A+Votz - Google Android Platform for a Mobile - Voting System with Cloud Based Storage and Data hiding Features

[1]Ragunath G, [2] Aarthi R, [3] Dhanalakshmi A S

ME Scholar

[1] Dept of Computer science and Engineering,

[1] SSN College of Engineering,Kalavakkam, Chennai, India

[1] ragunath@cse.ssn.edu.in,[2]aarthi1201@cse.ssn.edu.in,[3]dhanalakshmi1207@cse.ssn.edu.in

***Abstract*—Elections in India are conducted almost exclusively using electronic voting machines developed over the past two decades by a pair of government-owned companies. These devices, known in India as EVMs, have been praised for their simple design, ease of use, and reliability, but recently they have also been criticized because of widespread reports of election irregularities. Despite this criticism, many details of the machines' design have never been publicly disclosed, and they have not been subjected to a rigorous, the method of voting through mobile by the people, to determine their own government from any-where in the world, is needed. This paper is all about developing a new "Voting through Mobile, with Combined Finger Print Authentication, integrated with Inter Could Computing and Automated Load Balancing, fused with Data Hiding Security the over-all process is carried out on** ANDROID^{TM} PLATFOTM**". To make it possible, vote can be made through mobile by using wireless network with combined finger print biometric identification systems. We suggest GPS based postioning to focuses on adding geography to the voting paradigm. A data hiding method, which is applicable to fingerprint images compressed with wavelet-based scheme and provide full security for biometric data that is passed through the network from different places. This combined method creates a new evaluation of process with 100% security, 100% privacy & 100% voting by any kind of people from anywhere.**

***Index Terms*— Cloud computing; Data Security; Untrusted Server, Encrypted data; Biometric, Android**

I. INTRODUCTION

Biometric authentication, or simply biometrics, offers a natural and reliable solution to the problem of identity determination by establishing the identity of a person based on "who he is", rather than "what he knows" or "what he carries". A biometric system is essentially a pattern recognition system that operates by acquiring biometric data from an individual, extracting a feature set from the acquired data, and comparing this feature set against the template set in the database. Depending on the application context, a biometric system may operate either in verification mode or identification mode. Information hiding is a general term encompassing many sub disciplines, is a term around a wide range of problems beyond that of embedding message in content. The term hiding here can refer to either making the information undetectable or keeping the existence of the information secret. Information hiding is a technique of hiding secret using redundant cover data such as images, audios, movies, documents, etc. This technique has recently become important in a number of application areas. The idea of "Cloud Computing" reflects an approach to computing in which dynamically scalable computing hardware and software resources are provided as a service over the Internet. Cloud Computing is often equated with the concept of a utility, in which an organization can "plug-in" to this virtual computing environment and use the computing resources available on an as-required basis [1]. With cloud computing, the applications you use are there when you need them, and wherever you need them you just need a connection to the Internet. Further, you don't have the expense or need to buy/lease, manage, and maintain your own IT infrastructure [2]. The description relates to a system designed to protect data exchange involved with use of cloud computing infrastructures by services and the individuals. The system is designed so that a cloud resource and its middleware access point are protected in transferring data among themselves and end users a system designed to spread the data and then reassemble the data.

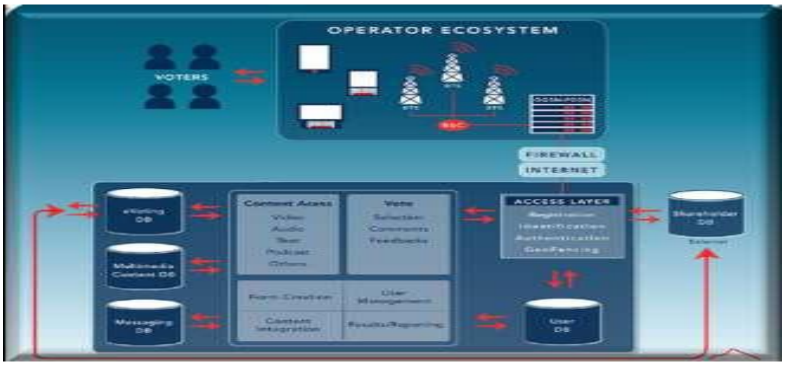


Fig. 1. Architecture of A+ Votz

II. RELATED WORKS

In a Mobile voting system and methods, which among other things, provides increased transparency to the public and verification for the individual voters regarding the tallying of their respective votes? A business method involves the use of general purpose computer hardware together with a software platform, made up of one or more open-source or proprietary certified software programs, including a voting software program, a voting record can be made available electronically, thereby eliminating the need to provide a voter with a paper ballot. A voting record identifier is generated without use of, or reference to, voter identify. The voting record identifier is provided to the voter, such that the voter can access a record of his ballot selections and vote number sequence. In addition, a biometric authentication mechanism is provided to reduce, or eliminate, the potential that a voter is able to vote more than once.

Novel business methods further include supplying the general purpose computers to voting administrators, processing them and re- purposing the machines by placing them in the hands of eleemosynary institutions or organizations which promote or manage educational services, particularly for children.

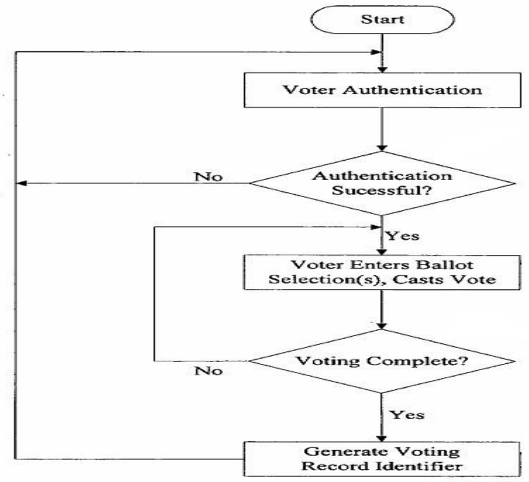

Start
Voter Authentication
No
Authentication Sucessful?
Yes
Voter Enters Ballot Selection(s), Casts Vote
No
Voting Complete?
Yes
Generate Voting Record Identifier

Fig. 2. Flow of Traditional Voting System

A. BIOMETRICS IN VOTING USING FINGER PRINTS

Fingerprints are often seen as the optimal biometric be-cause of their wide acceptance of uniqueness. Fingerprints used for law enforcement identification use all fingers and a rolled fingerprint. This provides maximum data input for analysis comparison. Commercial fingerprint readers and solutions generally do not use all fingers or a rolled image. Such readers have now been incorporated in a range of devices including keyboards, mice and Personal Digital Assistants. This approach lowers the cost but does decrease the performance in comparison with law enforcement solutions. For example, most commercial solutions suffer from problems with finger orientation. Many devices will suffer from dirty environments and generally deteriorate in performance as users leave dirt on the reader enforcement solutions. We get the Finger prints modal from the layman and store it in the template database and then perform verification and identification technique, which prevents the people instead of carrying their voter and fully avoid fraud voting.

III. PROPOSED SCHEME

The method for combining two templates. A first template having a first minutia set and a second template having a second minutia set are provided. The first template is com-paring it the second template to obtain a matching minutia set. Registration parameters are calculated from the matching minutia set. The registration parameters can be referenced to either the first minutia set or the second minutia set. All minutiae in the first or the second minutia set are translated to be in the same co-ordinate system as the other minutia set. The minutia sets are then combined to construct a combined minutia set.

In one embodiment, an overlap region is drawn for the first template and the second template the overlap region containing at least minutia from the matching minutia set. The combined minutia set is constructs from the matching minutia in the first or the second template, minutia in the first minutia set that are not in the matching minutia set, and minutiae in the second minutia set that are not in the matching minutia set. In another embodiment, minutiae in the overlap region but not part of the matching minutia set are discarded.

A. BAYESIAN DECISION FUSION ALGORITHM

A Bayesian framework formalizes the design of a personal identification system that can adaptively increase or reduce the security level as well as adapt to each users physical characteristics. The key is to use multiple biometric modes, adapt the error costs, and vary the sensor operating points giving the system robustness and adaptability.

As a brief review, the problem of personal identification can be formulated as a hypothesis testing problem where the two hypotheses are:

H0: the person is an imposter
H1: the person is genuine.

Accuracy: Which is the focus of this paper, refers to the rates at which the two types of errors occur: false rejection rate (FRR) and false acceptance rate (FAR).

The four possible decisions are:

1. The genuine person is accepted
2. The genuine person is rejected
3. The imposter is accepted
4. The imposter is rejected

B. PLATFORM FOR A+

The A+VOTZ voting platform recognizes and improves upon three critical problems inherent with GPS location-based solutions for trustworthy voting and polling: Almost all voting and polling activity is conducted indoors where GPS location sensing signals generally are not operable or reliable.

GPS location can be ”spoofed” to mislead identifying voter or device being at a location when in reality they are not there. GPS sensor-based mobile device chipset approaches require the sensors to be activated on the personal handset and this adds power drain to the consumer mobile device’s battery, resulting in rapid recharging needs (and an inferior user experience). In contrast, A+VOTZ improves upon prior GPS solutions with a system and method that is near-instant and non-spoofable. A+VOTZ solutions apply an A-GPS (”Assisted GPS”) location-based technique by cell tower triangulation location reporting that is fast, reliable and not dependent on being indoors to vote in an election or polling process.

A+VOTZ offers cloud power solutions to manage large and small voting and/or polling events. Cloud solutions add power to grow ... or shrink, as needed. These solutions enable ground-breaking innovation through increased productivity, new development and new breeds of online mobile device collaboration and productivity tools being developed each day. A+VOTZ is committed to delivering on the promise of cloud computing. The company’s leadership is broad in scope: we take a systems and architectural approach that builds upon the network-centric nature of cloud computing and location-based services, then apply that platform to verification and authentication with voting. eVOTZ is working in partnership with private and public cloud providers as they build and operate services, as well as leading university research groups in France and Canada for geolocation techniques made possible by emerging Global Network Satellite solutions and mobile device sensors planned for the EU with the launch of Galileo satellite systems.

The A+VOTZ platform was engineered to ensure ease of operation, offer a breadth of features, support a wide range of workloads and facilitate migration. The planned mobile voting communication and collaboration solutions connect geographically dispersed organizations, communities and individuals through rich, real-time experiences authenticated for trustworthy results with aforementioned geolocation techniques. If a user is in the right place at the right time, voting is permitted.

A+VOTZ will also focus on market leadership in security, ’context, content and identity,’ location-based awareness and consolidated policy management to increase transparency in shareholder meetings and communication as well as local government voting and polling solutions (all cloud-based and trustworthy). A+VOTZ works with a rich ecosystem to deliver complete solutions. Key partners have been identified to provide storage, systems management, virtualization software, application development, open source platforms, backup and disaster recovery solutions, and a variety of readyto- deploy components. In addition, the eVOTZ hosting and service provider partners are propelling connectivity and public cloud services to businesses and consumers alike.

A+VOTZ makes new voting and polling business models possible. Companies (or governments) can: Respond quickly to changing customer needs by polling for input Collaborate more effectively to drive innovation and business value Execute on strategies that might not have been cost-effective or reliable in the past. Furthermore, companies can purchase these cloud-based services via a subscription modelpaying only for what they need as it’s necessary.

IJEDR

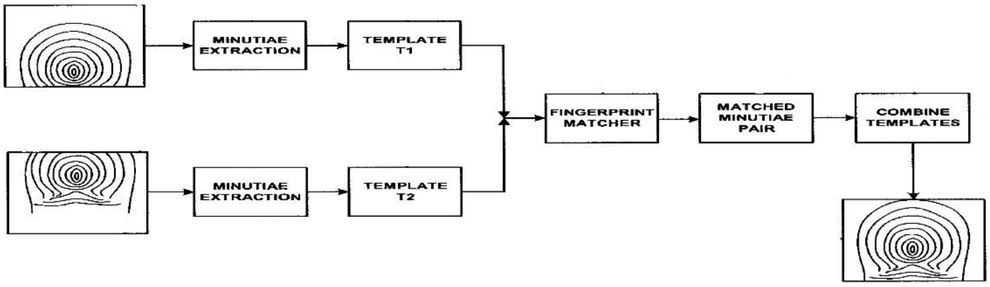


Fig. 3. Proposed System Extraction Process

C. OUR NEW IMPLEMENTAITON OF VOTING ONLY WITH BIOMETRIC AUTHENTICATON

Thus the voting process starts with the clear authentication and various levels of techniques are followed and votes are stored in the database one by one. If the vote was not stored in to it, then the load balancing techniques will intimate the user to resend the vote again. The result can be viewed by using the SQL queries.

IV. GENERAL STEGANOGRAPHY FRAMEWORK:

A general Steganography framework is shown in Figure 1. It is assumed that the sender wishes to send via Steganographic transmission, a message to a receiver. The sender starts with a cover message, which is an input to the stego-system, in which the embedded message will be hidden.

The hidden message is called the embedded message. A Steganographic algorithm combines the cover massage with the embedded message, which is something to be hidden in the cover The algorithm may, or may not, use a Steganographic key (stego key), which is additional secret data that may be needed in the hidden process. The same key (or related one) is usually needed to extract the embedded massage again. The output of the Steganographic algorithm is the stego message.

The cover massage and stego message must be of the same data type, but the embedded message may be of another data type. The receiver reverses the embedding process to extract the embedded message.

A. PROBLEM IN HIDDING THE DATA

1 Having low robustness against attacks which try to reveal the hidden message.

2 Having low robustness against distortions with high average power.

THE SOLUTION

Accordingly, there are two following solutions for mentioned problems:

1 The solution for first problem: Making more difficult discovering which bites are embedded by modifying the bits else than LSBs in samples, and selecting the samples to modify privately-not all samples.

2 The solution for second problem: Embedding the message bits in deeper layers and other bits alteration to decrease the amount of the error.

To integrate these two solutions, embedding the message bits in deeper layers that is a part of second solution also can satisfy modifying the bits else than LSBs in samples of second solution. In addition, when we try to satisfy other bits alteration to decrease the amount of the error of second solution, if we ignore the samples which are not adjustable, also selecting not all samples of first solution will be satisfied. Thus, intelligent algorithm will try to embed the message bits in the deeper layers of samples and alter other bits to decrease the error and if alteration is not possible for any samples it will ignore them. It is clear that the main part of this scenario is bit alteration that it should be done by intelligent algorithms which use either genetic algorithms or a symbolic AI system.

V. HOMOMORPHIC ALGORITHM

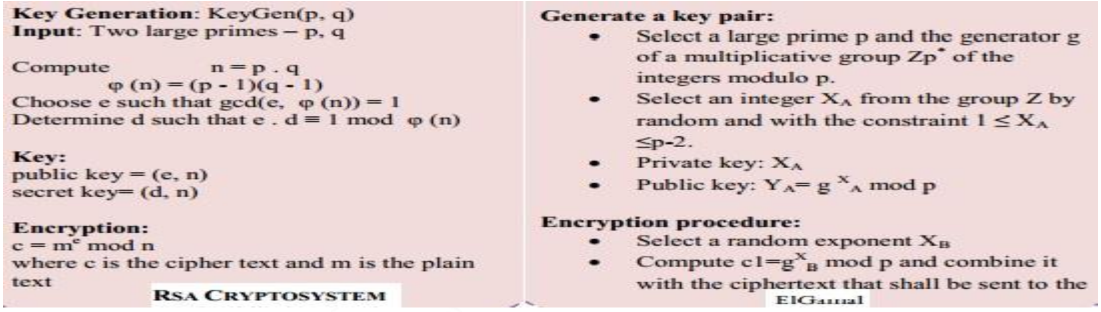
This Module takes chunck files as input and produce encrypted text as output using the Homomorphic Algorithm. Property of homomorphic encryption algorithm is discussed below.

The idea of performing simple computations on encrypted messages was first introduced by Rivest, Adleman,andare: Cloud computation, Electronic voting, Data mining,Financial transactions, Electronic cash, Medical records. A form of encryption where a specific algebraic operation is performed on the plaintext (information a sender wishes to transmit to a receiver) and another, possibly different,algebraic operation is performed on the ciphertext .

Tolerance Agianst Attacks A cryptosystem may be semantically secure against chosen plaintext attacks (CPA) or even non-adaptive chosen ciphertext attacks (CCA1) while still being malleable. Homomorphic encryption systems use oneway function candidates to achieve CCA2. A one-way function is a function that is easy to compute on every input, but hard to invert given the image of a random The original motivation for these homomorphisms was to allow for an encrypted database to be stored by a third party and to allow the owners and other authorized people to perform calculations with the data without decrypting it. A multiplicative homomorphic cryptosystem has an encryption function E that satisfies the following property:

$$E(M1) * E(M2) = E(M1*M2)$$

where M1 and M2 are plain text messages Some of the applications of homomorphic encryption are: Cloud computation, Electronic voting, Data mining,Financial transactions, Electronic cash, Medical records. A form of encryption where a specific algebraic operation is performed on the plaintext (information a sender wishes to transmit to a receiver) and another, possibly different,algebraic operation is performed on the ciphertext (result of encryption over the plaintext).



Key Generation: KeyGen(p, q)
Input: Two large primes – p, q

Compute $n = p . q$
$\varphi (n) = (p - 1)(q - 1)$
Choose e such that $\gcd(e, \varphi (n)) = 1$
Determine d such that $e . d \equiv 1 \bmod \varphi (n)$

Key:
public key = (e, n)
secret key= (d, n)

Encryption:
$c = m^e \bmod n$
where c is the cipher text and m is the plain text

RSA CRYPTOSYSTEM

Generate a key pair:

- Select a large prime p and the generator g of a multiplicative group Zp^* of the integers modulo p.
- Select an integer X_A from the group Z by random and with the constraint $1 \leq X_A \leq p-2$.
- Private key: X_A
- Public key: $Y_A = g^{X_A} \bmod p$

Encryption procedure:

- Select a random exponent X_B
- Compute $c1=g^{X_B} \bmod p$ and combine it with the ciphertext that shall be sent to the

ElGamal

Fig. 4. Multiplicative and Addictive Homomorphic Encryption

A. Searchability

Cloud storage is an increasingly popular means for archiving, backup, sharing of data, synchronization of multiple devices and it is also envisioned for future primary storage of (enterprise) data. However, when outsourcing data to the cloud it would be nice to have the functionality of a semantic file system, i.e., being able to perform index search. However, downloading all the data and performing local search is far too inefficient. To let the cloud perform the search while preserving the confidentiality of the data would be desirable. Cryptographic protocols to efficiently search on encrypted outsourced data without revealing neither data nor search queries allow to realize this task. Our focus is on pairing based searchable encryption schemes.

VI. CONCLUSION

The problem of data security in cloud data storage is detailed, which is essentially a distributed storage system. To ensure the correctness of users data in cloud data storage, we proposed a Searchable Encryption Algorithm scheme with explicit dynamic data support, including block update, delete, and append. By utilizing the homomorphic Algorithm, our scheme achieves the integration of storage correctness and data error minimization. In order to provide more security a special mechanism for key distribution and one time password is proposed to be implemented in future.

REFERENCES

[1] Holmes B., E-voting: the promise and the practice. Report given by Parliament of Australia.
[2] Elleithy K.M, Rimawi I. (2006) Design, Analysis and Implementation of a Cyber Vote System, Advances in Computer, Information, and Systems Sciences, and Engineering: Proceedings of IETA 2005, TeNe 2005 and EIAE 2005, Springer.
[3] Jefferson D., Rubin A.D., Simons B., Wagner D.(2004) A Security Analysis of the Secure Electronic Registration and Voting Experiment (SERVE), ETS 300 506. Security aspects (GSM 02.09 version 4.5.1), Digital cellular telecommunications system (phase 2).
[4] Internet voting pilots announced for 2013. Report given by Ministry of local government and regional development, Norway.
[5] International institute for Democracy and Electoral Assistance, Voter turnout A global Survey
[6] Estonia parliamentary elections, 6 March, 2011, OSCE/ODIHR election assessment mission report. Available on Organization for Security and Co-operation in Europe website E- voting, Uncovering the veil on Geneva's internet voting solution. A report by State Chancellery of Geneva , Information Technology Centre of the State of Geneva,
[7] Statistics about Internet voting in Estonia. Report given by Electoral Commission of Estonia.
[8] Norway, Internet voting pilot project local government elections, 12 September 2011. Available on Organization for Security and Co-operation in Europe website.
[9] Meiner N., Hartmann V., Richter D. (2004) Verifiability and Other Technical Requirements for Online Voting Systems Electronic Voting in Europe, volume 47 of LNI 101-109
[10] Schryen G. (2004) Security aspects of internet voting, System Sciences. Proceedings of the 37th Annual Hawaii International Conference on System Sciences. 5-8 Jan. 2004 116 124.
[11] Simons B., Jones D.W. (2012) Internet voting in the U.S., Communications of ACM, Vol.55, No. 10.
[12] Yasinsac A., Childs J. (2001) Analyzing Internet security protocols, High Assurance Systems Engineering, 2001. Sixth IEEE International Symposium, 22-24 Oct. 2001 149 159.
[13] International institute for Democracy and Electoral Assistance, Voter turnout from 1945 to date countryview.cfm

[14] Elleithy K.M, Rimawi I. (2006) Design, Analysis and Implementation of a Cyber Vote System, Advances in Computer, Information, and Systems Sciences, and Engineering: Proceedings of IETA 2005, TeNe 2005 and EIAE 2005, Springer.

[15] Hoke C.(2012) Internet voting: structural governance principles for election cyber security in democratic nations, Proceedings of the 2010 Workshop on Governance of Technology, Information and Policies, ACM New York, NY, USA, 2010.

IJEDR