An Online Voting Application using Elgamal Algorithm

ChandraPrabha K[1] Abinaya S[2]
[1]Student [2]Assistant Professor
[1,2]K. S. Rangasamy College of Technology, Tiruchengode, Tamilnadu, India

Abstract— Propelled security strategies are important to present viable internet casting a ballot (e casting a ballot) inside the whole world. Decisions directed on paper devour numerous assets and add to the pulverization of woodlands, which winds up in atmosphere weakening. Ongoing web based democratic encounters in nations simply like the us, India and Brazil exhibited that further research is require to fortify security ensures for future decisions, to ensure the classification of votes and empower the check of their uprightness and legitimacy. during this paper, we propose a positioned decision online appointive framework, which tends to these difficulties. It kills all designed limitations on the potential assignments of focuses to various applicants steady with the voters' very own inclinations. in order to monitor the classification of the votes, each cast voting form is scrambled utilizing the exponential ElGamal cryptosystem before accommodation. Besides, during casting a ballot the framework guarantees that verifications are produced and put away for each component inside the cast polling form. These verifications are wont to confirm the rightness and accordingly the qualification of each polling form before tallying without decoding and getting to the substance of the voting form. This approves the votes inside the tallying procedure and at a proportionate time looks after secrecy. the security and execution examinations included during this paper show that our strategy has accomplished critical upgrades as contrasted and the past frameworks. The results of our trials likewise show that our proposed conventions are plausible for down to earth executions.

Keywords: An Online Voting Application, Elgamal Algorithm

I. INTRODUCTION

A. Elections in India

A democratic setup in any country requires a periodic organization of an event where the people are allowed to express their inclinations and thoughts. No system captures these thoughts in a democratic system better than a voting system. In the scheme of things on a larger scale, democracy is relatively new and thus susceptible to evolution. This holds true for voting systems as well.

Election is the stepping-stone of Indian democratic setup and leads to the formation of a responsible government vested with great powers in it. With the implementation of globalization and an increase in the education levels across the country, the citizens of India are becoming more aware of not only their rights but also their responsibilities. These are the responsibility of the citizens of the country. “Right to Vote”, provided to the citizens of India through Article 326 of our Constitution and through Representation of People’s Act 1951, act as a tool through which the citizens decide on the immediate and long-term future of our country. Thus, competent authorities like Election Commission, Central Government etc. should put in efforts to ensure that more and more citizens participate in the electoral process.

Over the years, efforts have been taken to make the voting processes as secure as possible, while focusing on reliability, neutrality and efficiency. The advancement in the field of Information Technology has led to the provision of a variety of optimized solutions. It makes an effort to determine the best voting system that should be adopted in an under-developed or developing democracy by analysing the reliability, security, neutrality and efficiency of the voting system.

Elections are a transformative tool for democratic governance. They are the means through which people voice their preferences and choose their representatives. Elections are unique. They change the fate of nations, influence participation and activism in politics, and deeply affect the lives and attitudes of society.

B. Data Mining Concept

Data Mining is an analytic process designed to explore data (usually large amounts of data typically business or market related) in search of consistent patterns and/or systematic relationships between variables, and then to validate the findings by applying the detected patterns to new subsets of data. The ultimate goal of data mining is prediction and predictive data mining is the most common type of data mining and one that has the most direct business applications. Data Analysis and modeling and it shares with them both some components of its general approaches and specific techniques. The process of the data mining consists of three stages: (1) the initial exploration, (2) model building or pattern identification with validation/verification, and (3) deployment.

1) Stage 1: Exploration:
This stage usually starts with data preparation which may involve cleaning data, data transformations, selecting subsets of records and - in used to predict.

2) Stage 2: Model building and validation:
This stage involves considering various models and choosing the best one based on their predictive performance. This may sound like a simple operation, but in fact, it sometimes involves a very elaborate process.

3) Stage 3: Deployment:
That final stage involves using the model selected as best in the previous stage and applying it to new data in order to generate predictions or estimates of the expected outcome.

C. An electoral System

An electoral system, usually referred to as a voting system, acts as the backbone of any democratic institution. Characterized by its involvement of the most important players in a democracy, that is, the common people, a voting system essentially consists of a set of certain protocols and rules that must be abided by in order to consider a vote to be valid, and how votes are essentially counted and culminated in order to yield a commensurate result. It involves two sets

of entities, a set of voters and a set of candidates. The voter makes a choice between a provided set of candidates based on their understanding of a situation and their inclinations.

In a democratic setup, the process of voting takes place in an environment that is governed by an independent agency. Their responsibility includes the setting up of a voting station where the electorates can cast their vote, collection of votes using a ballot system, transportation of the recorded votes to a place for counting and aggregation, counting of all the votes cast and finally the announcement of the results based on the votes cast. A democratic system may have different types of environments where the votes are casted. The environment could be an election or a referendum, based on the type of situation in which the votes are being casted. Proportional Voting Systems guarantee a certain degree of proportionality by ensuring that each winning candidate represents the same number of vote casters.

To summarize briefly, a voting system consists of the following players:

1) The Voter – The voter is a member of the electorate that casts their opinion about the environment in the form of a vote. A voter cannot cast more than one vote. In many democratic institutions, a voter is determined on the basis of age restriction in order to ensure that the voter makes a mature decision in context of the environment.
2) The Candidate – The candidate is the person for whom the voter casts a vote. Normally, the candidate with the maximum number of votes in a constituency is adjudged the winner of the election.
3) The Election Manager – The election manager acts as an intermediate between the voter and the candidate. It is the election manager's job to ensure the setting up of a proper election environment and the counting of votes. The three players must all be isolated from each other in the sense that they do not have the capability to influence each other.

D. Desisting the Fraud in India's Voting Process through Multi Modalbiometrics

In India, voting procedure strictly adheres to the principle of Electronic Voting Machines (EVM'S) known as offline E-Voting. EVM'S have the flexible characteristics like simple design, ease of use, reliability and fast accessing. Unfortunately, these EVM'S are criticized for the irregularity reports in elections. Therefore, these criticisms lead to damaging the main objective of the voters and Election commission faces arduous task to conduct free and fair elections. It has many advantages that overcome the drawbacks of the ordinary voting process.

Tampering the machine state is very dangerous state, if the system may build with honestly but an attacker has a chance to modify the machine state by replacing the original hardware part. To decrease these criticisms many of the researches are into the survey to find out the legitimate voter. Due to lack of photo clarity in the identity cards or any other reasons like Hardware problems in EVM'S, malfunctioning officer's invalid votes are being casted. This result in dishonest vote count or replacing the votes with the person criteria based etc. These may results in hardware and software problems and security problems too.

Although finger print recognition system has many benefits and at the same time it has certain drawbacks also. Firstly the image of the finger will be captured and with the image dirt, greases, and other contaminated content will also be recorded and these certain chances allows the fingerprint to get rejected. Unfortunately, the person had the cuts on his finger or he had any mark on his finger then at the verification time the person will be seemed as an invalid voter.

Even though the enrolment phase work well, this is not possible always when working with the common database. This may cause more opportunity in increase of errors and duplications. It is better to get register as unique user otherwise too many users' registrations in common database May leads to many powerful attacks.

Multi model biometrics is the fusion of two or more traits either finger and palm or finger or iris etc. This type of biometrics fusion can be performed in different levels like after scanning the traits or after extraction of the features etc. These types of fusions may lead to high-level security, which cannot be modified by any intruders. Also, helps in improving the performance of the biometrics systems. Some of the advantages are False Rejection and False Acceptance Rates, Accuracy.

E. Secure Voting System through SMS and using Smart Phone Application

Mobile voting system is used to cast their votes in secure manner. This process consists of three steps: online registration of voter, vote casting of voter and display of results, through the concept of SMS (short messaging service). In this system, the voters can cast their votes from anywhere and anytime, no need to go to polling booths through internet. This saves the time and cost. It also avoids the tiredness and violence. The procedures used are easy, transparent and secure. No expensive hardware was used in this system and serves the demand for remote voting. The important aspect of this is to provide more security until the core, since every vote count and each of the votes are to be remained confidential. This prevents voters to cast their vote more than once with the use of OTP (one-time password) for every sign in and login. It also reduces the paper work and eliminates the manual counting process. Here the security is provided through the RSA encryption algorithm. Without eliminating the security threats like buying of vote, hacking of online registered passwords, secrecy of ballot, double time voting the mobile voting system is designed. This consists of the mobile phone that uses Subscriber Identity Module (SIM), which provides identity privacy, user identity verification and subscriber data privacy. The key features of this system include the following:

1) Secrecy: no one will be able to find for whom the user is voting.
2) Portable: the mobile phones are portable, henceforth the system.
3) Eligibility: only the authorised user can access the logins.
4) Uniqueness: each user has the individual identity.
5) Integrity: Changes will not be allowed once the vote is casted.

F. Smart Voting

The machine is placed in the poll booth centre and is monitored by higher officials. Due to some illegal activities the polling centre are misused and people's vote to right has been denied. This seldom occurs in rural areas as well as in urban cities because the educated people are not interested in casting their votes to candidates who represent their respective areas. To ensure 100% voting automation came into play. This system proposed a secure online voting system by utilizing the concept of biometric and stenographic authentication. Homomorphic technique encrypts the casted vote stored and decrypts it during the results. It enhances our country with a better voting system to ensure 100% voting. Our digital voting system generates the list of all the people in the state above 18 years from the aadhar card database since it is made mandatory in our country today. From the generated list, our system will automatically generate a voter id for people above the age of 18. Hence, by way nobody will be left out without getting his or her right to vote which fails in the existing system. Therefore 100% voting will be achieved. During the time of voting, the voter can download the voter id from the net by using the aadhar card number. By using this number, he/she can cast his/her vote. Instead of using the existing voting machine, A new machine is supplied which is capable of tracking the aadhar card details of the voters. It will automatically give a notification to the voter to cast their vote. So, the people can cast their vote with the latest technology and high security than the existing system. The security is maintained by making a voter to cast his/her vote only once. If he/she tries for the second time, he/she will not be able to vote since tracking feature is included in our system.

The user has to first login into the system through the fingerprint. Authentication is being granted from the aadhar finger print database. If both the fingerprint matches, the user has to go through the scanning process of his/her face and retina. If it matches, the voter will be allowed to enter their voter id and cast their vote for their interested party.

G. A Fingerprint Matching Technique using Minutiae Based Algorithm for Voting System

For voting purpose, there should be a biometric authentication, which is secure, & privacy protected. If the system designed is insecure then it may be prone to certain attacks in database. Some researchers have worked on different techniques based on fingerprint matching considering FRR rate, but not yet implemented in designing a voting system. Here the fingerprints are matched using minutiae algorithm. A Minutiae based algorithm, which is connected with the other voting devices through the internet that use two stage fingerprint matching technique, in which minutiae position from one fingerprint image & orientation from other is used to create combined fingerprint image. Proposed system aims implements a voting system using minutiae-based algorithm with low FRR rate. In Minutiae based algorithm, the two different fingerprint templates are used for creating a new identity, which can be used for enrolment & authentication, propose. Here the minutiae of fingerprints of both fingers are used to produce a new template. The new template is formed by the combination of two minutiae of fingers. The combined fingerprint image is constructed in two phases, in first phase fingerprint image is captured from both fingerprints. A reference point and orientation from first fingerprint and reference point & minutiae extraction is taken from both fingerprints to create a new combined fingerprint, which is stored in database. By using the minutiae-based algorithm, the complete minutiae feature of a both in new combined fingerprint will not be reconstructed when the database is robbed. By using the two fingerprints matching technique, the FRR may reduce & performance of the system increases.

H. Smart Electronic Voting System Based on Biometric Identification-Survey

Traditionally, the election commission in India uses electronic voting machines, which need more work forces, time-consuming, and they are less trustworthy. Even though the existing voting machine is fast and accurate, this system needs more work forces and it is not much more reliable. To increase the reliability of the voting, many algorithms have been introduced. One of the major ideas of developing the system is to use the person's identity. In the field of biometric identification, it can get the better results and it is also trustworthy. The major unique identity of each person is his fingerprint, Iris etc. So, one of the cheapest ways of recognition is fingerprint recognition. Not only the developers use this biometric, the government also has taken necessary steps to collect the biometric data and stored into a database. The concept of getting the fingerprint impression of a voter that is entered as input to the system, which is then compared with the available data in the database. If the particular pattern matches with anyone on the available record, access to cast a vote is granted. The government also issued aadhar card to identify the person's unique identity. Using the aadhar card, the voters to cast the vote without difficulty.

II. EXISTING SYSTEM

Online voting system by utilizing the concept of biometric and stenographic authentication. Homomorphic technique encrypts the casted vote stored and decrypts it during the results. It enhances our country with a better voting system to ensure 100% voting. Our digital voting system generates the list of all the people in the state above 18 years from the aadhar card database since it is made mandatory in our country today. From the generated list, our system will automatically generate a voter id for people above the age of 18. Hence, by way nobody will be left out without getting his or her right to vote which fails in the existing system. Therefore 100% voting will be achieved.

Traditionally, the election commission in India uses electronic voting machines, which need more work forces, time-consuming, and they are less trustworthy. Even though the existing voting machine is fast and accurate, this system needs more work forces and it is not much more reliable. To increase the reliability of the voting, many algorithms have been introduced. One of the major ideas of developing the system is to use the person's identity. In the field of biometric identification, it can get the better results and it is

also trustworthy. To overcome the issues in online voting and to improve the existing voting system the android application is used which will give better system security and vote casting become less time-consuming process and it will provide better results. Voter can cast vote remotely from anywhere in the country with the help of an android device and voting application on his device. Voters must have internet connection on their android device to cast vote from remote place. Android application will be compatible with almost all the android devices so that every voter should get benefit of online voting system. It has higher level of security as it has two stage authentication technique i.e. Facial recognition and One Time Password (OTP). Voter data that is his facial images and voter id will be stored on the database. Server itself does verification process. Facial image of voter will be fetched by android application which will be then forwarded to server for further verification, also thereafter One Time Password will be provided to the voter on his registered mobile number for further verification process for vote casting. Voter is allowed to cast his vote after successful verification with facial recognition and One Time Password. Results of election will be displayed on individual voter's device in terms of notification and voter will get updates about election to enhance the system performance.

III. PROPOSED SYSTEM

Homomorphic encryption is the encryption scheme, which means the operations on the encrypted data. Homomorphic encryption can be applied in any system by using various public key algorithms. When the data is transferred to the public area, there are many encryption algorithms to secure the operations and the storage of the data. However, to process data located on remote server and to preserve privacy, homomorphic encryption is useful that allows the operations on the cipher text, which can provide the same results after calculations as the working directly on the raw data.

The main focus is on public key cryptographic algorithms based on homomorphic encryption scheme for preserving security. The case study on various principles and properties of homomorphic encryption is given and then various homomorphic algorithms using asymmetric key systems such as RSA, ElGamal, Paillier algorithms as well as various homomorphic encryption schemes such as BrakerskiGentry-Vaikuntanathan (BGV), Enhanced homomorphic Cryptosystem (EHC), Algebra homomorphic encryption scheme based on updated ElGamal (AHEE), Non-interactive exponential homomorphic encryption scheme (NEHE) are investigated.

IV. ENHANCED HOMOMORPHIC CRYPTOSYSTEM

Homomorphic encryption has been used in online voting systems, for example. The homomorphic property makes it possible to tally all encrypted ballots without decrypting them and accessing the content of any individual ballot.

Helios is the first web-based voting system. It used ElGamal encryption to achieve open-audit voting. Helios did do not claim any cryptographic novelty apart from that fact that, assuming that there were enough auditors, even if all the authorities fully colluded to corrupt the system, they would be unable to counterfeit the election result without a high chance of being caught. However, the security of the Helios relies on the trust of all participants in the Helios server. The security level of Helios depends on a mix-net shuffling mechanism implemented by the server. It follows that a corrupt Helios server can attempt to shuffle submitted votes incorrectly or decrypt shuffled votes incorrectly. Further, the performance results reported in show that the computation time is quite long.

V. SECURITY OF THE HELIOS

The security of the Helios relies on the trust of all participants in the Helios server. The security level of Helios depends on a mix-3. net shuffling mechanism implemented by the server. It follows that a corrupt Helios server can attempt to shuffle submitted votes incorrectly or decrypt shuffled votes incorrectly. Further, the performance results reported in show that the computation time is quite long.

The verification and auditing process took more than three hours on a server and a complete audit took more than four hours on voter, even though there were only 2 questions in each vote and 500 voters in total. Thus, provided the time achieved in only one experiment with a fixed number of voters. All previous voting systems including imposed several security assumptions required on their systems. The authors assumed that there were several honest authorities and a central honest server. If any authority is compromised, they can attempt to shuffle the votes incorrectly. Likewise, a corrupt Helios server knows the usernames and passwords of all users, and can easily authenticate and cast ballots on behalf of users. Several improvements to Helios were made in Helios 2.0, which was used in a real election (UCL election). Helio 2.0 could handle 25,000 potential voters. In the UCL election, 5000 participants registered and nearly 4000 voted in each round of the election. Helio 2.0 updated the open-audit mechanism, so that it could provide more evidence of the counters' works to all voters. However, their proposed approach distributed the key-generation and decryption code among a few trusted members of the election commission. This required the trustees to be technically savvy and honest. There is no indication of the running time of any new experiments in.

VI. ELGAMAL DSA

A multi-authority e-voting system introduced in applied the distributed ElGamal DSA with an inherited additive homomorphism property. In addition to the authorities and the voters in the election, a trusted third party was introduced and was used to distribute the shared secret key among the multiple authorities. The proposed system became receipt-free, because the encryption of each ballot now is done by the trusted third party. This means that the voters could not prove how they voted by using their encrypted vote, and the authorities of the election could not learn the content of each vote from its encryption. However, the drawback of the system was that the third party could collude with any of the authorities and together they could recover the contents of submitted votes, which would violate

the privacy of voters. The proposed a model, which can tackle all earlier issues encountered in a conventional (manual) voting system such as paper printing, distribution, storage huge investments in transportation etc. With the use of an e-voting system, as the one proposed in this paper, many of the issues, that have challenged traditional voting systems in the past, are bound to be resolved providing peace of mind to both electorates and election candidates. This model is transparent, secure, easy to understand and can be implemented as an option with the other existing technologies. The proposed system became receipt-free, because the encryption of each ballot now is done by the trusted third party. This means that the voters could not prove how they voted by using their encrypted vote, and the authorities of the election could not learn the content of each vote from its encryption.

VII. Conclusion

Recent advances in new technologies to support electronic voting are the subject of great debate. Several researchers advocate the benefits it can bring such as improved speed and accuracy in counting, robustness, accessibility, voting from home etc. Many are also concerned with the security issues it poses, such as unequal access (digital divide), violation to secrecy and anonymity, alteration of the results of an election (because of malicious attacks, bad design/coding, or procedural weaknesses). Electronic voting systems have been introduced to improve the voting process. They also could lead to increased voter turnout, thus supporting democratic process. The proposed a model, which can tackle all earlier issues encountered in a conventional (manual) voting system such as paper printing, distribution, storage huge investments in transportation etc. This model provides comfortable facility to the busy electorates to vote. They have to perform some simple steps on their mobile phone to cast their votes. Here the homomorphic algorithm is replaced by ElGaml alogorithm to yield more efficiency in short time. This model also motivates people those who avoid visiting to voting centre to cast their vote. It is designed to increase the participation of busy electorate, so that their valuable vote can help in supporting democratic process. With the use of an e-voting system, as the one proposed in this paper, many of the issues, that have challenged traditional voting systems in the past, are bound to be resolved providing peace of mind to both electorates and election candidates. This model is transparent, secure, easy to understand and can be implemented as an option with the other existing technologies.

References

[1] Alt.F, Schnessgass.S, Shirazi.A.S, Hassib.M, and Bulling.A(2015),"Graphical passwords in the wild understanding how users choose pictures and passwords in image-based authentication schemes," in Mobile HCI.

[2] Bo.C, Zhang.L, Li X.-Y, Huang.L, and Wang.Y, "Silent sense: silent user identification via touch and movement behavioral biometrics," in Proc. of the 19th Annual International Conference on Mobile Computing and Networking, 2016, pp. 187– 190.

[3] Cao.H and Lin.M, "Mining smartphone data for app usage prediction and recommendation: A survey," Pervasive and Mobile Computing, pp. 1–22, 2017.

[4] De Luca.A, Hang.A, Brudy.F, Lindner.C, and Hussmann.H, "Touch me once and i know it's your Implicit authentication based on touch screen patterns," in CHI '12, 2017, pp. 987–996.

[5] Falaki.H, Mahajan.R, Kandula.S, Lymberopoulos.D, Govindan.R, and Estrin.D, "Diversity in Smartphone Usage," ser. MobiSys, 2016, pp. 179–194.

[6] Feng.T, Liu.Z, Kwon K.-A., Shi.W, Carbunar B., Jiang.Y, and Nguyen.N, "Continuous mobile authentication using touchscreen gestures," ser. 2015 IEEE Conference on Technologies for Homeland Security (HST), 2015, pp. 451–456.

[7] Findling.R D and Mayrhofer.R, "Towards face unlock: On the difficulty of reliably detecting faces on mobile phones," in Proceedings of the 10th International Conference on Advances in Mobile Computing &; Multimedia, ser. MoMM '12, 2014, pp. 275–280.

[8] Frank.M, Biedert R., Martinovic.I, and Song.D, "Touchanalytics: on the applicability of touch screen input as a behavioral biometric for continuous authentication," IEEE Trans. on Info. Forensics and Security, vol. 8, no. 1, pp. 136–148, 2013.

[9] M. Lin, H. Cao, V. Zheng, K. C. Chang, S. Krishnaswamy, "Mobility profiling for user verification with anonymized location data", pp. 960-966, 2015.

[10] Matyas.F., and Riha.Z, "Toward reliable user authentication through biometrics," Security Privacy, IEEE, vol. 1, no. 3, pp. 45– 49, 2013.

[11] Muslukhov.I, Boshmaf Y., Kuo.C, Lester.J, and Beznosov.K, "Know your enemy: The risk of unauthorized access in smartphones by insiders," in MobileHCI '13, 2013, pp. 271–280.

[12] Schneegass.S, Steimle.F, Bulling.A, Alt.F, and Schmidt.A, "Smudge safe: Geometric image transformations for smudge resistant user authentication," in UbiComp '14, 2014, pp. 775–786. vol. 37.

[13] Xu.H, Zhou.Y, and Lyu M. R, "Towards continuous and passive authentication via touch biometrics: An experimental study on smart phones," ser. Symposium On Usable Privacy and Security (SOUPS 2014), 2014, pp. 187–198.

[14] Y. Ren, Y. Chen, M. C. Chuah, J. Yang, "Smartphone based user verification leveraging gait recognition for mobile healthcare systems", pp. 149-157, 2013.

[15] Zheng.N, K. Bai, H. Huang, and H. Wang, "You are how you touch: User verification on smart phones via tapping behaviors," ser. IEEE 22nd Int. Conf. on Network Protocols (ICNP), 2014, pp. 221–232.

