ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Special Issue 4, April 2018

Crowdsourcing based Disease Analyzer

Bhuvanesh E[1], Bhaskar N[2]

B.Tech, Department of Information Technology, KCG College of Technology, Chennai, India[1]

Assistant Professor, Department of Information Technology, KCG College of Technology, Chennai, India[2]

ABSTRACT: This paper watches out for the issue of sharing individual specific growth without disparaging the assurance of their data subjects to help broad scale biomedical research roll. This point is impelled by how limit is more affordable than figuring in current circulated processing evaluating plans. Likewise, counting the amount of matches between the inquiry pictures and a progression; lucid OR matches where a request picture is allowed to facilitate a subset of the letter set thusly making it possible to manage support for the widened letter set of nucleotide base codes that encompasses ambiguities in groupings request that show the amount of occasions of each kind of picture in the predefined breakthrough an edge request whose answer is "yes" if the amount of matches outperforms a request decided breaking point For all inquiry sorts we can disguise the fitting reactions from the analyzing server, with the objective that solitary the client takes in the proper reaction.

I. INTRODUCTION

This paper provides a new method that addresses a larger set of problems and provides a faster query response time than the technique introduced. Our approach is based on the fact that, given current pricing plans at many cloud services providers, storage is cheaper than computing. Therefore, we favor storage over computing resources to optimize cost. Moreover, from a user experience point of view, response time is the most tangible indicator of performance; hence it is natural to aim at reducing it. Our method enhances the state of the art at both the conceptual level and the implementation level. Moreover, our encoding of the data makes it possible for us to handle a richer set of queries than exact matching between the query and each sequence of the database, including. Our system deals with analyzing the disease through web application. In existing system collision occurs between the admin who records all the details of user in a database and processer. In our proposed system, load balancing algorithm is used for avoiding collisions. The user who enters the details in web application, admin gets that data, stores it and sends to related processer at a time by giving a password for security. The doctor sends the reply to the admin and it sends to the patients by giving a secure password. Counting the number of matches between the query symbols and a sequence. Logical OR matches where a query symbol is allowed to match a subset of the alphabet thereby making it possible to handle (as a special case) a “not equal to” requirement for a query symbol. Support for the extended alphabet of nucleotide base codes that encompasses ambiguities in DNA sequences. Queries that specify the number of occurrences of each kind of symbol in the specified sequence positions. A threshold query whose answer is ‘yes’ if the number of matches exceeds a query-specified threshold.

II. RELATED WORK

System addresses the problem of sharing person-specific genomic sequences without violating the privacy of their data subjects to support large-scale biomedical research projects. The proposed method builds on the framework but extends the results in a number of ways. One improvement is that our scheme is deterministic, with zero probability of a wrong answer. It also provide a new operating point in the space-time tradeoff, by offering a scheme that is twice as fast as theirs but uses twice the storage space. This point is motivated by the fact that storage is cheaper than computation in current cloud computing pricing plans. Moreover, our encoding of the data makes it possible for us to handle a richer set of queries than exact matching between the query and each sequence of the database, including: (i) counting the number of matches between the query symbols and a sequence; (ii) logical OR matches where a query symbol is allowed to match a subset of the alphabet thereby making it possible to handle a “not equal to” requirement for a query symbol (iii) support for the extended alphabet of nucleotide base codes that encompasses ambiguities in DNA

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

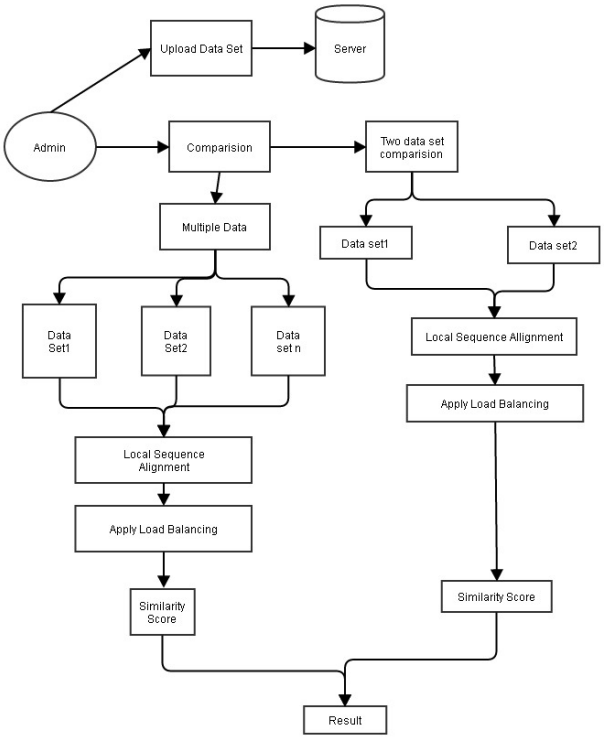
International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Special Issue 4, April 2018

sequences (iv) queries that specify the number of occurrences of each kind of symbol in the specified sequence positions (v) a threshold query whose answer is 'yes' if the number of matches exceeds a query-specified threshold. (vi) For all query types we can hide the answers from the decrypting server, so that only the client learns the answer. (vii) In all cases, the client deterministically learns only the query's answer, except for query type (v) where we quantify the (very small) statistical leakage to the client of the actual count. Our system deals with analyzing the disease through web application. In the existing system collision occurs between the admin records all the details of user in a database and processer. In the proposed system, Load Balancing Algorithm is used for avoiding collisions. The user who enters the details in web application, admin gets that data, stores it and sends to related processer at a time by giving a password for security. The doctor sends the reply to the admin and it sends to the patients by giving a secure password. There is no universal method to create a protocol for secure multi-party computation and handling aggregate queries on encrypted data is not an exception. Several holomorphic systems only support a subset of mathematical operations, like addition, or exclusive- From a security perspective, only the additive and the multiplicative are classified to be IND-CPA (stands for in distinguish ability under chosen plaintext attack). Partially holomorphic cryptosystems are more desirable from a performance point of view than somewhat holomorphic cryptosystems, which support a limited operation depth. Fully holomorphic systems have a huge cost and cannot be deployed in practice.



Block diagram

III. METHODOLOGY

1. User Counseling

The User Counselling form is used to communicate with the doctor whom the user booked the services from the medical service provider. The user can enquire about the needed information with the doctor. Each data owner (e.g., patient) is a trusted authority of her own PHR.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Special Issue 4, April 2018

2. Access Control

The members can be classified into three categories: the directly authorized doctors in the local healthcare provider who are authorized by the patients and can both access the patient's personal health information and verify the patient's identity and the remote healthcare providers who are authorized by the directly authorized physicians for medical consultant (i.e. since they are not authorized by the patients, we use the term 'indirectly authorized' instead). They can only access the personal health information, but not the patient's identity

3. Security Analysis

The security purpose of user information is enhanced by user approved encrypting the user phr information. More significantly, without the knowledge of which doctor in the healthcare provider is professional in treating his illness, the best way for the patient is to encrypt his own PHR under a specified access policy. As a result, the authorized doctors whose attribute set satisfies the access policy can recover the PHI and the access control management also becomes more efficient.

4. Distributed Cloud Computing

It consider the server to be semi-trusted, the information in the server is not secure. On the other hand, some users will also try to access the files beyond their privileges. So For user privacy the user can easily encrypt their information to protect the information from piracy.

5. M-Healthcare System

Propose a scheme where the user can access remote doctor in any provider hospital registered and using this system, the user can counsel doctor and update user phr information and also increase their privacy by encrypting their information.

6. Over All Report

A novel authorized accessible privacy model and a patient self-controllable multi-level privacy preserving cooperative authentication scheme realizing. The user can also view their information. The doctor can view the patient list and also the new counsel patient.

ALGORITHM

STEP 1
Derive the set of round keys from the cipher key
STEP 2
Initialize the state array with the block data
STEP 3
Add the initial round key to the starting state array
STEP 4
Perform nine rouinds of state manipulation
STEP 5
Perform the tenth and final round of state manipulation
STEP 6
Copy the final state array out as the encrypted data

Attribute based Encryption:

Anonymous access control is a very desirable property in various applications e.g. encrypted storage in distributed environments; and attribute based encryption (ABE) is a cryptographic scheme that is targeted to achieve this property. ABE is an encryption mechanism that is useful in settings where the list of users may not be known apriori, but all users may possess certain credentials which can be used in determining access control and at the same time providing a reasonable degree of anonymity. Ciphertext policy attribute based encryption is a scheme that gives a natural way to link the access policy with the ciphertext, and attributes with the keys; and cleverly combine them at a later stage to

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Special Issue 4, April 2018

provide secure access to protected data. In most ABE schemes the size of the ciphertext is quite large and is of the order of the number of attributes.

IV. CONCLUSION

In this paper, it have revisited the challenge of sharing person-specific sequences without violating the privacy of their data subjects in order to support large-scale biomedical research projects. We have used the framework based on additive homomorphism encryption, and two servers: one holding the keys and one storing the records. The proposed method offers two new operating points in the space-time tradeoff and handles new types of queries that are not supported in earlier work. Furthermore, the method provides support for extended alphabet of nucleotides which is a practical and critical requirement for biomedical researchers. Big data analytics over genetic data is a good future work direction. There are rapid recent advancements that address performance limitations of holomorphic encryption techniques. Wehope that these advancements will lead to more practical solutions in the future that can handle larger-scale genetics data. It is worth mentioning that our approach is not restricted to a fixed holomorphic encryption technique and therefore, it would be possible to use and inherit the advantages of newly developed ones.

REFERENCES

1. Design of Capacity-Approaching Constrained Codesfor DNA-based StorageSystems Kees A. Schouhamer Immink, Fellow, IEEE and Kui Cai, Senior Member, IEEE in the year 2017
2. Scalable and Secure Sharing of Personal Health Records in Cloud Computing Using Attribute-Based Encryption Ming Li, Member, IEEE, Shucheng Yu, Member, IEEE, Yao Zheng, Student Member, IEEE, Kui Ren, Senior Member, IEEE, and Wenjing Lou, Senior Member, IEEE in the year 2013
3. An SMDP-Based Service Model for Interdomain Resource Allocation in Mobile Cloud Networks Hongbin Liang, Student Member, IEEE, Lin X. Cai, Member, IEEE, Dijiang Huang, Senior Member, IEEE,Xuemin (Sherman) Shen, Fellow, IEEE, and Daiyuan Peng, Member, IEEE
4. M. Li, S. Yu, K. Ren, and W. Lou, "Securing Personal HealthRecords in Cloud Computing: Patient-Centric and Fine-GrainedData Access Control in Multi-Owner Settings," Proc. Sixth Int'lICST Conf. Security and Privacy in Comm. Networks (SecureComm '10),pp. 89-106, Sept. 2010.
5. "At Risk of Exposure - in the Push for Electronic Medical Records,Concern Is Growing About How Well Privacy Can Be Safeguarded,"he-privacy26, 2006.
6. K.D. Mandl, P. Szolovits, and I.S. Kohane, "Public Standards andPatients' Control: How to Keep Electronic Medical RecordsAccessible but Private," BMJ, vol. 322, no. 7281, pp. 283-287,Feb. 2001.
7. J. Benaloh, M. Chase, E. Horvitz, and K. Lauter, "PatientControlled Encryption: Ensuring Privacy of Electronic MedicalRecords," Proc. ACM Workshop Cloud Computing Security(CCSW '09), pp. 103-114, 2009.
8. S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving Secure, Scalable,and Fine-Grained Data Access Control in Cloud Computing,"Proc. IEEE INFOCOM '10, 2010.
9. H. Lo¨ hr, A.-R. Sadeghi, and M. Winandy, "Securing the E-HealthCloud," Proc. First ACM Int'l Health Informatics Symp. (IHI '10),pp. 220-229, 2010.
10. J. Hur and D.K. Noh, "Attribute-Based Access Control withEfficient Revocation in Data Outsourcing Systems," IEEE Trans.Parallel and Distributed Systems, vol. 22, no. 7, pp. 1214-1221, July2011.
11. S. Jahid, P. Mittal, and N. Borisov, "Easier: Encryption-BasedAccess Control in Social Networks with Efficient Revocation,"Proc. ACM Symp. Information, Computer and Comm. Security(ASIACCS), Mar. 2011.
12. S. Ruj, A. Nayak, and I. Stojmenovic, "DACC: Distributed AccessControl in Clouds," Proc. IEEE 10th Int'l Conf. Trust, Security andPrivacy in Computing and Comm. (TrustCom), 2011.
13. S.D.C. di Vimercati, S. Foresti, S. Jajodia, S. Paraboschi, and P.Samarati, "Over-Encryption: Management of Access ControlEvolution on Outsourced Data," Proc. 33rd Int'l Conf. Very LargeData Bases (VLDB '07), pp. 123-134, 2007.