Provider-driven interventions

Provider-driven interventions are desired and initiated by the service owners to shield themselves from malicious clients. For instance, requests of clients performing a denial of service attack by sending multiple requests in relatively short intervals are blocked (instead of processed) by the service.

B. Modules

1. *Admin Module.*
2. *User Module.*
3. *Nominator Module.*

1. Admin Module

This module tells all about an automated ballot vote department who are conducting elections in our country. By using this module Automated ballot vote can release election schedule which involves type of elections (parliament, Assembly),election zone (area) in addition with nomination starting date, ending date and also election starting date, ending date.

2 User Module

This module tells all about voters. By using this module any citizen who is crossing 18 years old can register their names to get electoral authentication, and also they can go for online voting. This module consists following sub modules.

3. Nominator Module

By using this functionality political leaders can go for nomination by providing voter Id.

V. RELATED WORK

Many researchers investigated the coercion resistance in online voting. The proposed protocol of Alireza Toroghi Haghighat, Mohammad Sadeq Dousti, and Rasool Jalili also focus on providing security against to coercion. The JCJ is basic for all investigation. JCJ is protocol in which the author discussed about steps to accomplish online voting, But they didn't given mechanism to avoid attacks on system or to protect the system. Selections also proposed e-voting protocol which is also based on JCJ protocol with addition to that. The selections protocol uses some other physical assumptions as well. The main aspect is providing security to the online voting system.

Unlike JCJ protocol Spycher et al. proposed e-voting protocol. His protocol removes duplicate votes using the linear-time method of Smith and Weber et al.

VI. CONCLUSION

In this paper we presented the I-voting system which makes effective use of all proposed e-voting protocols. I-voting system uses JCJ protocol and in addition to that we implemented mechanism to avoid coercion, provided security to e-voting. Our voting system provides security, efficiency. I-voting system has verification phase during registration new user that may be voter or candidate. Verification phase checks the user being requested is valid or not. Depend upon the result of verification administrator accept or reject the applicant. We can also say that I-voting is practical implementation of all existing voting protocols.

REFERENCES

[1] Alireza Toroghi Haghighat, Mohammad Sadeq Dousti, and Rasool Jalili, "An Efficient and Provably-Secure Coercion-Resistant E-voting Protocol", IEEE 2013.

[2] A. Juels, D. Catalano, and M. Jakobsson, "Coercion-resistant electronic elections," in Proceedings of the 2005 ACM workshop on Privacy in the electronic society (WPES '05). ACM, 2005, pp. 61–70.

[3] A. Acquisti, "Receipt-free homomorphic elections and write-in ballots," Cryptology ePrint Archive, 2004.

[4] J. Schweisgut, "Coercion-resistant electronic elections with observer," in 2nd International Workshop on Electronic Voting, Bregenz, 2006.

[5] R. Araujo, N. Rajeb, R. Robbana, J. Traor´e, and S. Youssfi, "Towards practical and secure coercion-resistant electronic elections," in Cryptology and Network Security. Springer, 2010, pp. 278–297.

[6] J. Clark and U. Hengartner, "Selections: Internet voting with overthe-shoulder coercion-resistance," in Financial Cryptography and Data Security. Springer, 2012, pp. 47–61.

[7] W. Smith, "New cryptographic election protocol with best-known theoretical properties," in Proc. of Workshop on Frontiers in Electronic Elections, 2005.

[8] S. G. Weber, R. Araujo, and J. Buchmann, "On coercion-resistant electronic elections with linear work," in The Second International Conference on Availability, Reliability and Security (ARES 2007), april 2007, pp. 908–916.

[9] R. Araujo, S. Foulle, and J. Traore, "A practical and secure coercionresistant scheme for remote elections," Frontiers of Electronic Voting, vol. 7311, 2007.

[10] R. Araujo, S. Foulle, and J. Traore, "A practical and secure coercionresistant scheme for internet voting," in Towards Trustworthy Elections. Springer, 2010, pp. 330–342.

[11] O. Spycher, R. Koenig, R. Haenni, and M. Schlapfer, "A new approach towards coercion-resistant remote e-voting in linear time," in Financial Cryptography and Data Security. Springer, 2012, pp. 182–189.

[12] A. Juels and M. Jakobsson, "Coercion-resistant electronic elections," Cryptology ePrint Archive, 2002, http://eprint.iacr.org/2002/165.

[13] T. Pedersen, "A threshold cryptosystem without a trusted party,"

BIOGRAPHY

Ashwinkumar Panchal is student of BE in computer engineering from Sinhgad Institute of Technology, Lonavala, Pune affiliated to AICTE under Savitribai Phule Pune University and Completed Diploma in computer engineering in the year 2012 from Gramin Polytechnic, Vishnupuri, Nanded in MSBTE.

Shailesh Indrale is student of BE in computer engineering from Sinhgad Institute of Technology, Lonavala, Pune affiliated to AICTE under Savitribai Phule Pune University and Completed Diploma in computer engineering in the year 2012 from Gramin Polytechnic, Vishnupuri, Nanded in MSBTE.

Nitin Jadhav is student of BE in computer engineering from Sinhgad Institute of Technology, Lonavala, Pune affiliated to AICTE under Savitribai Phule Pune University and Completed Diploma in computer engineering in the year 2012 from Gramin Polytechnic, Vishnupuri, Nanded in MSBTE.

Nandkishor Karlekar has received BE in Computer Science and Engineering from Dr. Babasaheb Ambedkar Marathwada University, Aurangabad, Maharastra, India in the year 2001 and ME in Computer Engineering from University Of Mumbai, India and currently pursuing Phd in computer from Veltech, Avadi, Chennai, India also he is working as a asst. Prof. in department of Computer Engineering Sinhgad Institutes of Technology, Lonavala, Pune affiliated to AICTE under Savitribai Phule Pune University.