Journal of Advances and Scholarly Researches in Allied Education
Vol. 16, Issue No. 5, April-2019, ISSN 2230-7540

An Analysis on Different Techniques Highly Secure Biometrics Voting System

Er. Kailash Aseri*

Principal, Shree Devi Woman Polytechnic College, Hanumangarh Junction, Rajasthan, India

Abstract – A voting system in which election figures is documented, kept and managed as digital facts is called an electronic voting system. An e-voting system has two categories: on-line e-voting and offline e-voting. On-line e-voting done using internet and offline e-voting done using by a voting machine or ballet papers. The main challenge of e-voting is authentication of voters, safety of voting method, locking voted figures. It is the major reason why a protected e-voting method is very essential. In this paper i have discussed the validating voters and polling data safety characteristics for e-voting. For make sure that vote casting cannot be changed by unofficial person. The voter verification in online e-voting procedure can be through by prescribed registration through officers and by entering otp. In offline e-voting procedure verification can be done using iris reorganization, finger vein sensing which permits the electronic ballot reorganize for permitting voters to cast their votes. The voted data and voter's details with cryptography technique received at database administration unit (dau) using timely manner using gsm system.

I have proposed an online e-voting system with protected verification which is provided by biometric as well as password safety to voter accounts. On the basis of core image the secret key merge with the cover image is basic idea. Outcome of this process produces a stego image which looks quite similar to the cover image. The core image is a biometric measure and stego image is take out at the server side to accomplish the voter verification purpose. This system decreases the threats as the hackers have to find both secret key and template that sorts the election process to be safe and healthy.

Key Words: Database Administration Unit, E-Voting, Stego Image.

----------X----------

INTRODUCTION

The recent communications and internet facility gets the growing necessity for electronic facilities and its safety. An e-voting system is a new technology in which the election data is documented, kept and handled as digital material. Previously information security was used typically in military and government organizations but now day's information security consumption in everyday usage. To insure that data, communications are sufficient protected and privacy empowered information security is essential in computing and e-services. The cryptographic techniques provides noble confidentiality on e-voting systems. Security is very important role in e-voting procedure that's why a secure e-voting system is essential.

A method to achieve security and privacy of an election can be time-consuming, costly for officers and difficult for voters. An e-voting security achieved through different levels. For e-voting systems the authenticating voters and polling data security aspects are: (i) confirms that vote casting cannot be reformed by unofficial person. (ii) Voter verification in online e-voting process can be done by proper registration through administrators and by entering OTP certificate.

In offline e-voting procedure verification can be finished by facial reorganization, fingerprint sensing which empowers the electronic ballot reset for permitting voters to cast vote. The voted facts and voter's particulars can be directed to the near database administration unit in a well-timed routine using GSM system using with cryptography.

Online voting system has been established to abridge a manner of forming elections & create it appropriate for votes, to vote remotely from their home location however compelling into thought of security, secrecy & providing testing skills. Consumers are persons who act together with system through web browsers. To fetch human biological features e.g. finger print with a computerized machine both authentication and identification. The biometric products should

www.ignited.in

eliminate the essential of password. The finger print is most commonly use biometric feature.

E-VOTING SYSTEMS

A voting organism in which the election facts is documented, stored and managed mostly as digital information called an electronic voting system. So we say that a voting process in which an electronic resources is used for votes casting, results counting is e-voting. It is an election arrangement that permits a voter to record their ballots in secured technique.

Securities of E-Voting Systems -

To ensure the privacy of the voters and accuracy of votes, e-voting structure need confident e-voting to acquire this a secure e-voting has following necessities-

***Eligibility*:** votes must cast by genuine voters

***Un-reusability*:** each voter is allowed to cast a single vote;

***Anonymity*:** votes are secure secret;

***Accuracy*:** cast ballot can't be changed. Thus, it essential not be possible to erase ballots nor to add ballots, once the election has been shut;

***Fairness*:** partial formulation is impossible;

***Vote and go*:** once a voter has casted his vote, no additional action preceding to the end of the election;

***Public verifiability*:** everyone should be capable to freely check the validity of the entire voting procedure.

Issues of Present Voting System -

Here we have existed numerous studies where the use of computer technologies to improve elections these studies risk avoidance against the moving too rapidly to accept electronic voting system, for the reason that software engineering experiments, insider threats, network vulnerabilities, and the tests of auditing.

Accuracy: it's impossible for a vote, to be altered removed the invalid vote can't be calculated from the lastly tally.

Democracy: it authorize only authorized voters to vote and, it confirms that eligible voters vote only once.

Privacy: neither power nor someone else can linkage any ballot to the voter.

Verifiability: autonomously verification of that all votes have been calculated appropriately.

Resistance: the collection of individuals, running the election can work in a conspiracy to introduce votes or to prevent voters from voting.

Availability: from the start to the finish of the poll this arrangement works appropriately as long as the poll stands and some voter can have access to it.

Proposed System of Online E-Voting -

Formerly the election procedure, the process of voter registration done by administration. In voter registration process voter information like voter id (11-digit number RJ/13/0000015—in this, RJ indicate the state, subsequent two digit identifies district id and third one insist on unique id for each eligible voter), name, age, sex, address and district in the database and mobile number for OTP. Above all condition are stratification means person has valid the polling section.

BIOMETRIC IDENTIFICATION IN E-VOTING

A biometric systems aiming on their importance for e-voting systems. One of the main issues we like to stress is the difference between biometric authentications compared to "classic" authentication as e.g. smart cards. In this comparison we ignore the well-known concept of card readers based on biometrics, e.g. card readers with fingerprint authentication; in this case, the biometric input is not used to authenticate the user to the e-voting system, but rather to authenticate his/hers smart card. The e-voting system does not interact in any way with the biometric characteristics of the actual users, but still authenticates the user with the help of the user's authentication certificate as present on the card. Seen from this perspective, this solution is not a biometric approach to e-voting. From now on, we will focus on biometric approaches that actually use the biometric data to authenticate the e-voting system. Another issue with biometric systems is their relative young age, there is still currently a set of standardization efforts going on. We will first have a look at some of the possible biometric stuffs that can be used for the authentication of individual persons.

In this paper, I will restrict myself to present just a subsection of changed biometric properties. I clearly do not emphasis on their achievability, but rather try to demonstration the wide range of "theoretically" promising human stuffs that can be used in biometric systems.

With this I tried to provide a quick outline to the diverse kinds of biometric systems and now I focus on certain of their technical sides which are applicable to an e-voting system.

Initially, I will deliberate on the infrastructure mandatory to use biometric contribution as the

verification means for an e-voting system. As previously stated before, I will not stare at limited biometric measures, but attention on the strictly biometric input to the actual e-voting system.

METHODOLOGY

The planned system voting can be finished through internet with the idea of steganography technology & biometrics. The user pin & secret key are conveyed to server strongly by steganography. Steganography is idea of hiding reserved or delicate statistics within somewhat that performs to be unknown out of the ordinary. If a person sights the digital article, he or she will have no idea that there is any secreted information, and so the person will not effort to decrypt the evidence. Common model of steganography declares if you need to send certain secret memo then select a cover image, find its terminated bits and replace these bits with data bits of the message. The message can be simply removed by doing some actions on the other end.

Least significant bit attachment is a common approach to embed information in a cover file. This process overwrites the LSB of a pixel value with a message bit. If we choose a 24-bit image as cover, we can easily store 3 bits in each pixel. Human eye will not be bright to catch the modification in any case. Unluckily, this process of LSB amendment changes the statistical properties of the cover image, so eavesdroppers can identify the distortions in the resulting stego image. This is quite viable that we can't embed somebody's private information in this manner. So, what we can do is that, we can encrypt the message before embedding, or we can perform steganography providing strong encryption at the same time.

Fingerprint pictures are selected as keys for encoding the secret key. Fingerprint acknowledgment is used for user verification because it is the most arranged biometric method, both in civil and illegal claims, because of its high development and cost-effective capture and treating.

Some evidence about the voter should be composed to maintenance such a system. First of all, each and every discrete in the country should be provided with a delicate identification number. It's required for keep of voter accounts in the database. Secondly, we need thumb impressions (fingerprint images) of all the persons. Thirdly, throughout the account creation every remarkable will be provided with a system generated secret key which he/she should not reveal to anyone.

Supposing all voters' information in a country is securely collected, biometric reader available for voting, the system is online during the election period only, the methodology is as follows.

To cast a vote, a voter logs into the system by entering the personal identification number and secret key. Along with this voter has to give the thumb impression on the fingerprint sensor.

CONCLUSION

Electronic voting systems have various benefits over the traditional technique of voting. Some of these benefits are reduced cost, faster tabulation of outcomes, better accessibility, superior accuracy, and minor risk of human and mechanical mistakes. An ideal e-voting system which can allow security and privacy on the high level with no compromise is very inspiring scheme. By adding both biometric and password security the user verification process of the system can be improved. A random distribution of message bits into the cover image called steganography portion of the system which is secured.

The main assumption of my paper is that biometric methods for e-voting systems should be remarkably carefully arranged. Really, I would even indication to encouragement from using biometric systems. Currently, the negation rates are fair too high for an atmosphere as sensitive as electronic votes.

REFERENCES

Alok Kumar Vishwakarma and Atul Kumar (2011). "a novel approach for secure mobile-voting using biometrics in conjunction with elliptic curve crypto-stegano scheme", International Journal of Technology and Engineering Systems, march 2011.

Braun, N., P. Heindl, et. al. (2003). E-voting in der schweiz, deutschland undösterreich ein überblick. Arbeitspapiere zum tätigkeitsfeldnformationsverarbeitung und informationswirtschaft. Wien, irtschaftsuniversität. 2003,2.

"E-voting through biometrics and cryptography-steganography technique with conjunction of gsm modem" emerging trends in computer science and information technology 2012(etcsit2012) proceedings published in international journal of computer applications® (dc a) by shobha lokhande.

"E-voting and biometric systems?" sonja hof university of lin7 austria institute of applied computer science, division: business, administration [and society; university of linz, Austria sonj a.hof@ ifs.imi-linz. Ac. At

J. Bannet, D. Price, A. Rudys, J. Singer, D. Wallach: Hack-a-vote: security issues with

www.ignited.in

electronic voting systems, IEEE security & privacy Vol. 2 NR1 p. 32

Robert Krimmer (ed.) "*Electronic voting 2006"*2nd international workshop co-organized by council of europe, esf ted, ifip wg 8.5 and e-voting.cc.

Shivendra Katiyar, Kullai Reddy Meka, Ferdous A. Barbhuiya, Sukumar Nandi (2011). "*Online voting system powered by biometric security using steganography",* 2011 second international conference on emerging applications of information technology.

William Stallings (2003). "*Cryptography and network security, principles and practices"*, Third Edition, pp. 67-68 and 317-375, Prentice Hall, 2003.

B. Swaminathan, J. Cross Datson Dinesh (2012). "Highly secure online voting system with multi security using biometric and steganography", international journal of advanced scientific research and technology, Issue 2, Volume 2 (April 2012)

Corresponding Author

Er. Kailash Aseri*

Principal, Shree Devi Woman Polytechnic College, Hanumangarh Junction, Rajasthan, India

kailash.aseri@gmail.com