

# Securing Internet Voting Protocol using Implicit Security Model and One Time Password

Shumeza Abidi<sup>1</sup>, Hod. Amit<sup>2</sup>

<sup>1,2</sup>Dept. of Computer Science, Truba College of Science and Technology, Bhopal, India

\*\*\*

**Abstract** - This paper gives a cramped view about a web enabled application which has being originated and called Internet Voting System using Implicit Data Security which enhances security involving Login System & One Time Password. To brief more about Internet Voting System, this was being created in a more conventional way which was displayed as a dynamic website limited to users only on the computer or laptops but this is now being restructured to expand its usage to mobile users as well so that people can install it on their phones which will expand the volume of remote cast & increase the count of voters. These probable voters could be physically challenged, elder citizens, armed forces, youth and NRI's who are eligible to cast their votes.

**Keywords**- Internet Voting System, Implicit Data Security, One Time Password, Login System.

## 1. INTRODUCTION

Internet Voting has intensively considered since in last few years. Various Internet Voting Protocols, therefore, have been scheduled in last few years and progress its effectiveness and security in various term. Internet Voting Protocol allow voter to involve in an election over the network via internet. Internet Voting Protocol encourages two voters and elections organizer where Voters has the facility to cast his vote ballots when and where, most suitable for them and in addition it aid election organizers by publishing accurate election result on the evening of the election. Nevertheless, the leading, Solution with no errors has been found for large scale election.

Design of complete Internet Voting Protocol over a network is exceptionally complex job as various requirements of the Internet Voting System have to be met. Breakdown in any specification may lead to failure of whole system. A good Internet Voting Scheme makes sure that the participants should keep his ballots private. In other words, the participant must not be able to prove anyone that user has cast a particular ballot. User shall not be able to make an evidence of the content of his/her ballots.

For the Internet Voting System to function efficiently it ensures error-free and robust online voting, it must gratify the following criteria.

1. **Eligibility** – Except eligible voter, no one can vote.
2. **Anonymity** – Voter should have no knowledge where his/her vote is.

3. **Verifiability** - A voter should have the knowledge about his/her vote be added to the final reckoning and whole process of voting should be fair.
4. **Fairness** – Process of Voting and Counting should be completely fair.
5. **Forcibility** - A voter can cast his/her vote under no pressure.
6. **Receipt-freeness** – voter should not have proven of his vote.
7. **Privacy** – vote of voter shall be secure and not shared by any voting authorities except counting poll process.
8. **Robustness** – any wrong behaviour of any particular voter should not influence the entire process of internet voting system.

Internet Voting over the network via Internet would be much more profitable voters has the facility to cast users vote from anywhere across the globe. Many voters would appreciate the feature of Internet voting because by this, rate of legal voter is increases as it as fast, cheap and convenient which give great slam on the contemporary democratic society. But simultaneously, this feature of Internet Voting Protocol decreases the rate of voter to cast users vote because voting process held over electric media that is computer or laptop and at the time of voting, user cannot cast his ballot without computer. For a successful process of traditional Internet Voting System, user has to go to the website via computer and internet and have to perform various authentications and verification task which cannot be make possible without computer and laptop.

Thus it is conclude that, for sensitive issues like elections, security is the major worry but at the same time, Simplicity is also an important factor to ensure the participation of common users.

Besides Security and simplicity, there may be some other issues that need to be considering in order deploying a successful internet online voting election. The next important factor that needs to be considered is authentication and authorization. these factors ensures that only entitled voters shall cast a ballot that is only a legal voter can participate in voting process over Internet Voting System . To ensure authentication and

authorization, uses normally traditional Login system is used in which a static ID and Password is used to ensure authentication and fairness to the system. But while using static ID and Password is vulnerable against eavesdropping, replay attack and Man-in-the-middle.

Traditionally, Internet voting system uses Modern cryptographic voting execution in which multiple layers of encryption are present and decryption key for each encrypted layer is with different authorities this action is prime for improving fairness, confidentiality and verifiability to the Internet Voting System. In modern Cryptography Voting, uses multiple layer of encryption and decryption of data at various levels such as a master public/private key pair is cast off for encrypting and decrypting of data that is ballots. Also, an individual's public/private k-key pair for respectively record legal voter. This multi-level of encryption and decryption leads to the system load.

## II. LITERATURE SURVEY

In this paper [1], the author tries to emphasis on the action of storing election data in Online Voting System. In order to achieve outrageous security in system, Author introduces two level of authentication technique. Face Detection and recognition system is first authentication technique and another authentication Technique is One Time Password. Both authentication techniques help in enhancing Vulnerability of the system.

In this paper [2], author focused on security bases on cloud data storage. , Thus uses flexible and effective distribution scheme. In which data partition method involves roots of a polynomial in restricted field. A data is breakdown into several small and store it on random chosen server on the network and for retrieving original data, data needs to be reconstructed which is further secure using Login system and one time Password system.

In this paper [3], authors try to modernize the security of an online storing system that is cloud computing. Revamp in security is done by duo authentication mode. Dual authentication mode consist of Login System and One Time Password .In One Time System enhancing security by force of access control over cloud computing whereas Login system enrich the power by Inc. authentication and flexibility to the system.

In this paper [4], the author demonstrated that propose a downright utilitarian System called online data storage. The plan has picked to make online system more secure using data partitioning scheme in which uses multiple roots in finite field. In data Partitioning Scheme, partition stored on apparently servers of the network and to recreate data, partition has to be reconstruction. In order to reconstruct, access to each server is necessary and for that credentials of each servers need to be know.

In this paper [5], the author studied that the technology for securing online data that is implicit security techniques. In

this paper , author specially focus on cloud computing as an online data storage system where try to enhance security in cloud computing using implicit security and different facts like One time System and traditional Login System which more authentication to the system.

In this paper [6], Author introduces TSOTP, a fair and effective OTP method. In which an isolated password is generated for one time use and this isolated password is generated based on both time stamps and sequence number. This paper also conclude that while accessing mobile phone devices as a OTP generator has vulnerabilities to many attacks , memory scan attacks and software clone blitz.

In this paper [7], Author mainly concentrates on the attacks using static ID and password and to avoid such attacks uses One Time password concept thus introduces a method to generate One Time Password by using Genetic Algorithm and Elliptic Curve Cryptography.

In this paper [9], Author tries to enhance the correctness of user's data in Cloud Computing. By this way, author increases security in Cloud Computing based on Data partitioning Scheme and Security Key Distribution scheme. In different expressions author introduces a technology which includes the Implicit Storage of encryption Keys rather than the data and retrieving of data can be done by reconstructing of data.

In this paper [10], author mainly concentrate on issues of Cloud Computing that is Security of Data stored in the servers of data centers of Cloud Computing, Author uses Implicit Security Technology using information dispersal and Secret Sharing Algorithm. By using this technology in the Cloud Computing gains data security, reliability and availability of information.

In this paper [11], author proposed a new idea using One Time Password to secure static password in an Online based application. In this paper[11], performance and security is enhance by sending Encrypted One Time Password to the users and users can only be login by Mobile based technologies.

In this paper [12], the author discussed about ways to reduce security of system by password. Generally , Text based words are used for authentication which prone to various attacks like password stealing attacks , password reuse attacks , password cracking attacks , brute force attacks , etc . Also, author discusses all the advantages of using One Time password over text based words password for improving security of a system.

Web Based Mobile Application First, from many past year, Internet Voting System Our main research and development activities are mature on Ensuring Security and swell usability and availability in Internet Voting System. For ensuring security we are applying Implicit

Data Storage technology which enhances data security, reliability and availability of information and fairness of the system. For extend usability and availability we introduce new authentication method using Two-way authentication which provide dual protection to the system. In other word, two-way authentication provide high level authentication to the system by verifying mobile number using One Time Password system also, verifying username and password using Login system. Combination of One Time Password system and Login system protects the Internet Voting system from many attacks likes Phishing attacks, man-in-the-middle, Malware Trojan, Reply attack, Delay attacks, eavesdropping.

#### A. Web Based Mobile Application

First, from many past year, Internet Voting System using in various countries as an real Voting system where votes of the votes are taken via official website and voting is done under various security aspects. This present scenario of taking votes on a website decreases many votes such as its difficult to manage system and internet connection with respect to login on a website and in case of re-voting, user has to login again and again thus the possible of hacking an account is high and also its inconvenient for a user to visit again and again on system. Therefore, in this Paper, Problem is solved by creating a Mobile Application for Internet Voting System under various security aspects.

#### B. Implicit Data Model

Implicit Data Model In, Implicit Data Model, the Data partitioning scheme is used with multiple servers where each partitioning piece is stored in different servers. In order to retrieve data user should be familiar with the password & server where the subset is uploaded. This information is kept in the HTTP Virtual Directory. Therefore the partitioning piece is implicitly secure as it shouldn't give the complete information to any hacker. This technique increases load balancing as it simplifies the storage of each partitioning piece.

Internet Voting Protocol demands confidentiality & verifiability as traditional researches focused on securing of each vote which was done by cryptography using multiple layers of encryption and decryption key for each layer assigning it to different authorities which creates an element of doubt that which authority is trustworthy. Hence the entire process of Implicit Data Security will remove such hindrances of encryption/decryption in Internet Voting Protocol where Implicit Data Security involves data partitioning scheme, which means each vote will be further divided into  $m$  or more pieces and each piece is stored in different servers. Each server consists of a unique ID and password which will enable each server to keep the segregated data in it. Original data can be redeeming by reconstructing the partitioned pieces whenever required.

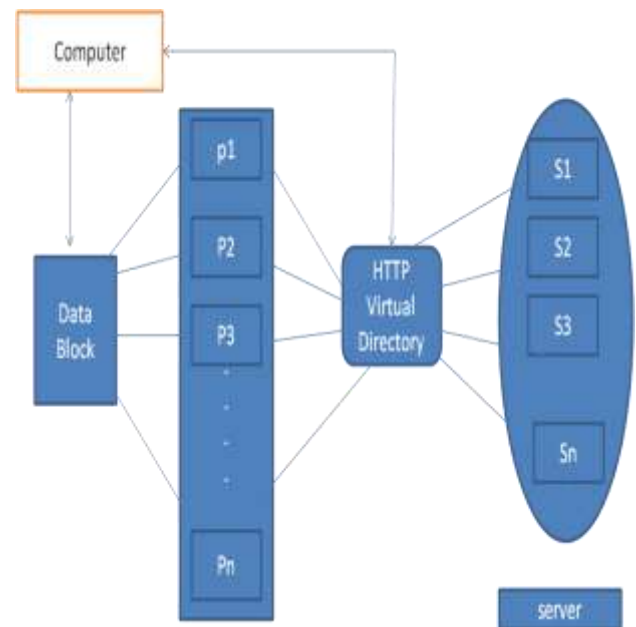


Figure 1 : Implicit Data Model

#### C. Two-Way Authentication

In this Paper, Internet Voting System is get further secure by getting Two-way Protection that is double protection. Two-Way Protection gives security to the system in two ways. Before going to Internet Voting Protocol, two special systems are building up with respect to boost the security such as. For dealing with sensitive data, Single-factor authentication is not effective thus recommended to use Multi-factor authentication because in single factor authentication, authentication is done with using ID and password as they are inexpensive, ease of implementation and familiarity that is remain common. But they are not as secure and may reach to brute force attack, phishing attack, where in multifactor authentication helps in minimizing the rate of online identity theft, phishing expedition and other online fraud.

##### 1. One Time Password:

A Time-based One Time Password is a unique password that is valid for certain time period for only single Login session or transaction, on a mobile application or on a computer system. One Time Password can be sending in many ways via email, SMS etc. Here, we are practicing SMS Gateway which acts as super high priority gateway which delivers instantly. In this paper, Internet voting system is getting more secure by use of One Time System. In Internet Voting System, One Time Password is used every time prior to the Login System. Thus by this process, Internet voting System ensures legitimacy.

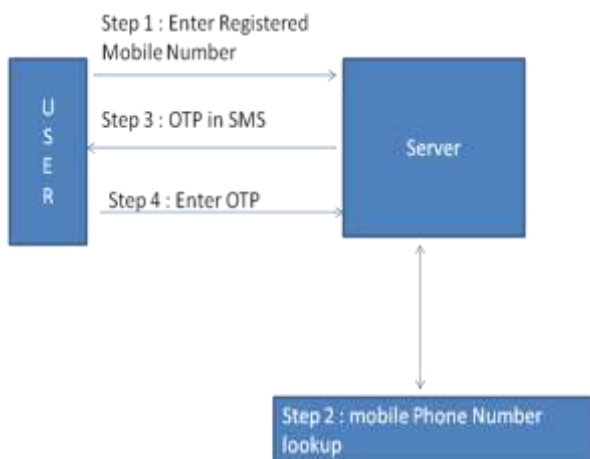


Figure 2 : One Time Password System

## 2. Login System:

Login system helps in improving system's verification, fairness and authentication. If in any case, a hacker is able to hack a login system then also he cannot cast any illegal bullet because every time prior to sign in, he/she has to enter his registered mobile number and an One Time Password will cam to that number and when user enter correct One Time Password then only he/she can go to Login System of Internet voting system.

## III. RELATIVE WORK SOLUTION

By way of this process we will ensure providing secure services to the internet voting protocol via partitioning the user data stored in different servers which can be further improvised using advanced security techniques. Current models of Internet Voting System are being used only on dynamic websites which restricts the count of users since it is not feasible to carry computers or laptops everywhere hence by creating the web application we can increase the count of ballots as users can easily vote using this application on their mobile phones.

Now days, Internet voting Protocol is working on the concept of cryptography, that is votes of voters is secured using Encryption and Decryption which is very effective but at the same time it's very hectic, time consuming and tuff to handle storing of Encrypted layers data. In order to secure votes, a vote has to go under many layers of encryption and at the same time , for reading the data then that layers has to go to many decryption layers thus its bit hectic to deal with this huge data of encryption and decryption layers and its keys. Therefore, this paper introduces new technique which helps in replacing the disadvantage of cryptographic technique and that technique is Implicit Security Model.

Another way of enhancing security is adopting One Time Password which is sent via registered email or SMS to the user. User can access the data only if the correct One Time Password is entered. The One Time Password is unique

which means the user can access it only once as it shouldn't be used again. When a user is asked for One Time Password to authentication then ideally of typing code in the screen, user only have to click send button. As user click on it, the code is sent through your phone to server, where it will check and then user will allow going for login page. This One Time Password system, increase Easiness, Eligibility, Reliability and usability of the system. In other word, a potential intruder who rule to record a valid one time password but then also user shouldn't be able to abuse it because for a successful one time password transaction, user must enter a right one time password from the user mobile devices, thus the mixture of one time password and unique id (creates on installation time) need for a successful transaction.

Finally final technology to enhance security is login system which ensures confidentiality of the system & helps in maintaining the record of user to fetch individual user information when needed. When user installs application on his/her mobile phone, the mobile application generates a isolated credential ID tried to the user, thus ID is registered must registered by the admin of application or by the user themselves.

Once the registration process is done, then for every new sign in process, user must provide a valid one time password which will only valid for a min.

## IV. PROPOSED MODEL.

### D. The proposed model for Client Side is as follows :

Internet voting system is the most commonly used programme in all counties that's the reason the client side template has been created so generic and also the usability is high so that the leman user may also take a advantage from it without facing any trouble .

- 1) First of all user have to enter registered mobile number.
- 2) An OTP will be sent to registered mobile number also he can proceed only after inflowing that OTP.
- 3) If he enters approved OTP, he will be able to progress and then a login page will appear that will ask for user's id and password.
- 4) User should be able to cast ballot only if he enters right password
- 5) Id diverse phases are integrated in this proposed model such as Registration Phase, Login Phase and many more that will be done in the conventional manner.

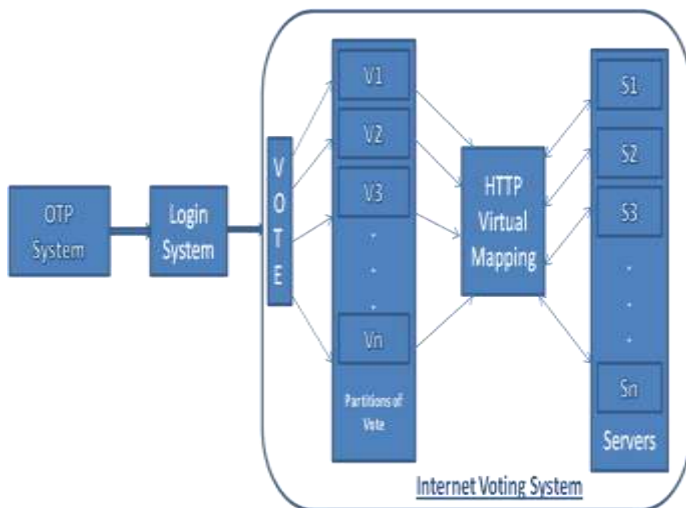


Figure 3 : Secure Model of Internet Voting Protocol

E. The proposed model of Server Side is as follows :

- 1) Segregate each cast secret ballot into m or more pieces such that each Server stored one of the piece.
- 2) This eliminates the worry of entrusting any Server with all polls and if any one try to cheat by deleting some of the cast ballots from any server, then the votes should be recreated using abide partitions.
- 3) Such a system implicitly provides a back-up for the votes. Also help in eliminating the process of Cryptography which is very time consuming.

## V. CONCLUSION

In this paper, the proposed technique may be proved valuable in terms of security; authentication as well as it will save bandwidth of network as via One Time Password prior to Login phase will guarantee legitimacy of the user to a great extent and further Login phase will serve the security purpose. Also, this paper concludes that our proposed method of replacing Cryptographic technique by implicit data storage for securing data leads to load balancing.

## Acknowledgment

We express our warm gratitude to Prof. Amit Sharma, Department of Computer Science and Engineering, Truba Institute of Technology, Bhopal, for her valuable guidance and timely suggestions during the entire duration of my project work, without which this work would not have been possible.

We would also like to convey our deep regards to all other faculty members and staff of Department of Computer Science and Engineering, Truba Institute of Technology, Bhopal, who have bestowed their great effort and guidance

at appropriate times without which it would have been very difficult on my part to finish this project work. Finally I would also like to thank my friends for their advice and pointing out our mistakes.

## References

- 1) E-voting Using One Time Password and Face Detection And Recognition : International Journal of Engineering Research & Technology (Ayesha Shaikh, Bhavika Oswal, Divya Parekh, Prof. B. Y. Jani).
- 2) Implicit Security Architecture Framework in Cloud Computing Based on Data Partitioning and Security Key Distribution: International Journal of Emerging Technologies in Computational and Applied Sciences ( S.Hemalatha<sup>1</sup>, Dr.R.Manicka Chezian<sup>2</sup> <sup>1</sup>Ph.D Research Scholar, <sup>2</sup>Associate Professor).
- 3) Access Control for Cloud Computing Through Secure OTP Logging as Services: International Journal of Computer Applications ( Priyanka Patel, Nirmal Gaud).
- 4) Online data storage using implicit security: Elsevier Journal (Abhishek Parakh , Subhash Kak).
- 5) Security in Cloud using Implicit Security Model and OTP: International Journal of Advanced Research in Computer and Communication Engineering(Akanksha Rana).
- 6) A new One-time Password Method: Elsevier Journal (Yun Huang, Zheng Huang, Haoran Zhao, Xuejia Lai) .
- 7) One Time Password Generator System : International Journal of Advanced Research in Computer Science and Software Engineering (Tamanna Saini).
- 8) OTP Encryption Techniques in Mobiles for Authentication and Transaction Security: International Journal of Innovative Research in Computer and Communication Engineering (Dr.AnanthiShesashaayee, D. Sumathy)
- 9) Implicit Security Architecture Framework in Cloud Computing Based on Data Partitioning and Security Key Distribution : International Journal of Emerging Technologies in Computational and Applied Sciences (IJETCAS)( S.Hemalatha, Dr.R.Manicka Chezian)
- 10) Review of Implicit Security Mechanisms for Cloud Computing: International Journal of Computer Applications (0975 - 8887)( Makhn Singh, Sarbjeet Singh)
- 11) Secure Login Using Encrypted One time Password And Mobile Based Login Methodology : International Journal Of Engineering And Science Vol.2, Issue 10 (April 2013), Pp 14-17(Ms. E.Kalaikavitha, Mrs. Juliana gnanaselvi)
- 12) A Survey on One Time Password : International Journal of Science and Research (IJSR) (Mirza Tanzila Maqsood, Pooja Shinde)
- 13) Online Banking Security System Using OTP Encoded in QR-Code : International Journal of Advanced Research in Computer Science and Software

Engineering( D. R. Anekar, Binay Rana, Vishal Jhangiani, Aziz Kagzi, Mohammed Kagalwala)

- 14) Analysis of an internet voting protocol :2010 (Kristian Gj\_steen\_)
- 15) US Election Assistances Commission : A Survey of Internet Voting(Voting System Testing and Certification Division 1201 New York Avenue, NW, Suite 300 Washington, DC 20005)