ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 10, October 2015

Democratic Platform for E-Voting & E-Forum Using Android to Administer Student Council

Nishant Tirpude, Akshaya Waghmode, Anuja Kulkarni, Manish Shinde, Nutan Dhange

Student, Dept. of I.T., Atharva College of Engineering, Mumbai University, Mumbai, India

Student, Dept. of I.T., Atharva College of Engineering, Mumbai University, Mumbai, India

Student, Dept. of I.T., Atharva College of Engineering, Mumbai University, Mumbai, India

Student, Dept. of I.T., Atharva College of Engineering, Mumbai University, Mumbai, India

Assistant Professor, Dept. of I.T., Atharva College of Engineering, Mumbai University, Mumbai, India

ABSTRACT: The advancement in the mobile devices, wireless and web technologies have given rise to newapplication that will make voting process very easy and efficient. This Democratic Platform provides the specificationand requirements for e-Voting & e-Forum using an Android platform. E-Voting means the voting process in election byusing electronic device and e-forum comprises of managing reviews as well as feedback to enhance the teamwork viaweb. The aim of this work is to design and implement an electronic voting & forum application for the Androidplatform that will enable students to vote securely & get notified from anywhere. This new concept is also aimed atbeing localized the forums to be central platform for the members of students council to conduct discussions and offlinemeetings and to share the happenings throughout academic semesters.

KEYWORDS: AES (Advanced Encryption Standard) algorithm; GCM (Google Cloud Messaging) service, Android.

I. INTRODUCTION

Democratic rights are owned by every human on this planet. Government promises democratic platform by fair and free elections;being the citizens, a chance to take an active participation in politics and civic life and so on. Aiming towards this project, every college has a COUNCIL that look forward to conduct various events and decisions of college. This council consists of various posts that governs different fields such as cultural, sports, academic, etc. To make this council strong enough to run these events smoothly, appropriate candidates must be elected as per the posts. To carry out this e-voting, an application is built on android platform, in very suitable manner so that every legal student gets a chance to vote for their candidate whom they find liable for the posts. Allowing every student to vote only once, the results are calculated and are kept confidential from everyone i.e. voter, admin and the candidate. After the set time, the voting line is closed and the admin gets the result, which is displayed on forums and the voting counter is reset. Besides, e-forums are used to display notice and alerts of the upcoming events i.e. the festivals or competitions, along with the registration links. Any student willing to participate in events or competitions can register for the same and then the alerts for it will be received only to those.

II. RELATED WORK

The registered voter will use an android app which is developed throughout this work. As depicted in figure, the backend i.e. the database is in MySQL which stores the data. Looking on the middleware created in PHP, is controlled by the admin. Although, it keeps the votes confidential from the admin. Front end, consist of the phone running on android platform that restricts the user to cast the vote only once. The forum on the other hand, notifies the user about the events and the important notice using email service and GCM (Google Cloud Messaging). Keeping security in mind, the above data will be encrypted using AES (Advanced Encryption Standards) algorithm.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 10, October 2015

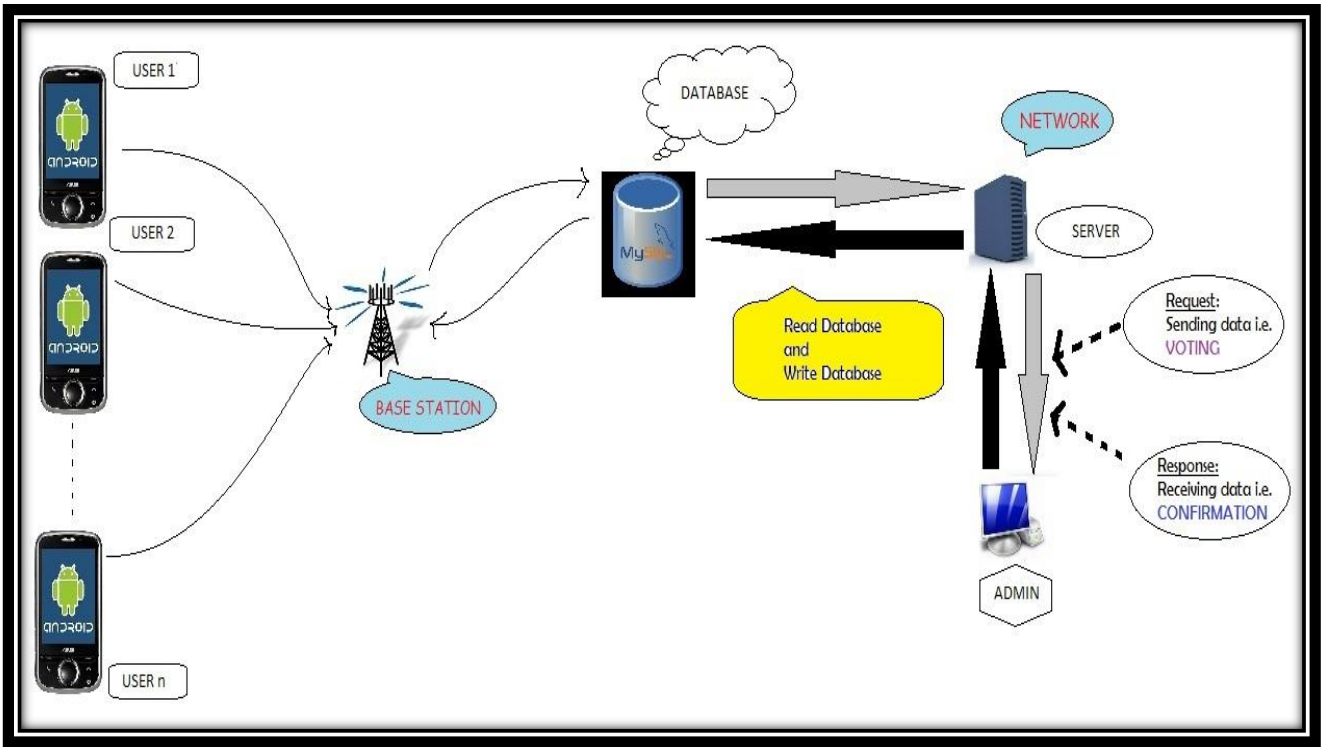

Figure 1. The general architecture of the system

III. PROPOSED ALGORITHM

A. *Design Considerations:*

- Derive the set of round keys from the cipher key.
- Initialize the state array with the block data (plaintext).
- Add the initial round key to the starting state array.
- Perform nine rounds of state manipulation.
- Perform the tenth and final round of state manipulation.
- Copy the final state array out as the encrypted data (cipher text).

B. *Description of the Proposed Algorithm:*

AES is based on a design principle known as a substitution-permutation network, combination of both substitution and permutation, and is fast in both software and hardware. Unlike its predecessor DES, AES does not use a Feistel network. AES is a variant of Rijndael which has a fixed block size of 128 bits, and a key size of 128, 192, or 256 bits. By contrast, the Rijndael specification *per se* is specified with block and key sizes that may be any multiple of 32 bits, both with a minimum of 128 and a maximum of 256 bits.

AES operates on a 4×4 column-major order matrix of bytes, termed the *state*, although some versions of Rijndael have a larger block size and have additional columns in the state. Most AES calculations are done in a special finite field.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 10, October 2015

For instance, if you have 16 bytes, b_0, b1,..., b15, these bytes are represented as this matrix:

$$\begin{bmatrix} b_0 & b_4 & b_8 & b_{12} \\ b_1 & b_5 & b_9 & b_{13} \\ b_2 & b_6 & b_{10} & b_{14} \\ b_3 & b_7 & b_{11} & b_{15} \end{bmatrix}$$

The key size used for an AES cipher specifies the number of repetitions of transformation rounds that convert the input, called the plaintext, into the final output, called the cipher text. The number of cycles of repetition are as follows:

- 10 cycles of repetition for 128-bit keys.
- 12 cycles of repetition for 192-bit keys.
- 14 cycles of repetition for 256-bit keys.

Each round consists of several processing steps, each containing four similar but different stages, including one that depends on the encryption key itself. A set of reverse rounds are applied to transform cipher text back into the original plaintext using the same encryption key.

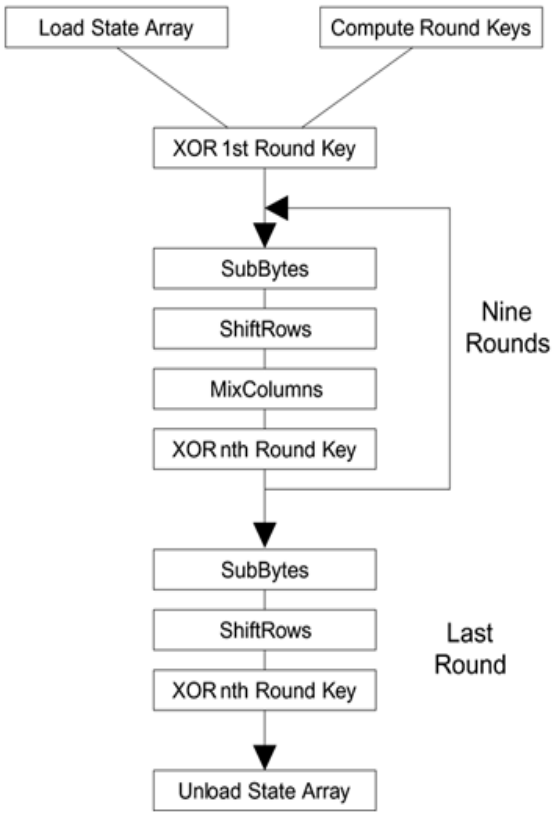

Figure 2. Summary of AES encryption

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 10, October 2015

IV. PSEUDO CODE

For admin:
Step 1: Login.
Step 2: Upload the list of candidates with their respective design / upload notice regarding the events.
Step 3: Set a particular duration for voting / post the link for registration.
Step 4: After that duration, analyze the result and display.
Step 5: Logout.

For user:
Step 1: Login to vote by entering your username and password.
Step 2: Select the candidate and cast your vote / review the notice and apply for the same if interested.
Step 3: Logout and wait for the results.

V. SIMULATION RESULTS

The block diagram of the system is shown below. As seen, there are 3 main constraints, ANDROID USER, ADMIN PANEL & DATABASE. The students can register themselves & can vote or access forums whenever needed. The admin too has to register and these data of students and admin will be saved in the database, which will be accessible through server. The admin will register the candidates and their profile will be viewable to the students before the elections. To cast a vote, the student has to sign in vote for the candidates in only certain duration. The results will be declared by the admin on forums. Besides, forums will be used for uploading various notices about the events and registrations for the same.

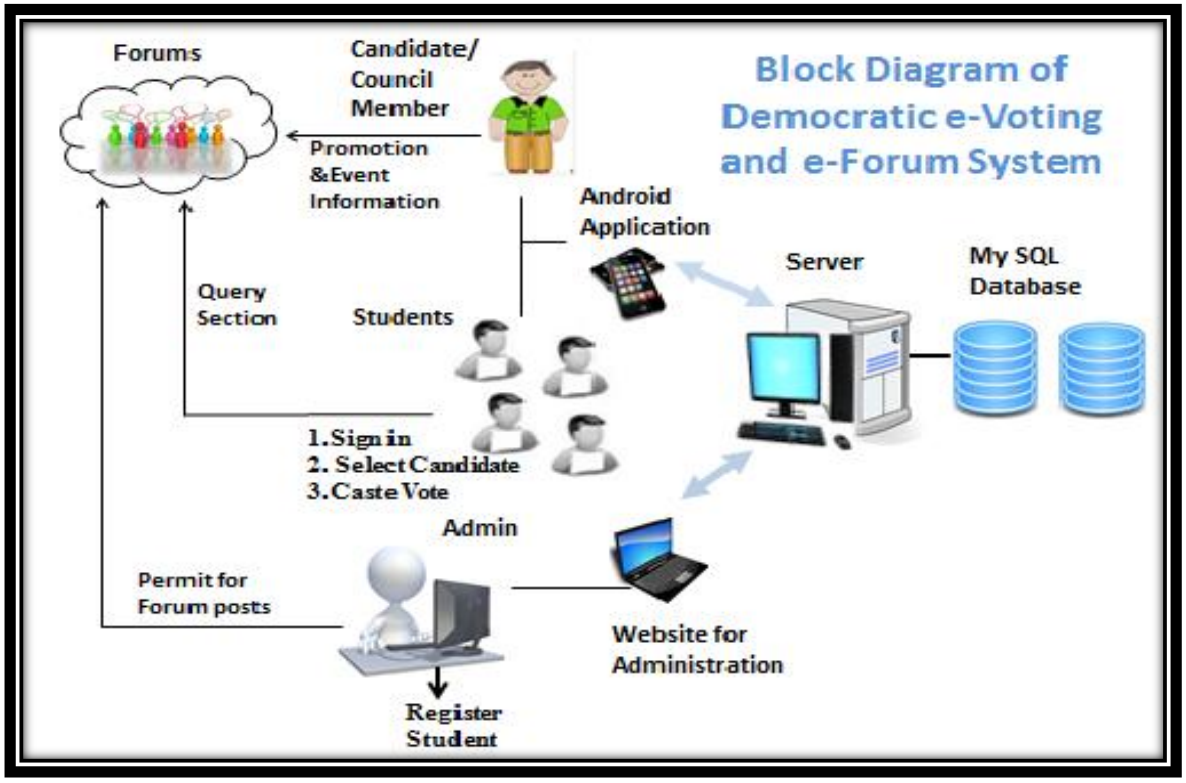

Figure 3.The block diagram of the system

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 10, October 2015

The simulation studies first involves the voting process. The voter simply cast his/her vote ONLY ONCE. Once voting is successfully completed, one cannot retrieve it again. The voter is identified by his/her username by the database that keeps a check and gets updated after every vote. On the other side, the admin keeps the constant watch on the ongoing process. He/she knows that the voting is being done, but not by whom and to whom. This the data is kept confidential from both, the user and the admin. After the time elapsed the duration, the voting is closed. Now, no new user can vote. As soon as the voting line expires, the data, i.e. the votes are calculated by the system and the result is displayed to the admin. The admin, then, displays the result on forum and prepares for the next vote by same process and resetting the voting counter to zero.

E-forum will displays all the notices about the events like festivals, exams time-tables, notice for submissions, etc. This job is again of the admin. The logged in users will receives the notifications of the same. If there is any registration required for any event to participated, the admin will also post the register form or the link for it so that the users can submit it directly.

VI. CONCLUSION AND FUTURE WORK

This review paper proposed a real time e-voting and e-forum system based on android phones. The usability of e-voting system is very high that it will be definitely helpful for the users to vote.The proposed e-voting and e-forum system minimizes the need for recounts as everything is tabulated by the computer and it's not necessary for the student to go college to see the notice.

REFERENCES

1. Campus E-Voting for Android and Web Based Application by Mr. Prashant Pandit, Mr. Sagar Bhawar, Prof .Manisha. Desai,RMD Sinhgad School of Engineering, Computer Department, International Journal of Emerging Engineering Research and Technology Volume 2, Issue 7, October 2014, PP 95-100 ISSN 2349-4395 (Print) & ISSN 2349-4409 (Online).
2. Efficient E-voting Android Based System by Dr.Aree Ali Mohammed Ramyar Abdolrahman Timour, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 11, November 2013 ISSN: 2277 128X ,Research Paper Available online at: www.ijarcsse.com.
3. E-Voting System on Android Platform from International Journal of Engineering Research & Technology (IJERT), Vol. 3 Issue 2, February – 2014, ISSN: 2278-0181.
4. Security algorithm - http://etutorials.org/Networking/802.11+security.+wi-fi+protected+access+and+802.11i/Appendixes/Appendix+A.+Overview+of+the+AES+Block+Cipher/Steps+in+the+AES+Encryption+Process/