International Journal of Trend in Scientific Research and Development (IJTSRD)
International Open Access Journal
ISSN No: 2456 - 6470 | www.ijtsrd.com | Volume - 2 | Issue – 3

A Survey on Web Based Application of Secure Online Voting System

Shanthi S
Assistant Professor, Dept of CSE, Sri Eshwar College of Engineering, Coimbatore, India

Ilakkiyavani R
PG Scholar, Dept of CSE, Sri Eshwar College of Engineering, Coimbatore, India

Amsaveni P
Software Engineer, Financial Software and Systems, Chennai, India

ABSTRACT

Data Mining is an analysis tool which is used to extract various knowledge from the vast amount of data with security for the effective decision making. Online voting system uses data mining technique, to increase transparency at the highest level and to increase operational effectiveness to minimize piracy of data and also to have faster access for effective decision making with secure data. Since some years ago, different methods, such as the punch card systems or the secret ballot method have been held to carry on electoral processes, where people have to visit the booth to cast their votes in the existing system. Since then fast evolution of Information Technology, voting systems have emerged, which allow a voter to be part of an automated process that can only be possible through Voting Systems. The proposed system is online and hence even people who live out of their home town can also vote. Increasing the voting percentage is the major goal. The main objective of proposed system is to provide, a quick and efficient retrieval of information.

Keywords: *Data Mining, Voting System, Electoral Process, Secured Voting, Encryption and Decryption*

1. INTRODUCTION

Online voting system is an online voting technique, without any difficulty, a voter can use his\her voting right online in "online voting system". He\She has to fill a registration form to register himself\herself. All the names of voter with complete information is maintained by the election commission, where the information is stored in the database. All the entries about the information of the voter which is already stored are checked by the database. The user id and password is given to the voter, if all the entries are correct and then by using that id and password he\she can view the candidate lists, choose and caste his\her vote. Then that entry will be discarded, if conditions are wrong. And in the proposed system of web based application for online voting will make the voting process very easy and more efficient.

2. LITERATURE SURVEY

2.1. AN EFFICIENT MOBILE VOTING SYSTEM SECURITY SCHEME BASED ON ELLIPTIC CURVE CRYPTOGRAPHY

The wide-spread use of mobile devices has made it possible to develop mobile voting system as a complement to the existing electronic voting system. However, due to limited onboard resource, it is challenging to achieve both efficiency and security strength for mobile voting system. Conventional solution is to either use symmetric encryption algorithms or hybrid symmetric and asymmetric algorithms at the expense of weaker security strength. In the proposed mobile voting scheme, the user votes are secured by using the elliptic curve cryptography (ECC) algorithm [17].

ECC is chosen as it has smaller key size than other public key cryptographies, and its homomorphic encryption property which is able to keep user's anonymity. The system evaluates the method of ECDH with AES and ECC in comparison with proposed method.

In general, e-voting systems must meet the principles and requirements for an election which include,

- Confidentiality
- Anonymity
- Integrity

2.2. ELECTION VOTING SYSTEM USING MOBILE M- VOTING

M-voting[1] is the technique of casting the votes through the cell phones. The iris scanner will check the person for the validity. The eye patterns will transmit to the server. After getting the permission from server , the person can vote by sending the keys. The m-voting can have access anywhere from the world with the help of satellite communications. Hence, the combination of mobile communication and the biometric techniques paves the way for new generation of voting. Physiological characteristics are more stable characteristics such as,

- Face recognition
- Finger print recognition
- Iris recognition
- DNA recognition

Behavioral characteristics is the reflection of make up

- Signatures
- Voices

2.3. DISTRIBUTED E-VOTING SYSYEM USING THE SMART CARD WEB SERVER

Voting in elections is the basis of democracy, but citizens may not be able or willing to go to polling stations to vote on election days. Remote e-voting[11] via the Internet provides the convenience of voting on the voter's own computer or mobile device, but Internet voting systems are vulnerable to many common attacks, affecting the integrity of an election.

Distributing the processing of votes over many web servers installed in tamper-resistant, secure environments can improve security this is possible by using the Smart Card Web Server (SCWS) on a mobile phone Subscriber Identity Module (SIM). This system proposes a generic model for a voting application installed in the SIM/SCWS[11], which uses standardised Mobile Network Operator (MNO) management procedures to communicate (via HTTPs) with a voting authority to vote.

2.4. PRIVATE QUERY ON ENCRYPTED DATA IN MULTI-USER SETTINGS

Searchable encryption schemes allow users to perform keyword based searches on an encrypted database. Almost all existing such schemes only consider the scenario where a single user acts as both the data owner and the querier. However, most databases in practice do not just serve one user; instead, they support search and write operations by multiple users. In this system, it states systematically about the study of searchable encryption[4] in a practical multi-user settings. The results include a set of security notions for multi-user searchable encryption as well as a construction which is provably secure under the newly introduced security notions.

Searchable encryption[4] is used, which in general allows a user to search among encrypted data and find the data containing a chosen keyword. The approaches improve the search efficiency at the cost of a large storage for the constructed indexes (the bit-length of the index for each document is proportional to the total number of keywords). A formal security notion of searchable encryption is defined in which it also constructs schemes with secure against non-adaptive and adaptive adversaries. The work considers the variation of simultaneous search of conjunctive keywords.

2.5. FORMAL VERIFICATION OF TAMPER-EVIDENT STORAGE FOR E-VOTING

The storage of votes is a critical component of any voting system. In traditional systems there is a high level of trans-parency in the mechanisms used to store votes, and thus a reasonable degree of trustworthiness in the security of the votes in storage. This degree of transparency is much more difficult to attain in electronic voting systems, and so the specific mechanisms put in place to ensure the security of stored votes require much stronger verification[3] in order for them to be trusted by the public.

The proposed system states about already existing formal techniques that can help to alleviate many of the verification problems that the adoption of new e-voting technologies can introduce. For the specific modelling and verification in the study, the event-B method [3] are used, based on the B notation. It is unreasonable to expect the public to trust a system (or part of a system) to behave correctly just because it is developed using a formal method.

2.6. AD-HOC NETWORK BASED SMART I-VOTING SYSTEM: AN APPLICATION TO COGNITIVE RADIO TECHNOLOGY

A financially savvy and effortlessly implementable i-voting (web voting)[12] framework particularly for India in view of adhoc network. The essentials of cognitive radio innovation and Adhoc organize in view of cognitive radio technology are initially presented. The idea of smart i-voting[12] framework is then proposed and how it can be executed in suburban region where web services are not effortlessly accessible, but rather can be made accessible utilizing Cognitive Radio innovation[12] researched as a part of subtle elements.

Aadhar ID is utilized as a first level of validation where a voter needs to enter 12 digit Aadhar ID number.
There are two parts of confirmation in i-voting frameworks:
• Verification of voters identity characters assert.
• Verification of voter's right to vote.

2.7. REPLICA VOTING BASED MECHANISMS FOR DISSEMINATION OF MULTI-MODAL SURVEILLANCE DATA

Surveillance applications consist of computational devices that collect data representing the external environment (e.g., terrain conditions and vehicle tracking). The data collected is prone to errors because the processing algorithms in devices often have only limited capabilities that result in a fuzzy and imprecise representation of the external event.

Here, replicating[13] the devices and voting on the environment data collected by them enhances the trust-worthiness of data reported to the application. Voting-based data validation may be provided as a generic building block for surveillance applications. Here, the fuzzy data generated by devices operating on partial and/or incomplete inputs are accommodated in the approach (e.g., multimedia images).

2.8.IMPLEMENTATION OF AUTHENTICATED AND SECURE ONLINE VOTING SYSTEM

Shridharan [15] Implemented a three models such as, Authentication model, franchise excising model, distributed database and central server model. In authentication model voter with smart card and voter identification number and also gives the biometric information this all information is used in future election voting process. After verification and validation voting interface means candidate name and sign are displayed, this is verified by vote casting database, and then votes are counted and declared the result. In this system security and traceability also ensures to auditing the vote and voter information.
In such a system, the correctness burden on the voting terminal's code is significantly less as voters can see and verify a physical object that describes their vote and are allowed to vote in terminal only after their identity is proved. The voters, who cast multiple votes during the process of voting is ensured to be prevented.

Also to ensure the maintenance of authenticity, any biometric identification of the voters could be used for accessing the terminal to cast their vote and restricting them to cast again. The process of online voting could be deployed with three phases - the voter registration online vote capturing and the instant online counting and result declaration.

2.9. A SECURE APPROACH FOR WEB BASED INTERNET VOTING SYSTEM USING MULTIPLE ENCRYPTION

Jambhulakar, chakole and pradhi [9] proposed a novel security for online voting system by using multiple encryption schemes. Provide security for cast vote when it is submitted from voting poll to voting server. Multiple encryptions to avoid DOS attack. Security provide submissive as well as active interloper. This system is to take a judgment of certain issues. This paper use cryptography concepts to take pros of digital signature. Encrypting the send forth vote to client server then send to voting server with the help of net.

After sending encrypted vote then server side decrypt the vote before counting. On server side decryption of that vote is done before counting. We require two keys for this purpose one for encryption on voter system, which should be publicly known and second key for decryption of encrypted vote before counting on voting server, this key must be private. So for this purpose we need a pair of asymmetric keys. To provide security from active intruder who can alter or tamper the casted vote when vote is transferring from voter to voting server, we are using digital signature.
When a voter cast his/her vote after that he/she will digitally sign on that by using his/her own private

digital signature, and send this to voting server, on voting server side that signature is checked by digital signature verifier of that voter which is publicly known.

For this purpose each voter should have a private digital signature and a public digital signature verifier, for this we are using a pair of asymmetric keys for each registered voter.

2.10. WEB-BASED VOTING SYSTEM USING FINGERPRINT DESIGN AND IMPLEMENTATION

Firas I. Hazzaa, Seifedine Kadr [6] This paper deals with the design and development of a web-based voting system using fingerprint in order to provide a high performance with high security to the voting system also we use web technology to make the voting system more practical. The new design is proposed an election for a university for selecting the president of the university.

The proposed EVS allows the voters to scan their fingerprint, which is then matched with an already saved image within a database. Developed Web-based Voting System using Fingerprint Recognition. This system has provided an efficient way to cast votes, free of fraud, and make the system more trustable, economic and fast. We have used Minutiae-base fingerprint identification and matching with high accuracy.

2.11. ONLINE VOTING SYSTEM POWERED BY BIOMETRIC SECURITY USING STEGANOGRAPHY

Shivendra Katiyar, Kullai Reddy Meka, Ferdous A. Barbhuiya, Sukumar Nandi [14] Using Cryptography and Steganography at the same time, we try to provide Biometric as well as Password security to voter accounts. The scheme uses images as cover objects for Steganography and as keys for Cryptography. The key image is a Biometric measure, such as a fingerprint image.

Proper use of Cryptography greatly reduces the risks in these systems as the hackers have to find both secret key and the template. The basic idea is to merge the secret key with the cover image on the basis of key image. The result of this process produces a stego image which looks quite similar to the cover image but not detectable by human eye. The system targets the authentication requirement of a voting system.

In this paper we proposed a method for integrating cryptography and steganography. The strength of our system resides in the new concept of key image. We are also able to change the cover coefficients randomly. This strategy does not give any chance to steganalytic tools of searching for a predictable set of modifications. Also, considering the complexity of elections, we have provided sufficient proof of authenticity of an individual in form of both biometric measures and secret key.

2.12. ONLINE VOTING SYSTEM FOR INDIA BASED ON AADHAAR ID

Himanshu Agarwal and G.N.Pandey [8] proposed aadhar id based online voting system for Indian election is proposed for the first time in this paper. The proposed model has a greater security in the sense that voter high security password is confirmed before the vote is accepted in the main database of Election Commission of India. The additional feature of the model is that the voter can confirm if his/her vote has gone to correct candidate/party. In this model a person can also vote from outside of his/her allotted constituency or from his/her preferred location. In the proposed system the tallying of the votes will be done automatically, thus saving a huge time and enabling Election Commissioner of India to announce the result within a very short period.

This system is much secure and efficient than the traditional voting system. Manipulation of votes and delay of results can be avoided easily. A unique AADHAAR identity is the centre point of our proposed model. It leads to the easier verification of both voters and candidates. This AADHAAR Identity number is unique for every citizen or voter of India. This AADHAAR Identity number has been introduced by government of India and this also recognizes the constituency of the voter. But the registration of the voter should be completed only after the verification of all documents by the field officer

2.13. HIGHLY SECURED ONLINE VOTING SYSTEM OVER NETWORK

K. P. Kaliyamurthie1, R. Udayakumar, D. Parameswari and S. N. Mugunthan [10] The aim of this paper is to people who have citizenship of India and whose age is above 18 years and of any sex can give their vote through online without going to any physical polling station. Election Commission Officer

(Election Commission Officer who will verify whether registered user and candidates are authentic or not) to participate in online voting. This online voting system is highly secured, and its design is very simple, ease of use and also reliable.

The proposed software is developed and tested to work on Ethernet and allows online voting. It also creates and manages voting and an election detail as all the users must login by user name and password and click on his favorable candidates to register vote. This will increase the voting percentage in India. By applying high security it will reduce false votes.

Method for integrating cryptography over network to present a highly secure online voting system. The security level of our system is greatly improved by the new idea of random cover image generation for each voter. The user authentication process of the system is improved by adding both face recognition and password security.
The recognition portion of the system is secured by the cover image. This system will preclude the illegal practices like rigging. Thus, the citizens can be sure that they alone can choose their leaders, thus exercising their right in the democracy. The usage of online voting has the capability to reduce or remove unwanted human errors.

4. PROPOSED CONCEPTION

Proposed Architecture is online voting system. In this system there are three models.

i. Voter registration server
ii. Authentication server
iii. Vote recording and casting server.
In voter registration server, voter will be registered personal information and biometric information eg. Thumb Impression. Only registered users are allowing to vote at the time of election.
The proposed system is shown in fig. 1.

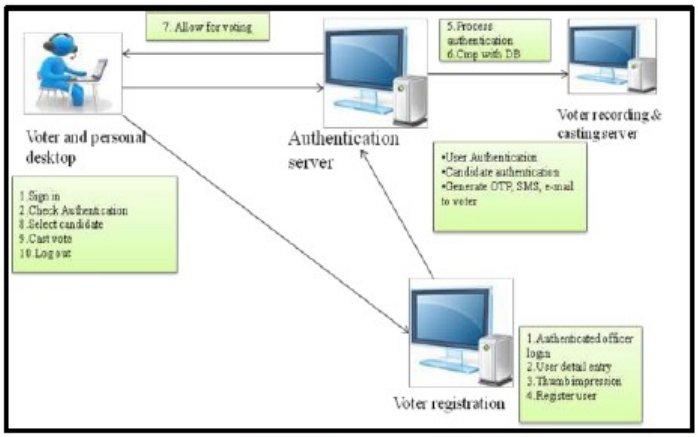

Fig. 1 Architecture of Online Voting System

In proposing system user does registration process first. Send all information to authentication server send password and ID to voter after he/she is login. If it is authenticated then allowing for voting after voter cast his/her vote and this vote is encrypted form stored in vote casting and recording server.

5. CONCLUSION

In this paper different online voting system technique is studied based on homomorphic encryption, blind signature. From study we proposed a secure online voting system and user friendly system using biometric authentication. In previous system cannot provide casted vote and is not stored securely or separately. We can provide security casted vote and only authenticated person can cast their vote. A system provides strong security of the online voters and protects them against various security attacks. It is reliable system for casting votes and recording vote.

REFERENCES

1. S.Bhargavi, N.Bhavithra devi,B.Ranganayaki priya,B.yamuna,"Election voting system using mobile m- voting"Proceedings of International Conference on Optical Imaging Sensor and Security,July 2013.
2. Divya G Nair, Binu. V.P, G. Santhosh Kumar,"An Improved E-voting scheme using Secret Sharing based Secure Multi-party Computation", arXiv: 1502.07469v1 [cs.CR] 26 Feb 2015.
3. Dominique Cansell and J.Paul Gibson,"Formal verification of tamper-evident storage for e-voting" , 2007 Fifth International Conference on Software Engineering and Formal Methods.

4. Feng Bao, Robert H. Deng, Xuhua Ding, and Yanjiang Yang ,"Private query on encrypted data in multi-user settings".
5. S.Shanthi, S.Saranya, R.Rajeshkumar, "A Survey On Anomaly For Discovering Emerging Topics" ,International Journal of Computer Science and Mobile Computing – Volume 3-Issue 10.
6. Firas I. Hazzaa, Seifedine Kadry, Oussama Kassem Zein,"Web-Based Voting System Using Fingerprint Design and Implementation",International Journal of Computer Applications In Engineering Sciences ISSN:2231-4946.
7. S.Shanthi, R.Rajeshkumar, S.Saranya, "A Survey on Optimized Structural Diversity" ,International Journal of Computer Science and Mobile Computing – Volume 3-Issue 10.
8. Himanshu Agarwal, G.N.Pandey, "Online Voting System for India Based on AADHAAR ID", Eleventh International Conference on ICT and Knowledge Engineering 2013.
9. Prof. S.M. Jambhulkar, Prof. Jagdish B. Chakole, Prof.Praful. R. Pardhi "A Secure Approach for Web Based Internet Voting System using Multiple Encryption",2014 International Conference on Electronic Systems, Signal Processing and Computing Technologies,2014.
10. K.P. Kaliyamurthie, R. Udayakumar, D. Parameswari and S. N. Mugunthan , "Highly secured online voting system over network", 4833 Indian Journal Science and Technology Print ISSN: 0974-6846 Online ISSN: 0974-5645 Vol 6 (6S) May2013.
11. Lazaros Kyrillidis , Sheila Cobourne , Keith Mayes, Song Dong and Konstantinos Markantonakis,"Distributed e-voting using the smart card web server", in 2012 7th International Conference on Risks and Security of Internet and Systems (CRiSIS).
12. Rahul V Awathankar,Dr. Rajeshree D. Raut,Dr. M S S Rukmini,"Ad-hoc network based smart i-voting system: an application to cognitive radio technology",in 2016 International Conference.
13. K.Ravindran and M. Rabby, "Replica voting based mechanisms for dissemination of multi-modal surveillance data",in 2012 32nd International
14. Conference on Distributed Computing Systems Workshops.
15. Shivendra Katiyar, Kullai Reddy Meka, Ferdous A.Barbhuiya, Sukumar Nandi, " Online Voting System Powered By Biometric Security Using Steganography" Second International Conference on Emerging Applications of Information Technology, 2011.
16. Srivatsan Sridharan, "Implementation of Authenticated and Secure Online Voting System", 4th ICCCNT 2013,Tiruchengode, India No.6, July 2013. IEEE – 31661.
17. Tohari Ahmad, Jiankun Hu "An efficient mobile voting system security scheme based on elliptic curve cryptography" in 2009 Third International Conference on Network and System Security.