RESEARCH ARTICLE OPEN ACCESS

Online Votes and Fund analysis for political parties with Data Security

Ashwin Shinde*, Sumedha Chokhandre**, Ketki Khante***, Chandrashekhar Gode****

*(Department of Computer Science and Engineering, RTMNU University, Nagpur-Maharashtra)
** (Department of Information Technology, RTMNU University, Nagpur-Maharashtra)
*** (Department of Information Technology, RTMNU University, Nagpur-Maharashtra)
*** (Department of Computer Technology, RTMNU University, Nagpur-Maharashtra)

ABSTRACT
With the traditional fund management and vote bank analysis, it was difficult to manage and analyze the details of fund collection and vote bank where all the records and relevant details were maintained at manual level, which is always a troublesome process. To overcome these problems, an online web application is being developed which provide the means of maintaining the funds gathered, Analyzing vote bank generated, Analysis of area wise grievances and providing data security using encryption algorithms like Advanced Encryption standard enabling two step verification mechanisms such as legitimate user authentication and secured access to data. Also various reports will be generated depicting graphical assessment of information gathered.

Keywords **-** Registration and Fund donations, Data Security, Report Generation

I. INTRODUCTION

With the changing nature of today's politics it is necessary to have a professional approach towards it. Politicians need to analyze the "Vote Bank" on the various categories (State wise, City wise). This project as title "Fund analysis and management with Data Security over Website" comes under the Relational Database Management System (RDBMS). This application is developed with the help of Visual Studio 2008 and SQL server.

Fig. 1. Research Work Flow

II. User Registration

In order to be a member or volunteer of a political Party user will have to register him/her by filling an online registration form. The analysis of the members or donors will be done State, City, Gender, Age category etc. The problem analysis will be done with the problem specified by the people.

III. Fund Donations

There will be no need for the user to be a member of this party for donating. Name of the person will be kept as anonymous or will be displayed on the web-site as per his/her wish.

IV. Vote Bank Analysis

This website is going to prove beneficial for the political party which is going to use It will give a complete analysis about the funds which they are going to be receiving through various donors. This facility will enable to keep all the tracks of their receiving funds and also the transparency will be persevered.

V. Data Security(Administrator Mode)

Administrator will have all the rights to access any part of the database. Only he can register the new committee members (volunteers). He will also have rights to share database with trusted third party" with some predicates such as number of attempts to access the database within a mentioned time span. If some intruder tries to hack the system through invalid random no. (Authentication code) he will get an access to the fake database in-order to prevent any kind of unauthorized access.

VI. Data Security(Member Mode)

Member will have certain rights but not all as compared to Administrator. Data is protected through different encryptions algorithms in here. Whenever, the member will enter his/her user

name and the password a random key will be automatically generated and will be sent to his/her mobile no or e-mail id for authentication.

VII. Data Security(Member Mode)

Privacy of the data will be maintained as per users' wish.

VIII. Algorithms

8.1 Random Key Generation Algorithm

This is one of the most important algorithms used for data security. A random key will be sent to the user's mobile/email id as soon as he/she logs in. This will provide a tight security as well as prevent any intruder from hacking the important data.

1.2 Mechanism in Project

This is process involves two steps to verify the identity of the legitimate user. Whenever a user will try to login his/her account by valid username and password he/she will receive an auto-generated random key which will help that user to prove his/her legitimacy. Following are the steps that will show how this algorithm works: -

- ¬ Initially two character sets will be defined by the developer (which will generate a random key.).
- ¬ The length will be also defined by the developer.
- ¬ Now the shuffling will take place between the two character sets and finally a random key will be generated.

This key will be sent to the users mobile or email id.when that user will enter this random key, access to his/her account will be provided.

IX. Encryption/Decryption Algorithm

9.1 Advanced Encryption Standard

Cryptography plays an important role in the security of data. It enables us to store sensitive information or transmit it across insecure networks so that unauthorized persons cannot read it. The basic unit for processing in the AES algorithm is byte (a sequence of eight bits), so the input bit sequence is first transformed into byte sequence. In the next step a two bi-dimensional array of bytes (called the State) is built. The State array consists of four rows of bytes, each containing Nb bytes, where

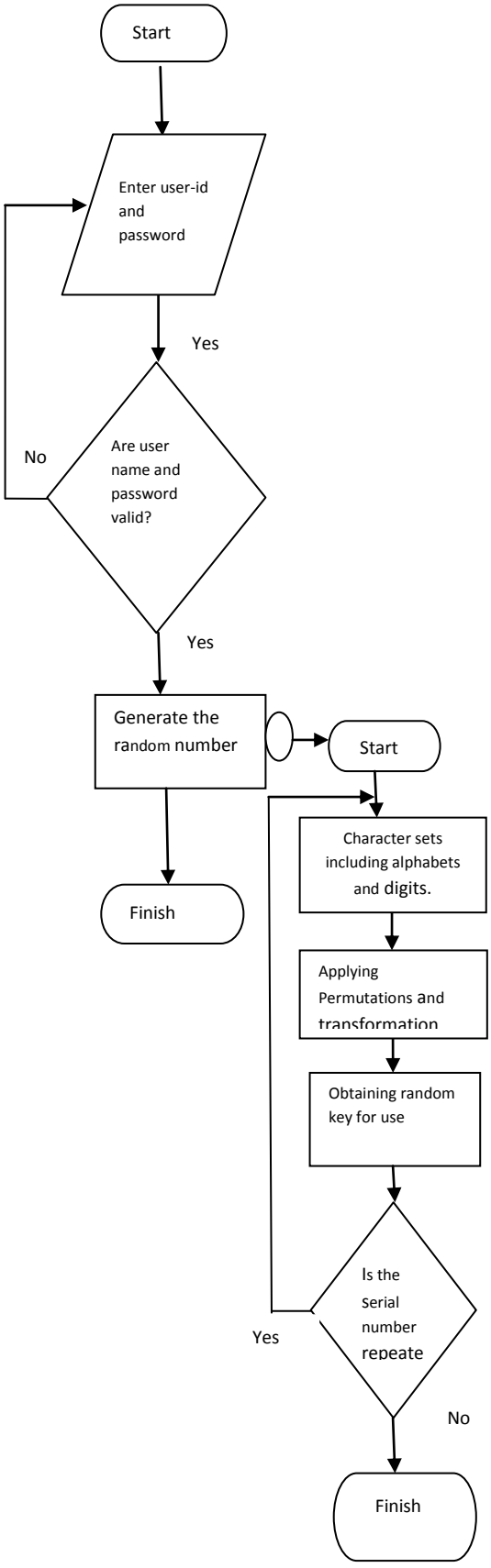

Fig.2 Mechanism Implemented

Nb is the block size divided by 32 (number of words). All internal operations (Cipher and Inverse Cipher) of the AES algorithms are then performed on the State array, after which its final value is copied to the output (State array is transformed back to the bit sequence). [2]

The input and output for the AES algorithm each consist of sequences of 128 bits (digits with values of 0 or 1). These sequences will sometimes be referred to as blocks and the number of bits they contain will be referred to as their length. The Cipher Key for the AES algorithm is a sequence of 128,192 or 256 bits. The AES algorithm consists of ten rounds of encryption, as can be seen in Figure 3 First the 128-bit key is expanded into eleven so-called round keys, each of them 128 bits in size. Each round includes a transformation using the corresponding cipher key to ensure the security of the encryption.

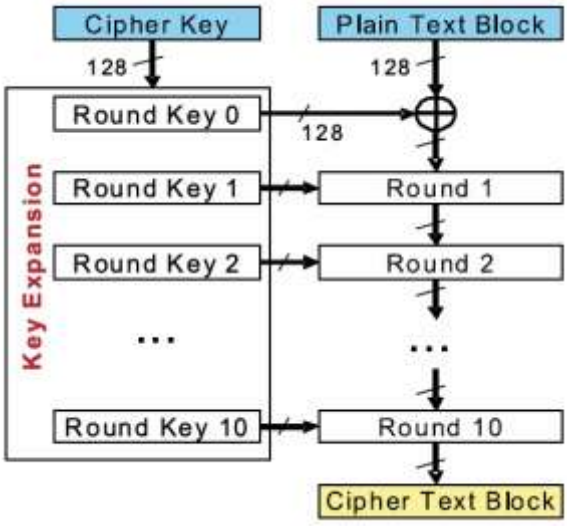

Fig. 3 AES Algorithm Structure [3]

X. Report Generation.

Following Reports will be generated: -

I. Area wise collection of Total Fund Amount
II. Area wise Vote Density
III. Area wise grievance

Following reports are shown on the basis of amount collected and there possible required graph. The input to the database are from donor and output i.e. graph are generated accordingly.
Likewise other reports will be generated.

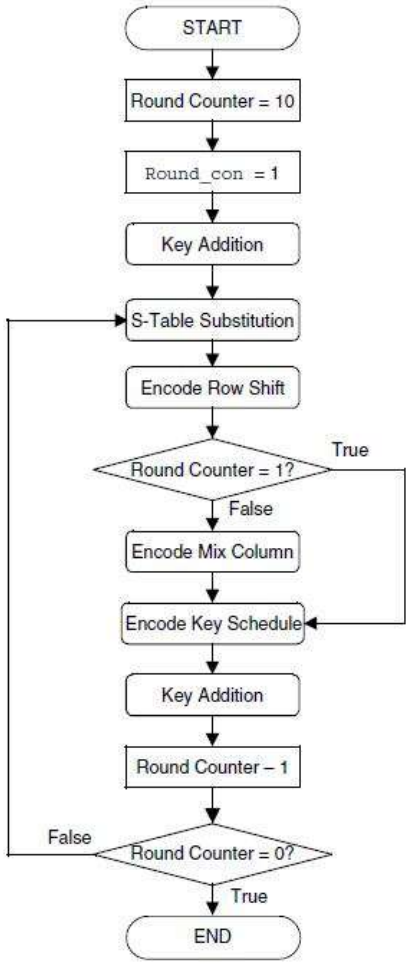

Fig. 4 AES Encryption Flow [3]

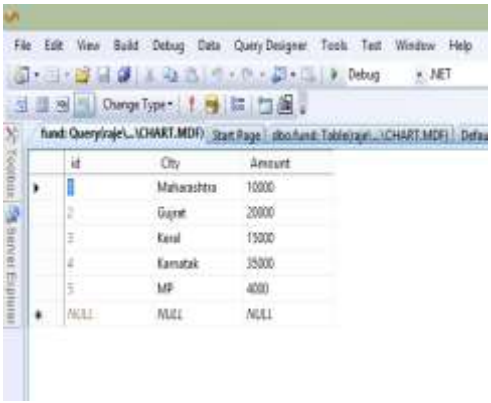

Fig. 5 Snapshot of database

Fig. 6. Snapshot of Graph

XI. Conclusion

This research deals with various aspect of analysis. Here we have analyzed total fund amount, vote density and grievances according to area. We have applied two-step verification and AES algorithm for data security. This will enable data to access in a secure manner.

REFERENCES

[1] William Stallings, *Cryptography and network Security principles and Practices"* International Edition, 2007.

[2] William Stallings, *Cryptography and network Security principles and Practices"* International Edition, 2003.

[3] National Institute of Standards and Technology (NIST). *NIST FIPS PUB 185, Escrowed Encryption Standard*, February 1994.

[4] Gohil, Rikitaben, Karsanbhai, Mary Grace Shajan,"AES Algorithm for Secured Wireless Communication", National Conference on Recent Trends in Engineering and Technology, 13-14 May 2011.