e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
Volume:03/Issue:06/June-2021 Impact Factor- 5.354 www.irjmets.com

# A DIGITAL DNA SEQUENCING ENGINE FOR RANSOMWARE DETECTION USING MACHINE LEARNING

**K. Nithya[*1], K.Madhavan[*2], T.Bharath[*3], R.Monesh[*4]**

[*1,2,3,4]B.TECH - IT DR.M.G.R Educational And Research Institute,

Maduravoyal, Chennai, India.

## ABSTRACT

This paper settle the issue of sharing individual express genomic groupings without dismissing the assurance of their data subjects to help gigantic extension biomedical assessment projects. The proposed procedure develops the construction proposed by Kantarcioglu et al. [1] anyway widens the results in different habits. One improvement is that our arrangement is deterministic, with zero probability of a misguided answer (rather than a low probability). We also give another functioning point in the space-time tradeoff, by offering an arrangement that is twice basically as fast as theirs anyway uses twofold the additional room. This point is pushed by how limit is more affordable than computation in current conveyed registering esteeming plans. Also, our encoding of the data makes it useful for us to manage a more lavish course of action of requests than cautious planning between the inquiry and every progression of the informational collection, including: (I) counting the amount of matches between the request pictures and a gathering; (ii) real OR directions with where a request picture is allowed to organize with a subset of the letter set accordingly making it possible to manage (as an exceptional case) a "not identical to" essential for an inquiry picture (e.g., "not a G"); (iii) support for the comprehensive letter set of nucleotide base codes that wraps ambiguities in DNA progressions (this happens on the DNA plan side as opposed to the request side); (iv) requests that demonstrate the amount of occasions of each kind of picture in the predefined course of action positions (e.g., two 'A' and four 'C' and one 'G' and three 'T', occurring in any solicitation in the inquiry decided gathering positions); (v) a breaking point request whose answer is 'yes' if the amount of matches outperforms a query specified edge (e.g., "at any rate 7 matches out of the 15 query specified positions"). (vi) For all request types we can disguise the fitting reactions from the interpreting laborer, with the objective that single the client learns the suitable reaction. (vii) In all cases, the client deterministically learns only the inquiry's answer, except for request type (v) where we assess the (little) genuine spillage to the client of the genuine check.

**Keywords:** Dna Databases, Cloud Security, Secure Outsourcing.

## I. INTRODUCTION

DNA or Deoxyribonucleic Acid is the mode of long term stockpiling and transmission of hereditary data for all advanced living life forms. Human DNA information (DNA arrangements inside the 23 chromosome sets) are private and delicate individual data. In any case, such information is basic for directing biomedical exploration and studies, for instance, conclusion of pre-mien to foster a particular sickness, drug hypersensitivity, or forecast of progress rate in reaction to a particular treatment. Giving an openly accessible DNA data set for cultivating research in this field is essentially defied by protection concerns. Today, the plentiful calculation and capacity limit of cloud administrations empowers viable facilitating and sharing of DNA information bases and productive preparing of genomic successions, for example, performing arrangement correlation, accurate and estimated grouping search and different tests (analysis, personality, family and paternity). What is missing is an effective security layer that safeguards the protection of people's records and doles out the weight of question handling to the cloud. While anonymization strategies, for example, de-recognizable proof [2], information increase [3], or data set apportioning [4] tackle this issue mostly, they are not adequate on the grounds that as a rule, re-ID of people is conceivable [5]. It follows that the DNA information should be secured, not only unlinked from the relating people.

In this paper, we consider the structure proposed in where the DNA records coming from a few clinics are scrambled and put away at an information stockpiling site, and biomedical specialists can submit total tallying inquiries to this site. Tallying questions are especially fascinating for factual investigation.

This paper gives another strategy that addresses a bigger set of issues and gives a quicker inquiry reaction time than the strategy presented in [1]. Our methodology depends on the way that, given current valuing plans at

many cloud administrations suppliers, stockpiling is less expensive than processing. Thusly, we favor stockpiling over registering assets to upgrade cost. Besides, from a client experience perspective, reaction time is the most substantial pointer of execution; thus it is normal to target decreasing it. Our strategy upgrades the cutting edge at both the theoretical level and the execution level. All the more solidly:

- At the theoretical level, we give a deterministic plan, with zero likelihood of an off-base answer (instead of a low likelihood). This offers certainty to the clients that they get precise outcomes to every one of their inquiries, without affecting security.
- We likewise give another working point in the space-time tradeoff, by giving a plan that is twice pretty much as quick as theirs however utilizes double the extra room. A variation of this plan utilizes just 1.5 their extra room to the detriment of extra dormancy.
- Moreover, our encoding of the information makes it feasible for us to deal with a more extravagant arrangement of questions than precise coordinating between the inquiry and each succession of the data set, including:

i. Counting the quantity of matches between the question images and an arrangement.

ii. Logical OR matches where a question image is permitted to coordinate with a subset of the letters in order along these lines making it conceivable to deal with (as a unique case) a "not equivalent to" prerequisite for an inquiry image (e.g., "not a G").

iii. Support for the all-inclusive letters in order of nucleotide base codes that includes ambiguities in DNA arrangements (in spite of the past thing this occurs on the DNA grouping side rather than the inquiry side).

iv. Queries that indicate the quantity of events of every sort of image in the predetermined succession positions (e.g., two 'A' and four 'C' and one 'G' and three 'T', happening in any request in the inquiry determined grouping positions).

v. A edge question whose answer is 'yes' if the quantity of matches surpasses an inquiry indicated limit (e.g., "at least 7 matches out of the 15 question determined positions").

vi. For all inquiry types we can conceal the appropriate responses from the unscrambling worker, so just the customer learns the appropriate response.

vii. In all cases the customer deterministically learns just the inquiry's answer, aside from question type (v) where we measure the (exceptionally little) factual spillage to the customer of the genuine tally.

- At the execution level, we exploit GMP measured number juggling schedules to accomplish a lot quicker execution of the methodology in [1], just as for the new methodologies proposed in this paper.

## II. RELATED WORK

There is no widespread technique to make a convention for secure multi-party calculation and dealing with total inquiries on encoded information isn't an exemption. A few homomorphic frameworks just help a subset of numerical tasks, similar to expansion (Paillier [19], Benaloh [23]), increase (ElGamal [24], RSA [25]), or selective or (Goldwasser and Micali [26]). From a security viewpoint, just the added substance Paillier and the multiplicative ElGamal are characterized to be IND-CPA (represents vagary under picked plaintext assault) [27]. Mostly homomorphic cryptosystems are more alluring from a presentation perspective than to some degree homomorphic cryptosystems,which support a restricted activity profundity. Completely homomorphic frameworks have a gigantic expense and can't be sent practically speaking.

A few works center around ensuring biometric calculations over genomic succession records with regards to get multiparty calculations (SMC). Secure re-appropriating is a specific instance of SMC where a customer with low assets (energy, memory, CPU) demands the help of at least one rethinking specialists with plentiful assets. Secure rethinking tracks down a genuine projection in the current plans of action on account of the multiplication of cloud-based administrations. Distributed computing and capacity security issues have been dependent upon ostensive exploration in the previous years [6]. Spaces of interest incorporate customer confirmation, equipment virtualization dangers, flooding and forswearing of administration assaults just as issues of responsibility, stockpiling security and calculation insurance. With regards to DNA information security, related works can be isolated into five gatherings relying upon the capacity or the inquiry being tended to: criminological data sets, profile coordinating, succession examination, testing by limited automata and total questions.

**A. Forensic information bases**

In a measurable information base, a presume record must be tried against a whole data set. A record of the information base can be decoded just on the off chance that it coordinates with the speculate record. This shields different records from being revealed [7]. Additionally, negative data sets forestall the identification of its individuals by contrarily saving the non-individuals, in a packed structure [8].

**B. Profile coordinating**

In [9] the creators address a huge number of tests like personality, lineage and paternity tests dependent on Short Tandem Repeat (STR) profiles. The STR profile is made out of various loci and for every locus the quantity of redundancies for a given recurrent design. The creators make an interpretation of each test into an arithmetical articulation and give a homomorphic encryption conspire permitting two semi-legitimate gatherings to think about their put away profiles in a semantically secure way. The proposed approach permits accurate answers or little blunder resistance as basically needed by the tests.

**C. Sequence examination**

The alter distance is the ideal expense of addition, erasure and replacement of characters to go from a succession to a arrangement . The alter script is the outline of the means prompting the ideal alter distance. Atallah et al. [10] offers an answer for safely rethink a powerful programming answer for finding the alter distance and the alter script for two given groupings (especially genomic arrangements with little letter set size). The re-appropriating convention depends on two noncolluding (fair yet inquisitive) specialists that safely team up to performing table query and least finding. The protected least discovering convention decides the base of an additively parted vector dependent on Yao's confused circuits and a visually impaired and-permute convention for concealing the record of this base. In [11] their plan has been improved for execution and requires space just straight in the info size. The work in [12] addresses a comparable dynamic programming answer for tracking down the longest normal aftereffect. By utilizing the "four Russians" procedure in another way, the creators propose a correspondence effective SMC convention that improves over the nonexclusive arrangement dependent on Yao's jumbled circuits. Their outcomes highlight a lopsidedness in the work needed by every member, which makes it more appropriate to a reevaluating situation. In [13] the creators address the longest normal aftereffect as a private hunt issue.

Another illustration of genome succession correlation is the Smith-Waterman calculation which performs neighborhood arrangement. In [14] the creators change the definition of this calculation for publicly supporting (i.e., moving to disseminated volunteers). Their plan, in light of calculation with clouded information, safeguards a healthy degree of exactness yet doesn't provably secure the protection of the data sources.

**D. Sequence testing by limited automata**

Now and again the inquiries on DNA need to consider different mistakes like superfluous changes, fragmented determinations and sequencing blunders. Thusly, the example of the question ought to be communicated utilizing customary articulations. Numerous works address reasonable and security safeguarding rethinking of this normal articulation kind of questions, executed as careless assessment of limited automata [15]–[17].

**E. Aggregate questions**

For biomedical scientists, significant inquiries have frequently the structure "The number of records contain a finding of Alzheimer illness and quality variation X?" Secure rethinking of the data set and permitting such kind of questions without requiring the worker to decode the information has been tended to in [1]. The paper presents exceptionally down to earth results. For instance, an include question more than 40 records in a data set of 5000 records requires 30 minutes. Our paper broadens these outcomes by proposing a variation stockpiling and calculation plot.

## III. LITERATURE REVIEW

**1. A Cryptographic Approach to Securely Share and Query Genomic Sequences:**

Associations contribute scrambled genomic arrangement records into a brought together store, where the executive can perform questions, for example, recurrence checks, without decoding the information. We assess the effectiveness of our structure with existing information bases of single nucleotide polymorphism (SNP) successions and exhibit that the time expected to finish check inquiries is possible for true applications. For

instance, our trials show that an include inquiry more than 40 SNPs in a data set of 5000 records can be finished around 30 min with off-the-rack innovation.

**2. Transforming Semi-Honest Protocols to Ensure Accountability:**

Secure multi-party calculation (SMC) balances the utilization and classification of appropriated information. This is particularly significant for security protecting information mining (PPDM). Most secure multi-party calculation conventions are just demonstrated secure under the semi-legit model, giving deficient security to numerous PPDM applications. SMC conventions under the malignant foe model for the most part have unreasonably high intricacies for PPDM. We propose a responsible figuring (AC) structure that empowers obligation for protection bargain to be alloted to the party in question without the intricacy and cost of a SMC-convention under the malignant model. We tell the best way to change a circuit-based semi-genuine two-party convention into a straightforward and effective convention fulfilling the AC-structure.

**3. Protocols for secure calculations:**

The creator examines the accompanying issue: Suppose m individuals wish to process the worth of a capacity f(x1, x2, x3, ..., xm), which is a whole number esteemed capacity of m number factors xi of limited reach. Accept at first individual Pi knows the worth of xi and no other x's. Is it workable for them to figure the worth of f, by conveying among themselves, without unduly parting with any data about the upsides of their own variables. The creator gives an exact definition of this overall issue and depict three different ways of addressing it by utilization of single direction capacities (i.e., capacities which are not difficult to assess yet difficult to reverse). These outcomes have applications to secret democratic, private questioning of data set, negligent exchange, playing mental poker, and so forth

## IV. SCOPE OF PROJECT

The ascent in a large number of ransom ware assaults has incited governments, associations and clients to make sure about and make reinforcements of their basic information. The paper proposes DNA act-Ran, a ML-based computerized DNA sequencing motor for identifying and

grouping ransom ware through sequencing it computerized DNA utilizing a dynamic ML approach. DNA act-Ran first chooses key highlights from the pre-processed information utilizing Multi-Objective Gray Wolf Enhancement (MOGWO) and Binary Cuckoo Search (BCS) calculations. From that point the computerized DNA arrangement is created for the chose highlights utilizing the plan limitations of DNA arrangement and k-means recurrence vector.

## V. PROJECT OBEJECTIVE

Most current payoff product area strategies depend on conduct examination of the malware. In any case, making disclosure marks requires getting rehearses in any case. This by then recommends that a 'first attack' should be compelling to get the huge information expected to make distinguishing proof imprints. Regardless, to keep an essential separation from disclosure, malware planner's utilization disarray strategies for instance, twofold code squeezing. Code squeezing is the methodology of scrambling the principal code including the data additionally, recovery routine limit with the stuffed program itself. By then when the squeezed program is executed, the reconstructing routine code restores the principal code and data to its extraordinary construction. Altogether all the seriously testing code haziness strategies are the layered polymorphic malware that changes their code similarly as their deciphering method what's more, simply uncovers a piece of the code at any execution stage and extraordinary malware that changes their code in its decoded structure achieving different malware strands in each new change.

## VI. EXISTING SYSTEM

Human DNA information (DNA arrangements inside the 23 chromosome sets) are private and delicate individual data. Notwithstanding, such information is basic for directing biomedical exploration and studies, for instance, finding of pre-air to foster a particular infection, drug sensitivity, or forecast of accomplishment rate in light of a particular therapy. Giving a freely accessible DNA information base for encouraging exploration in this field is primarily faced by security concerns. Today, the bountiful calculation and capacity limit of cloud administrations empowers viable facilitating and sharing of DNA information bases and effective handling of genomic successions, for example, performing grouping correlation, careful and rough arrangement search also, different tests (finding, character, parentage and paternity). What is missing is a proficient security layer that

saves the protection of people's records and relegates the weight of inquiry preparing to the cloud. While anonymization methods like de-ID, information increase, or data set dividing tackle this issue part of the way, they are not adequate since as a rule, re-ID of people is conceivable.

**DISADVANTAGE:**

- In the creators address the longest normal aftereffect as a private hunt problem.4
- In our model, clinics that have DNA successions don't have the registering and handling capacities to deal with specialists' solicitations, so they all store their DNA arrangements at a worker.
- We have introduced two new working focuses in the space-time tradeoff of the private question issue.

## VII. PROPOSED SYSTEM

Ransomware attacks have been growing all through continuous years, and various techniques have been proposed to perceive and prevent them. Most current payment product revelation what's more, examination procedures fall into two head groupings - dynamic or on the other hand static methodologies. Dynamic examination method incorporates setting up a disengaged environment and running the malware inside that environment to see its utilitarian direct. Static strategies, then again, incorporate change planning the threatening code to grasp the working of the malware and a while later to foster protections against it. Saundra et al. proposed Elder Ran apparatus that checks brand name recover product marks by researching a lot of exercises during the basic times of the attack stream execute chain. Senior a dynamically distinguishes and describe deliver product by exploring movement works out, for instance, vault key undertakings, calls from Windows APIs, coordinator and record structure assignments. Senior Ran utilizes Logical Regression classifier computation a ML estimation, to portray each customer application, and has additional handiness to perceive and make marks for as of recently dark payment product.

**ADVANTAGES:**

- another technique that utilizes Digital DNA Sequencing Engine for deliver product Analysis utilizing an AI Machine Learning Network to distinguish and characterize recover product.
- The utilization of MOGWO and BCS calculations to create Digital DNA Sequences calculation.
- advanced DNA grouping imperatives and k-implies recurrence vector dependent on the DNA successions.

## VIII. REQUIREMENT ANALYSIS

**Reason**: The primary reason for setting up this report is to give an overall knowledge into the investigation and prerequisites of the current framework or circumstance and for deciding the working qualities of the framework.

**Scope**: This Document assumes an imperative part in the improvement life cycle (SDLC) as it depicts the total prerequisite of the framework. It is intended for use by the engineers and will be the fundamental during testing stage. Any progressions made to the necessities later on should go through conventional change endorsement measure.

**FUNCTIONAL REQUIREMENTS:**

**Input:**

The significant contributions for Web Based Accommodation can be ordered module-wise. Fundamentally all the data is overseen by the product and to get to the data one needs to create one's character by entering the client id and secret word. Each client has their own space of access past which the entrance is progressively held back rather denied .

**Output:**

The significant yields of the framework are tables and reports. Tables are made progressively to satisfy the necessities on need. Reports, as it is self-evident, convey the essence of the entire data 67 that streams across the foundation. This application should have the option to create yield at various modules for various sources of info.

**Performance Requirements:**

Execution is estimated as far as reports created week by week and month to month.

**Intended Audience and Reading Suggestions:**

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
Volume:03/Issue:06/June-2021 Impact Factor- 5.354 www.irjmets.com

The report is arranged keeping is perspective on the scholastic builds of my Bachelor's Degree/Master's Degree from college as halfway satisfaction of my scholarly reason the archive determines the overall method that that has been trailed by me, while the framework was contemplated and created. The overall record was given by the business as a source of perspective manual for comprehend my duties in fostering the framework, as for the necessities that have been pin highlighted get the specific design of the framework as expressed by the real customer. The framework as expressed by my undertaking chief the real norms of the determination were wanted by leading a progression of meetings and polls. The gathered data was coordinated to frame the detail record and afterward was demonstrated to suite the guidelines of the framework as planned.

**Document Conventions:**

The general reports for this venture utilize the perceived demonstrating norms at the product enterprises level.

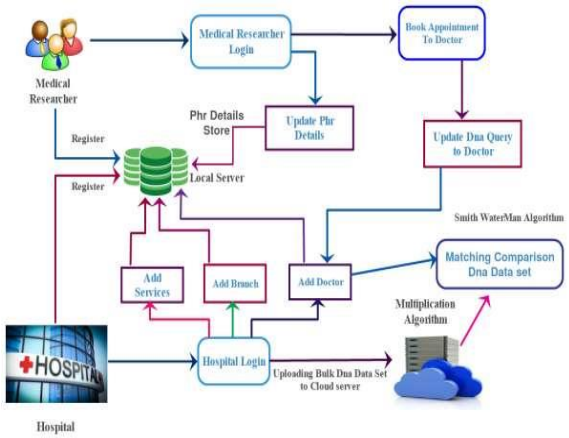
• ER-Modeling to focus on the social states existing upon the framework regarding Cardinality.

• The Physical administer, which express the general information look for the social key while an exchange is executed on the wear elements.

• Unified demonstrating language ideas to give a summed up blue print for the general framework.

• The principles of stream diagrams at the necessary expresses that are the usefulness of the activities need more focus.

## IX. OVERALL ARCHITECTURE




## X. MODULES DISCRIPTION

**PRIVACY PRESERVING:**

Medical clinics need to ensure the secrecy of the DNA groupings that they own and no outside party has the privilege to get to these DNA successions for protection reasons. Consequently, different gatherings (be it the worker or the customers) should just work on scrambled successions and never approach the DNA. In this, modules the record which is put away by the clinic will be scrambled and afterward put away in mists.

**SECURE OUTSOURCING:**

The encoded document will be moved to the mists. This arrangement points not exclusively to give classification and access controllability of rethought information with solid cryptographic ensure, be that as it may, all the more significantly, to satisfy explicit security necessities from various cloud administrations with compelling methodical way.

**AGGREGATE QUERIES:**

In this modules, significant inquiries have frequently as the number of records contain a conclusion of sickness and quality variation. Secure re-appropriating of the data set and permitting such kind of inquiries without requiring the worker to unscramble the information. In this emergency clinic will set the DNA by an enormous succession of characters from the letter set addressing the four nucleotide types. This letters in order can be total with extra characters addressing expanded in the grouping.

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
Volume:03/Issue:06/June-2021 Impact Factor- 5.354 www.irjmets.com

**SEQUENCE TESTING:**

In this module, the inquiries on DNA need to consider different mistakes like insignificant transformations, inadequate details and sequencing blunders. Customers are approved substances in which they are permitted to perform inquiries on the encoded DNA sequences

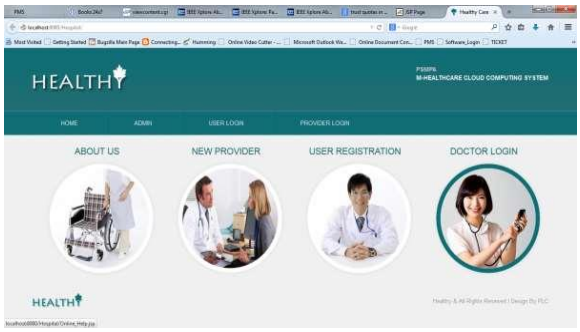
**SET MATCH QUERY:**

In this module, we will verify that the inquiry which is asked by the specialist match with the question which is given by the cloud. The emergency clinic will set the in sequential order grouping of DNA, and a similar the Alphabetic succession must be given by the scientists.

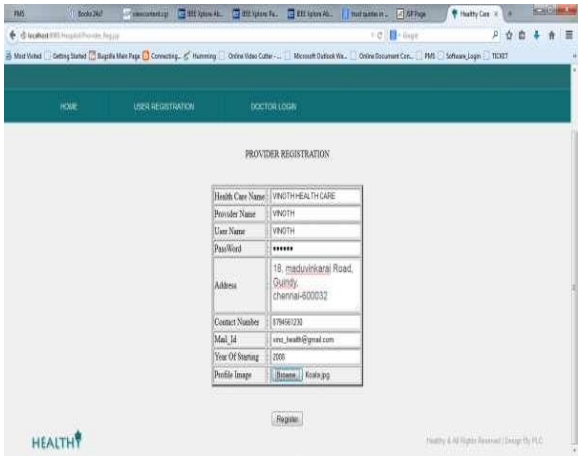
**HIDING FROM THE DECRYPTED SERVER:**

In this module, the clinic will store the scrambled record to the cloud. The cloud will inside make cloud1 as a key holder and cloud2 has an information holder. In which each time the analyst will question the document at first the cloud1 will return the key and on the off chance that it matches with the medical clinic secret key, cloud2 will return the unscrambled information.

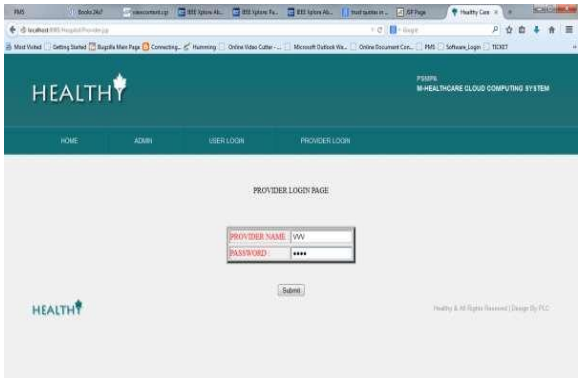
## XI. RESULTS




1. HOME LOGIN

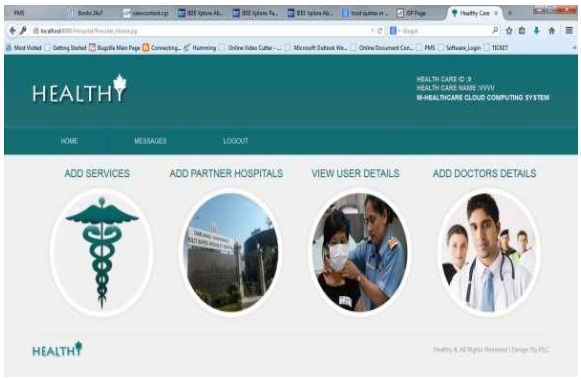



2. PROVIDER REGISTRATION

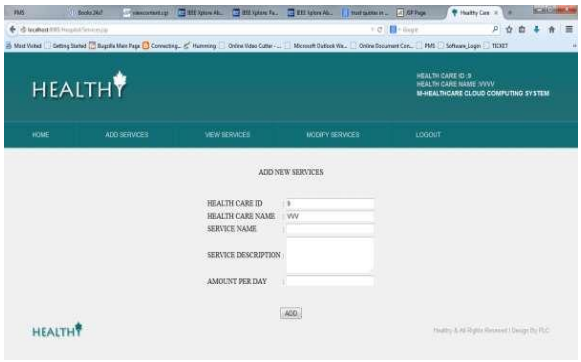



3. PROVIDER LOGIN

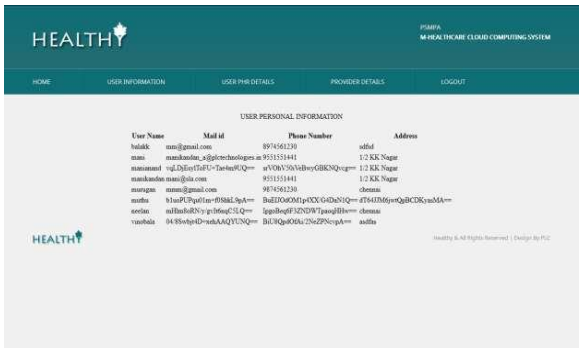
e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
Volume:03/Issue:06/June-2021 Impact Factor- 5.354 www.irjmets.com




4. PROVIDER HOME




5. ADD SERVICES




6. USER PERSONAL REPORT

## XII. CONCLUSION

In this paper, we have returned to the test of sharing individual explicit genomic successions without disregarding the protection of their information subjects to help enormous scope biomedical exploration projects. We have utilized the system dependent on added substance homomorphism encryption, and two workers: one holding the keys and one putting away the encoded records. The proposed strategy offers two new working focuses in the space-time compromise and handles new sorts of questions that are not upheld in prior work. Besides, the strategy offers help for expanded letters in order of nucleotides which is a reasonable and basic prerequisite for biomedical scientists. Large information investigation over hereditary information is a decent future work bearing. There are fast late headways that address execution restrictions of holomorphic encryption procedures. We trust that these progressions will prompt more viable arrangements later on that can deal with bigger scope hereditary qualities information. It merits referencing that our methodology isn't confined to a fixed holomorphic encryption strategy and accordingly, it is feasible to utilize and acquire the upsides of recently created ones.

**FUTURE ENHANCEMENT**

Enormous information investigation over hereditary information is a decent future work course. There are fast ongoing headways that address execution impediments of homomorphic encryption methods. We trust that these headways will prompt more practical arrangements later on that can deal with bigger scope hereditary

qualities information. It is worth referencing that our methodology isn't confined to a fixed homomorphic encryption procedure and along these lines, it is feasible to utilize and acquire the advantages of recently created ones.

## XIII. REFERENCES

[1] M. Kantarcioglu, W. Jiang, Y. Liu, and B. Malin, "A cryptographic way to deal with safely offer and question genomic successions," Inf. Technol. Biomed. IEEE Trans., vol. 12, no. 5, pp. 606–617, 2008.

[2] B. Malin and L. Sweeney, "How (not) to ensure genomic information security in a dispersed organization: utilizing trail re-recognizable proof to assess and plan secrecy assurance frameworks," J. Biomed. Advise., vol. 37, no. 3, pp. 179–192, 2004.

[3] Z. Lin, A. B. Owen, and R. B. Altman, "Genomic examination and human subject protection," Science (80-. )., vol. 305, no. 5681, p. 183, 2004.

[4] A. E. Nergiz, C. Clifton, and Q. M. Malluhi, "Refreshing re-appropriated examined private information bases," in Proceedings of the sixteenth International Conference on Extending Database Technology, 2013, pp. 179–190.

[5] L. Sweeney, A. Abu, and J. Winn, "Distinguishing Members in the Personal Genome Project by Name," Available SSRN 2257732, 2013.

[6] E. Aguiar, Y. Zhang, and M. Blanton, "An Overview of Issues and Recent Developments in Cloud Processing and Storage Security," in High Execution Cloud Auditing and Applications, 2014, pp. 3–33.

[7] P. Bohannon, M. Jakobsson, and S. Srikwan, "Cryptographic Approaches to Privacy in Forensic DNA Databases," in Public Key Cryptography, vol. 1751, H. Imai and Y. Zheng, Eds. Springer Berlin Heidelberg, 2000, pp. 373–390.

[8] F. Esponda, E. S. Ackley, P. Helman, H. Jia, and S. Forrest, "Ensuring information security through hard-to invert negative information bases," Int. J. Inf. Secur., vol. 6, no. 6, pp. 403–415, 2007.

[9] F. Bruekers, S. Katzenbeisser, K. Kursawe, and P. Tuyls, "Protection safeguarding coordinating of dna profiles," IACR Cryptol. ePrint Arch., vol. 2008, p. 203, 2008.

[10] M. J. Atallah and J. Li, "Secure rethinking of grouping examinations," Int. J. Inf. Secur., vol. 4, no. 4, pp. 277–287, Mar. 2005.

[11] M. Blanton, M. M. J. Atallah, K. B. K. Frikken, and Q. Malluhi, "Secure and Efficient Outsourcing of Succession Comparisons," Comput. Secur. 2012, pp. 505–522, 2012.