South Asian Journal of Research in Engineering Science and Technology

www.sajrest.com
SAJRESTⓒ2016 e-ISSN: 2455-9261

Volume 1, Issue **1, December 2016**

pp. **31—34**

SECURE MOBILE BASED ONLINE VOTING SYSTEM

[1]Rajra Vignesh R, [2]Jeevitha.B,[3]Kavibharathi.N,[4]Nandhini.R,
[1] Assistant Professor, [2,3,4] UG Scholar,
Arasu Engineering College
Kumbakonam, TamilNadu.
nandhinishyam04@gmail.com

***Abstract*— The aim of this work is to design and implement an electronic voting application for the Android platform that will enable people to vote securely from anywhere. The application as a whole is aimed at being compatible with devices from many manufactures and running different versions of the operating system with the use of IRIS and VOTER ID CARD VERIFICATION**

Keywords—IrisScanner,Voteridcard,OTP

I.INTRODUCTION

Voting is a delicate matter. Whoever the voter is, he or she usually wants to vote as transparently and freely as possible. In most cases, this is achieved by strict rules which often make it necessary for the voter to be physically present at the place where the voting takes place. But what about the one member of the board who is always traveling? What about a member of a council that is stuck in a traffic jam on the way to the council hall?

In today's world we are witnesses of a process that is merging two devices into one. The PDA - Personal Digital Assistant and the cell phone. This means that more and more people carry in fact powerful computers in their pockets that enable them to perform a lot of tasks without the need of being at their desks. It also enables a person to vote safely and easily while he is unable to attend a meeting in person.

This text, along with the source code, guides and installation les are located on the website.

II.LITERATURE REVIEW

Mobile Voting System Dipali More1, et.et.2016, *Mobile voting system is very secure, efficient and easy way to casting of vote. In this paper used* RSA algorithm for security purpose. Our proposed system provides a new e-voting system which fulfills the security requirements of voting process. In our project total three steps are required

Secure Mobile Based Voting System Manish Kumar1, T.V.Suresh Kumar1, M. Hanumanthappa2, D Evangelin Geetha1.2015, The foundation of a strong democracy is an informed and engaged citizenry. And what better way to both inform and engage citizens than through the power of today's information and communication technologies? Citizens around the world recognize and embrace the benefits of e-Government services such as online tax filing, license renewal, and benefits claims. Now governments are initiating strategies that support e-democracy and in doing so, engaging more citizens in democratic processes.

III.METHODOLOGY

A. Proposed Architecture:

The user LOGIN to the Voter Login system. For the Authentication purpose, this system used two technologies. VOTER ID VERIFICATION to check particular user is valuable or not and IRIS SCANNER for security purpose, this iris scanner checks the iris that stores in a database. Further proceed with OTP Recognization, OTP verify and checks registered mobile number. This system reduced berybery.Finally nominee form will display and user cast their vote without fails and the vote saved in database and the results are maintained by admin (database).

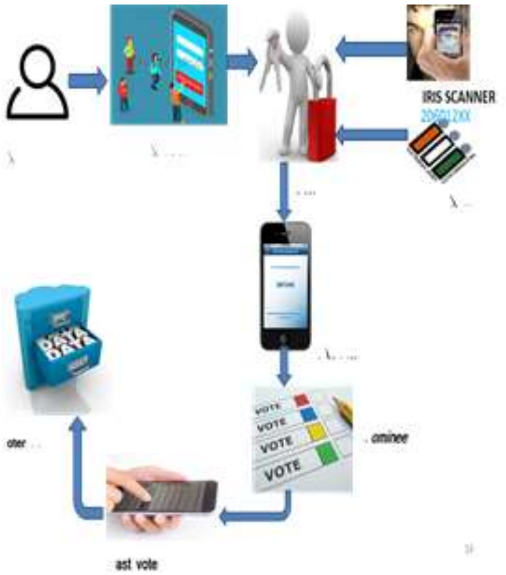


Fig 3.1.proposed architecture

In voter module, it displays login section. Which contains VOTER details, Login section Register User details for identification and verification

In Authentication module, it is used for security purpose. It follows Daughman algorithm and Time based OTP algorithm. For security it used two techniques

1. IRIS SCANNER
2. VOTER ID CARD VERIFICATION

Further proceed with OTP generation in a register mobile number.

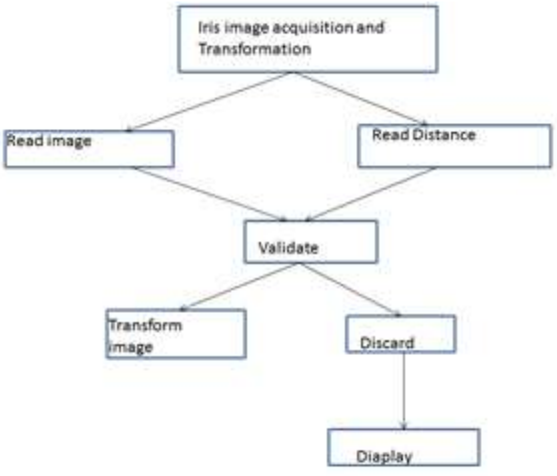


Figure 3.2 IRIS PROCESS

In One Time Password module, OTP follows Time Based Algorithm. It works after authentication is done. It generates a password as number to register mobile number. Password life time is up to 60 seconds.

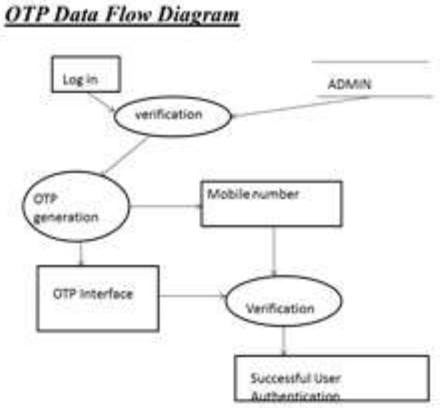


Figure 3.3 OTP PROCESS

In Nominee module, it displays who are willing to govern the country. It includes nominee Name, Symbols and their Wards, User used this module for cast their own votes.

In this module, it is used to get election results and also reset database after all process is completed. It displays results of current Election, It also stores results in a database.

IV.IMPLEMENTATION and RESULT

A. Package and Result

1. Structured Query language.
2. Android studio 2.1

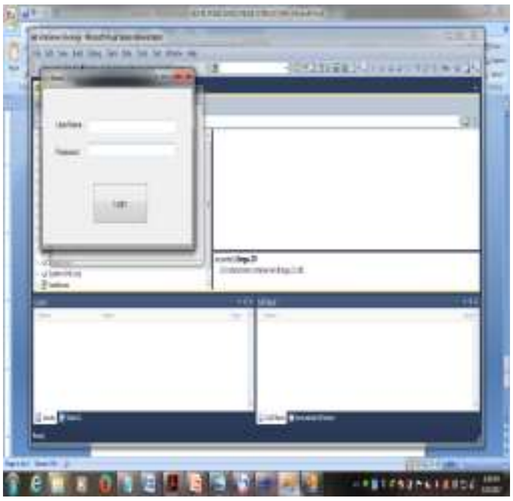
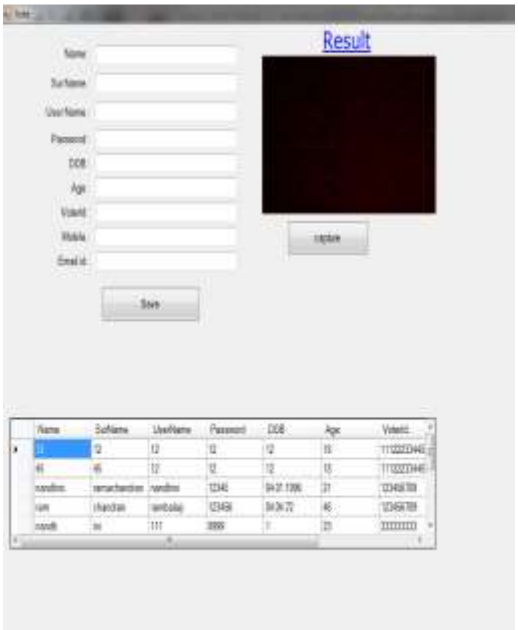
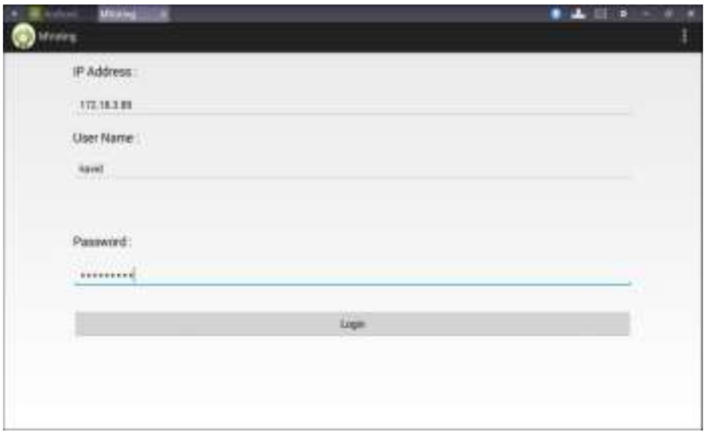


Figure 4.1.screen shot1.



Name	SurName	UserName	Password	DOB	Age	Voterid
11	12	12	12	12	15	1112223344
46	45	12	12	12	15	1112223344
nandini	ramachandran	nandini	12345	04.07.1996	21	123456789
ram	chandran	rambalaj	123456	04.04.72	45	123456789
nandh	ini	111	9999	1	21	333333333

Figure 4.2. Screenshot 2



IP Address :

172.18.3.89

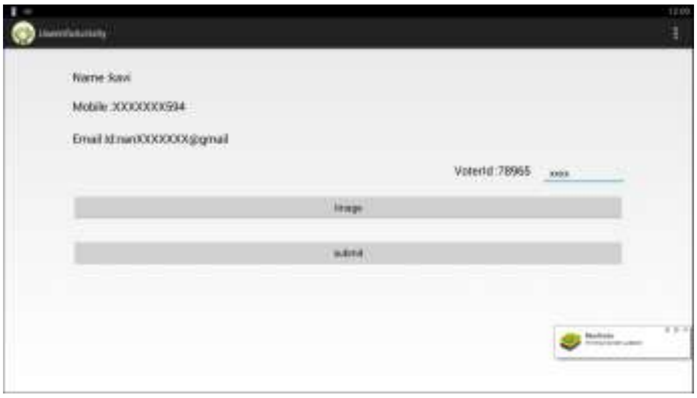
User Name :

kavel

Password :

•••••••••

Figure 4.3. Screenshot 3



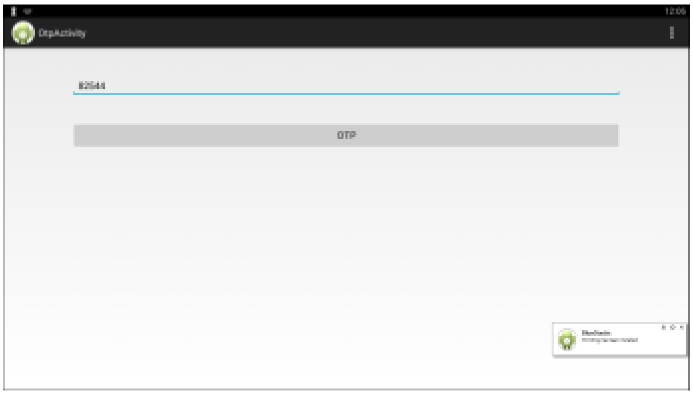
Name :kavi

Mobile :XXXXXXX594

Email Id:nanXXXXXXX@gmail

VoterId :78965 xxxx

Figure 4.4. Screenshot 4



82544

Figure 4.5. Screenshot 5

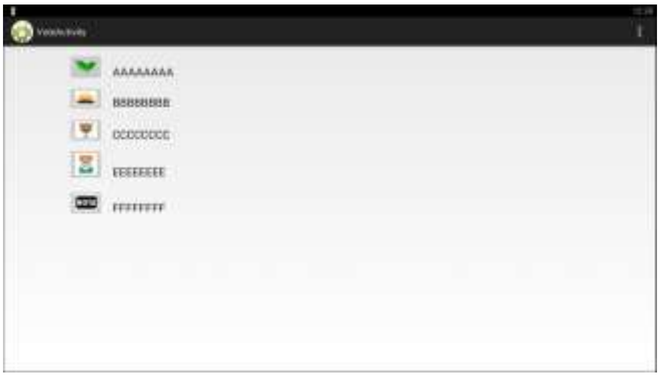
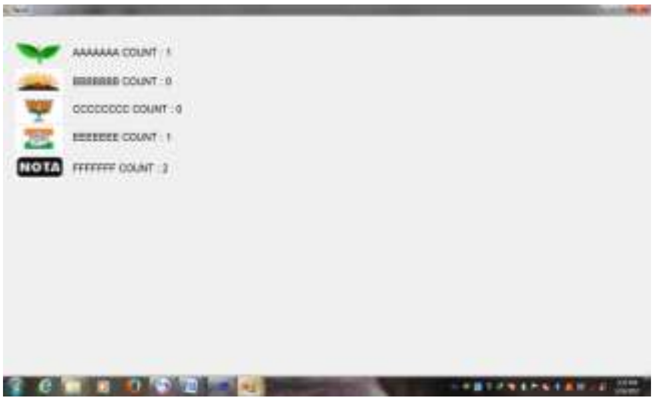


Figure 4.6. Screenshot 6



AAAAAAA COUNT : 1
BBBBBBB COUNT : 0
CCCCCCCC COUNT : 0
EEEEEEE COUNT : 1
FFFFFFF COUNT : 2

Figure 4.7 Screenshot 7

V.CONCLUSION

The aim of this work was to enhance the mobile voting system originally created by Jakub Valenta in his bachelor's thesis. The goals were to implement SSL, add internationalization and create an Android client that follows the good practices for Android applications. These goals were supplemented with goals outlined in the analysis part of the project and developed as time progressed and I gained a better understanding of the area. The whole system performs well, however as I had no real knowledge of creating Android applications I was not able to resolve some performance issues on this side. The communication system is not handled by as an Android service but it is a part of a normal application. This does not act the usability of the application but may act performance. On the plus side the whole system is ready to be used in a real situation. For this, however, testing on a larger scale is recommended. Almost all use cases were implemented apart from the timed logout. This was ignored because the memory management on this device performs this function just as well.

As for the continuation of this project, it needs more compatible clients. The analysis and design of the mobile client in this thesis is in my opinion a good foundation for the creation of other mobile clients - the iOS platform from Apple and BlackBerry OS from RIM are two platforms that come to mind as the targeted audience of this project is very likely to own one of these devices.

Another possibility is to create a UDP retransmitted to overcome broadcasting limitations and provide the automatic server discovery to a wider range of voters. Currently the most pressing issue is the, however, the performance of the Android client. This should have priority.

REFERENCE

[1] Fujioka, T. Okamoto, and K. Ohta. (2016) A practical secret voting scheme for large scale elections. In J. Seberry and Y. Zheng, editors, Advances in Cryptology Auscrypt'92, volume 718 of Lecture Notes in Computer Science, pages pp. 244–251, Gold Coast, Queensland, Austrailia, 13-16. Springer-Verlag.
[2] Chaum. D (1915) Blind signatures for untraceable payments. In D. Chaum,R. Rivest, and A. Sherman, editors, Advances in Cryptology—Crypto'82, pages 199–203, New York, 1983. Plenum Press. Emerging Technologies in E-Government 330
[3] Jefferson, D., Rubin, A D, Simons, B. and Wagner. D (2015) A Security Analysis of the Secure Electronic Registration and Voting Experiment (SERVE), ETS 300 506. Security aspects (GSM 02.09 version 4.5.1), Digital cellular telecommunications system (phase 2), 2014
[4] Hirt M and Sako, K. (2015) Efficient receipt-free voting based on homomorphic encryption. In B. Preneel, editor, Advances in Cryptology—EUROCRYPT '00, volume 1807 of Lecture Notes in Computer Science,pages 539–556. Springer-Verlag,
[5] Lin, Y. and Chlamtac, I. (2016) Wireless and Mobile Network Architectures. Wiley Publications.