DESIGN OF SECURE ELECTRONIC VOTING SYSTEM USING CRYPTO-ALGORITHM

K.Arun[1],B.Venkatraman[2],Anitha Selvakumar[3]

[1]Student,Computer Science And Engineering,New Prince Shri Bhavani College Of Engineering And Technology

[2]Student,Computer Science And Engineering,New Prince Shri Bhavani College Of Engineering And Technology

[3]Assistence Professor, Computer Science And Engineering And Technology, New Prince Shri Bhavani College Of Engineering And Technology

ABSTRACT

The conventional voting scheme employ's paper-based ballot to verify votes . This voting scheme is insecure due to the attributed shortcoming including ballot stuffing ballot snaching and vote's impersonation. So we present the design and development of secure e-voting to ensure a free, fair and credible election. The proposed system solve the authentication integrity and confidentiality security issues of e-voting by using elgamal algorithm it can be more efficient cryptographic construction E-voting involves election processing at a easy phase so that voting percentage also increase . Citizens should also be trained on how to vote online before time .It also save huge time and enables election commissioner to announce the result within a short period of time

Keyword: Network traffic distribution, data aggregation, privacy preservation, malicious security.

INTRODUCTION

The issue of handling as far as possible parts, parts whose check is more significant than a given quality. Private is extraordinarily convincing in various application . A normal application that incorporates such primitive is framework development spread, Where n framework sensors need to commonly examine the security caution appeared by different sources rememnering the final objective to find potential suspet destinations. In such application, and without losting agreement, each of such sensors has a course of suspects and may need to helpfully register the most progressive part on each of these sets. Formally, let there be n customers meant by ui; each of them has a private multistepXi of cardinality k. For ease, expert that each of the multisets has the same cardinality.

SCOPE OF THE PROJECT

Ther have been a lot of approaches to improve the efficiency of SMC-basedgeneral solutions. One key direction is to devise a specific tool for a solution to this cryptographic problem. A closely related work is a protocol proposed by Burkhart and Mitropoulos. Their solution efficiently operates with respect to its computation complexity, but has two critical drawbacks.

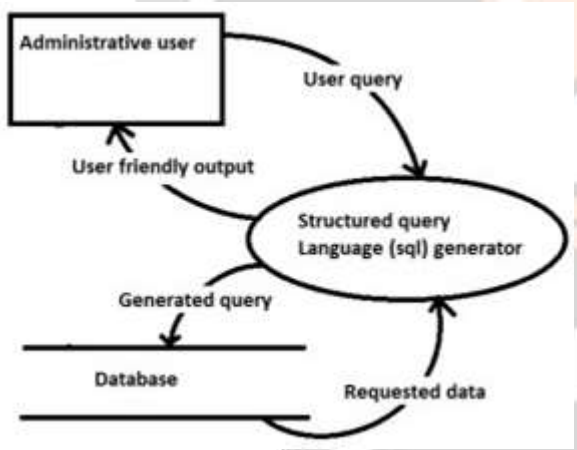
EXISTING SYSTEM

Existing blend arranges re-randomize data ciphertexts without changing the plaintexts of the data ciphertexts. On the other hand possibly, a twofold encryption arrangement does not protect the plaintexts of data ciphertexts in the midst of executing our traditions, yet it still gives a way to deal with recover the plaintexts. Considering everything. Our rule technique is to revamp doubly encoded segments. At that time they use Shuffle schemes Algorithm.

EXISTING SYSTEM METHOD

Remembering the deciding objective to achieve this goal, we grasp a profitable limit E that drives with a concealed publickey encryption (E). For the most part, we ask that: (i) without the secret keys relating to s and pk independently. We call this thought twofold encryption.

OVER ALL DIAGRAM



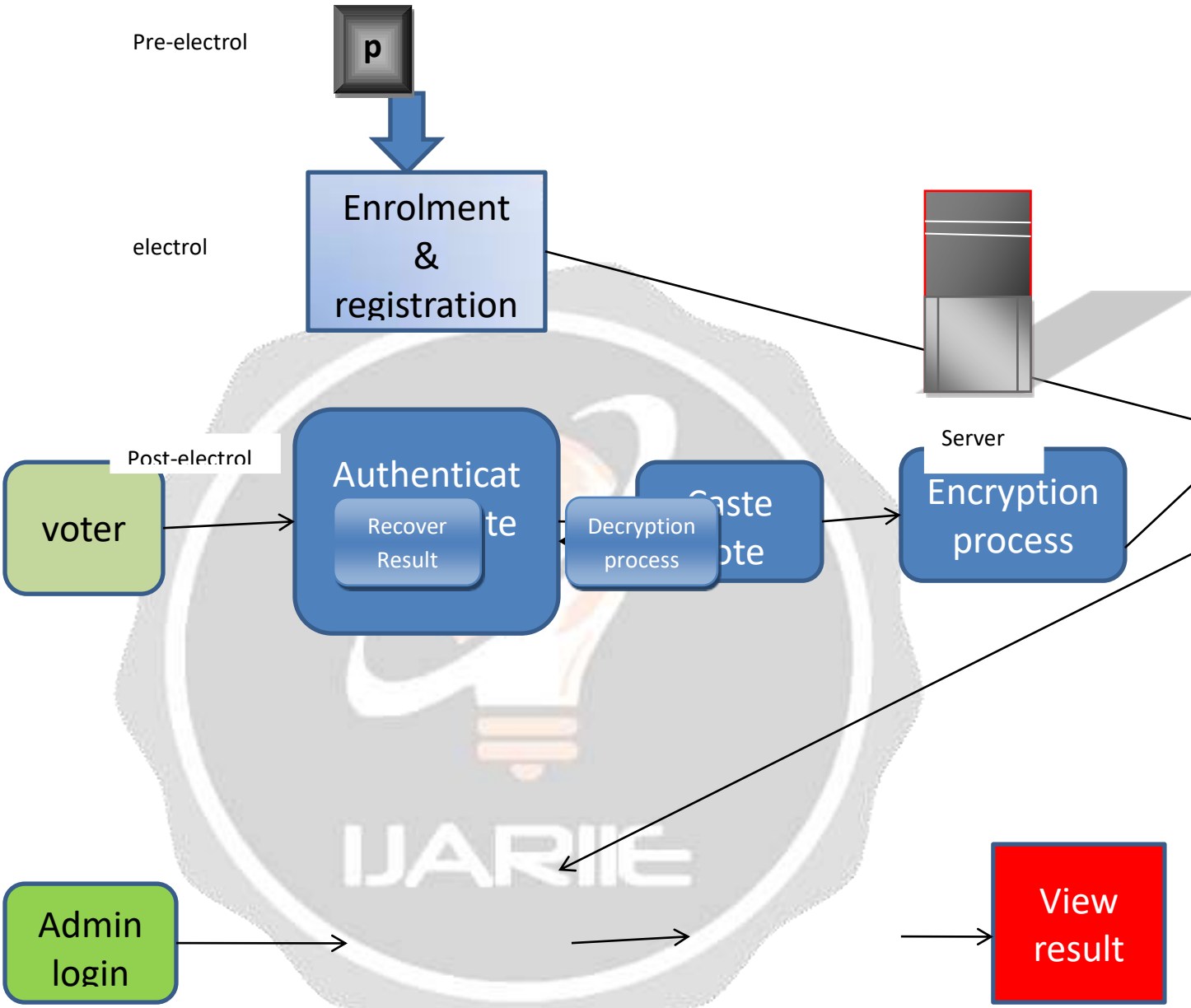
PROPOSED SYSTEM

The proposed approach deals with encrypting plain text i.e. ballot count efficiently. So the ballot count cant be theft and violated.on checking with recent key i.e.Mystery key which make the e-voting more secured and make the ballot efficient to count and produce result of each candidates.In this we are using elgamal algorithm

PROPOSED SYSTEM METHOD

The total computational complexity is dominated by. Decrpyt shuffle algorithms. Putting the computational complexities together shows that the total is O(n2k) in O(n) communication rounds. The proposed protocol has O(n2k log p) bits of communication in total.

System architecture:



LITRATURE SURVEY

The problem of computing the over-threshold elements. Elements whose count is greater than a given value , in a private manner is of particular interest in many appications. (i) No polynomial-time algorithm can learn any elements other than the output of a K^+ protocol, and (ii) No polynomial-time algorithm should know which output of the execution belongs to which user[1]. As pointed out in [2],using a trusted third party (TTP) to solve the private k^+ aggregation problem is impractical since it is hard to find such entity in many settings. Also, using secure multiparty

computations(SMC) is impractical since they are computationally expensive. A final approach is to use existing private set-operation protocols such as[3],[4]-especially multiset union protocols. These protocols securely compute all elements appearing in the union of input multisets; in particular[5] allows to find all elements whose multiplicity is atleast T. Scince these protocols given an output as a set, the output does not have the multiplicity information. While this feature can be beneficial from a privacy standpoint, it risks the functionality of applications relying on the multiplicity of elements, including k^+ aggregation.

REFERENCES

[1] A.Mohaisen, D.Hong, and D.Nyang. privacy in location based services: Primitives toward the solution. In *NCM*,2008.

[2] M. Kim, A. Mohaisen,J.H. Cheon, and Y.kim. Private over-threshold aggregation protocols. In T.Kwon,M-K Lee, and D.Kwon, editors, *ICISC* 2012,LNCS7839,pages 472-486,2012.

[3] L. Kissner and D. Song. Private-preserving set operations. In V. Shoup, editor, *Advances in CryptologyCrypto*, LNCS3621, pages 241-257,2005.

[4] Y. Sang and H. Shen. Efficient and secure protocols for privacy-preserving set operations. *ACM Transactions on Information and System Security(TISSEC),* 13(1):9:1-9:35,2009.

[5] L.Kissner and D. Song. Private-preserving set operations. In V.Shoup, editor, *Advances in CryptologyCrypto* LNCS3621, pages 241-257,2005.