International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 2 Feb 2022, pp: 1386-1390 www.ijaem.net ISSN: 2395-5252

DNA-Seal: Sensitivity Levels to Optimize the Performance of Privacy-Preserving Dna Alignment

Dr. T. Nalini, Sivabaalan.S,Sudarsanan.E,Sakthivel.G
[1,2]*Professor Dr MGR Educational and Research Institute, Chennai.*
B. Tech Computer Science Engineering Dr MGR Educational and Research Institute, Chennai
B. Tech Computer Science Engineering Dr MGR Educational and Research Institute, Chennai
B. Tech Computer Science Engineering Dr MGR Educational and Research Institute, Chennai

Submitted: 15-02-2022 Revised: 25-02-2022 Accepted: 28-02-2022

ABSTRACT: This paper watches out for the issue of sharing individual specificspecific genomic progressions without slighting the assurance of their data subjects to help broad scale biomedical research projects. The proposed procedure develops the framework. However, extends the results in different waysOne change is that our arrangement is deterministic, with zeroprobability of a wrong answer (instead of a low probability). We in like manner give another working point in the space-time tradeoff, by offering an arrangement that is twice as brisk as theirs however uses twofold the storage space.This point is impelled by how limit is more affordable than figuring in current circulated processing evaluating plans. Likewise, our encoding of the data makes it plausible for us to manage a wealthier plan of inquiries than revise organizing between the request and each gathering of the database

KEYWORDS: Bioinformatics,GenomicsCloud computing,Sensitivity,Privacy, Data privacy,Sequential analysis

I. INTRODUCTION

Sometimes the queries on DNA need to consider various errors such as irrelevant mutations, incomplete specifications and sequencing errors. Therefore, the pattern of the query should be expressed using regular expressions. Many works address practical and privacy- preserving outsourcing of this regular expression type of queries, implemented as oblivious evaluation of finite automata. stroke

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 distinguishability 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.

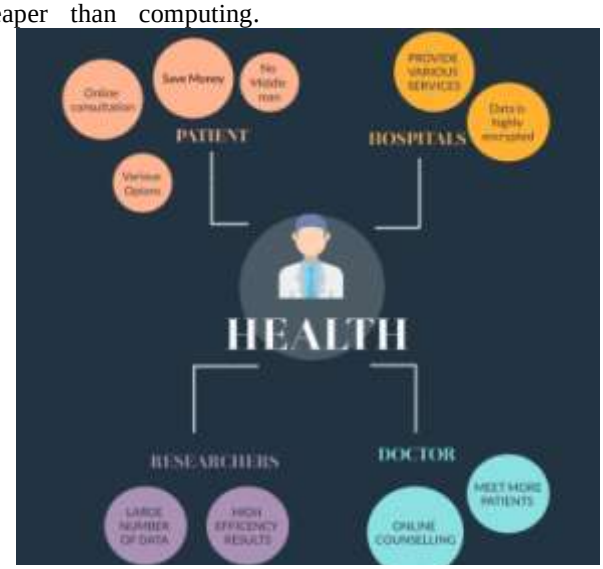
II. EXISTING SYSTEM

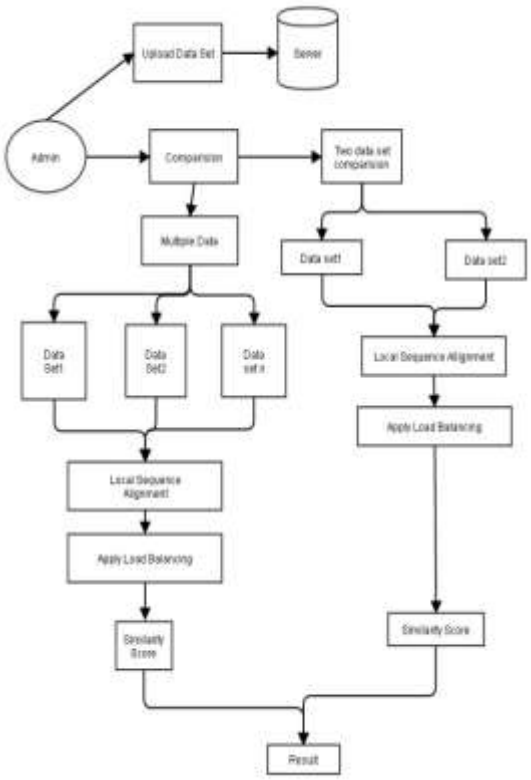
Human DNA data (DNA sequences within the 23 chromosome pairs) are private and sensitive personal information. However, such data is critical for conducting biomedical research and studies, for example, diagnosis of pre-disposition to develop a specific disease, drug allergy, or prediction of success rate in response to a specific treatment. Providing a publicly available DNA database for fostering research in this field is mainly confronted by privacy concerns. Today, the abundant computation and storage capacity of cloud services enables practical hosting and sharing of DNA databases and efficient processing of genomic sequences, such as performing sequence comparison, exact and approximate sequence search, and various tests (diagnosis, identity, ancestry and paternity). What is missing is an efficient security layer that preserves the privacy of individuals' records and assigns the burden of query processing to the cloud. Whereas anonymization techniques such as de-identification, data augmentation, or database partitioning solve this problem partially, they are not sufficient because in many cases, re-identification of persons is possible.

International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 2 Feb 2022, pp: 1386-1390 www.ijaem.net ISSN: 2395-5252

III. PROPOSED SYSTEM

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. tangible indicator of performance hence it is natural to aim at reducing itOur 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





International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 2 Feb 2022, pp: 1386-1390 www.ijaem.net ISSN: 2395-5252

IV. PROPOSED ARCHITECTURE

Our Project Consists of six modules The modules are

•Privacy preserving
•Secure Outsourcing
•Aggregate queries
•Sequence testing
•Set match query
•Hiding from the decrypting server

•Privacy preserving

Hospitals want to protect the confidentiality of the DNA sequences that they own, and no external party has the right to access these DNA sequences for privacy reasons. Thus, other parties (be it the server or the clients) should only work on encrypted sequences and never have access to the DNA. In this, modules the file which is stored by the hospital will be encrypted and then stored in clouds

•Secure Outsourcing

The encrypted file will be outsourced to the clouds. This solution aims not only to provide confidentiality and access controllability of outsourced data with strong cryptographic guarantee, but, more importantly, to fulfill specific security requirements from different cloud services with effective systematic way.

•Aggregate queries

In this modules, important queries have often in the form of how many records contain a diagnosis of disease and gene variant. Secure outsourcing of the database and allowing such type of queries without requiring the server to decrypt the data. In this hospital will set the DNA by a large sequence of characters from the alphabet representing the four nucleotide types. This alphabet can be aggregate with additional characters representing augmented in the sequence.

•Sequence testing

In this module, the queries on DNA need to consider various errors such as irrelevant mutations, incomplete specifications and sequencing errors. Clients are authorized entities in which they are allowed to perform queries on the encrypted DNA sequences

•Set match query

In this module, we will authenticate that the query which is asked by the researcher match with the query which is given by the cloud. The hospital will set the alphabetical sequence of DNA, and the same the Alphabetic sequence must be given by the researchers.

•Hiding from the decrypting server

In this module, the hospital will store the encrypted file to the cloud. The cloud will internally make cloud1 as a key holder and cloud2 has a data holder. In which every time the researcher will query the file initially the cloud1 will return the key and if it matches with the hospital secret key then cloud2 will return the decrypted data.

➢ DATA DICTIONARY

➢ Fields	Type	Null	Constraints	Description
H_Name	varchar (45)	No		Hospital Name
P_Name	varchar (45)	No		Patient Name
P_Image	LongBlob	No		Patient Image
Age	Int	No		Age
Ad_Time	Int	No		Admit Time
Icu_ward	varchar (45)	No		ICU_Ward
H_Treatment	varchar (45)	No		Heart Treatment
add	varchar (45)	No		Address
City	varchar (45)	No		City

International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 2 Feb 2022, pp: 1386-1390 www.ijaem.net ISSN: 2395-5252

V. ALGORITHM

Key Size: [8]
Generated prime numbers p and q
p: [139]
q: [151]
The public key is the pair (N, E) which will be published.
N: [20989]
E: [1423]
The private key is the pair (N, D) which will be kept private.
N: [20989]
D: [17587]
Recovered plaintext: [vinoth]

Require: A combinatorial design $(X, \mathcal{A})$ where
$X = \{x_1, x_2, \ldots, x_v\}$,
$\mathcal{A} = \{B_1, B_2, \ldots, B_b\}$,
$\mathcal{N} = \{n_1, n_2, \ldots, n_t\}$,
$f : \mathcal{N} \to \mathcal{A}$ is a one-one map,
A $c \times r$ Matrix G,
v number of $c \times c$ Matrices $D_1, D_2, \ldots, D_v$.
Ensure: A key predistribution in sensor nodes of $\mathcal{N}$.

for all $x_j \in X, 1 \leq j \leq v$ **do**
  Find ordered set $S = \{B_{j_1}, B_{j_2}, \ldots, B_{j_r}\}$ be such that $B_{j_k} \in \mathcal{A}, x_j \in B_{j_k}; \forall k \in \{1, 2, \ldots, r\}$; $B_{j_k} \neq B_{j_l}, 1 \leq k, l \leq r$ and $\forall B \in \mathcal{A} \setminus S, x_j \notin B$.
  Compute $A_j = (D_j.G)^T$
  for all $i \in \{1, 2, \ldots, r\}$ **do**
    if $f^{-1}(B_{j_i})$ exists **then**
      Store the ith row of matrix A_j in node $f^{-1}(B_{j_i})$
      Store the 2nd row of G in node $f^{-1}(B_{j_i})$
      In node $f^{-1}(B_{j_i})$, store $POS(B_{j_i}, x_j) = i$.
    end if
  end for
end for

VI.CONCLUSION

In this paper, we have revisited the challenge of sharing person-specific genomic sequences without violating the privacy of their data subjects in order to support large- scale biomedical research projectsWe have used the framework based on additive homomorphism encryption, and two servers: one holding the keys and one storing the encrypted recordsThe proposed method offers two new operating points in the space-time trade-off and handles new types of queries that are not supported in earlier workFurthermore, 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. We hope that these advancements will lead to more practical solutions in the future that can handle larger-scale genetics dataIt 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]. T. Hara, V. I. Zadorozhny, and E. Buchmann, Wireless Sensor Network Technologies for the Information Explosion Era, Stud. Comput. Intell.Springer-Verlag, 2010, vol. 278.
[2]. Y. Wang, G. Attebury, and B. Ramamurthy, "A Survey of Security Issues in Wireless Sensor Networks," IEEE Common. Surveys Tuts., vol. 8,no. 2, pp. 2–23, 2006
[3]. A. A. Abbasi and M. Younis, "A survey on clustering algorithms for wireless sensor networks," Comput. Commun., vol. 30, no. 14-15, pp.2826–2841, 2007
[4]. W. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "An Application-Specific Protocol Architecture for Wireless MicrosensorNetworks," IEEE Trans. Wireless Commun., vol. 1, no. 4, pp. 660–670, 2002.
[5]. A. Manjeshwar, Q.-A. Zeng, and D. P. Agrawal, "An Analytical Model for InformationRetrieval in Wireless Sensor Networks Using EnhancedAPTEEN Protocol," IEEE Trans. Parallel Distrib. Syst., vol. 13, pp. 1290–1302, 2002.
[6]. S. Yi, J. Heo, Y. Cho et al., "PEACH: Power-efficient and adaptive clustering

hierarchy protocol for wireless sensor networks," Comput.Commun., vol. 30, no. 14-15, pp. 2842–2852, 2007

[7]. K. Pradeepa, W. R. Anne, and S. Duraisamy, "Design and Implementation Issues of Clustering in Wireless Sensor Networks," Int. J. Comput.Applications, vol. 47, no. 11, pp. 23–28, 2012

[8]. L. B. Oliveira, A. Ferreira, M. A. Vilac¸a et al., "SecLEACH-On the security of clustered sensor networks," Signal Process., vol. 87, pp.2882–2895, 2007.

[9]. P. Banerjee, D. Jacobson, and S. Lahiri, "Security and performance analysis of a secure clustering protocol for sensor networks," in Proc.IEEE NCA, 2007, pp. 145–152

[10]. K. Zhang, C. Wang, and C. Wang, "A Secure Routing Protocol for Cluster-Based Wireless Sensor Networks Using Group Key Management,"in Proc. WiCOM, 2008, pp. 1-5.