International Journal of Research in Advent Technology (IJRAT) Special Issue
E-ISSN: 2321-9637
Available online at www.ijrat.org
National Conference on "Role of Information Technology in Social Innovations"
26th & 27th February 2019

Data Visualization in Secure Voting System using Hybrid Cryptography

Mrs.Aarti Gaikwad[1], Malhar Shinde [2], Gaurav Karmankar [3], Omkar Eknath Shinde[4]. Swapnil Bhagwan Vaidha[5]
Department of Information Technology[1,2,3,4,5] DYPCOE,Ak,Pune,SPPU Pune.[1,2,3,4,5]
aratig.2010@gmail.com

Abstract—In this system we will be able to provide online voting, conduct poll and online surveys. System resides in the new concept of secure QR-Code with scanner application, encryption of data for secrecy and data visualization. Voter and admin will login through the app, fill all details after verifying them they are allowed to vote and create poll respectively. Through scanner application the QR-Code is scans details of poll, candidates to vote for are retrieved. Then the voting is performed. In the proposed system, we are using QR code for recognizing image codes using smart phones to provide various services that can recognize the authenticity of any voter details. We have two applications one for voter to register and register his vote or give his opinion and one for admin who will create poll. Poll can be created for selected amount of voters or it can be open for all.As voting goes live admin can see real time results with data visualization techniques by showing results in bar plot, charts, heat maps, histogram and various other techniques. We propose several goals for statistical graphics divided into "discovery" goals and "communication" goals. Discovery goals for data visualization include giving an overview of the content of a dataset here we will give results voting, poll, surveys using different data visualization techniques.

1.INTRODUCTION

In this system we will be able to provide online voting, conduct poll and online surveys. System resides in the new concept of secure QR-Code with scanner application, encryption of data for secrecy and data visualization. Voter and admin will login through the app, fill all details after verifying them they are allowed to vote and create poll respectively. Through scanner application the QR-Code is scans details of poll, candidates to vote for are retrieved. Then the voting is performed. In the proposed system, we are using QR code for recognizing image codes using smart phones to provide various services that can recognize the authenticity of any voter details. We have two applications one for voter to register and register his vote or give his opinion and one for admin who will create poll. Poll can be created for selected amount of voters or it can be open for all.

As voting goes live admin can see real time results with data visualization techniques by showing results in bar plot, charts, heat maps, histogram and various other techniques. In this system data visualization is an integral part of modern statistics and political science. We propose several goals for statistical graphics divided into "discovery" goals and "communication" goals. Discovery goals for data visualization include giving an overview of the content of dataset here we will give results voting, poll, surveys using different data visualization techniques.

2.LITERATURE SURVEY

A.*A Way to Secure a QR Code: SQR:*

To propose a mobile implementation of an e-voting protocol. We also provide a formal analysis to validate a security property of our system. In particular, we show the portability of an e-voting protocol, based on the census protocol, and already defined for polling from a fixed location, on mobile devices. We call our mobile voting system M-SEAS, i.e. the Mobile Secure E-voting Applet System. We will give details of our mobile implementation. Also, we perform a formal verification of the protocol. Indeed, the architecture of M-SEAS has been thought to fix a well-known vulnerability of census, that basically allows one of the entities involved in the election process to cast votes of eligible users that, although registered, abstain to vote. These illegitimate votes would fall into the final tally.

B. *Who Votes for What? A Visual Query Language for Opinion Data:*

Surveys and opinion polls are extremely popular in the media, especially in the months preceding a general election. However, the available tools for analyzing poll results often require specialized training. Hence, data analysis remains out of reach for many casual computer users. Moreover, the visualizations used to communicate the results of surveys are typically limited to traditional statistical graphics like bar graphs and pie charts, both of which are fundamentally noninteractive. We present a simple interactive visualization that allows users to construct queries on large tabular data sets, and view the results in real time. The results of two separate user studies suggest that our interface lowers the learning curve for naïve users, while still providing enough analytical power to discover interesting correlations in the data.

3.PROPOSED SYSTEM

System resides in the new concept of secure QR-Code, Encryption of data and Data visualization. We have two applications one for voter and one for admin who will create poll. Poll can be created for selected amount of voters or it can be open for all. Details are verified of user as he scans QR to vote. QR code we are using here is encrypted with high standards and only authorised users can access it. Encryption makes sure no one can alter with anything in the system. Once user is verified he can register his vote. As voting goes live and voters starts registering votes, admin can see real time results with data visualization techniques by showing results in bar plot, charts, heat map and various other techniques

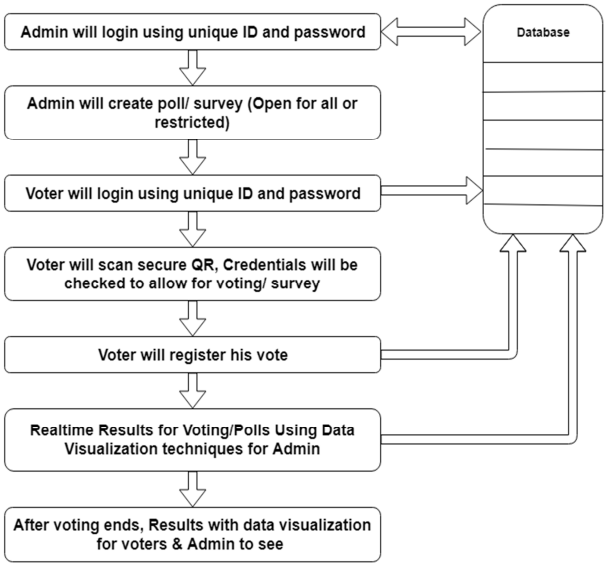

Fig1: Proposed System

Data Visualization:

Data visualization refers to the graphical representation of information and data. By using visual elements like charts, graphs, and maps, data visualization is an accessible way to see and understand trends, outliners and patterns.
When you think of data visualization, your first thought probably immediately goes to simple bar graphs or pie charts. While these may be an integral part of visualizing data and a common baseline for many data graphics, the right visualization must be paired with the right set of information. Simple graphs are only the tip of the iceberg. There's a whole selection of visualization methods to present data in effective and interesting ways.

Common general types of data visualization:

- Charts
- Tables
- Graphs
- Maps
- Infographics

More specific examples of methods to visualize data:

- Area Chart
- Bar Chart
- Circle View
- Dot Distribution Map
- Gantt Chart
- Heat Map
- Histogram
- Scatter Plot

3.SYSTEM ARCHITECTURE

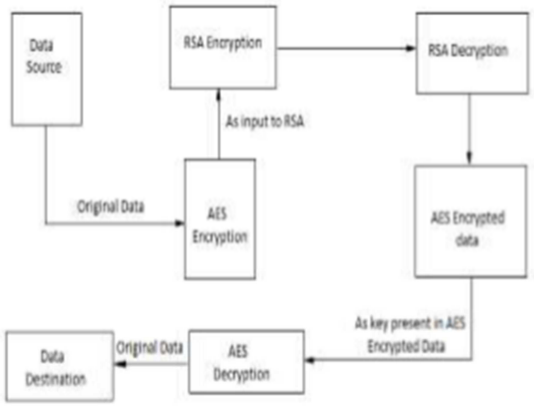

Fig 2: System Architecture (Cryptography)

4.ALGORITHM USED

AES (Advanced Encryption Standards): AES is a symmetric encryption algorithm. It uses the same key for encryption and decryption. Large amounts of data can be encrypted using a symmetric encryption algorithm. The AES rule is capable of using cryptographic keys of 128, 192, and 256 bits.

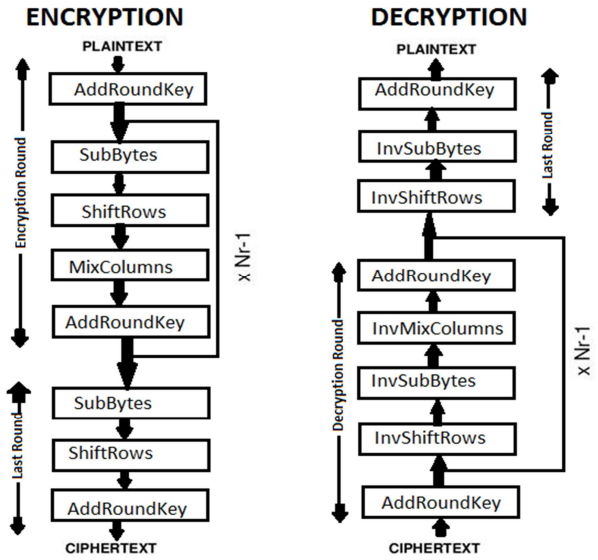

Fig: AES

• RSA(Rivest–Shamir–Adleman): RSA an asymmetric encryption algorithm, based on using public and private keys. A message is encrypted using a public key and decrypted only with a private key only. Asymmetric means that there are two different keys. This is also called public key cryptography, because one of the keys can be given to anyone.

An RSA public-key /private-key pair can be generated by the following steps:
1. Generate a pair of large, random prime's p and q.
2. Compute the modulus n as n = p*q.
3. Select an odd public exponent e between 3 and n-1 that is relatively prime to p-1 and q-1.
4. Compute the private exponent d from e, p and q.
5. Output (n, e) as the public key and (n, d) as the private key.

For Encryption operation:

$$c = \text{ENCRYPT}(m) = m^e \bmod n.$$

For Decryption operation:

$$m = \text{DECRYPT}(c) = c^d \bmod n.$$

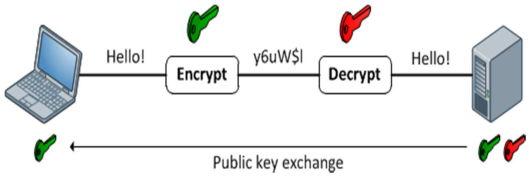

Fig: RSA

• Hybrid AES with RSA:

In proposed algorithm (Hybrid AES-RSA) the goal had been achieved by combining two algorithms called RSA and AES.

A. For Encryption of Data

1. The input is considered as Text and image (.jpeg), is being converted to 128bit plain text.

2. In this hybrid encryption approach, sender uses 128- bit session key value with AES to encrypt the message.

3. The hash value of message was encrypted using RSA algorithm with 2048bit public key of the receiver.

4. Such two sets of encryption AES and RSA to texts and images are then transmitted for further decryption.

B. For Decryption of Data

1. The 2048bit encrypted data is applied to RSA algorithm, which provides decrypted set of data.

2. This one set of data is then further divided into AES dataset.

3. These data sets are then further applied to AES algorithm to get the decrypted set of output.

4. In this sets of 2048 bit decrypted data it gives single original size of output data.

5. ACKNOWLEDGMENT

We have taken efforts in this projecthowever, it would not have been possible without the kind support and help of many individuals and organizations. We would like to extend our sincere thanks to all of them. We are highly indebted to Mrs. Aarti Gaikwadfor her guidance and constant supervision as well as for providing necessary information regarding the project & also for her support in completing the project. We would like to express our gratitude towards our parents & our Head of I.T. Department Dr.Preeti Patil for their kind co-operation and encouragement which helped us in completion of this project. Furthermore, we would also like to acknowledge with much appreciation the crucial role of the staff of

DYPCOE Akurdi, who gave the permission to use all required equipment and the necessary materials to complete the project. We are also deeply grateful to the Principal ofDYPCOE,Dr. VijayWadhaiand our parents for their financial and logistical support and for providing necessary guidance concerning project's implementation.

REFERENCES

[1] Prerna Mahajan, Abhishek Sachdeva, "A Study of Encryption Algorithms AES, DES and RSA for Security", Global Journal of Computer Science and Technology Network, Web & Security, Vol.13, Iss. 15, Vol. 1, 2013.

[2] Who Votes for What? A Visual Query Language for Opinion Data by Geoffrey M. Draper and Richard F. Riesenfeld in November/December 2008.

[3] RSA Implementation for Data Transmission Security in BEM Chairman E-Voting Android Based Application by FransiskusPancaJuniawanin 2016

[4] A Way to Secure a QR Code: SQR by Nishant Goel, Ajay Sharma, Sudhir Goswami in 2017