Design and Strategies for Online Voting System

Sayan Mazumder
U.G. B.Tech Student
Sikkim Manipal Institute Of Technology,
Sikkim Manipal University, Sikkim

Bijoyeta Roy
Assistant Professor
Sikkim Manipal Institute Of Technology,
Sikkim Manipal University, Sikkim

ABSTRACT
If a closer look is taken to the voting system of India, one will find that, it is as flawed, as the ones implementing the procedures, thereby depriving the citizens of India, one of the most important ideals of democracy, i.e, "FREE AND FAIR ELECTION". This is mainly due to the unfair practices, undertaken by the so-called "Powerful" and "Influential" people, involved in the system. Hence this project aims, to transfer the responsibilities of conducting the entire "ELECTION VOTING" procedure, to computing machines, which are expected to behave in an impartial way. Moreover, since this project will make the system totally online, and users will be able to vote, sitting behind their personal devices, rather than physically going to the polling booth, there is a very high probability that this project will encourage, more participation of Indian citizens, in the voting process, thereby making the election truly "Free And Fair". This project analyses various real-time implementation problems and provides a solution for each. This project also introduces, a concept of "RANDOM PARTY CODE", in order to enhance the integrity of the system, i.e , to prevent the adversary from comprehending the vote, even if he/she manages to take a look at the vote. This project also gives an ideal solution for "PUBLIC VOTING".

Keywords
Online Voting, Random Party Code, Public Voting, Implementation Problems.

1. INTRODUCTION
In the 21st century life, people use various devices at home, for example, Televisions, Computers, mobile phones, etc. to help ease various daily life tasks, like banking, shopping, education etc. which , otherwise , will induce wastage of huge amount of time and money, if the client have to be physically present, every time he/she requests a service. Since this system has already been used in banking, which protects one of the most important assets in human life, i.e., money, therefore, developing the system to conduct "Free and Fair Elections", seems like a really viable and attractive idea.

Online voting is different from e-voting systems, in the way that, in "Online Voting", the user can vote directly from home, using devices that are used in daily life, like, laptop, computers, whereas, in e-voting, the voter needs to go physically to the polling centre, where, he/she will be verified for voter identification authentication, by authorized personnel, and, only then, will be allowed to use a voting machine, with which, the voter will cast his/her vote.

The advantage of online voting system is that the voter will be able to vote, irrespective of his/her physical location. Further, it would speed up the vote counting and seat allotment processes. Also if the system is designed in a proper way, the process would be "FREE and FAIR", as machines don't take sides.

Implementations of such projects induce several real-time problems, which will be discussed in the next section.

Any type of Online Voting System needs to fulfill some security requirements which are as follows:-

- **Eligibility and Authentication** — only the authorized personnel can cast his/her vote.
- **Integrity** — it should be impossible for the adversary to modify/delete/forge the vote.
- **Uniqueness**—No voter should be able to vote more than once.
- **Accuracy**—System should record the votes correctly.
- **Verifiability and Audit-ability**— in the final vote tally, all the votes should be counted properly and there should be provision to check, whether, all the votes are counted.

This paper deals with the design issues of the system and provides a detailed problem study of various real-time scenarios that could compromise the impartial functioning of system during its implementation.

This paper, also introduces, a concept of Random Party Code, to enhance the ballot secrecy of the voter. This concept may also be used to implement Open Public Voting Systems, because this concept will prevent the adversary to comprehend the vote even if he/she manages to take a peek.

2. REAL TIME PROBLEMS AND SOLUTION ANALYSIS
2.1 In such systems, a situation may arise, whereby, the adversaries may threaten the voter to go through all security verifications, like, Facial Recognition, One-Time-Password Verification, VoterID verification, etc., and then, force the voter to cast their vote, to the party of the adversary's interest, as such systems, lack physical supervision of the voting procedures by trained and armed personnel.

To deal with situations such as this, Random Party Codes , are needed to be provided to each online voting system user, over internet, using facial recognition(biometric) authentication, at least 7 days before the voting day. If this document is rigged, 7 days before the election, then, the design would provide ample opportunity and time for concerned authorities to take appropriate steps. This document would contain random 1-digit integer party codes, corresponding to each party, and these party codes will be stored in the unique record of the logged in user, in the database table. The party codes will be altered, and, new and randomized set of party codes would be provided, each time a new user logs in. Like for example, party code for person A, to vote for party X, might be 4, while, the party code for person B, to vote for the same party X, might be 2.The database record for a specific user looks like this:

Table1. Unique record for a user

uname	bjp	congress	tmc	cpm	password	pid	port
'Sayan'	6	2	3	5	'Maz'	1	25000

These codes will be used by the user, to cast his/her vote.

The entered code would be compared against the party name, that corresponds to the code, in the unique record of the voter, in the database table.

Then, the vote count, for the retrieved party name is incremented, in the results table.

Since 7 days before the election, the user usually knows, which party he's going to vote for, and remembering a 1-digit integer is no big deal, the user will be allowed to view this document only once, and has to remember or note down the 1-digit integer code, for voting purpose, after 7 days, for security reasons.

If a situation arises, where the codes are lost/forgotten, the user will be issued a new set of party codes, but only at the physical election office, before the voting day.

Hence, when an adversary, forces a voter, to go through with biometric, voterID, password and other authentication procedures and then, threatens the user to cast his/her vote, to the party of the adversary's choice, the concept of "Random Party Codes" will not allow the adversary to comprehend, to whom the user is voting, since the codes are given in a random order, and the code sets are different for different users, taking away the ability of the adversary to evaluate the vote, even if he manages to take a look at it.

Hence, there would be a scope for the user, to vote for the party, according to his/her own autonomous choice, despite being threatened, after all verifications are successfully completed.

2.2 There might be a situation where, the biometric or facial recognition might be faked, whereby, the adversary may try to fake the facial recognition procedure, using a still image, or facial masks of the authorized voter, thus compromising the whole design.

Such problems can be solved using the concept -—image properties, of a real time facial object in the environment, produced by the webcam, which always differs from the image properties of a facial object, taken from a still photo, using the same device[2].

The project "Face Spoof Detection with Image Distortion Analysis", as cited, which is implemented over Image Distortion Algorithm (IDA) using features like specula reflection, blurriness, chromatic moment, color diversity, etc. can be used to solve this problem.

2.3 Another situation may be considered, where the inability of the adversaries to penetrate the system, might drive them, to tamper various objects of interest to the system, in publicly accessible areas, like the streets. For example, if the system is designed over Socket Programming and Networking, the adversaries might tamper street cables, routers, etc. thereby disrupting the whole voting procedure.

Satellite Communication is the ideal solution to this problem, as it reduces the number of objects of interest to the system that requires protection, although the communication system is not very reliable. To overcome the reliability factor, each application might be given, a time period of 5 days for use, as the communication system is expected to work, at least for a few hours, within that time frame.

Since the system is sound enough, to support "public voting", i.e, voting in front of other people, due to the concept of Random Party Code, the system would function at its best, if the applications are built into TV Set-Top-Box applications. As maximum homes, these days, has at-least one TV, the device can be used as a voting machine, by an entire family, to go through with the voting procedures, thereby, reducing cost.

3. SYSTEM FRAMEWORK DESIGN

The design of the system will include a **registration application**, whose servers would be open throughout the year, and would be closed only 15 days before the voting day.

This application would be used by eligible citizens of India, to register for "Online Voting" who are interested to vote online. A facial record would be generated by this application and would also register the user's unique voter identification authentication records along with a personal mobile number of the user, in the user's unique record in the registration

database. The registered face, and its corresponding voting requisites would be verified with the real Election commission database, to ensure that, only authenticated and verified, personalities are allowed to vote, i.e, the voter is an authenticated and eligible citizen of India.

The **second application** would be used to **generate, store and deploy the random party codes**, to the already registered voters, after proper biometric (facial) verification, with the biometric record of the corresponding user, which should already be present in the registration database, provided the user is an authentic one. The servers for this application would be closed 7 days before the election and the users will be allowed to use this application only once, to view their unique set of random party codes, which they would have to remember or note down, and then, keep it safe for 7 days. Since the majority of the voters already know which party they are going to vote for, 7 days before the election, and the random party codes are only 1-digit random integers, remembering a single integer for 7 days, should not be a problem. Still, if the codes are lost by an user, new codes for that user can be generated, but only at the physical election office.

Now, if this document is tried to be rigged, 7 days before the voting day, the situation should provide ample time and information about the parties which are availing unfair means, so that proper and stern steps can be taken, by the concerned authorities.

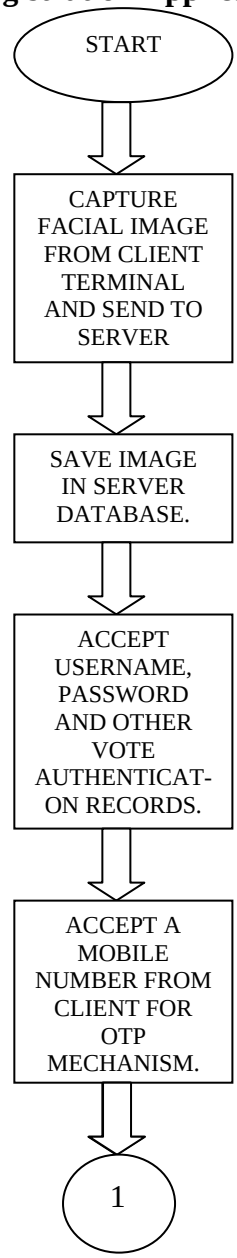
The **third application** will be used for **voting**. The servers for this application would be opened only on voting days and each user would be able to use this application, just once.

This application will first perform a biometrical verification of the user, using the biometric record of the user in the database, and his/her log-in username and password. Then, the application would proceed to verify the user's voter identification authentication records (for eg, Aandhar Card Number, etc.).Upon successful verification, a One Time Password would be generated and sent to the registered mobile number of the user, since 2 users with same biometrics and device number are impossible to find. The application would accept and verify the OTP. Upon successful verification, the user will be allowed to enter the voting mechanism, where he/she will enter his/her coded vote. The code entered by the user will be matched, to retrieve the party name, with which, the code corresponds to, in the user's unique record, in the database table. Then, the count for the retrieved party name, is incremented in the results table.

The user then receives a “vote registered" authentication message, and then, the servers are blocked for that user, using a boolean variable, so that he/she cannot enter for the second time.

4. PROGRAM FLOW

4.1 Registration Application Flow



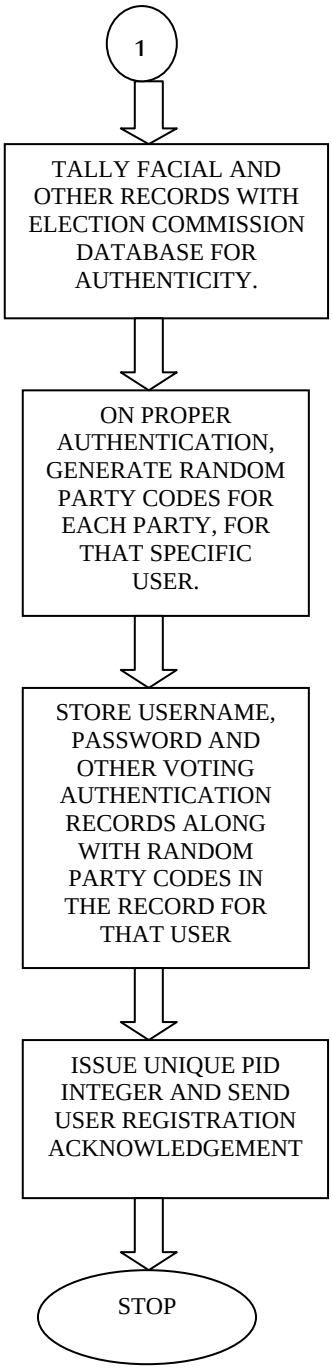


Fig1. User Registration Flowchart

4.2 Party Code Release Flow

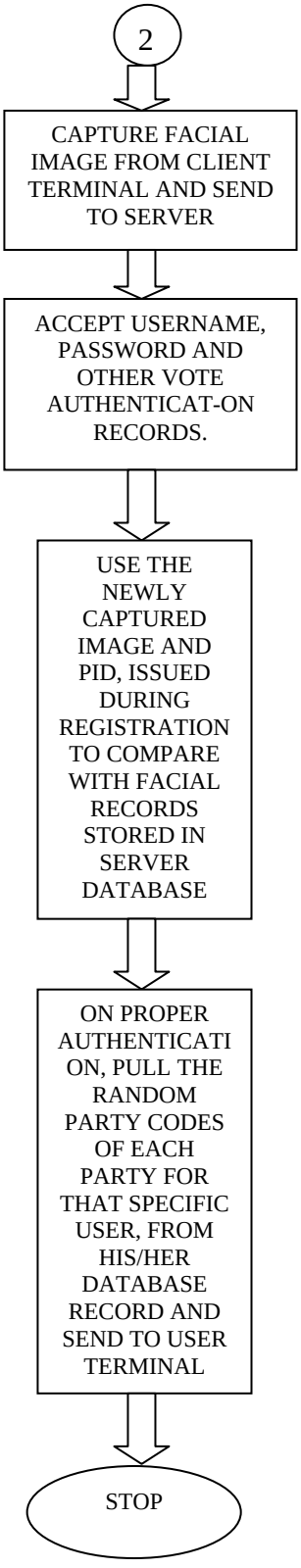
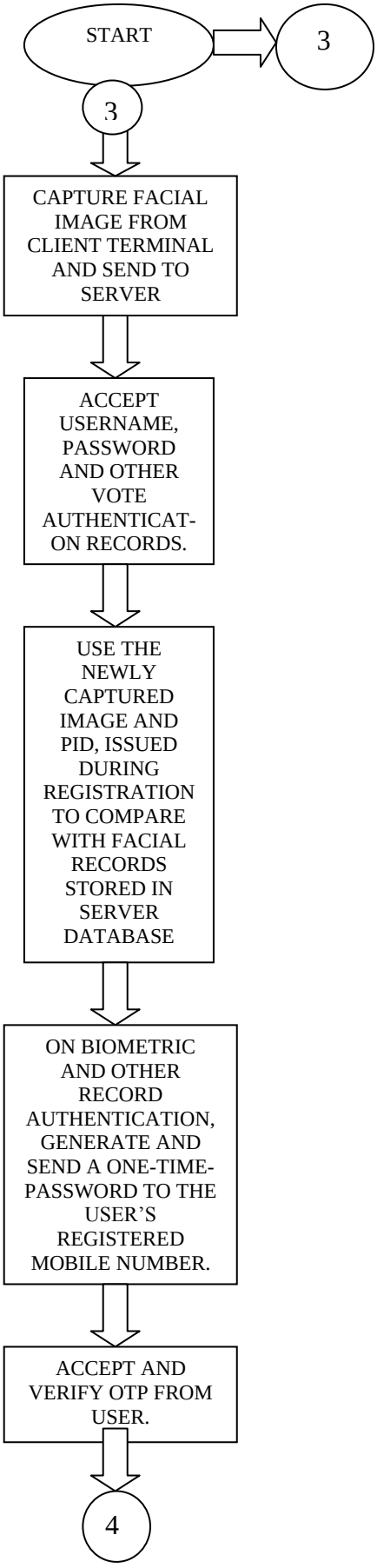


Fig2. Party Code Release

4.3 Voting Flow



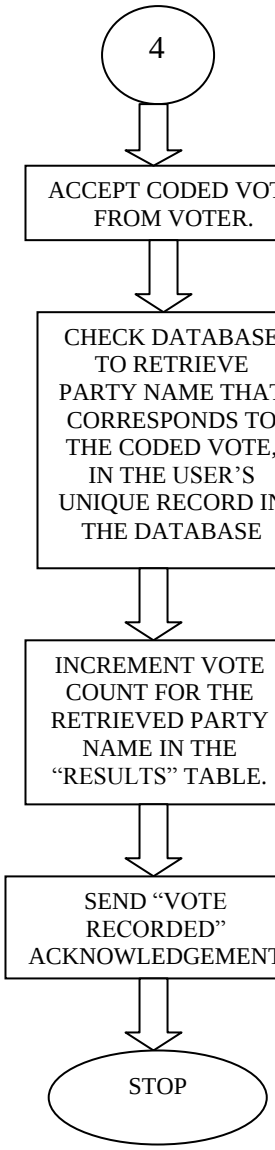


Fig3. Voting

5. EXPERIMENTAL RESULTS

Although, the system would work at its best over satellite communication, as mentioned above, the demonstration is done using Java Socket Programming, MySql Database, Luxand FaceSDK, Eclipse Window Builder, Eclipse Mars.

Note that, the applications are built just for demonstration.

```
mysql> select * from result;
+------+----------+------+------+-----+
| bjp  | congress | tmc  | cpm  | pid |
+------+----------+------+------+-----+
|    0 |        0 |    0 |    0 |   1 |
+------+----------+------+------+-----+
1 row in set (0.00 sec)

mysql>
```

Fig4. Result database before voting process

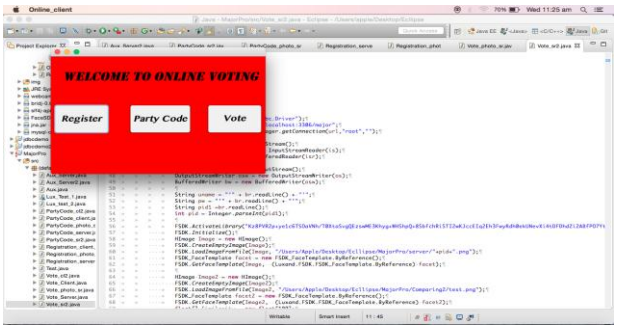


Fig5. User Login Window

5.1 Registration Output

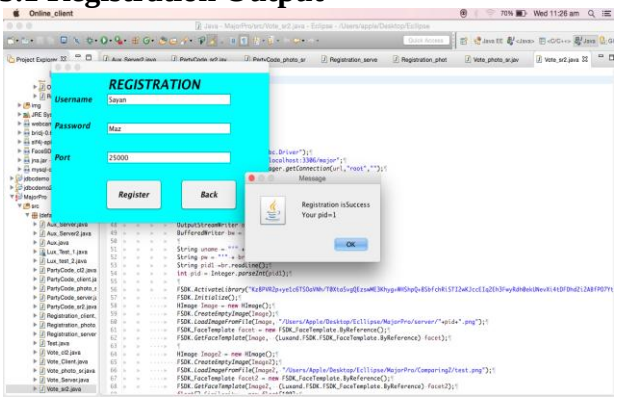


Fig6. Registration Window

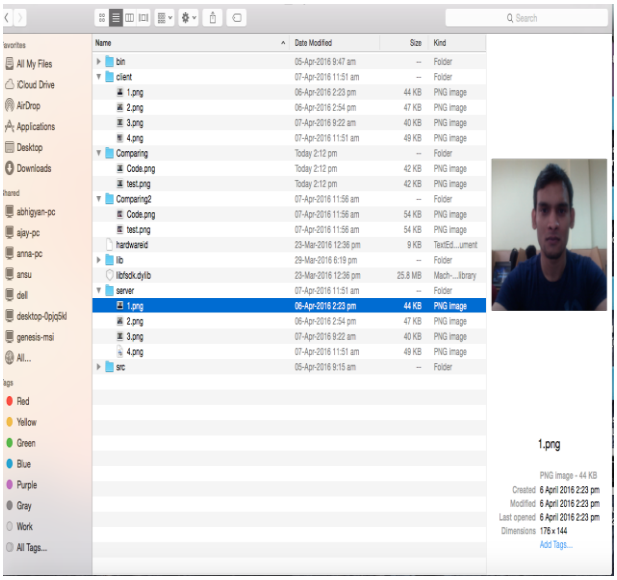


Fig7. User's Facial Record in Server

```
mysql> select * from voting;
+--------+------+----------+------+------+----------+-----+-------+
| uname  | bjp  | congress | tmc  | cpm  | password | pid | port  |
+--------+------+----------+------+------+----------+-----+-------+
| 'Sayan'|    0 |        8 |    1 |    5 | 'Maz'    |   1 | 25000 |
+--------+------+----------+------+------+----------+-----+-------+
1 row in set (0.00 sec)
```

Fig8. User's unique record in Database

5.2 Party Code Release

5.2.1 Authentic user login

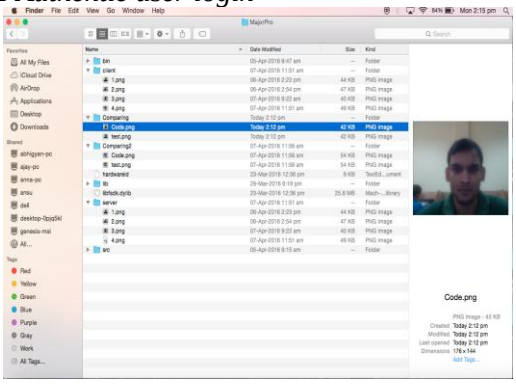


Fig9. Newly Taken Image For comparison

Fig10. Image in server (Image to be compared against)

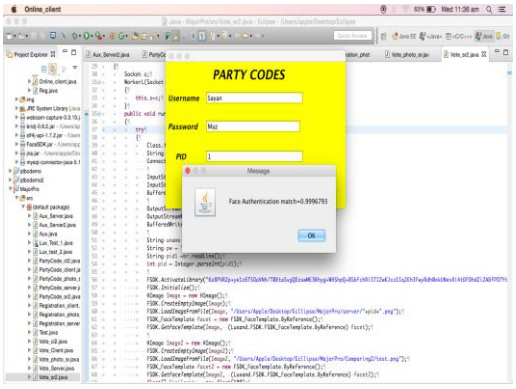


Fig11. Party Code Window

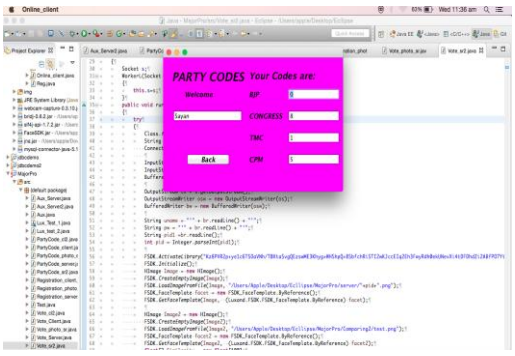


Fig12. Party Code Release

5.2.2 Fake user login

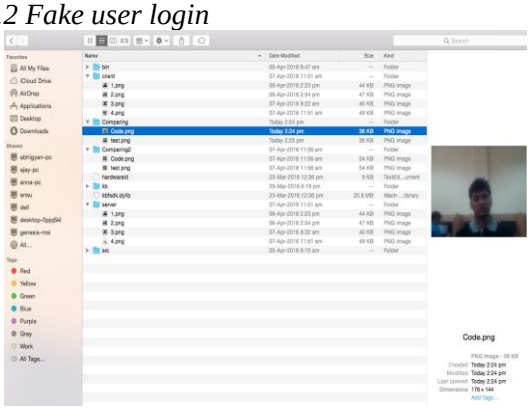


Fig13. Newly Taken Image For comparison

Fig14. Image in server (Image to be compared against)

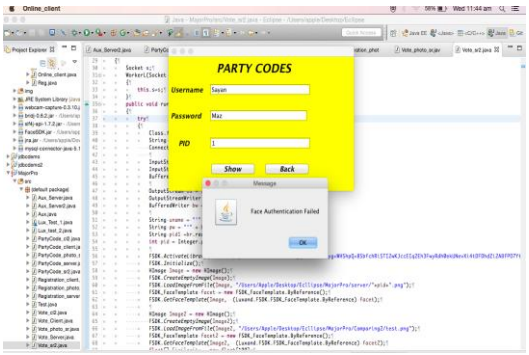


Fig15. Fake User Window

5.3 VOTING

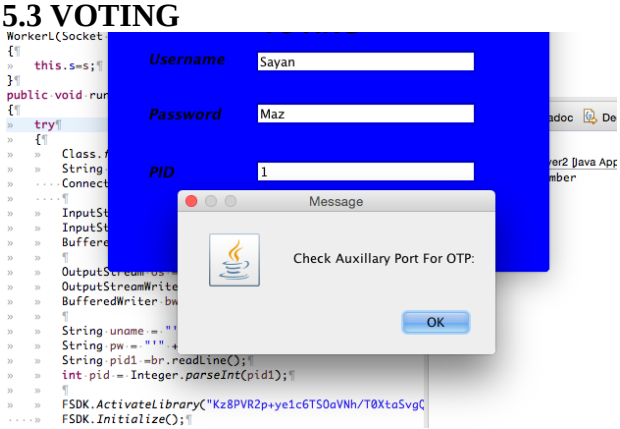


Fig16. Authentic User Vote Login Window

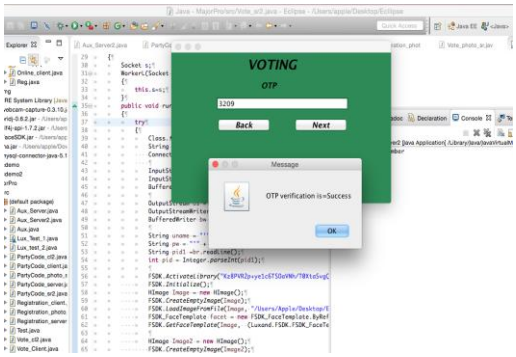


Fig17. OTP Window

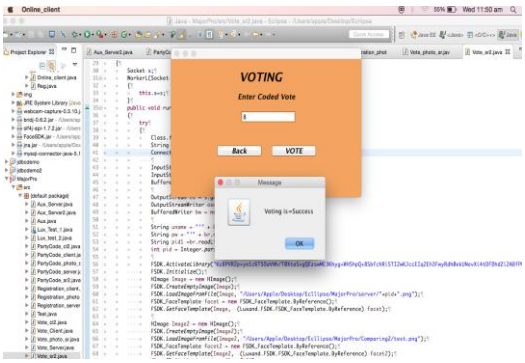


Fig18. Coded Voting Window

5.4 Result Set after casting a vote

```
mysql> select * from result;
+-----+----------+-----+-----+-----+
| bjp | congress | tmc | cpm | pid |
+-----+----------+-----+-----+-----+
|   0 |        1 |   0 |   0 |   1 |
+-----+----------+-----+-----+-----+
1 row in set (0.00 sec)
```

Fig19. Result incremented

6. CONCLUSION

In this paper, an idea for voting online, directly from the voter's home is presented, keeping in mind, the present day Indian Voting System scenarios, along with its real time implementation problems. It overcomes problems of rigging, taking a step towards, making the voting system secure, and, introduces OPEN PUBLIC VOTING , where everyone would be allowed to vote in front of other people .This paper also aims to promote voting, by saving the voters, from huge waiting time in the queues.

7. REFERENCES

[1] Di Wen, Hu Han, Anil K. Jain,"Face Spoof Detection with Image Distortion Analysis", IEEE Transactions on Information Forensics and Security, 2005.

[2] D.Chaum ,"Secret-ballot receipts: True voter-verifiable elections"IEEE Security & Privacy, 2(1):38–47, 2004.

[3] Robert Krimmer, Rudiger Grimm (Eds.) Electronic Voting 20083rd international Conference on August 6th-9th, 2008, In Castle Hofen, Bregenz, Austria.

[4] Craig James British Columbia "Discussion Paper: Internet Voting"August 2011 Prentice Hall, 2003.

[5] "A Survey of Current Secret-Ballot Systems", David. Chaum.

[6] "A Report on the Feasibility of Internet Voting", California Internet Voting Task Force, 2000

[7] T. Kohno, A. Stubblefield, A.D. Rubin, and D.S. Wallach. Analysis of an electronic voting system. In 2004 IEEE Symposium on Security and Privacy, 2004., pages 27–40, May 2004.

[8] National Securities Depository Limited (NSDL). www.evoting.nsdl. com/[accessed 17- August-2015].

[9] National Science Foundation. Report on the National Workshop on Internet Voting: Issues and Research Agenda. March 2001. http://news.findlaw.com/cnn/docs/voting/nsfe-voterprt.pdf [accessed 15–August–2015].

[10] Atsushi Fujioka, Tatsuaki Okamoto, and Kazuo Ohta. A practical secret voting scheme for large scale elections. In Workshop on the Theory and Application of Cryptographic Techniques: Advances in Cryptology, ASIACRYPT '92, pages 244–251. Springer-Verlag, 1993.