A HOMOMORPHIC ENCRYPTION BASED ON-LINE VOTING SYSTEM

D.Suresh[1], A.Thomas Paul Roy[2], R.Karthikeyan [3]
1.Professor, PSNA College of Engineering and Technology, Dindigul
2.Professor, PSNA College of Engineering and Technology, Dindigul
3.Professor, PSNA College of Engineering and Technology, Dindigul

Abstract— This paper developed for the risk free and person oriented Online Voting System. The Online Voting gadget is made for the humans of the united states living round the world and needs to vote for their representative. The election can be carried out in two methods the paper ballot election and the computerized ballot elections. The automatic ballot elections are referred to as the digital voting. The on line vote casting device is rather developed and the on-line polling machine can be changed through precisely and at once vote casting on line and on the spot results. The on line balloting gadget is completed by using the net so it can be known as the Internet Voting. The gadget proceeds the on-line vote casting machine in a new approach known as Homomorphic Encryption . Homogeneous encryption is the form of encryption, which lets the computer generate encrypted end results in ciphertexts, as though they were performed in a plaintext, when decrypted, which matches the end result of the operations. In this paper we have a digital voting device based on homomorphic encryption to make sure that the vote is confidential. The benefits of multi-homorphic encryption systems are all presented in our suggestion. The proposed electoral system is suitable for elections that include non-partial votes and for multi-candidate elections. For outsourced storage and counting, homomorphic encryption can be used.

Keywords— Online Voting System, Electronic Voting, Internet Voting, Homomorphic Encryption.

I. INTRODUCTION

Voting is a technique for a group, for example, an assembly or an electorate, to make a common collective election or to express a categorical opinion after discussions, debates or elections. With the help of votes, democracy chooses excessive workers. Residents of a vicinity represented via an elected reputable are known as "constituents", and these components who forged a ballot for their chosen candidate are known as "voters". There are one-of-a-kind structures for gathering votes [1-3]. In smaller organisations, balloting can show up in special ways. Formally by way of ballot to go with others for instance inside a workplace, to opt for participants of political associations or to pick roles for others. Informally vote casting ought to appear as spoken settlement or as a verbal gesture like a raised hand. This Voting System offers with a technique of vote casting with encryption approach to grant the characteristic of stopping the fraudulent vote casting on the election process.

II. RELATED WORK

Sensus: Internet digital polling machine with a security consciousness, Sensus, a convenient, impenetrable and un-public polling gadget (performing polls and election), for PC Networks, presented the diagram and implementation. Sensus is increasingly using blind signatures in Fujioka, Okamoto and Ohta's work (1993) to ensure that the vote can be taken only

Copyright © Authors

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

by registered voters and that all registered voters can vote only once and that they are kept in the same time as they do. Sensus allows voters independently to confirm that their votes have efficiently been counted and that the effects of their votes must be misrepresented anonymously. We define seven relevant voting houses and show, that Sensus is in some cases superior to typical voting systems, which meet these houses well [4-6].

Online balloting gadget linked with AADHAR, Vibhu Chinmay This paper offers with the on line balloting device that will make the vote casting gadget smart. OVS(online vote casting system)is secured and it have easy design. We will use bio matrix machine in this. That makes it extra secure. We linked it with AADHAR card. In the entire world finger print of each and every man or woman is unique. So we will use this technique. The proportion of balloting will be extend surly. And additionally it minimize the false vote[7-9].

An environment friendly and impervious cell telephone balloting system, Mohib Ullah Electronic balloting device gives comfort and get entry to to the citizens except the geographical restrictions. Mobile cell phones are one of the new technologies for operating e-voting with democratic standards and concerns about privacy. In this article we propose a protocol on cellular smartphone voting mainly based on hybrid cryptosystems. The Protocol consists of three phases: Online registration; voting casting; accumulation of votes and the final outcome phase. The proposed protocol provides for closely closed and environmentally friendly casting of votes online and can also be applied in parallel with the voting system on paper ballots. Because it relies on SMS messages but requires web connectivity, the proposed protocol has efficiency, safety and deployability in creating nations.

Indian Online polling system based entirely on Himanshu Agarwal, AADHAAR ID. This paper proposes for the first time an online voting gadget for Indian elections. The proposed model is safer in that it is well-known in the most important database of the Indian Election Commission that a voting excess protection password has been confirmed before the vote. The additional feature of the mannequin is that the voters can check that the right candidate/party has taken his/her vote. This model allows a man or a woman to vote either out of his disbursed electoral district or from the desired place. The proposed gadget automatically calculates the votes, thus saving a lot of time and enabling Indian election officers to announce the final results in a very quick period[10-11].

III. ONLINE VOTING SYSTEM BASED ON HOMOMORPHIC ENCRYPTION

Online Voting are simple, pleasing and ease to use. It reduces guide efforts and bulk of data can be treated easily. But out of all these facets there are some drawbacks with this gadget are, there can be software program failure issue, insecure get entry to of web and additionally voter must be acquainted with internet. The vote casting server collects the votes and filters out replica and invalid votes[12-15]. Each voter can then test her/his vote on-line to make certain that her vote has been counted correctly. In suggest device far flung and customers can exercise. In the proposed gadget we can get the end result except manually counting. The computerized counting is simple. We talk of digital vote casting when casting of votes is carried out via the voter without delay by means of digital means, as a consequence acquiring an cease to give up digital vote .The use of paper and different bodily structures is non-compulsory and auxiliary.

Copyright © Authors

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

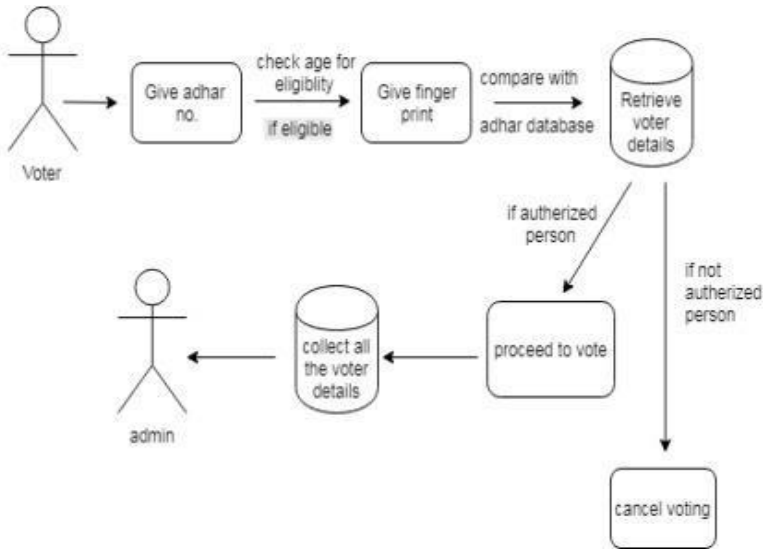
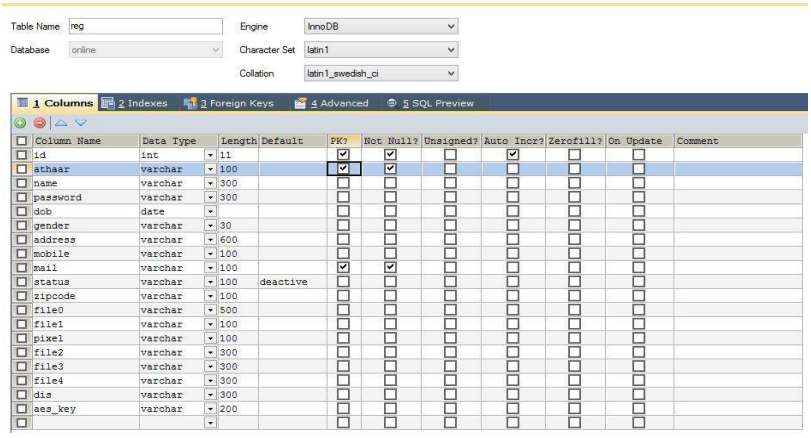
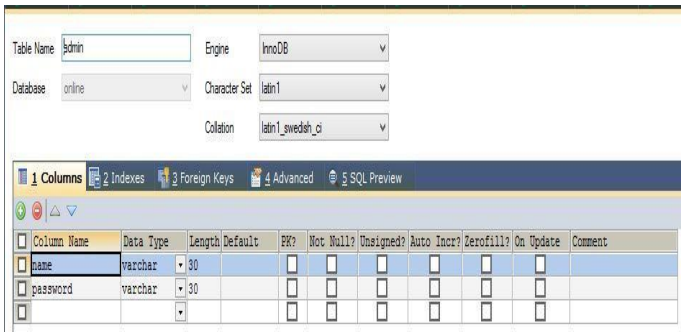


Figure 1. Architecture of online voting system





An on-line vote casting machine for Indian election is planned for the first time in this paper. The proposed mannequin has a increased protection in the feel that voter receives an conformation mail which is to be established earlier than the vote is regular in the primary database of Election Commission of India. The extra characteristic of the mannequin is that the vote which is polled through the voter is encrypted and decrypted ONLY by means of the

Copyright © Authors

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

Election Commission of India. In this mannequin a character can additionally vote from outdoor of his/her dispensed constituency or from his/her desired location. In the proposed machine the tallying of the votes will be carried out robotically, as a result saving a big time and enabling Election Commissioner of India to announce the end result inside a very brief period.

The homomorphic things in cryptosystem are exploited to gain two necessary vote casting Requirements: Firstly, machine protection used for casting digital votes by voters. Secondly, the voter can choose voluntarily and with confidence. In a system additionally are implemented the typical voting requirements such as eligibility, privacy, precision, fairness, freedom of receipt, resistance to coercion, mobility, simplicity, personal verification, scalability and disponibility.

IV.SECURITY CHECKING PROCESS IN ONLINE VOTING

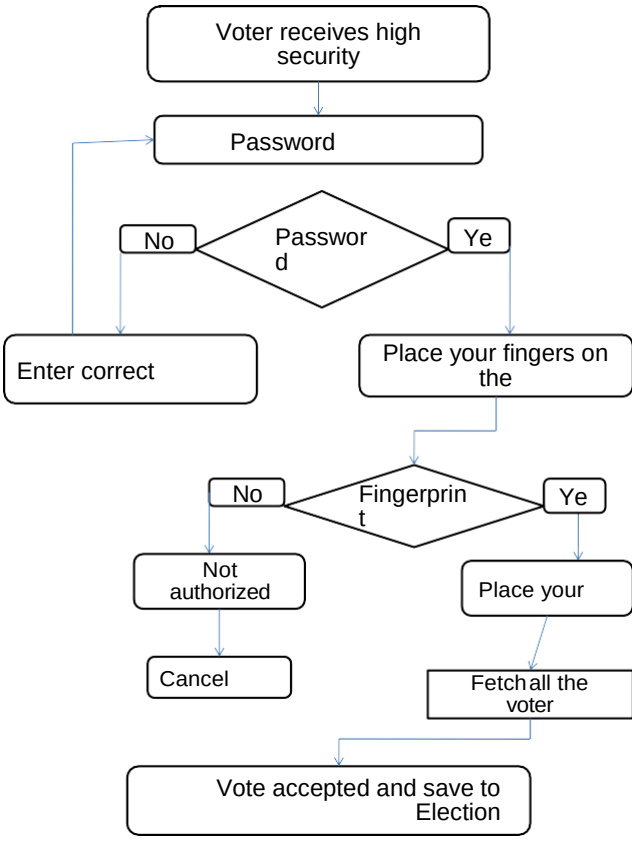


Figure 2. Security checking process in omline voting

Homomo encryption is a kind of encryption which enables the production of encrypted final results to be calculated in cyphertexts, as if they had been performed on the plaintext, if decrypted. This is the end result of the operation. For outsourced storage and computation, homomorphic encryption can be used. This allows data to be encrypted and outsourced, while encrypted, to business cloud environments for processing. Homomorphic encryption can be used

Copyright © Authors

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

in exceptionally regulated industries like fitness to enable new offers through private limits Sharing of statistics Homorphic coding is a coding form with additional comparison functionality for computing coded statistics that prevent the secret key from being entered. The final outcome of the calculation remains encrypted. Homorphic encryption can be considered as a symmetric or public-key cryptography extension. Crypt and decryption features can be understood as homomorphism between plaintext and ciffer text spaces. Homorphic refers to homomorphism of algebra: Homorphic encryption consists of several kinds of encryption systems that can use one-of-a-kind calculation lessons over encrypted data. Some common types of homomorphic encryption are partly homomorphic, fully homomorphic, and completely homomorphic. The calculations are shown as Boolean or arithmetical circuits. Partially homorphic encryption includes systems that help contrast circuits that consist of just one type of gate, e.g. adding or multiplying. Two sort gates can be considered by some homomorphic encryption schemes, but only by a subset of circuits. Comparison of arbitrary circuits of bound (pre-determined) depth supports leveled fully homomorphic cryptogram. Fully homomorphically encrypted (FHE) is a concept of homomorphic encryption that enables the evaluation of arbitrary circuits with unlimited depth. The multiplicative circuit depth is the main realistic problem with the calculation of encrypted data for the majority of homomorphic encoding schemes. Inherently mixable is homomorphic encryption schemes. Homomorphic coding systems have less residential security than non-homorphic coding schemes in mallleability sentences.

There are three main types of homomorphic encryption: partly homomorphic encryption (mains uncontrollable touch facts by using only the selection of mathematical features on encrypted data); partly homomorphic encryption (supports confined operations that only a certain number are possible); (this is the gold fashionable of homomorphic encryption that maintains statistics impenetrable and accessible). The problem is that you should decrypt it to work with it. It should be encrypted. It is inclined to do the very things from which you tried to protect it by encrypting them. This scenario has an effective answer: homomorphic encryption. In the end, homomorphic encryption can respond to companies wishing to process data while nonetheless protecting the security of their privacy.

The encryption makes it possible not only to disclose records to someone but to analyze or manipulate encrypted records. An easy way to find an espresso guard when out of town, shows massive volumes of data with 1/3 events, helping you satisfy your coffeine craving — the fact that you're looking for an espresso shop, the place you are looking for, the time and more. Had this fictional espresso search been carried out by homomorphic encryption, none of this would occur in any of the 0.33 events or providers, like Google. Furthermore, they would not be able to see the answer you were given regarding how to get there and where the espresso saves are.

Whereas, when looking for our subsequent caffeine fix, we may be inclined to section with records which are uncovered, homomorphic encryption has a massive potential, for example in areas of highly private records such as economic offers or health services where the privacy of a man or woman is paramount. In such cases, homomorphic encryption can still analyze and process sensitive key points of the true data. As with various encryption types, homomorphous encryption uses a public key for the encryption of data. In contrast to various types of encoding, it uses an algebraic machine to allow records to perform features while still encoded. Only a matching non-public key can then be accessed right after the features have been completed by

Copyright © Authors

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

the unencrypted information. This allows the facts to be imperceptible and personal even if anybody is using them.

IV. ANALYSIS

A wide array of primary and extended requirements must be complied with in every online voting machine. All these necessities cannot be met at the same time, however Our casting machine for online voting meets the following requirements and homes:

1) Eligibility: Registrars Prove and verify the individual's eligibility for voting. You refused to elect any person who did not fulfill the requirements described above.

2) Privacy: no one in the system, including the tally authorities, can link an elector's identification and vote. The privacy is preserved by using the protocol and reference technology for homomorphic encryption.

3) Accuracy: By using homomorphic cryptosystem property the gadget can record valid votes with excessive accuracy.

(4) Receipt-free/coercion-resistant: the gadget make reference use is free of charge and prevents votes from being purchased. Voters cannot demonstrate what they are voting for in other elections.

5) Mobility: the gadget requires that the elector only reaches certain locations some day after registration. The voter can confirm his vote from somewhere, throughout the voting day, on the Internet.

6) Simplicity/Comfort: the device is quite straightforward. The interface for the person is unobtrusive and does not require the voters excessive skills.

7) Individual verification: the elector should be able to confirm that, apart from any modification, the vote he casted is accounted for in the tally. This property has been completed by the machine by posting the receipt on its precise mail account. Every voting person can easily access their e-mail account and test if they have changed or not.

V. CONCLUSION

In this article we have an entirely homomorphic encryption digital voting system which ensures confidentiality and privacy in voting. Our concept is greatly utilized by the multiplying homomorphic encryption systems. The proposed voting system is appropriate for multi-candidate and non-partisan voting elections.

Online voting machine is important and impenetrable. The device ensures that voters are confidential through homomorphic encryption. The device no longer needs an invulnerable channel at any time in the voting process. The inutile encryption of votes ensures that the voter cannot change his vote. Regrettably, completely homomorphic e-voting systems for encryption require excessive computer lodging and time. The overall cost of counting increases as the number of electors, candidates and parameter values increases. The device is realistic and increasingly measured with small and massive elections with additional calculation

VI. REFERENCES

[1]. Tadayoshi Kohno, Adam Stubblefield, Aviel D. Rubin ,Dan S. Wallach, “Analysis of an Electronic Voting System”, Johns Hopkins University Information Security Institute Technical Report, TR-2003-19, July 23,2003.

[2]. http://newindianexpress.com/states/ andhra_pradesh/Maoists-strike-fear-make-off- with-poll-papers-in- agency/2013/07/15/article1684243.

Copyright © Authors

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

[3]. Executive Summary of "Genesis and Spread of Maoist Violence and Appropriate State Strategy to Handle it", Bureau of Police Research and Development, Ministry of Home Affairs, New Delhi.
[4]. David l. Dill, Bruce Scheiner, and Barbara Simons, "Voting and Technology. Who gets to count your vote?", Communications of the ACM, vol. 46(8), Aug. 2003, pp. 29-31
[5]. David Evans and Nathanael Paul, "Election security: Perception and reality", IEEE Security & Privacy, vol. 2(1), Jan. 2004, pp. 24-31.
[6]. Huijie Lin, Jia Jia, Quan Guo, Yuanyuan Xue, Jie Huang, Lianhong Cai, Ling Feng, "Psychological stress detection from cross-media microblog data using deep sparse neural network," IEEE - International Conference on Multimedia and Expo, pp. 1-6, 2014.
[7]. Yingming ZHAO, Yue PAN, Sanchao WANG et al., "An anonymous voting system based on homomorphic encryption", Communications (COMM) 2014 10th International Conference on. IEEE, pp. 1-4, 2014.
[8]. M. A. Based and S. F. Mjølsnes, "Security requirements for internet voting systems," in Emerging Trends in Computing, Informatics, Systems Sciences, and Engineering, pp. 519– 530, Springer, 2013
[9]. D. Boneh, E. Goh, and K. Nissim, "Evaluating 2- DNF formulas on ciphertexts," in Theory of Cryptography Conference, pp. 325–341, 2005
[10]. Y. Chen, J. Jan, and C. Chen, "The design of a secure anonymous internet voting system," Computers & Security, vol. 23, no. 4, pp. 330– 337, 2004.
[11]. B. Chevallier-Mames, P. Fouque, D. Pointcheval, J. Stern, and J. Traor´e, "On some incompatible properties of voting schemes," in Towards Trustworthy Elections, pp. 191–199, 2010.
[12]. J. D. Cohen and M. J. Fischer, A robust and verifiable cryptographically secure election scheme, Department of Computer Science, Yale University, 1985.
[13]. J. C. Corena and J. A. Posada, "Multiplexing schemes for homomorphic cryptosystems," Elementos, vol. 1, no. 1, 2013
[14]. R. Cramer, R. Gennaro, and B. Schoenmakers, "A secure and optimally efficient multi-authority election scheme," European Transactions on Telecommunications, vol. 8, no. 5, pp. 481– 490, 1997.
[15]. T. ElGamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," in Workshop on the Theory and Application of Cryptographic Techniques, pp. 10–18, 1984.

Copyright © Authors

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731