PROVIDING SECURITY TO E-VOTING BY USING EL-GAMMAL ENCRYPTION

[1]Ragu G
ragu253170144@gmail.com
Assistant Professor
[2]Aishwarya C [3]Anusuya S [4]Hemavathi S
aishuchandra9021@gmail.comanusuyasri26@gmail.comhemasaravanan1909@gmail.com
[2][3][4]UG students
Department of Computer Science and Engineering
T.J.S Engineering college

Abstract

The private over-threshold data collection problem is taken and is analyzed,providing the definition of the problem as both data and user privacy.The problem is to examined and an efficient cryptographic construction is made with its proxy variant to overcome the issues with efficiency.Adouble encryption algorithm,which involves two tightly-coupled encryption function and a public key encryption for both the constructions and its malicious variants is constructed.This construction proves to be better than existing protocols.The construction provides the round complexity,computation and communication with linear complexity.The devised protocol is stronger than the existing protocol and is secure in malicious environment.

Index Terms – ***Network traffic distribution, data aggregation, privacy preservation, malicious security***.

1. Introduction

The problem of enumerating the over –verge elements, whose poll is preeminent than a given value in a independent manner is of peculiar interest in many application. A typical application that involves such basic is network traffic distribution , where n network sensors need to resolve the security alert announced by various sources in order to evaluate possible suspect sites. In this application, and without losing any abstraction, individual sensor has a set of suspects and would like to collude and compute the most frequent elements on individual sets (e.g., the poll preeminent than k, assigned as k^+) after exposing the set of suspects to different sensors.
According to, let us consider n user denoted by a_i , $1 \le i \le n$, individual of them has independent multisetY_i of cardinality k. For modesty, consider that individual multiset has the same cardinality.

Let μ,k € M and, for a bent Z and α € X, let F(α) denote the number of occurrences of α in X. Formerly the problem at hand is denoted as follows: given n multiset of cardinality k, find a bent $Z=\{\alpha_1,\ldots\ldots \alpha_\mu\}$ C U = $\ddot{U}^n_{i=1} X_i$ such that,

(i)For all components α € U, if α has multiplicity preeminent than or equal to k, then α € Z, i.e.,

$$Z =\{\alpha \in \ddot{U}^n_{i=1}X_i| F(\alpha) \ge k\},$$

(ii)There is no polynomial –time method can determine any component other than the output of a K^+covenant

(iii)no polynomial-time method should know which output of the execution belongs to which user.

As pointed out in using a devoted third party to solve the independent k^+ aggregation problem is quixotic after all it is hazard to find bent creature in many framework.Using guard multiparty computation(SMC) is quixotic after all they are computationally lavish.A final way is to use actual independent set operation protocols such as multiset union protocols.These protocols securely enumerate all components appearing in the union of input multisets; in peculiar allows to find all components whose multiplicity is at least τ.

This feature can be profitable from a independent standpoint, it exposure the performance of application depending on the multiplicity of components, including k^+ aggregation.

1.1 Our approach-Informal Description

In these protocols, eachballot is mixed with a shuffle scheme to removelinkability between voters and ballots. Thus, wheneach element in a multiset is encrypted and shuffledusing e-voting protocols, all encrypted elements canbe decrypted while hiding linkability. We need to find a way to preserve data privacy even when all encrypted elements are decrypted.

In order to achieve this goal, we adopt an efficientfunction E that commutes with an underlying

publickeyencryption (E). Roughly speaking, we demand that:

(i) commutativity: $E_{\circ} E = E_{\circ} E$,

(ii) doubleprivacy: given $\bar{\alpha} = E_{s} \circ E_{pk}(\alpha)$, no algorithm can efficientlyfind α without the secret keys correspondingto s and pk respectively. We call this notion doubleencryption.Existing shuffle schemes re-randomize input ciphertextswithout changing the plaintexts of the input ciphertexts . Rather, a double encryption scheme does not preserve the plaintexts of input ciphertexts during executing our protocols, but it still gives a way to recover the plaintexts. In conclusion, our main technique is to shuffle doubly encrypted elements.

2. Related work

We assume the existence of a TTP, the cryptographic problem we are considering becomes trivial. Thus all the related work in the literature has been attempting to find a way to replace the TTP while providing security at the same level as when assuming the existence of such a TTP. The general-purpose solution rely on fundamental theorem of cryptography. The special-purpose group suggests carefully tuned methods to efficiently solve the problem compared with the general purpose solution. Lastly, the proxy-based schemes introduce some special entities and assign a set of tasks to them, and thus these schemes can achieve a further improved efficiency.

General-purpose approaches:

The first approach we consider is a general solution based on SMC. The notion of SMC allows n users to create a virtual trusted party. Yao first introduced this notion and a method for performing SMC was developed by Goldriech, Micali and Wigderson in [17]. Their result is called the fundamental theorem of cryptography, stating that assuming trapdoor permutations exist, there exists an SMC protocol for every polynomial-size function. Unfortunately, due to the trade-off between generality and efficiency, we cannot achieve an efficient solution for our problem using this tool.

Special-purpose approaches:

There have been a lot of approaches to improve the efficiency of SMC-based general 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 Dimitropoulos [4]. Their solution efficiently operates with respect to its computation complexity, but has two critical drawbacks: if input datasets are disjoint, the accuracy of their construction decreases sharply because the solution is probabilistic and their round complexity is linear in the number of bits in the elements.

Proxy-based approaches:

Their scheme introduces two special entities: a randomizerand a computing server, all of which should be semi-honest. One issue with their solution is thatit cannot support the aggregate operation over multisets. This solution is based on an efficiency strategyby adding a proxy and database (DB) for theconstant round complexity. Both entities are also assumedto be semi-honest to prevent coalition betweenthem. Furthermore, their protocolextensively uses two semantical secure encryptionschemes at the same time: ElGamal encryption

3. Literature Review

Many different approaches have been proposed focused on distributed top-*k* computation. This work as interested in the following privacy-preserving distributed top-*k* problem. secure multiparty computation (MPC) techniques to solve this problem and design two MPC protocols, PPTK and PPTKS, putting emphasis on their efficiency. PPTK uses a hash table . PPTKS uses multiple hash tables. This protocols using efficiently and aggregate to find IP addresses and port numbers.

Mix-nets are used in e-voting schemes and other applications that require anonymity. Shuffles of homomorphic encryptions are used in the construction of mix-nets. To prove the correctness of a shuffle it is necessary to use zero-knowledge arguments .The propose an verifier zero-knowledge argument for the correctness of a shuffle of homomorphic encryptions. This argument has sublinear communication complexity that is smaller than the size of the shuffle itself.

Secure multiparty computation (MPC) allows privacy-preserving computations on data of multiple parties. MPC has building solutions that are practical in terms of computation and communication cost is major challenge. The practical usefulness of MPC for multi-domain network security and monitoring. Then designof privacy-preserving protocols for event correlation and aggregation of network traffic. This improvement for new applications of MPC in the area of networking.

Many existing privacy-preserving techniques for querying distributed databases of sensitive information for large databasesto use of heavyweight cryptographic techniques. These protocols several rounds of interactions between the participants in wide-area settings. A trusted party based approach provide scalability and individual databases to private information to the central party. The privacy-preserving properties of the scalability and practicality of the system using a real-world implementation.

A new signature scheme is proposed, together with an implementation of the Diffie-Hellman key distribution scheme that achieves a public key cryptosystem. The security of both systems on the difficulty of computing discrete logarithms over finite fields.

This is computed from series data contributed by individual mobile nodes can be very useful for many mobile sensing applications. To provide strong privacy of existing approaches add noise to each node. The data and the aggregator to get a noisy sum aggregate. These approaches either have high computation cost, high communication overhead and the high aggregation error. A novel ring-based interleaved grouping technique to efficiently deal with dynamic joins and leaves and achieve low aggregation error. It is very efficient in computation.

A shuffle consistsof a permutation andre-encryption of a set of inputs. One application of shuffle is to build mix-net.This scheme is more efficient than terms of communication and computational. They use Zero-knowledge argument and homomorphic encryptions.

4. Existing System

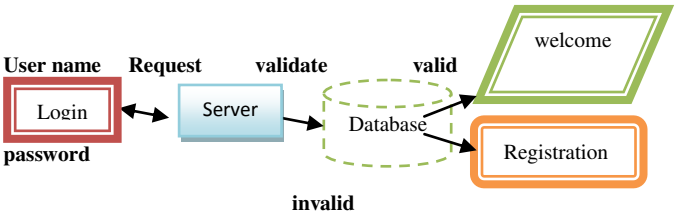
The existing system is based on the shuffle scheme algorithm.The problem of protecting the messages from the hackers is usually solved by cryptographic methods. This led tocreate various algorithms of encryption and decryption. It is called Perfect Shuffle Crypto Algorithm (PSCA) which is classified as a transposition or permutationtechnique in the crypto system.The PSCA is an asymmetry key encryption, uses a pair of keys, that are a public key forencrypting data, and a corresponding private secret key for decrypting. PSCA is very fast and simple for technical realization.For the linear plaintext length of $N=2_n$, it will take O (N log N) to complete both encrypting plaintext anddecrypting cipher text.The PSCA is reasonably secure, especially for chipper text-only attack. In this algorithm, randomly shuffling the elements of an array. The shuffle you are encouraged to solve this task according to the task description, using any language you many know. The data can be randomly shuffle in the database. Because of the huge number of user enter the data can be encrypted in the database randomly shuffle. The re-randomize data cipher text without chaining the plaintext of the cipher text . The two fold encryption arrangement does not protect the plaintext of data cipher text. Then the algorithm of existing system can not be secure manner. The disadvantages of existing system is plain text can not becipher texted. And then plain text easily theft.

5. Proposed System

The proposed system is based on the**El-gammal Encryption algorithm**. This algorithm is total computational complexity is dominated by Decrypt and Shuffle algorithms. Putting the computational complexities together shows that the total is O(n2k) in O(n)communication rounds. The proposed protocol hasO(n2k log p) bits of communication in total.It is same to the existing systemAnd then data can be encrypted in double time. In this algorithm can be used More secure manner. The algorithm work with the encrypting plain text (i.e. Ballot count) efficiently. Because of the double encryption as encrypted to datais randomly changed in the character in to the database. The count can not be theft and violated. Also used for mystery key which make the E-voting more secured. Then the advantages of plain text Can be cipher texted and security for Ballot count make E-voting more and more secured.

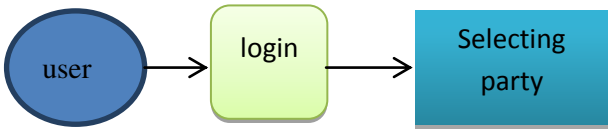
5.1. User interface design

To connect with server user must give their user name and password then only they can able to connect the server. If the user already exits directly can login in to the server else user must register their details such as User name, password and email id, into the server. Server will create account for the entire user to maintain Upload and download rate. Name will be set as user id …login in is usually used to enter a specific page.



5.2. Selecting the party

This module the user after login with their respective username and password, then user selecting the party who going to E-voting.

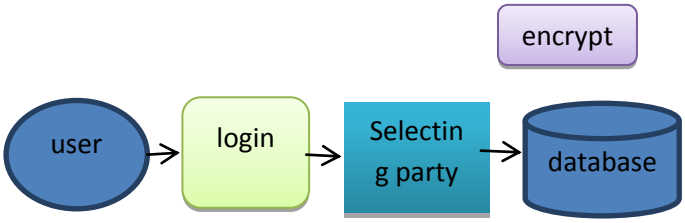


5.3. Encryption of all data

In this module the all data (information) are encrypted for securing all information. Manner for file encryption we used DES (DATA ENCRYPTION STANDARD

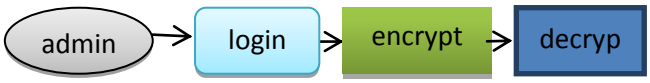
5.4. Store File To Database

In this module,All the encrypted files are stored in the database of several users. The unauthorized person are unable to access any information



5.5. Admin Decrypt All Data

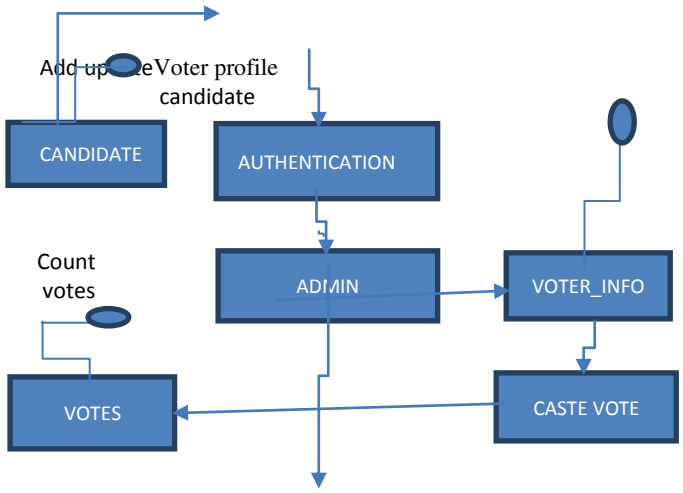
In this module, the admin maintaining and securing all the information in safely. Then admin decrypt all the encrypt information and provide result.



5.6. View Party Result

In this module, the admin provide all party result where unauthorized user cannot able to access the information and the admin provide all the information in secured without any third party access the file.

6. System Architecture



Let us consider the process of;

1. The candidate enter the details in online voting registration for the admin .
2. Next select the party to the candidate.
3. The details are stored in encryption of the database.
4. And then admin decrypted in the data .
5. Admin count the result in the number of vote .
6. Admin view the result.

7. Conclusion

In this proposed system we are using wearable technology it is easy to use, Ballot count for the effective So the count can't be theft and violated. Todeveloped the two protocols, with varying operation overhead, analyzed their security, and demonstrated practicality by analyzing its precise computational and theCommunicational cost. The zero knowledge proofis present interactive variant and then improve theCommunication complexity of our protocols.

8. References

[1].M. Burkhart and X. Dimitropoulos". Fast privacy preserving top-k queries using secret sharing".

[2].S. Bayer and J. Groth. "Efficient zero-knowledge argument for correctness of a shuffle".

[3].M. Burkhart, M. Strasser, D. Many, and X. Dimitropoulos .SEPIA:" Privacy-preserving aggregation of multi-domain network events and statistics".

[4].Q. Li and G. Cao." Efficient and privacy-preserving data aggregation in mobile sensing".

[5].J. Groth. "A verifiable secret shuffle of homomorphic encryptions".