ISSN: 0975-833X

Available online at http://www.journalcra.com

International Journal of Current Research
Vol. 15, Issue, 08, pp.25491-25495, August, 2023
DOI: https://doi.org/10.24941/ijcr.45729.08.2023

INTERNATIONAL JOURNAL OF CURRENT RESEARCH

RESEARCH ARTICLE

AUTHENTICATION OF USER FOR E-VOTING SYSTEM

[1,*]Dr. Dharmendra Bhatti and [2]Ms. Bhumika Patel

[1]Assistant Professor, Faculty of Computer science, Uka Tarsadia University, Bardoli, Gujarat, India
[2]Associate Professor, Faculty of Computer science, Uka Tarsadia University, Bardoli,Gujarat, India

ARTICLE INFO

Article History:
Received 14th May, 2023
Received in revised form
18th June, 2023
Accepted 20th July, 2023
Published online 28th August, 2023

Key words:

Electronic voting, Secure voting, Biometric, User Authentication.

**Corresponding Author:*
Dr. Dharmendra Bhatti

ABSTRACT

Voting is considered the fundamental right for being a citizen of a country; it allows a citizen to elect an appropriate candidate to form the ruling government. Electronic voting is better than the ballot voting system, but it has a lot of problems that cannot be overlooked. In this paper we have proposed that by creating an electronic system we can limit the tampering of the count by doing it using computer based system. Initially A user can be authenticated using many different techniques, here we have listed some of them and provided the more accurate combination for it. The problem with the existing system which works on a much basic and less technical standards, which occupies a lot of man power as well as the cost and the false authentication which is quite possible in the existing system that cannot be overlooked. Further we have learned that implementing the authentication using biometric is much reliable and efficient for e-voting among all the other techniques.

Citation: ***Dr. Dharmendra Bhatti and Ms. Bhumika Patel.*** **2023.** "Authentication of User for E-Voting System*". International Journal of Current Research*, 15, (08), 25491-25495.

INTRODUCTION

"Vote" is a Right for being a citizen of a country. In India voting is a constitutional right if one is a citizen over 18 years of age. It's a responsibility for each citizen to take part in election of the next candidate to work for our country/state/city/village. If the people of a country think that the ruling government is not performing their duties satisfactorily, they can show it the door by voting against it. And each vote matters for the development of country so it should take place in the righteous way. Considering the voting as an important part of functioning of a country, it needs to be legitimate and accurately conducted. There are political parties involved in corruption and which leads to the under grow the value and integrity of a country. The voting is so-far held using the traditional method in which the "Ballot voting" takes place. This probably can be tampered with and as a result gives out a false leader which is not quite expected. In this era of technology where everything works over the internet we are proposing a e-voting system which probably leads to accurate the counts of vote and allow each user to vote with least trouble and vote for their desired candidate without any manipulation. Considering an e-voting we might need to have a precise and ambiguities free authentication for user, which we are going to work on and find the best method for this process. By providing the best authentication techniques we can achieve a best way to collect the votes with a redundancy free and robust method. There are many ways of authenticating a user and all ways works magnificently in the desired situation, to provide the best way out of them we have listed out the the best outcome by comparing them with other techniques for the voting purpose. The Question arises "Why do we need it?" as it's a matter of power and prestige, the political party's which desired to be elected would be ready to try and play with the faith of the citizens so it's much more important to be done more precisely and without any false intentions. Recently there was a theory in US elections; tons of fabricated votes were encountered due to the fault in the system. So by providing accuracy in User authentication we can overcome it. By using the Biometrics authentication we can provide a reliable way to authenticate a user for e-voting. Further paper structured as, Section II as literature review, and followed by section III which explores the different methods for authentication. Section IV Discusses about e-voting around the world. Section V is Comparison and outcome. Section VI contains discussion over the papers. And Section VII concludes the paper.

LITERATURE REVIEW

What is Authentication?: In real-life scenario's people often ask for identification from people they don't know: A bank employee may ask for a driver's license before cashing a cheque, library employees may require some identification before charging out books and immigration officials ask for passports as proof of identity. In-person identification is usually easier than remote identification. So far organization and system have developed means of authentication, using documents, voice recognition, fingerprint and retina matching, and other trusted means of identification. In computing, the choice are more limited and the possibilities less secure. Anyone can attempt to

The most computing authentication systems must be based on some knowledge shared only by the computing system and the user.

Authentication mechanisms can use such qualities to identity User's:

Something user "knows": Password, PIN number, passphrase, a secret handshake, and mother's maiden name are example of what user knows.

Something user "Has": Identity badges, physical keys, a driver's license, or a uniform are common examples of things people have that make them recognizable.

Something user "Is": These authenticators, called biometrics, are based on a physical characteristic of the user, such as a fingerprint, the pattern of a person's voice, or a face (picture). Two or more forms can be combined for more solid authentication; for example a bank card and a PIN combine something the user has with something the user knows (Charles, 2011).

What is E-Voting?

Electronic voting (also known as **e-voting** or **EVM**) refers to voting using electronic means to either aid or take care of the tasks of casting and counting votes (https://en.wikipedia.org/wiki/Electronic_voting). Electronic government is defined as using Information and Communication Technology (ICT) to enhance government's operations, provide suitable services to citizens, and improve citizen's participation (World Bank, 2007). In their pursuit toward improved accountability to citizens (Carter, 2004), and improved public service quality (Irani, 2006), governments try to implement new technologies in all aspects of their operations. E-voting is one of the essential applications especially in the election process (Abu-Shanab, 2013) It is essential to realize the benefits gained from using electronic systems in the voting process, e-voting offers convenience to the election process, accuracy and accountability of results (Buchsbaum, 2005), time and cost savings (Bouras, 2005), increased public participation through open systems and Web 2.0 tools, and a flexible process for editing and updating voter's information (Weldemariam, 2007).

Authentication METHODS

Basic Authentication methods:

- Password Based.
- One-Time Password(OTP)
- Digital Signatures.
- Biometrics.
- "Something you have"(Smart-card's)

Password Based: The idea here is that you know a secret - often called a *Password* - which nobody else does. The Most common authentication mechanism for user is a Password. Passwords are mutually agreed-upon code words, usually known to the user and the system only. In some cases user chooses a password in other case the system assigns them. Password protection seems to offer a relatively secure system. Human practice sometimes degrades its quality. Most people understand that good password security is the first and most effective strategy for protecting sensitive systems or data (Here it's about authenticating User). Security using password is entirely based on the confidentiality and the strength of the password. They are widely used, still it can be compromised using some well-known techniques: Dictionary Attack, Brute force Attack, Phishing, Offline Cracking, Shoulder surfing, Guessing (known person) etc. When passwords are used for authenticating a user, the system must have a way to check whether the password entered is valid or not. Simply storing a file with the list of usernames and associated passwords, however, is a bad idea because if the confidentiality of this file were ever compromised all would be lost. Better not to store actual passwords on-line. So instead we might compute a cryptographic hash of the password, and store it somewhere in our system. Now when the user enters a password, the system computes a hash of that password, and the system then compares that hash with what has been stored in the password file. They can be secured by using many encryption techniques that can help secure the password authentication and provide a much reliable identification.

One-Time Password: A one-time password (OTP) is an automatically temporarily generated numeric or alphanumeric string of characters that authenticates the user for a single transaction or session. It is more secure then the static password, definitely more than the one user has created. They provide an additional layer of security while authenticating a user (4). Well the OTP which is generated is probably used for a very short period of time, so once the time runs out it becomes useless and this adds more secure feature to our authentication. OTP's can be accessible using Emails/SMS System to the registered Email-ID or Contact Number of the user. They are applicable for only for one time use. So they can't be reused and it reduces the security problems. There are many categories for OTP, such as Printed OTP, Soft Tokens, Voice calling, SMS text message and Email (5). There are different Algorithm's designed to make it more effective and secure, for example TOTP and HOTP (Time-based One Time Password Algorithm and HMAC-based One Time Password Algorithm respectively).

Digital Signature: It is a mathematical scheme that is used to authenticate the sender of an electronic document. It ensures that the document is really from the sender and not from someone else while at the same time ensuring that the message that reaches the receiving party is the same one sent without any alterations (2).

Digital signatures are probably used to send some sensitive information and to ensure it reaches the receiving party without any alteration. Commonly used for software distribution, financial transactions and in other cases where it is important to detect forgery and tampering. Considering the votes as our data, we can store the votes using digital signature so that they cannot be tampered and we get the accurate count at the end of the process. There are tons of advantages such as Speed, Costs, Security, Authenticity, Tracking, Imposter Prevention etc. (1) Digital signatures are like electronic "fingerprints." In the form of a coded message, the digital signature securely associates a signer with a document in a recorded transaction. Digital signatures use a standard, accepted format, called Public Key Infrastructure (PKI), to provide the highest levels of security and universal acceptance. They are a specific signature technology implementation of electronic signature (eSignature).

Biometrics: Biometric-based methods are based on the physical characteristics of the person that are different from one person to another (21). In computer science, in particular, biometrics is used as a form of identity access management and access control. However, biometrics is an ancient Greek word and is the combination of two words (bio) means life, (-metric) means measurement. Using biometrics such as: face recognition, fingerprint, iris and voice has several advantages based on its accuracy, uniqueness and complexity especially that it can't be stolen, altered or used by someone else other than the owner or the holder (21). As a result, systems that use biometrics in authentication process will increase the system's level of security and encourage people to use it in applications where high security is required. The performance of biometric-based authentication methods can be evaluated based on two main types of errors: *matching errors*, which occur during the voting period and *acquisition errors*, which occur during the preparation and registration stages. It has become one of the popular and trustable security systems that have become an alternative to password-based security system. Biometrics techniques have been developed for a machine-based verification of the identity of a person.

Something User Has: Instead of relying authentication on something a user knows and can forget, maybe we should work on something the user has. Various token/card technologies support authentication along these lines. Well, *two-factor authentication* becomes important

authentication process that involves two independent means of authenticating the user. So, we might require that a user not only possess a device but also know some secret password (often known as a PIN - 'Personal Identification Number'). Without two-factor authentication, stealing the device would allow an attacker to impersonate the owner of the device, with two-factor authentication, the attacker would still have another authentication burden to overcome. (20) A user may possess some of this technologies for authentication:

- A Magnetic strip card
- Proximity card or RFID
- Smart card

Considered Factors as attribute

There are three ways to perform authentication:

- Single-Factor Authentication
- Two-factor Authentication (2FA)
- Multi-factor Authentication (MFA)

In Single-factor Authentication the identification is performed by choosing a single technique either a password or any of the listed basic methods/techniques. It might be working in some situation but to give out the best positive outcome we should include the other factors. Two-factor Authentication works with two factors, which probably provides much better identification. For example: A user has his password and another factor such as OTP can be verified to check whether the user is valid by sending the OTP on the registered preferable contact/email such as phone or E-mail address. Multi-factor Authentication might work magnificently in some situation but it might annoy a user by giving them multiple trials to identify himself/herself. The concept behind Multi-factor is to include multiple (more than two) factors/techniques for identification of a user.

Comparative Study: Each authentication methods are different from one another. None of them has the same usage and each one will be used to fulfill specific needs. Moreover, different implementations of the same authentication method will provide very different levels of security.

E-VOTING AROUND THE WORLD: Here we have listed some countries which uses different ways of E-Voting. Additionally, it is important to highlight the lessons learned and the recommendations proposed for each case. E-voting has taken place in Brazil, Estonia, India, USA and Pakistan.

Brazil: Around 1996, after some tests conducted on more than 50 municipalities, the Brazilian Electoral Justice has launched their "voting machine". Since 2000, all Brazilian voters are able to use the electronic ballot boxes to choose their candidates (7). In 2010 presidential election, which had more than 135 million voters, the result was defined 75 minutes after the end of voting. The electronic ballot box is made up of two micro-terminals (one located in the voting cabin and the other with the voting board representative) which are connected by a 5-meter cable (7). Externally, the micro-terminals have only a numerical keyboard, which does not accept any command executed by the simultaneous pressure of more than one key. In case of power failure, the internal battery provides the energy or it can be connected to an automotive battery. The Brazilian electronic ballot box serves today as a model for other countries (8). The system was mainly based on the use of a unique ID for each voter. After entering this unique ID by the voter, a matching process carried out and the casting terminal is activated/deactivated based on this stage results (23).

Estonia: In Estonian each and every citizen possesses an electronic chip-enabled ID card, which allows citizen to vote over the internet. The ID card is inserted into a card reader, which is connected to a computer. Once citizen's identity is verified (using the electronic ID card as a sort of digital signature), he/she can then cast his/her vote using the internet (8). All the Votes collected are not considered final until the end of Election Day, so Estonian citizens can go back and re-cast their votes until Election Day is officially over. Popularity of Online Voting in Estonia has increased widely throughout the nation, as in the elections of 2014 and 2015, nearly one third of Estonian votes were conducted online. A small country like Estonia with a population of approximately 1.3 million, with a good infrastructure in communication, wide use of national ID cards, and a fair level of people's acceptance of e-services, all that play a central role in the success of Internet voting (I-voting) in Estonia. The Estonian e-voting experience occurred two times: the local governmental elections in October 2005, and the parliamentary elections in March 2007 (8). Using different methods for the authentication process in e-voting (e.g. public key infrastructure and the digital signature) has a significant impact on Estonia's I-voting process. (8) On the other hand, Estonian people have a high level of trust in their government and in the Estonian I-voting experience, which comes from the political support given to the I-voting system through several laws such as: the digital signature act in 2000 that gives Estonian people the ability to authenticate themselves by using identity cards with two digital certificates (PIN1 and PIN2), European Parliamentary Election Act, the Local Communities Election Act and many others (17). These certificates contain the cardholder name and personal information linked with two private keys embedded in the card (16).

India: The Indian electronic voting system is developed by the Electronics Corporation of India (ECIL) and Bharat Electronics Limited (BEL) which are government owned companies. Even though this system is characterized by its simple design, ease of use and reliability, several probable attacks and security issues need to be considered especially if any attacker can intercept the voting process and change the casted votes or vote more than one time. Several solutions to enhance the Indian voting system and overcome security issues were proposed. One of these solutions was using biometrics-based methods for authentication purposes based on storing people's fingerprint in a permanent database. This can be done in the voting preparation stage, where the matching process is done during the voting period to ensure that only registered and authenticated people can vote and for only one time (22). Since 2013 internet voting is gaining significant popularity in India but not as compare to other countries all around the World. There are certain instruction and guidelines set by Election Commission of India in terms of taking it into consideration due to some security reasons and to prevent internet frauds (Especially after the yahoo and google accounts hack drama). As per the set guidelines by Indian "samvidhan" and ECI act the e-voting can only be refer with a special approval by election body and relevant government depts. , and not before submitting the detailed report of "divisional results" to Returning Officers. It is then the responsibility of the Returning Officers to make a call based on the report whether to initiate the counting of e-voting or straight to declare the results on set date, as per the records e-voting has not yet played any role in Indian election system stated by Mr Achal Kumar Jyoti (Chief Election Commissioner of India).

Pakistan: Pakistan is one of the countries that have severe problems in the manual methods of voting in terms of trust, security and buying and selling votes. These problems call for a significant need to use an electronic way of voting that will guarantee voting accuracy and security with high level of people's trust in all stages of the voting process starting from the initial or preparation stage to counting votes and announcing the results. So an e-voting system is proposed to be used in Pakistan with an easy to user interface, minimum cost and a high level of security through enabling voters to use ID and password for login purposes and their fingerprints for authentication purpose before casting their votes (8).

RESULT AND DISCUSSION

Considering following attributes for each different basic method we have discussed:

- Time
- Overhead Calculations

- Prerequisite
- Cost
- Tampering

The question arise "why such attributes?" Looking at the facts there are almost 10 lakh voting booths in India and considering the eligible votes according the election commission of India, 814.5 million peoples were eligible to vote in 2009. Since the population is on such an huge scale the requirement of man power, the cost and the time consumed to perform voting is much high. Considering the prerequisite the adaption of new technology is not significant. Security is the major concern so system needs to be much reliable so that no tampering is possible. So considering this attributes we have tried to compare and conclude the better form of authentication.

Password

- **Time:** In password base system for Enroll user it will take around 0.10-0.20 microsecond and to authenticate a user it will take 0.001 to 0.010 microseconds. We have implemented using the PHP technology and the commonly used encryption method MD5.
- **Overhead Calculation:** Overhead time taken for a user to perform the voting using password based technique will be around 1 minutes max.
- **Prerequisite:** The only thing user needs to tag along is the username and a password.
- **Cost:** No cost at all, the user does not requires any device or anything, he/she just needs to think a pass-phase that nobody can think of but the user himself/herself.
- **Tampering:** Tampering is possible, there are a lot of ways to obtain an individual's password, which can be used to false vote or re-cast the vote (If system allows). Passwords can be stolen by an eavesdropper and can be used in order to gain access to the system.

One Time Password

Time: It totally depends on the response rate of the selected server, the OTP might be shared on the Mobile device. Sometimes due to network problem it might be possible that the user don't get the OTP in desired time interval. Normally it takes 30 seconds and its valid interval time is commonly about 5 minutes.

- **Overhead Calculation:** Overhead time taken for completing the single transaction using OTP depends on the receiving time and once the passcode is received, it takes about 30-60 seconds to authenticate a user to the server.
- Prerequisite: For Using the OTP based system, each user needs to possess a mobile device connected to the network which can be used to receive the OTP's. As well as the system also needs a functionality that provides such OTP's generating mechanism which will be having a linked email/number which was registered at the time of user registration.
- **Cost:** The possession of a mobile device for each user, sounds expensive. The system also needs to be handling/providing multiple users their OTP's, and such system is quite costly. Sending such number of messages are quite costly.
- **Tampering:** Tampering as an imposter is quite hard when it's used with other factors such as password. Using it as a single factor increases the chances of being tampered.

Digital Signature

- **Time:** Creating a digital signature might take a little bit of the time in the initial enrolment phase which is probably done using a private key. Recognition phase doesn't takes much time which is done using the public key available for all. Time consumed can be assumed less than a minutes.
- **Overhead Calculation:** Considering a user authentication it does not takes much of the time to validate the user's digital signatures.
- Prerequisite: Needs a pen and a pad at the booth to input user's signatures.
- **Cost:** The devices like pen and pad are much expensive to be implemented in a large scale. In order to effectively use digital signature, the system needs to have to buy digital certificates at some cost from the Trusted Certification Authorities. The software also needs to be bought and placed which might be costly as we are considering it on a large scale.
- **Tampering:** Tampering can be involved only when the signature of a person is compromised.

Biometrics

- **Time:** User enrolment using fingermight take maximum 0.9 sec, which can be lower as 0.3 sec (which might be increased to multiple trials). While recognition phase can be ranged under 0.2 sec to 0.5 sec. Increase in the ratio of recognition might take much longer time (For Example: 90% as parameter will take 0.9 sec).
- This statistic are obtained using the Visual Biometric Device, the implementation of code in C# Programming language, Using the technology .Net Framework, and for database we have used MySQL.
- **Overhead Calculation:** Overhead time taken for a user to perform the voting using biometric based technique will be around 1 minutes max.
- **Prerequisite:** Visual biometric devices: Analyses the visual features of the humans to grant access which includes IRIS recognition, Face recognition, Finger recognition and Retina Recognition
- **Cost:** Such devices are quite expensive, starting from 3k.
- **Tampering:** Tampering is not possible unless the prints are compromised. If someone has stolen those prints and have created wearable replica, in such case it might result in false identification.

Something You Have

- **Time:** Enrollment phase for card might take some time, as we are supposed to store all the information in encrypted form to be further authenticated. While recognition does not take much time as it just needs to verify the details from the servers, where the time depends on the response rate.
- **Overhead Calculation:** Overhead time taken for a user to perform the voting using Card based technique will be around 1 minutes max.
- **Prerequisite:** The voter needs to be occupied with the card which he is supposed to be used for authentication. Each booth needs to have card-reader which will be used to perform the identification of the user.
- **Cost:** Installing such devices in such a large scale will be much more expensive, still it is one time investment which be reused for a long time.
- Tampering: Stolen card might be a problem, which can be resolved by implementing 2FA. Magnetic card can be copied out and created a replica which might lead to a false vote.

DISCUSSION

We have studied different type of authentication method such as password based authentication, One Time Password based, Digital Signature, Biometrics and "Something You Have". After studied all these different type of method we discovered that the Biometric based is one of the best authentication method. In biometric authentication we can consider different traditions such as fingerprint scan, iris scan and face recognition. For any authentication method we consider different attributes such as Time, Overhead calculation, Prerequisite, Cost and Tampering.

Attribute / Method	Password	One Time Password	Digital Signature	Biometrics	"Something You Have"
Time	•Enrol user 0.10-0.20 microsecond. •Authenticate user 0.001 to 0.010 microseconds.	•Normally it takes 30 seconds	•Less than a minutes	•Enrol user 0.3-0.9 sec. •Recognize user 0.2 sec to 0.5 sec.	•Less than a minutes.
Overhead Calculation	•Around 2 minutes max per user.	•It takes about 30-60 seconds to authenticate a user to the server	•Around 2 minutes max per user.	•Around 1 minutes max per user.	•Around 1 minutes max.
Prerequisite	•Device that take user name and password as input.	•User have to Mobile. •OTP Generate system with election commission.	•Needs a pen and a pad which take signature as input.	•Visual biometric devices.	•Smart Card Reader at Booth. •Smart Card with each user.
Cost	•Zero	•Mobile and OTP System	•Signature pad and pen	•Visual biometric devices	•Card – Reader and Smart Card
Tampering	•Possible	•Possible	•Possible	•Not Possible	•Possible

Let's consider based on "Time" the password base authentication take less time than biometric, as in biometrics the data which we are retrieving is much more complex than the simple text but it might not be as secure as much we want for e-voting. Moving towards the next attribute "Overhead Calculation" Considering the predefined data acquired using the aadhar card number, it will take much lesser time in the recognition phase using biometrics. "Prerequisite" in smart card base voter needs to carry his/her smart card with them, but in biometrics voter needs to carry nothing with themselves. "Cost" which is the most important attribute of all, the biometric is one time investment to buy a Visual Biometric Devices and which can be used in all upcoming elections. Once installed it does not requires any other devices and it works much efficient than other techniques. And the last attribute which is one of the significant attribute, "Tampering". Biometric is considered the best method which offers least chances to acquire a false vote. Password can be forgotten, the smart card can be stolen and the OTP takes too much time if server response slowly .Therefore the biometric authentication method seems much reliable for authenticating a user for e-voting.

ADVANTAGES OF PROPOSED SYSTEM

- Reduce man power: many election officer are require for conducting election in large amount.
- Cost Reduction: Using the Biometric device it will reduce cost because it is a onetime investment

CONCLUSION

Initially in this paper we have discussed the importance of authentication of user in e-voting system. Stating the different techniques for authentication and trying to stat the flaws and strength for each techniques. Further we have indicated different ways depending on the factors, we have discussed the comparative studies for each technique we can use for identification, and we discovered that the biometrics seems to be more accurate in this arena. In the last section, we have discussed the attributes that are responsible for the effective implementation of the authentication techniques. So as an outcome we here by propose a system which uses the Biometrics to authenticate the user for E-Voting. The biometrics gives out a much secure and reliable authentication process, which decreases the chances of being tampered and removes the complications of false votes.

REFERENCES

https://www.ssh.com/manuals/server-zos-product/55/ch06s01s01.html

https://lerablog.org/technology/data-security/advantages-and-disadvantages-of-digital-signatures/

http://digitalindiainsight.com/advantages-and-disadvantages-of-digital-signature/

http://searchsecurity.techtarget.com/definition/one-time-password-OTP

https://www.portalguard.com/blog/2015/04/17/one-time-password-pros-cons/

https://en.wikipedia.org/wiki/Electronic_voting

https://en.wikipedia.org/wiki/Electronic_voting#By_country

Abu-Shanab, Emad, Rawan Khasawneh, and Izzat Alsmadi. "Authentication Mechanisms for E-Voting." *Human-Centered System Design for Electronic Governance*. IGI Global, 2013. 71-86.

World Bank. (2007). The World Bank website: Report from 2007. Retrieved May 26, 2011, from http://web.worldbank.org

Carter, L., & Belanger, F. (2004). Citizen adoption of electronic government initiatives. Proceedings of the 37th Hawaii International Conference on System Sciences, IEEE Conference, Chicago, USA, (pp. 1-10).

Irani, Z., Al-Sebie, M., & Elliman, T. (2006). Transaction stage of e-government systems: Identification of its location & importance. Proceedings of the 39th Hawaii International Conference on System Sciences, (pp. 1-9).

Buchsbaum, T. (2005). E-voting: Lessons learnt from recent pilots. International Conference on Electronic Voting and Electronic Democracy: Present and the Future, Seoul, Korea, March 2005, (pp. 1-22).

Saveourvotes.org. (2008). Cost analysis of Maryland's electronic voting system, 2008. Retrieved from www.saveourvotes.org

Bouras, C., Katris, N., & Triantafillou, V. (2003). An electronic voting service to support decisionmaking in local government. Telematics and Informatics, 20, 255–274. doi:10.1016/S07365853(03)00017-0

Weldemariam, K., Villafiorita, A., & Mattioli, A. (2007). Assessing procedural risks and threats in e-voting: Challenges and an approach. Proceeding VOTE-ID'07: 1st International Conference on E-Voting and Identity, (pp. 1-12).

Madise, U., & Vinkel, P. (2011). Constitutionality of remote internet voting: The Estonian perspective. Juridica International, 18(1), 4–16.

Maaten, E., & Hall, T. (2008). Improving the transparency of remote e-voting: The Estonian experience. Proceedings of 3rd International Conference on Electronic Voting, Austria, August 6-9, (pp. 31-43).

Selvam, P. Santhosh, S. Surya Prakash, and L. Balaji. "Advanced E-Voting System Using Finger Vein Sensor." *Asian Journal of Applied Science and Technology (AJAST)* 1.3 (2017): 304-306.

Charles P. Pfleeger, Shari Lawrence Pfleeger (2011), "Security in Computing" - Fourth Edition, Chapter-4, Page No. 242-244.

https://www.cs.cornell.edu/courses/cs513/2005fa/NNLauthPeople.html

Rao, G., & Patil, S. (2011). Three dimensional virtual environment for secured and reliable authentication. Journal of Engineering Research and Studies, 2(2), 68–75.

Reddy, A. (2011). A case study on Indian E.V.M.S using biometrics. International Journal of Engineering Science & Advanced Technology, 1(1), 40–42.

Esteve, J., Goldsmith, B., & Turner, J. (2012). International experience with e-voting. National Foundation for Electoral Systems (IFES). Retrieved from www.IFES.org

****