ONLINE VOTING SYSTEM BASED ON VISUAL CRYPTOGRAPHY AND BIOMETRIC

Anjali Dwivedi[1]
Information Technology, Usha Mittal Institute of Technology Mumbai, India

Gayatri Khandare[2]
Information Technology
Usha Mittal Institute of Technology Mumbai, India

Mariha Shaikh[3]
Information Technology, Usha Mittal Institute of Technology Mumbai, India

Mrs. Anita Morey[4]
Usha Mittal Institute of Technology Mumbai, India

---***---

Abstract—With growing internet usage, exploitation activity has also increased over the years' diverse online attacks have been extended and among them the most notable attack is phishing. Phishing is being undertaken by an individual or a social event to get singular restricted information like passwords, Master card information from confusing setbacks for discount fraud, monetary advantage, and other phony activities. But not only phishing is an activity we're trying to resolve but also the violation that is been observed is that the person who is authorized to vote lays hold of and instead other rambles the votes. In this paper, we have proposed the right that a voter gets without violating his/her rights and the candidates. Another procedure named" A Novel Anti-phishing structure reliant on visual cryptography" deals with the issue of phishing. Here an image-based confirmation using Visual Cryptography and another way of providing security is through Bio-metric finger sensor. The use of visual cryptography is researched to shield the security of an image manual human test by rotting the first picture manual human test into two successful images which can also be referred to as sheets that are taken care of in secluded information collection laborers (one with voter furthermore, one with laborer) which are covered until the two images are combined to get the real images(password) which are referred to as CAPTCHA. The mystery is permits access. And the final aim of implementing Bio-metric technology is achieving duplication and phishing of the voting register thus preventing multiple voter voting.

***Index Terms*- Voting System, Cryptography, AES Algorithm, Finger print sensor.**

I. INTRODUCTION

Earlier casting votes through internet ballot was impractical, before due to security reasons yet with the idea of two- layer authentication measure for ID of electors and voters. Projecting their cast vote by ballot recognizing their right to vote stalls will satisfy all the requests forced by the political decision commission of India. There was a various explanation by which this framework was sought after like on the final voting day people groups couldn't visit ballot stalls because of their medical condition, mature age people couldn't stroll to project their votes by remaining in line for an extensive stretch, working proficient who were out of their city on Election day and some more. To project their valuable votes which can bring the change, people need to enlist by giving their essential data and their citizen ids cards like the Aadhar card and voter ID card number. Its exceptional distinguishing proof strategy will straightforwardly divert to a specific corner for which that individual is permitted to cast a ballot vote and the Admin will be ready to see the rundown of applicants who have been enlisted from their area or ward or territory.

• The framework will produce just a one-time secret phrase on the date of political Election day through which individual can make their choice and when they cast, such individuals won't be permitted to project their vote once again. [1]

• Online Political Election Framework is the framework that empowers the client to cast a ballot on the web.[2]

• Explicitly, the Democratic framework comprised of worker administrations which are each connected with a data set for putting away industrious information. [3]

• Administrator will keep up all data with regard to citizen and tallies consequently they're deciding in favor of their chosen parties. [4]

II. LITERATURE REVIEW

This paper deals with the design and development of an "online -Based Voting System Using Visual Cryptography and Fingerprint Design and Implementation", to provide high performance with high security to the voting system have also used the web to make the voting system more practical. The proposed AES (Advanced Encryption Standards) algorithm security ensures just if it is adequately done an incredible key to the organization. The methodologies for phishing identification framework are email-based methodology,

visual piece of information-based approach data stream based methodology, and design closeness based methodology. In the existing arrangement of phishing locations, there is likewise a methodology where visual cryptography is utilized. [1] In this methodology when the client first registers as the Voter, at that point at the hour of enlistment itself a picture is chosen which is isolated into two consecutive parts. One portion of the picture is put away at the bank worker, what's more, the client gets another offer which he keeps with him. When the client needs to start the exchange with the Admin he sends his UID code to the voter. Vendor a worker at that point sends his sys ID secret phrase alongside the client's UID to the Administration [2]. Till now, projecting votes was finished utilizing electronic ballot performances what's more, by visiting their Ballot election area. If such individual was not accessible, they couldn't make their valuable choice, what's more, checking the number of decisions in favor of each assigned applicant was a period taking cycle in any event, when utilizing electronic ballots. Multiple layers of safety systems were unrealistic to carry out immense speculation. There was no system to accessibility and unwavering quality of the Internet casting a ballot framework and ID of the right individual who will project their vote. This system has provided a coherent way to cast votes, free of fraud, swindle free, and make the system more trustable, and fast. [3]

III. ALGORITHM

1. AES (Advanced Encryption Standards) AES plays out all its computations on bytes rather than pieces. In this way, These 16 bytes are coordinated in four segments and four lines for taking care of as a structure. [1]

2. AES uses 10 rounds for 128-digit keys, 12 adapts to 192- piece keys and 14 rounds for 256-digit keys. Each of these rounds uses other 128-cycle round key, which is resolved from the main AES key. [2]
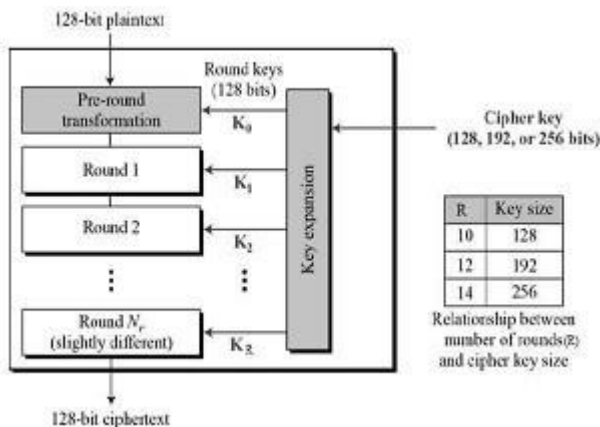

Fig.1. schematic of AES structure

3. AES is extensively gotten and maintained in both gear

and programming. Till date, no practical cryptanalytic attacks against AES has been found. In addition, AES has inborn versatility of key length, which allows a degree of 'future proofing' against progress in the ability to perform careful key requests. [3]

4. Similarly concerning DES, the AES security is ensured just in the event that it is adequately done and incredible key organization is used. [4]
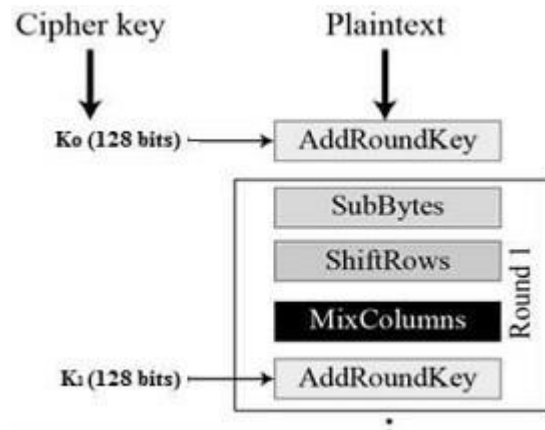

Fig.2. Encryption Process

IV. VISUAL CRYPTOGRAPHY

Extraordinary compared to other realized strategies to secure information is cryptography. It is the craft of sending and accepting encoded messages that can be decoded simply by the sender or the collector. Encryption and unscrambling are cultivated by utilizing numerical calculations so that nobody however the expected beneficiary can decode and peruse the message. Naor furthermore, Shamir presented the visual cryp- tography plot (VCS) as a basic and secure approach to permit the mysterious sharing of pictures with no cryptographic calculations.

V. BIOMETRIC FINGER SENSOR

Biometrics is robotized technique used for perceiving an in- dividual dependent on physiological or conduct characteristics. A unique finger impression scanner is a gadget that is used to distinguish an individual by examining their fingerprints. We have a few edges on our fingers. Moreover, every individual has an exceptional example. Thus, a unique mark scanner checks them to recognize.

VI. METHODOLOGY

This record is the Product Prerequisites Determination for the "Online Political race Framework" which is being created as part of a scholarly course. [1]

This record is expected to give a point by point determination of the prerequisites for the designers and fill in as a methods to unmistakably layout the venture highlights [2]

The overall necessities give an outline of the client's attributes, item viewpoint, and outline of useful also, information prerequisites. [3]

The particular necessities give a more refined adaptation of the general necessities. [4]
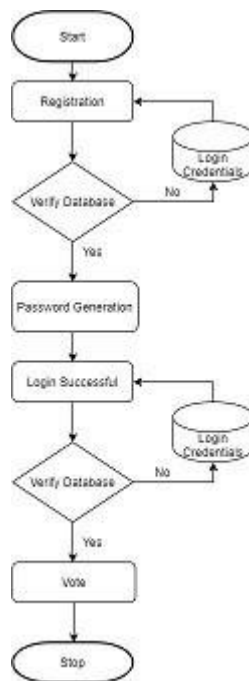
VII. FLOWCHART DIAGRAM

Fig. 3. Voting Flow

VIII. IMPLEMENTATION

I. Administrator Meeting:

• Login: Administrator need to enter substantial login certifications all together to login into the framework. [1]

• Add Political decision: Administrator can add political decision detail by entering name, choosing competitors and setting political decision end date. [2]

• View Political decision: By choosing the political race id, administrator can see political decision subtleties and the competitors with their photograph.

• Administrator can produce result from here itself. [3]

• Add Competitors: Administrator can enroll every single new up-and-comer detail with their photo. [4]

• View Applicants: Every one of the enrolled competitors will be shown. [5]

• View Result: Administrator can see result by choosing the political decision id from the view political decision module. [6]

• View Client: Every one of the enlisted clients will be shown here with their subtleties. [7]

ii. Citizen Meeting:

• Register: Client need to enroll first by topping off fundamental enrollment subtleties. While enrollment, secret key is put away into picture record and 2 picture documents are produced. One picture record is sent over mail and another is downloaded in neighborhood framework. [1]

• Login: Here, the genuine validation is performed where client need to enter their login id and select the two pictures which were sent and downloaded separately. Subsequent to blending the picture, the encoded secret phrase is appeared and client need the enter the encoded secret phrase to continue with login. [2]

• Vote: After fruitful login, client would now be able to choose political decision id and cast their decision in favor of the ideal competitor. [3]

• View Result: Client can see the political decision results here. At present surveying are occurring by manual democratic framework. Our proposed framework is internet casting a ballot framework with security measures. With the goal that client can capable survey at any spot in this world through Web. [4]

iii. Task Execution

The Task is stacked in Visual Studio 2010. We utilized Visual Studio for Plan and coding of task. Made and kept up all information bases into SQL Worker 2008, in that we make tables, put down inquiry for store information or account of venture.[1]

Equipment Prerequisite:

• i3 Processor Based PC or higher
• Memory: 1 GB Slam
• Hard Drive: 50 GB
• Screen
• Web Association
Programming
Prerequisite:
• Windows 7 or higher
• Visual studio 2010.
• SQL Worker 2008.

IX. MODULES
X. USER MODULE REGISTRATION

This is the registration page, where the voter can register themselves. The users have to enter their details which are required by admin through registration page. All the details registered on the portal are saved in the respective database. The Admin has authority to accept eligible user, otherwise he has right to reject their registration by providing reason of rejection.

Fig.4. REGISTRATION

XI. USER MODULE DASHBOARD

From here client can login to his record furthermore, can oversee entire democratic interaction by login, producing secret key, see competitor and vote. He has the option to cast a ballot.
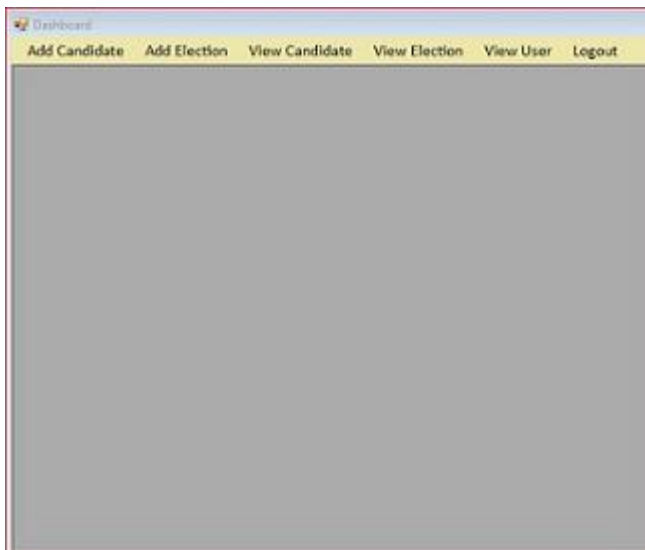

Fig. 5. USER-DASHBOARD

XII. USER MODULE AUTHENTICATION

It is utilized to create secret key with the assistance of visual cryptography two way verification.

Fig.6. AUTHENTICATION

XIII. ADMIN MODULE DASHBOARD

From here administrator can login to his record furthermore, can oversee entire democratic interaction by adding new political race, creating id for client, confirming the clients, creating result and some more. He has the privilege to create id for client by confirming the clients.
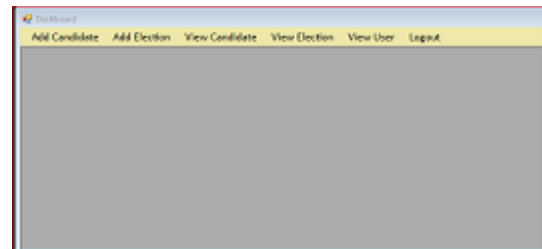

Fig. 7. DASHBOARD

XIV. ADMIN MODULE ADD CANDIDATE

This is a module which gives a rundown of all continuous political decision, this module is open just to those clients who have been checked by administrator. By this module client can project their vote by choosing an up-and-comer of a specific political race.

Fig.8. ADD CANDIDATE

XV. ADMIN MODULE ADD ELECTION DIAGRAM This a

module which add when election is going to be held along with election name and candidate which all are participating.

Fig.9. ADDELECTION

XVI. RESULT

This module provides the results of all the completed elections; user has the right to see the result of elections. All the results are being generated by admin after the successful completion of the election.
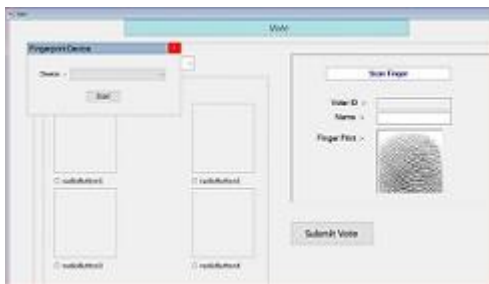

Fig. 10. VIEW RESULT

XVII. CONCLUSION

In this paper we have attempted to utilize Visual Cryptogra- phy to forestall Phishing. This paper has endeavored to inves- tigate the significance, need and simplicity of casting a ballot Future work remembers the working and testing the outcome for huge measure of information. This task can likewise be utilized in reality situation.Since Visual Cryptography Method is utilized, client can ready to see if he is in phishing site or unique site without any problem.Proposed internet casting a ballot framework is successful and it will valuable for citizens.

REFERENCES

1) Himanshu Agarwal and G.N. Pandey "Online Voting System for India Based on AADHAAR ID" 2013 Eleventh International Conference on ICT and Knowledge Engineering

2) Smita B. Khaimar, P. Sanyasi Naidu, Reena Kharat "Secure Authenti- cation for Online Voting System"

3) Shivendra Katiyar, Kullai Reddy Meka, Ferdous A. Barbhuiya, Sukumar Nandi "Online Voting System Powered By Biometric Security" 2011 Second International Conference on Emerging Applications of Informa- tion Technology.

4) Al-Ameen, A.; Talab, S.A., "E-voting systems vulnerabilities," Infor- mation Science and Digital Content Technology (ICIDT), 2012 8th In- ternational Conference on , vol.1, no., pp.67,73, 26-28 June 2012 URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=arnumber=6269229isnumber=6269212

5) Cui Zhe; Dai Xiang,"A practical distributed electronic voting system," Electric Information and Control Engineering (ICEICE), 2011 International Conference on , vol., no., pp.1095,1099, 15-17 April 2011 doi: 10.1109/ICEICE.2011.5777548 URL:

6) http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=arnumber=5777548isnumber=5776798

7) Gritzalis, D. (2002). Secure Electronic voting. Seventh Computer Secu- rity Incident Response Team Workshop Syros, Greece.

8) Krejcie, R. Morgan D. (1970). Determining Sample Size for Research Activities Educational and Psychological Measurement.

9) Melanie Volkamer (2010), —Electronic Voting in Germany‖, Data Protection in a Profiled World, DOI 10.1007/978-90-481-8865- 9$_1$0, *SpringerScience + BusinessMediaB.V.*2010