Securing Mobile Voting Process by Integrating Location Services with Encryption Algorithm

Bhavana Sinha
Department of Computer Science & Engg., Shankaracharya Group of Institutions, Bhilai (C.G.), India.

Reetika Singh
Asst.Professor, Dept. of Computer Science & Engg., Shankaracharya Group of Institutions, Bhilai (C.G.), India.

Abstract – As the advanced age keeps on growing, just time will tell until pretty much every human-took care of methodology gets to be mechanized. Versatile correspondence of later has taken the world by storm. Because of the various focal points they offer, various government and private business techniques are being completed under this stage. Voting is a formal evidence of a decision between two or more competitors or strategies, communicated regularly through hand-tallied paper ballots or by show of hands. Like all different parts of popular government, voting obliges straightforwardness, support and responsibility. In this manner, the effectiveness, unwavering quality and security of the strategies utilized are very discriminating. Business around the globe has generally, of later, been directed utilizing electronic means. Enlarging the current voting frameworks with portable voting will upgrade the voting process by expanding voter participation. The proposed work intends to expand security in order to diminish the possibilities of fake voting and build adaptability.

Index Terms – Encryption, Decryption, Location services,GPS, Voting.

1. INTRODUCTION

Information support turns into a basic part with fitting connection at all distinctive stages. Any social crisscross upon the genuine data can change the real importance of the decision, which is an awesome concern in the divisions. In present circumstance we are having both manual voting and electronic voting. Due to this situation all natives must be requested voter id and by utilizing this they can strive for manual voting. To do this operation each time voters must go to outlets and in the meantime legislators additionally must go to outlets for preparing selections. The frameworks additionally get to be false verification for information attractions at any stage, on the grounds that the general control of data is kept in the hands of distinctive organizations working at diverse levels. The subjective power of information control is taken care of lay with fitting verification, yet all the perceived activities in the framework can execute questions upon the framework according to the considerable institutionalizations as they emerge when the framework is under the operational models. As of late governments have grasped the thought of utilizing data innovation (IT) to enhance benefits, a pattern known as e-government. Different voting criteria are proposed here as takes after:

Reliability and Integrity of Data. All information included in entering and arranging votes must be carefully designed. Votes must be recorded accurately. .The PC frameworks (in equipment and framework programming) must be sealed. In a perfect world, framework changes must be precluded all through the dynamic phases of the race process. That is, once affirmed, the code, beginning parameters, and arrangement data must stay static. No run-time adjusting toward oneself product can be allowed. End-to-end design control is vital. Framework bootload must be shielded from subversion that could somehow or another be utilized to embed Trojan steeds. (Any capacity to introduce a Trojan horse in the framework must be considered as a potential for subverting a decision.) Above all, vote tallying must create reproducibly right results.

Data confidentiality and Voter anonymity. The voting tallies must be shielded from outer perusing amid the voting methodology. The relationship between recorded votes and the character of the voter must be totally obscure inside the voting frameworks. All individuals approved to manage a decision must get access with nontrivial confirmation components. Settled passwords are by and large not satisfactory. There must be no trapdoors - for instance, for upkeep and setup - that could be utilized for operational subversions.

Accountability. All inner operations must be observed, without abusing voter privacy. Checking must incorporate votes recorded and votes arranged, and all framework programming and regulatory operations, for example, preand post-decision testing. All endeavored and effective changes to design status (particularly those infringing upon the static framework honesty necessity) must be noted. This capacity is like that of an air ship flight recorder, from which it is conceivable to recoup immeasurably critical data. Besides, observing must be nonbypassable - it must be difficult to turn off or dodge. Checking and investigation of review trails must themselves be nontamperable. All administrator validation operations must be logged. ([Gre93] dissects responsibility further.)

Disclosability. The framework programming, equipment, microcode, and any custom hardware must be open for irregular investigation whenever (counting documentation), in spite of weeps for mystery from the framework merchants.

Availability. The framework must be ensured against both coincidental and vindictive refusals of administration, and must be accessible for utilization at whatever point it is relied upon to be operational.

System reliability. System development (design, implementation, maintenance, etc.) should attempt to minimize the likelihood of accidental system bugs and malicious code.

Interface usability. Frameworks must be manageable to simple use by nearby decision authorities, and must not require the on-line control of outside faculty, (for example, merchant supplied administrators). The interface to the framework ought to be inalienably safeguard, idiot evidence, and excessively wary in shielding against unplanned and deliberate abuse.

Documentation and assurance. The configuration, usage, advancement hone, operational methodology, and testing systems should all be unambiguously and reliably reported. Documentation should likewise depict what confirmation measures have been connected to each of those framework viewpoints. Other lower-level criteria from the TCSEC are also applicable, such as trusted paths to the system, trusted facility management, trusted recovery, and trusted system distribution. All of the above criteria elements require technological measures and some administrative controls for fulfillment. The following item requires primarily no technological factors.

Personnel integrity. People involved in developing, operating, and administering electronic voting systems must be of unquestioned integrity. For example, convicted felons and gambling entrepreneurs are suspect.

2. RELATED WORK

Electronic voting is now a reality [1]—and so are the many errors and vulnerabilities in commercial electronic voting systems voting systems are hard to make trustworthy because they have strong, conflicting security requirements. An electronic voting (e-voting) system [2] is a voting system in which the election data is recorded, stored and processed primarily as digital information. They could lead to increased voter turnout (USA 2001: 59%, 18-24 yrs: 39%), thus supporting democratic process. They could give elections new potential and they could open a new market, thus supporting the commerce and the employment. Today's E-Voting systems [3] use proprietary code and vendors have often asserted the confidentiality of this code. This conflicts with the transparency required for elections. Electronic voting systems form a critical part of election process. It has to be ensured that they are secure and transparent part of that process. Location based services provide [4] both information and entertainment and are accessible with mobile devices through mobile network. Context awareness is an excellent feature of Location Based Services and can be used for various aspects related to tracking programmers'security[5] is a value that is difficult to evaluate as it's not easy to quantify A system cannot be considered as 100% secure because such a system cannot be developed. But an optimized secure features can be implemented to make voting system secure and efficient.

3. PROBLEM IDENTIFICATION

Voting still faces a number of risks and challenges. These include:

A. **Third parties:** There is no guarantee, that a third party program would not be manipulated to allow the storage and printing of a form or document different from the one appearing on the screen.

B. **Errors and technical malfunctions:** More difficult to detect and identify the source of errors and technical malfunctions than with conventional procedures.

C. **Unreliability:** Possibility that fully digitized system would fail to produce results and lack physical back-up records, making a public recount difficult or impossible.

D. **Security:** In the context of remote e-voting, special attention should be given to the process guaranteeing a free and secret vote.

E. **Reliability:** Mobile Voting Systems have to interact with some database server, or some other server, over a network. There might be instances when this network goes down during the voting process which may cause a potential voter to miss out on casting his/her vote,

F. **Skepticism:** As governments begin to adopt e-voting, Mobile Voting for that matter, people doubt the security and transparency of such schemes just as they do for the internet.

4. PROPOSED METHODOLOGY

A. Encryption

- The main idea of maintaining security of voting system is by restricting the location of a user of a particular area so that bogus voting can be prevented.
- Include the latitude/longitude coordinate in the data encryption and thus to restrict the location of data encryption and decryption.
- A toleration distance (TD) is designed to overcome the inaccuracy and inconsistent problem of GPS receiver.
- When the target coordinate and TD (toleration distance) is given by the sender, an LDEA-key is generated from latitude/longitude coordinate and TD.

- The random-key generator issues a session key, called R-ey.
- The final-key for encrypting the plaintext is generated by exclusive-or R-key with LDEA-key.

B.Decryption

- When the receiver gets the TD and R-key, the LDEA-key can be generated from TD and the coordinate acquired from GPS receiver.
- The final-key can be generated by exclusive-or R-key with LDEA-key.
- If the acquired coordinate is matched with the target coordinate within the range of TD, the ciphertext can be decrypted back to the original plaintext.
- When the receiver gets the TD and R-key, the LDEA-key can be generated from TD and the coordinate acquired from GPS receiver.
- The final-key can be generated by exclusive-or R-key with LDEA-key.
- If the acquired coordinate is matched with the target coordinate within the range of TD, the ciphertext can be decrypted back to the original plaintext.

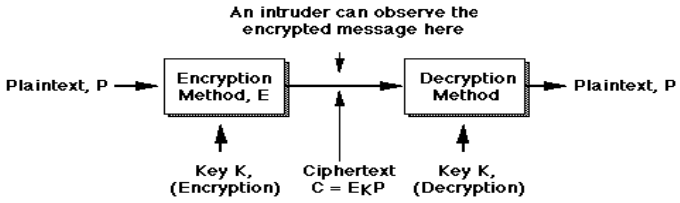

Fig1: Encryption/Decryption Process

C. Flow Chart

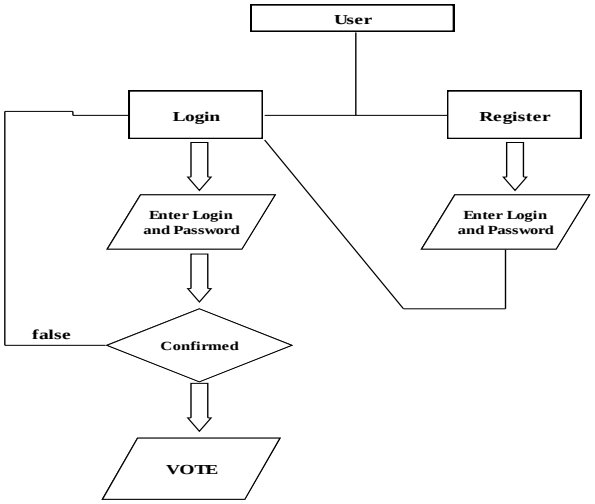

Fig 2: Proposed Methodology

5. CONCLUSION

Voting Systems can still be trusted as a platform to conduct free and fair elections in a secure and transparent manner given that they are well implemented. Voter authentication, integrity, voter anonymity and system accountability as some of the critical functional requirements that Mobile Voting Systems should have. Proposed work ensures the following:

- Accuracy – The proposed idea aims to increase accuracy by making it difficult to change someone else's vote.
- Anonymity. The proposed idea encourages anonymity by assigning a location restricted key for each user. This will decrease the chances of bogus voting from other locations.
- But in the rush to improve speed and scalability, accuracy has been sacrificed. And to reiterate: accuracy is not how well the ballots are counted by but accuracy is how well the process translates voter intent into properly counted votes.

REFERENCES

[1] Barbara Ondrisek "E-Voting System Security Optimization " Proceedings of the 42nd Hawaii International Conference on System Sciences - 2009 .
[2] JONATHAN BANNET, DAVID W. PRICE,ALGIS RUDYS,JUSTIN SINGER,AND DAN S.WALLACH "Hack-a-Vote: Security Issues with Electronic Voting Systems" IEEE COMPUTER SOCIETY 1540-7993/04/$20.00 © 2004 IEEE , IEEE SECURITY & PRIVACY
[3] Rong Chen,Xianhua Shu,Zhenjun Du,"Research on mobile loctation service design based on android,"fifth international conference on Wireless communications networking and mobile computing,pp 1-4,2009
[4] Tor-Morten,Gronli Jarle,Hansen Gheorghita,Ghinea,"Android,Java ME and Windows Mobile interplay,"IEEE 24th International Conference on Advanced information networking and applications workshop,2010.
[5] Xianhua Shu; Zhenjun Du ,Rong Chen "Research on Mobile Location Service Design Based on Android", Wireless Communications, Networking and Mobile Computing, 2009.
[6] http://www.tutorialspoint.com/sqlite/sqlite_overview.htm
[7] http://en.wikipedia.org/wiki/Google_Analytics
[8] Jan nealbert v. Calimag, pamela anne g. Miguel, romel s. Conde & luisa b. Aquino, "Ubiquitous Learning Environment Using Android Mobile Application IMPACT: International Journal of Research in Engineering & Technology (IMPACT: IJRET), , Feb 2014
[9] Fan Jiang and Saoping Ku,"How to display the data from database by Listview on Android," second International workshop on Intelligent Systems and Applications(ISA),2010.
[10] Gupta.A.kumar,S.Qadeer,M.A.,"Location based services using android(LBSOID)," IEEE International conference on Multimedia services architecture and applications,pp 1-5,2009.
[11] Hassan Z.S,"Ubiquitous computing and android ", third international conference on digital information management, PP: 166-171 (2008).