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

Shumeza Abidi
Dept. of Computer Science
Truba Institute of Engineering & Information Technology, Bhopal, India

Amit Saxena
Dept. of Computer Science
Truba Institute of Engineering & Information 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.

As we growing with technologies, people are getting dependent towards technologies an s a result technology is rapidly Inc in every field of human's life. Technology is playing vital role in every one's life. In industry set forth in the recent years is Information technologies has evolved with superlative momentum, and accrued a dignified status for itself, and all those associated with it. It should be either big industry, software companies, government organization all is dependent on the technologies these days.

One such technology is internet Voting System. Several government around the world have been experimentally as a mean to make election as their default layout. Though, to secure the data in large scale implementation is very tough to handle.

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.

2. LITERATURE SURVERY

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 distinct authorities which creates an element of doubt that which authority is trustworthy. Hence the entire process of Implicit Data Security will clear out 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 kept in distinct servers. Each server consists of a unique ID and password which will enable each server to store the segregated data in it. Original data can be recovered by reconstructing the partitioned pieces whenever needed.

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.

2.1 Web Based Mobile Application

First, from many past year, Internet Voting System using in various countries as a 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.

2.2 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.

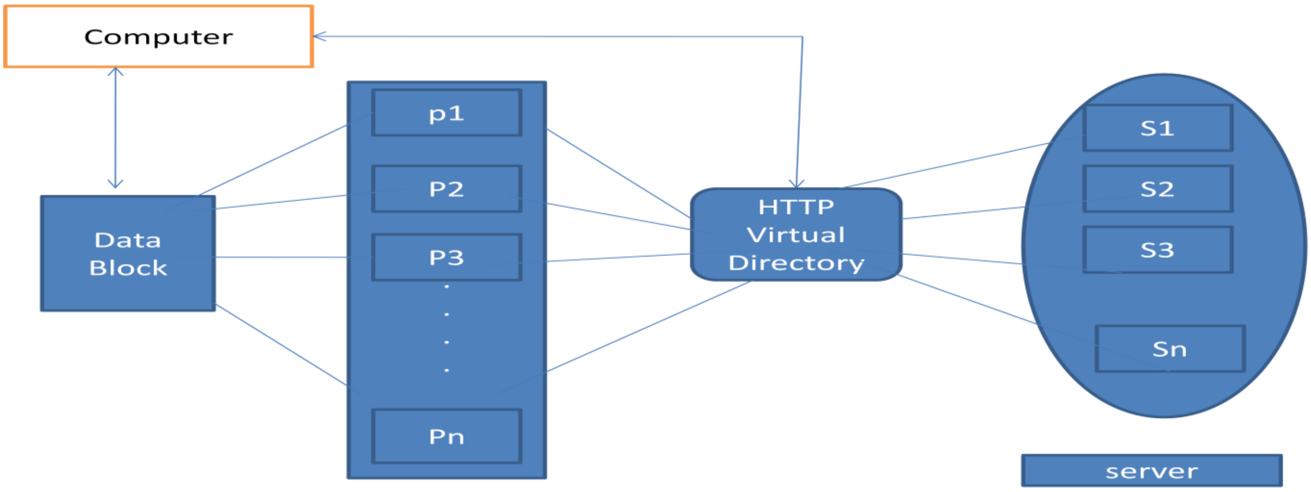


Figure 1 : Implicit Data Model

2.3 Two-Way Authentication

In this Paper, Internet Voting System is get further secure by getting Twoaaaaaaaaaaaaaaaaaa-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 attach, phishing attach, where in multifactor authentication helps in minimizing the rate of online identity theft, phishing expedition and other online fraud.

2.3.1 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.

2.3.2 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.

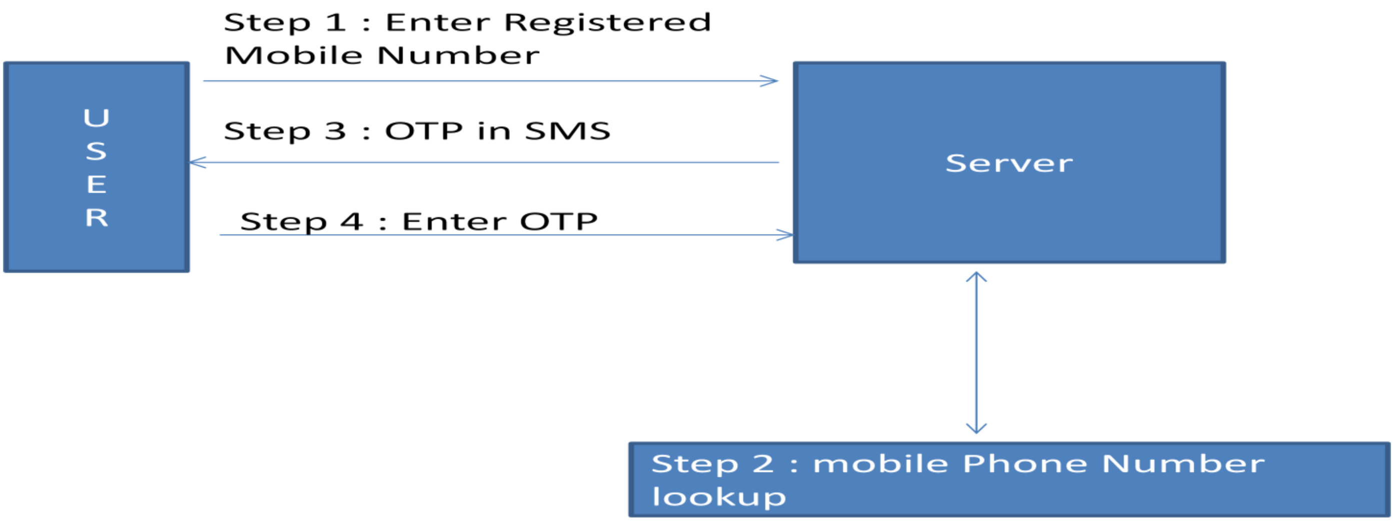

Step 1 : Enter Registered Mobile Number
USER
Step 3 : OTP in SMS
Server
Step 4 : Enter OTP
Step 2 : mobile Phone Number lookup

Figure 2 : One Time Password System

3. PROPOSED METHODOLOGY

First, from many past year, Internet Voting System using in various countries as an authentic 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 in order 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 come 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.

As to give high level security to an web based mobile application , a data partition schema is used in which data I partition into k parts such that each part are stored on randomly chosen server. Encryption is not obligatory to protected explicit partition because they are implicit secure as each partition, themselves don’t reveal any information. Data is revealed only when all the partitions are brought together. Total number of partition (k) of each data should be partition into same number where each partition should contain equivalent number of bits (b). However, total no of partition (k) should not be disclose to anyone thus it should be private therefore it should be equal to the total no of servers.

Let assume that k be the total no of partition of data of length (l) and is no publicly disclosed and m be the total no of servers in which partition has to stored. Then,

$$K = m;$$

K be the total no partition of data with length l, (any natural number) also m be the total no of servers in with each partition

Let us assume that if length of a string of data is l bits and m is the total no of servers in with each partition. Therefore,

$$l / m = r;$$

Where, r is the reminder of division and q is the question of division. Now, the two cases with be form on the basis of value of r that is if r is equal to zero or if r is not equal

CASE I: (r =0 ;)

If r is equal to zero then data of length l should partitioned into m parts such that each parts should conation q bits of data. Each partition of q bits is implicit secure hence themselves they don’t reveal any information.

CASE lI: (r =! 0 ;)

If r is not equal to zero then it cannot be negative number and it should be any natural number, also r should be less than m. Then, $m – r = z;$
Where, z can be any natural number. Then,

$$l + z = Y;$$

Where, Y is a natural number and is complete divisible by m such that:

$$Y / m = r$$

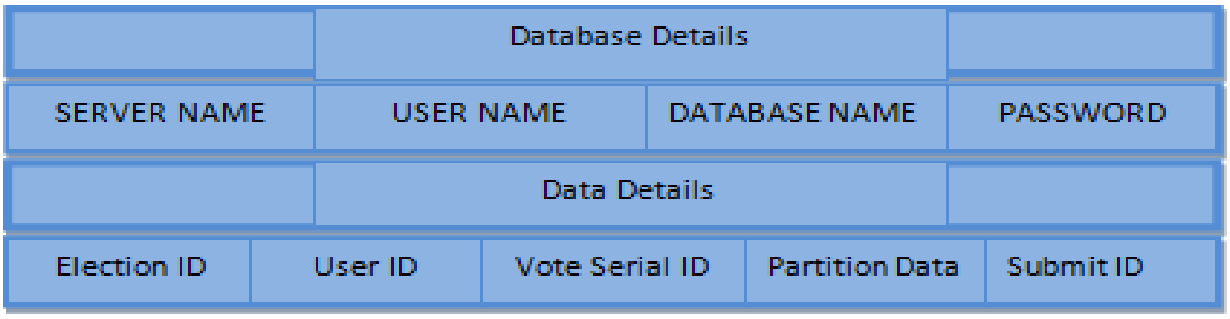
Where r = 0;

Thus then proceed to case l.

4. RESULT ANALYSIS

A wrap up is sending to store each partition of data on different server. Package include all the necessary details of database and also, contain partition data which is many other details is appended on it such as election id, user id etc. To became easy which reconstruction of data.

This package includes details of database such as server name, database name, username, password of database in which particular partition need to store. Apart from this, other information for instance election Id is the Id of particular election which is going on. User Id is the id of user who is pitch their vote serial Id the Id which help is getting the sequence of data so that later, it can arrange in correct sequence. Serial Vote data is one the partition from K no of partition with q bits which don’t reveal any useful information. Submit Id is generated at the time of user cast his ballot in a favors of any participant.



Database Details

SERVER NAME | USER NAME | DATABASE NAME | PASSWORD

Data Details

Election ID | User ID | Vote Serial ID | Partition Data | Submit ID

Figure 3: Data Packet

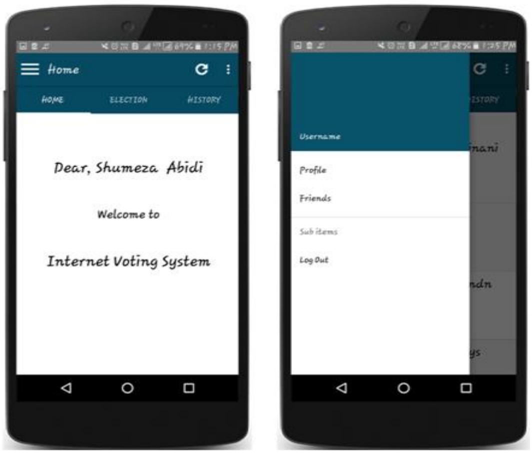
Table 1 : Result Comparisons

S. No	Paper Name	Technique	Drawback	Enhancement
1	Online Storage Using Implicit Security	Implicit Security for online data storage in cloud computing environment.	No authentication is used.	Two-way authentication is used: OTP & Login system.
2	Internet Voting Protocol based on Implicit Data Security	Internet Voting based on Implicit Data Security.	No authentication is used.	Two-way authentication is used: OTP & Login system.
3	E-Voting using OTP and Face Detection & Reorganization	Online Voting System using two-way authentication.	Face detection Technique under various consciences lead down usability.	Replacing Face detection with simple static login page. Creating an mobile app Which enhance the easiness and usability of system.
4	Security in cloud using Implicit Security Model and OTP	Implicit Security in Cloud Computing environment.	Authentication system is not secured.	Replacing Cloud computing environment by Online Voting environment.
5	Implicit Security Architecture Framework in Cloud Computing Based on Data Partitioning and Security Key Distribution	The implicit storage of encryption keys rather than the data in Cloud Computing Framework.	Secured authentication is not used.	Secured Two-way authentication and Mobile application is used to maintain high security and usability at the same time.

5. PROPOSED MODEL

5.1 Proposed Model for Client Side

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 .Common Layout involves all layouts which can be able to see by Admin Role, Voter Role, and Counter Role with respective data. This layout includes fragments Home Fragment, History Fragment, Side Page. Very first page user will be after successful login is Home Page which contains the details of user according to their role. All users with all roles can able to see history which involve details of past election which occurs in History Page. A Side tap layout is also visible by all users thus it is also common.



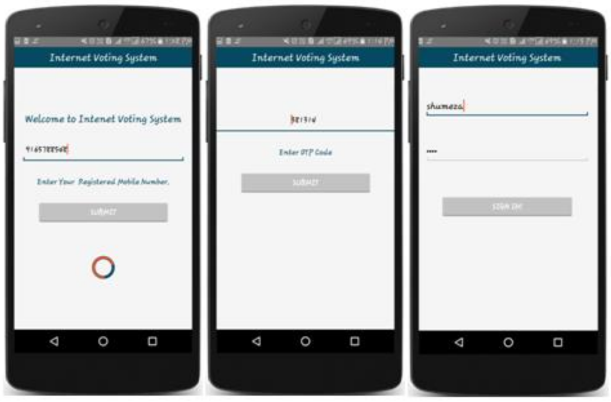
Dear, Shumeza Abidi

Welcome to

Internet Voting System

5.1.1 Authentication Phase

First step of Two-way authentication is that all users will be asked to enter his registered mobile number. If that mobile number is registered then only an OTP will be send to user's registered phone number and he can proceed only after entering the OTP. If he enters correct OTP, he will be equipped proceed further and a login page will appear that will ask for user's id and password. Then user have to enter correct id and password, after entering correct id & password he will be able to get admittance to his data. Various phases are included in this proposed model such as registration and login phase, that will be finished in the traditional manner .The proposed technique may be proved useful in terms of security plus it will save bandwidth of network as using OTP prior to login page and will ensure legitimacy of the client to a great extent and further login page will serve the security purpose.



Welcome to Intenet Voting System

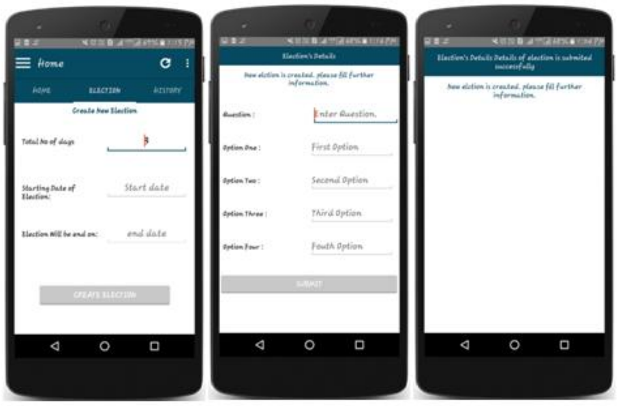
Enter Your Registered Mobile Number.

Enter OTP Code

shumeza

5.1.2 Admin Role

When user with admin role done successful login then he will able to see a sliding layout which displays three pages: Home Page, Election Page, and History Page. A home page carries user's information while Election pages helps in creating new election. When user select Election page then for creating new election, few questions asked from user then have to click submit button , after clicking on submit button , election had created and a new election id is generated at server point and save in database. After that user will reach to new page in which user have to add new question and 4 options in it and save it by click on button? When data will successfully saves then a confirmation message will display.



Home

HOME ELECTION HISTORY

Create New Election

Total No of days 3

Starting Date of Election: Start date

Election Will be end on: end date

CREATE ELECTION

Election's Details

New election is created, please fill further information.

Question : Enter Question.

Option One : First Option

Option Two : Second Option

Option Three : Third Option

Option Four : Fouth Option

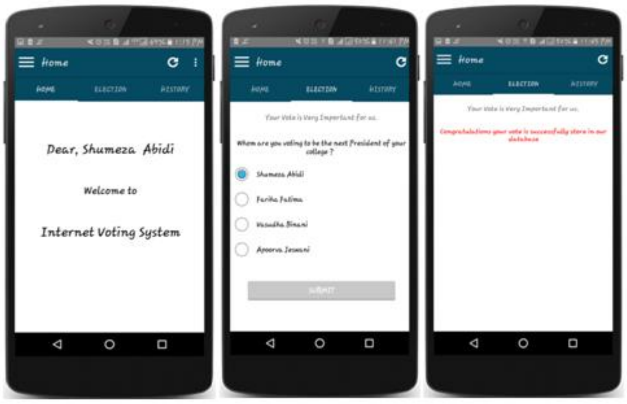
SUBMIT

Election's Details Details of election is submited successfully

New election is created, please fill further information.

5.1.3 Voter Role

Voter Role allow users to pitch user's vote thus any user with voter role will able to notice a sliding tab layout after login which contain 3 pages that is Home page , Election page and History page . In which election Pages gives user's functionality to pitch user's vote .As soon as user's vote is successfully cast then a successful massage will display. when user able to cast a successful vote then data of that vote is implicit secure as it will break into n parts and append some data in it and send that to different server .



Home

HOME ELECTION HISTORY

Dear, Shumeza Abidi

Welcome to

Internet Voting System

Your Vote is Very Important for us.

Whom are you voting to be the next President of your college ?

● Shumeza Abidi

○ Fariha Fatima

○ Vasudha Binani

○ Apoorva Jeswani

SUBMIT

Your Vote is Very Important for us.

Congratulations your vote is successfully store in our database

User should be able to cast ballot only if he enters right password Counter Voter allow user to recollect the data from the server and able to fetch the numbers of the votes for each party and then deliver the name of winner and also able to publish it to all user so that everybody get to know the result of the election and also get to know that election is closed. User with Counter role will able to see a sliding tab layout after login which contains 3 pages that is Home page, Election page and History page.

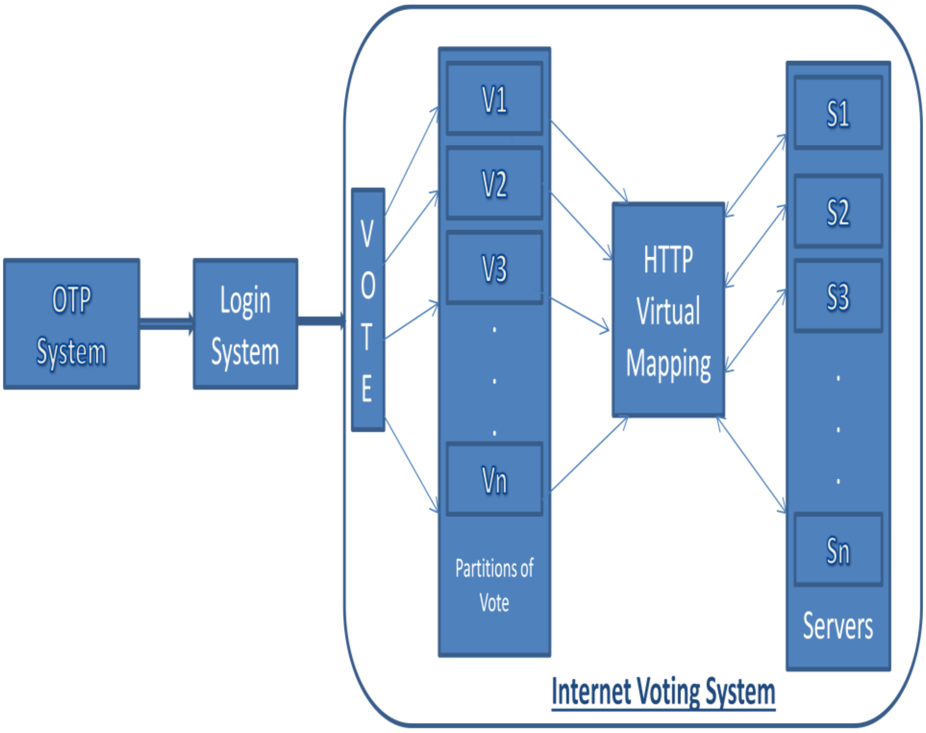


Figure 4 : Secure Model of Internet Voting Protocol

6. 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.

7. ACKNOWLEDGMENT

We express our warm gratitude to Prof. Amit Saxena , 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.

8. 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.Hemalatha1, Dr.R.Manicka Chezian2 1Ph.D Research Scholar, 2Associate 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)(Makhan 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)