INTERNATIONAL JOURNAL OF TECHNO-ENGINEERING
IJTE

ISSN: 2057-5688

A CUTTING-EDGE HEALTH MONITORING SYSTEM BASED ON IOT AND CLOUD COMPUTING THAT USES MACHINE LEARNING.

Srinivasa Rao Kadari, Research Scholar, Department of Computer science , Radha Govind University, Ramgarh,Jharkhand.
Dr. Sanjay Kumar ,Assistant Professor ,Supervisor, Department of Computer Science ,Radha Govind University, Ramgarh,Jharkhand.

Abstract:
The Internet of Things (IoT) has recently become one of the IT industry's most well-liked developing technologies. IoT is defined as a network of connected, intelligent physical objects. Through the use of wired or wireless networks, sensors are integrated into physically linked objects and communicate with one another. The interconnectedness of devices, smart, dynamic nature, sensing, enormous size, heterogeneity, and security are the main characteristics of IoT. A consumer may access a variety of cloud services across a network, including database, application, and storage. The Internet of Things (IoT) provides a wide variety of field applications for ongoing monitoring in many different fields, with health care being one of them. The Internet of Things (IoT) has become entrenched in industries that handle enormous amounts of data, particularly with the introduction of IoT-cloud-based devices. One of the newest uses for the IoT-Cloud is the healthcare system. Numerous studies are conducted to protect the confidentiality of patient data. The security of data and computational overheads continue to be the key problems with the IoT-based cloud-based health system. Another challenging area of health systems is the ability to predict illness using patient data from the IoT device.

Keywords: IoT, Cloud, Health, Data, Security

1 INTRODUCTION:

There are scalable resources available in several subscription plans on the cloud. In the end, you'll only be charged only for resources are actually used. This helps you deal with demand increases without having to invest in long-term hardware.

As an example, Netflix makes use of cloud computing's advantages, which it provides. The company experiences significant increases in server usage during periods of peak traffic due to its streaming on demand service. Moving from its internal data centers to the cloud allowed the company to increase its customer base exponentially without the need to invest cash on the setup and maintenance of costly devices.

ESSENTIAL FEATURES OF CLOUD COMPUTING

Cloud computing, or just "Clouds," has a number of distinctive characteristics. Six crucial features are covered out of them.

On-demand services: Using the cloud, consumers may get services for as long as they need them and as per their expectations. According on how much they used at that specific time period, the users get charged. Users get these services based on demand and specifications.

Broad network access: Users may access cloud computing services using thick or thin clients on a heterogeneous platform by exploiting the underlying network infrastructure in accordance with conventional processes. Users may connect, for instance, through laptops, smartphones, desktop computers, or tablets.

Resource Pooling: The cloud's resource sharing function is accomplished by generating virtual instances of computing resources, which are then made accessible to users across the network. Network, storage, servers, apps, and web services are examples of computing or storage resources that are kept as a pool of resources, and many users are permitted access to those resources for a certain period of time as needed.

Rapid elasticity is the capacity of cloud computing to manage utilisation by scaling up and down of resources during peak demands and off-peak workloads. By making resources available as needed, this feature enables our apps to operate without a hitch while adjusting to shifting requirements.

Measured service: Depending on the kind of service (for instance, storage, CPU, network bandwidth, servers, user accounts, etc.) offered to the user, cloud systems intuitively manage and enhance resource allocation and its utilisation using metering mechanisms at the relevant layer abstraction. Resource utilisation is overseen for monitoring, administered for controlling, and reported, giving cloud clients transparency. Due to the fact that cloud services are metered, consumers are only charged for the services they really use. The business model is known as "Pay-per-use" or "Pay-as-you-go," and it allows customers to access cloud services at an affordable price by metering and billing consumers for the specific period of time they use a certain service via a specific resource.

2 LITREATURE SURVEY:

In the Indian healthcare industry, electronic health records (EHRs) are a recent development. According to studies from the Ministry of Electronics and Information Technology (Sunil Kumar, 2016), EHR adoption is crucial for the development of smart health systems. For effective HR management, effective strategies must be used. The four most crucial aspects must be addressed. These include the ICT infrastructure, rules and regulations, standards and interoperability, and R&D with training. The administration of HRs includes a variety of tasks, such as sharing and exchanging safe information.

Both clinical and non-clinical practises may benefit from the archiving of healthcare data. In 2012, Shreekant Iyengar and colleagues performed a study on the availability of primary healthcare for Indians living in rural areas. Data from the states of Madhya Pradesh, Uttar Pradesh, Rajasthan, Karnataka, Andhra Pradesh, and Tamil Nadu have been gathered for this survey's clinical and non-clinical data sections. To maintain democratic accountability, Shirin Madon et al. (2010) also discussed the significance of decentralisation in health information systems. The biggest democratic nation in the world is India. The country has its own laws to uphold the transparency of all services provided to its residents. Accountability must be maintained in health information systems as well.

The information needed to create the tool for bettering mental health has been collected by Rahul Shidhaye et al. in 2019. For the purpose of designing the tool's several stages, the data from the year 2013 was analysed. The study was conducted in Madhya Pradesh's Sehore district. A large database of the patients over a six-year period is created using the information gathered from numerous testing. According to Peris D et al. (2019), there are several ways to gather information on the increased risk of cardiovascular disease in India's rural areas. The SMART health India initiative, which includes 18 PHCs in rural areas, goes by that name. Home CVD risk assessment data, clinical decision support data, and patient monitoring data were gathered.

A summary of several issues of managing EHRs is provided by Haas et al. (2011). Data gathering is done using the centralised health record management system. This framework will increase accessibility and comprehensiveness. The upkeep of HR records in a database presents difficulties with regard to security, privacy, data concealment, and accessibility to authorised users. A different data service may be utilised to connect users, such as patients, medical systems, external storage, and physicians, depending on the demand.

The statistics on reproductive healthcare in India, according to Amlan Majumder & Upadhyay (2004), may be used to predict future social and economic issues. Data collecting on service use, accessibility, and availability, family characteristics, social structure, and level of care are crucial in the area of reproductive healthcare. Keeping clinical records is beneficial for comparing diagnosis. Virostko et al. (2016) looked at the utility of keeping electronic medical records to assess patients with type 1 diabetes' pancreas size.

3 PROPOSED METHOD

In this exploratory analysis, "observing flaws in irrelevant or prior assessments is endeavoured." Early evaluation findings suggest that experts may use this form of assessment to somewhat, but not significantly, alter the course of their request efforts. It isn't even close to being as precise as the tested testing methods. The focus on action and its findings in the specific situation that was previously discussed will probably be clarified by Last's investigation. In any event, by describing how research activity may be shifted about, it adds to the systematic evaluation. The assessment strategy is seen as a thorough technique for responding in this line of thinking. My exploration review is set up with the test centre since new master hits are often attempted, where little or no research is done, some revelations are not discovered, and evaluation may give a more flexible method of working or bearing to meet certain examination areas with the newest resources.

Instead of attempting to foster another clinical idea security system or investigate the possibility of conveying one, this examination used a positivistic assessment approach that adequately analysed prior enthusiastic data while surveying the security of individual information in current IoT-based clinical idea structures. The maker's positivistic evaluation approach was an effective solution to the appraisal problem for a number of reasons. Such a system recognised the manner that IoT-based clinical advantage structures exist and dissected their strength, benefits, limitations, and potential starting with the onion approach for investigation. To guide the testing, information from a variety of sources was used. Due to the expert's thorough analysis of the situation, the examiner had the opportunity to get a thorough understanding of the present situation, as well as if and how it may be resolved.

A strategy for dispersing vulnerability by collecting, examining, and grabbing each cycle one at a time is included in an exploratory approach. As a follow-up, researchers should understand why people need to reflect on or examine the reality of the outside world. A few successful frameworks, designs, and innovations were thoroughly evaluated using data from a preceding research as well as the strong evidence that information on patients' clinical considerations might be reached. Because of advancements in innovation, there are challenges and solutions for developing the exploration structure further. Subjective, quantitative, and integrated assessment techniques are three of the most common types. Recently, quantitative data were shown and divided into inferential, test, and stimulatory tasks. to discuss the informational gathering technique used to compile the affiliations of residents. The broad audience is used as an example to imply that everyone will find the review's tangential findings to be instructive. Various components are used to assess the primary association in the evaluation environment. The creation of breathtakingly skewed or replicated environmental realities is a component of entertainment. It conveys the impression that an animal is growing and evolving in a stable environment. Innovative and socially conscious application: In this particular case, "redirection" refers to "the example of a genuine model, tending to the plan of a striking activity."

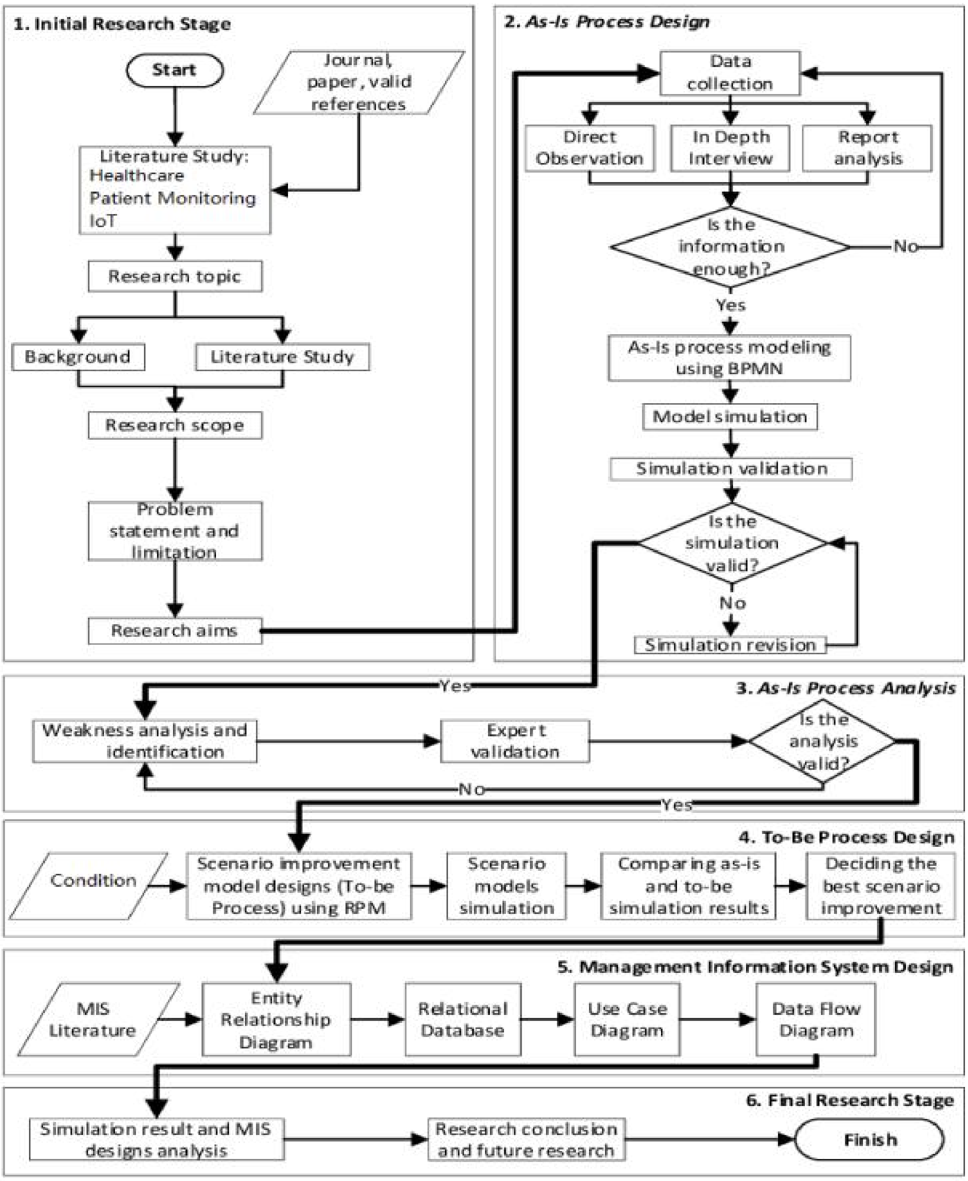

1. Initial Research Stage
Start
Journal, paper, valid references
Literature Study: Healthcare Patient Monitoring IoT
Research topic
Background
Literature Study
Research scope
Problem statement and limitation
Research aims
2. As-Is Process Design
Data collection
Direct Observation
In Depth Interview
Report analysis
Is the information enough?
No
Yes
As-Is process modeling using BPMN
Model simulation
Simulation validation
Is the simulation valid?
No
Simulation revision
Yes
3. As-Is Process Analysis
Weakness analysis and identification
Expert validation
Is the analysis valid?
No
Yes
4. To-Be Process Design
Condition
Scenario improvement model designs (To-be Process) using RPM
Scenario models simulation
Comparing as-is and to-be simulation results
Deciding the best scenario improvement
5. Management Information System Design
MIS Literature
Entity Relationship Diagram
Relational Database
Use Case Diagram
Data Flow Diagram
6. Final Research Stage
Simulation result and MIS designs analysis
Research conclusion and future research
Finish

Figure 3.1: Research Methodology for Proposed Research

This study was created using information from sources that were at least eight to ten years old. Monster hotspots were found, each piece of evidence was carefully examined, and significant efforts were made to decipher convoluted language and descriptions. The data was then evaluated to see if it was consistent. The most important information was kept, along with the presumptions that were based on it.

INTERNATIONAL JOURNAL OF TECHNO-ENGINEERING
IJTE

ISSN: 2057-5688

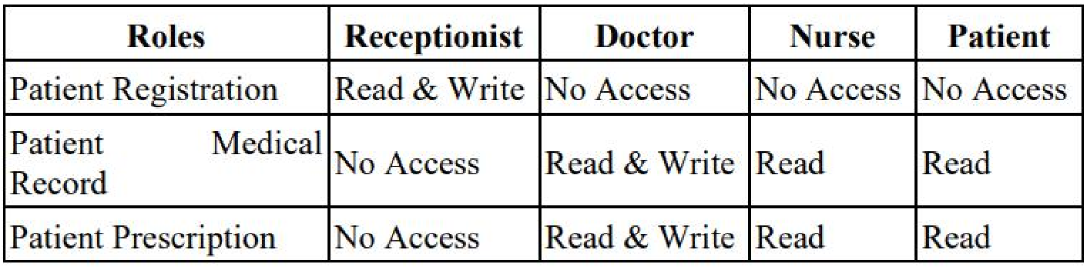
It may be challenging to maintain validity in research measures that incorporate data from several sources. Other sources included research papers, electronic databases, journal articles, data collection methods, and connection complaints. High impact journal articles were picked from all around the globe and either refereed or peer-reviewed to ensure validity. Representatives from renowned universities, social groups for educators, and mechanical organisations were contacted for further information. The analysis of several data sources produced valuable material, around thirty of which were pertinent evaluation reports. The delivery of clear contents at otherwise happy occasions, such as exam papers, summaries, extended developments, speeches, well-known copies, and other materials, was also considered as a reliable source of important information. The retention period for these systems was extended to eight years in order to eradicate outdated and obsolete data. Material that had been on display but hadn't been utilised for a while was thrown away.

HOMOLOGUE ENCRYPTION

The technique referred to as homomorphic encryption (HE) (4) permits sophisticated computations to be carried out with encrypted data, without compromising the security of encryption. In math, HE is a reference to the procedure of turning an existing dataset to another, with the same connections maintained between the elements in the two sets. The Greek terms that refer to "same structure" are where this phrase comes from. This is why logic-based calculations performed on encrypted or decoded data employ the same schema as the data used in this homomorphic encryption system.

4 EXPERIMENT AND RESULTS

Table 4.1 Access Control Policy Generation



Roles	Receptionist	Doctor	Nurse	Patient
Patient Registration	Read & Write	No Access	No Access	No Access
Patient Medical Record	No Access	Read & Write	Read	Read
Patient Prescription	No Access	Read & Write	Read	Read

Generation Key

An algorithm can be used to create keys in cryptography which is also known as key creation. Keys created by algorithm are typically used for encryption of data and decryption. A random choice of an integer "k" within between [1, N-1] gives an encrypted private key (keypr).The Generator function Gc as well as the public key (keypr) can be employed to establish that the private key (keypu).

Key generation in algorithm I

Generator function (Gc) as well as a random numbers (k) serve as two inputs.

Public Key (keypu) as well as Private Key (keypr) output

1. An random number will be selected from the number interval [1,n-1] in order to determine the private secret.

Keypr (private key) = K

Determine the your public key (keypu) is keypr*Gc the second step.

Encoding of Messages

Converting messages into elliptic curve points is known as message encryption. The ElGamal Curve (EGEC) techniques are unable to be used to decrypt or encode the input text information; they are able to only decrypt and encrypt points along the curvature. Think of an input message to be encrypted with the specified methods. The message input is divided into blocks of fixed size that are just one character. Each ASCII number is immediately converted to the Elliptic Curve point once each word in the text is transformed into the ASCII value.

Algorithm II: Encoding of Messages
input: message in plain text
Elliptic Curve points as output

ISSN: 2057-5688

To begin, you must divide messages into blocks of fixed size that are composed of one word.

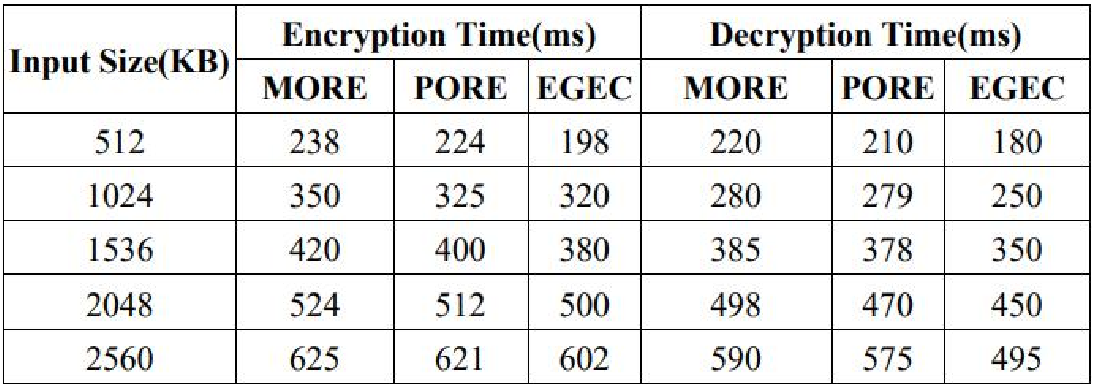
The second step is translating every text message character into the appropriate ASCII value.

3. Elliptic Curve points are instantly transformed to ASCII value.

Encryption using EGEC

An approach to convert plain text to cyphertext is known as encryption. The Elgamal-Elliptic curvature (EGEC) Homomorphic encryption system that is suggested in this work can secure plain text messages as well as increase security at the lowest cost. The data input to this method is the point on the curve (Pm) and keys for private and public (keypr) as well as keys for the public (keypu) to a particular chunk of text. The random 4-bit number "rn generated by the generator function, 'Gc can be used to generate the CipherText point "CT1'. This is then done by using the curve point "Pm" for a certain message block, the random number "rn," and thepublic key (keypu), CipherText point "CT2" is created. A collection of cypher text points is subjected to homomorphic computations using either the additive property or the multiplicative property. Finally, the cloud is used to store the encrypted point Ep= (CT1,CT2).

Table 4.2 Comparison of Encryption and Decryption time



Input Size(KB)	Encryption Time(ms)			Decryption Time(ms)		
	MORE	PORE	EGEC	MORE	PORE	EGEC
512	238	224	198	220	210	180
1024	350	325	320	280	279	250
1536	420	400	380	385	378	350
2048	524	512	500	498	470	450
2560	625	621	602	590	575	495

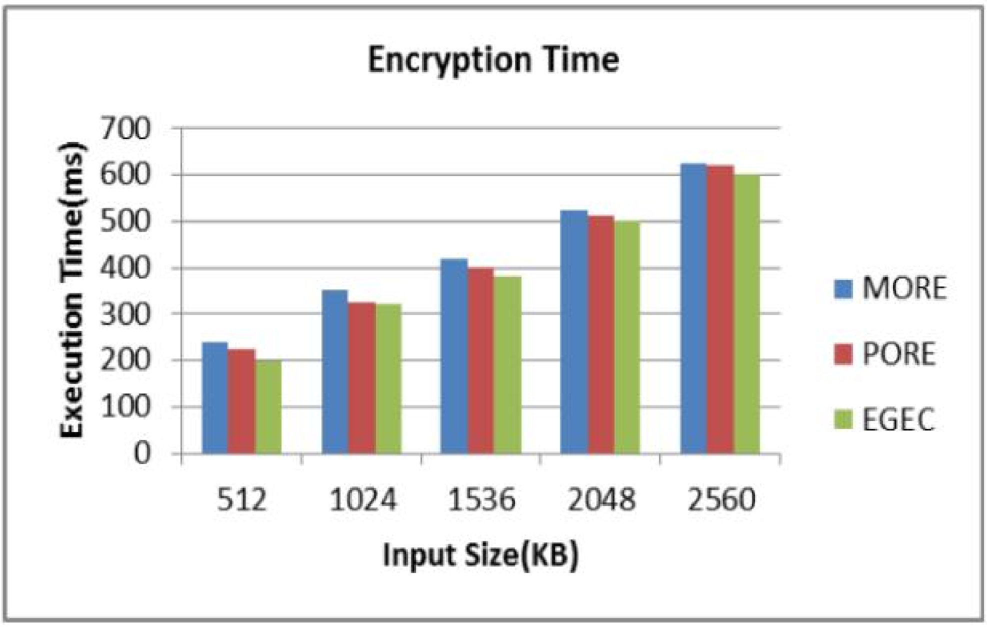


Figure 4.1 Comparison of Encryption Time

Decryption Time

The period of time that is required for the algorithm to convert the encrypted text into plain text is termed as decryption time. Milliseconds could be used as a way of describing the duration of decryption. Figure 4.5 shows the time taken to decrypt for the new EGEC method with the existing methods. Based on Table 4.7 it is apparent that current methods MORE use 220ms, 280ms and 385ms 498ms, 590ms and 220ms to encrypt input sizes that are 512KB, 102KB, 1536KB, 2048KB and 2560KB. On the other hand, PORE is 210ms long, 279ms long 3,78ms, 470ms and 575ms. The time to decrypt inputs of 512KB, 1024KB,1536KB, 2048KB and 2560KB when using the suggested EGEC homomorphic approach include 180ms and 250ms. 350ms, 400ms, and 495ms. In comparison to the current methods the proposed EGEC homomorphic technique offers a quicker decryption speed..

5 Conclusion

Partial homomorphic encryption was used in the creation of a secure EHR storage system for patient records. The PHE-BGN Cryptosystem is used to store sensitive patient data in the cloud while maintaining its confidentiality and integrity. Using the CRT and BSGS algorithms, the performance of the BGN crypto system is enhanced. The system's main benefits are that 1) EHRs are safely stored in the cloud and 2) EHRs are safe even while being transported since BGN Homomorphic encryption permits aggregate actions on the encrypted data. According to experimental findings, the BGN cryptosystem is more effective than the traditional Paillier Algorithm. Security of cloud-based data can be assured by ElGamal Elliptic curve homomorphic encryption which has been proposed. Six different processes are part of the suggested EGEC homomorphic encryption. These include key generation, message encryption, EGEC encryption, EGEC decryption and message decoding. When an end user wants access to the data in cloud storage it is the CSP confirms the access rights of that user. By using EGEC homomorphic encryption owner of the data secures the data. For encrypted data it is homomorphic process performed. In order to recover the original message to retrieve the original message, the EGEC encryption technique is employed. Time to execute, encryption time and decryption times and memory utilization along with encryption throughput as well as encryption throughput are employed to evaluate the efficacy for the proposed ElGamal Elliptic curve homomorphic encryption method. The system is compared to this proposed EGEC homomorphic encryption method as well as current systems like PORE and PORE.

6 REFERENCE:

1. Abbas, A & Khan, SU 2014, ‗A review on the state-of-the-art privacypreserving approaches in the e-Health clouds', IEEE Journal of Biomedical and Health Informatics, vol.18(4), pp. 1431–1441.

2. Abhijit V Banerjee, Rachel Glennerster & Esther Duflo 2008, ‗Putting a Band-Aid on a Corpse: Incentives for Nurses in the Indian Public Health Care System', Journal of the European Economic Association, vol. 6(2-3), pp. 487-500.

3. Acar, A, Aksu, H, Uluagac, AS & Conti, ε 2017, ‗A Survey on Homomorphic Encryption Schemes: Theory and Implementation', pp. 1–35. https://doi.org/10.1145/0000000.0000000.

4. Alabdulatif, I, Khalil, X, Yi & Guizani, ε 2019, ‗Secure Edge of

Things for Smart Healthcare Surveillance Framework,‘ in IEEE Access, vol. 7, pp. 31010-31021.

5. Alex Roehrs, Cristiano André da Costa & Rodrigo da Rosa Righi 2017, _OmniPHR: A distributed architecture model to integrate personal health records‘, Journal of Biomedical Informatics, vol. 71, pp. 70-81.

6. Alyami, ε 2017, _εanaging personal health records using meta-data and cloud storage.‘ IEEE/ACIS 16th International Conference on Computer and Information Science (ICIS) pp. 265-271.

7. Amlan εajumder, V & Upadhyay 2004, _n analysis of the primary health care system in India with focus on reproductive health Care services‘, ArthaBeekshan, vol.12(4), pp. 29-38.

8. Anthony Wellever, Gerald Hill & εichelle Casey 1998, _Commentary: M dicaid Reform Issues Affecting the Indian Health Care System‘, Public Health Policy Forum, vol.88(2), pp. 193-195.

9. Antonio Gonzalez-Perez, Raymond G Schlienger & Luis A García Rodríguez 2010, _Acute Pancreatitis in Association With Type 2 Diabetes and Antidiabetic Drugs, A population-based cohort study‘ Diabetes Care, vol.33, no. 12, pp. 2580-2585.

10. Aslett, LJM, Esperança, PM & Holmes, CC 2015, _A review of homomorphic encryption and software tools for encrypted statistical machine learning‘, pp. 1–21. Retrieved from http://arxiv.org/abs/ 1508. 06574.

11. Ateniese, G, Fu, K, Green, M & Hohenberger, S 2006, _Improved proxy re-encryption schemes with applications to secure distributed storage‘, ACM Transactions on Information and System Security, vol.9(1), pp. 1–30.

12. Awasthi, P, Mittal, S, Mukherjee, S & Limbasiya, T 2019, _A Protected Cloud Computation Algorithm Using Homomorphic Encryption for Preserving Data Integrity‘, In: Sa P, Bakshi S, Hatzilygeroudis I, Sahoo M. (eds) Recent Findings in Intelligent Computing Techniques. Advances in Intelligent Systems and Computing, vol. 707. Springer, Singapore

13. Bahga, A & εadisetti, VK 2013, _A cloud-based approach for interoperable electronic health records (EHRs)‘, IEEE J Biomed Health Inform. vol.17(5), pp. 894-906.

14. Bajpai, Nirupam & Goyal, Sangeeta 2004, ;Primary Health Care in India: Coverage and Quality Issues‘, CGSD Working Paper, vol.15, pp. 1-39.

15. Basu, S 2012, ‗Fusion: εanaging Healthcare Records at Cloud Scale,‘ in Computer, vol. 45, no. 11, pp. 42-49.

16. Bertrand, V, Smokvina, E, Masson, E & Bruel, H 2019, ‗Severe acute pancreatitis in a child with phenylketonuria,‘ Arch. Pédiatrie, vol. 26, no. 2, pp. 2018–2020.

17. Bitewulign Kassa Mekonnen, Webb Yang, Tung-Han Hsieh, ShienKueiLiaw, Fu-Liang Yang,

18. Bitewulign Kassa Mekonnen, Webb Yang, Tung-Han Hsieh, ShienKueiLiaw & Fu-δiang Yang 2020, ‗Accurate prediction of glucose concentration and identification of major contributing features from hardly distinguishable near-infrared spectroscopy,‘ Biomedical Signal Processing and Control, vol.59.

19. Bocu, R & Costache, C 2018, ‗A homomorphic encryption-based system for securely managing personal health metrics data‘, IBε Journal of Research and Development, vol. 62(1), pp.1:1-1:10.

20. Bondale, N, Kimbahune, S & Pande, A 2013, ‗mHEAδTHPHC: An ICT Tool for Primary Healthcare in India‘, IEEE Technology and Society Magazine, FALL 2013, pp. 31-38.

21. Camilla L Cunha, Alexandre R Torres & Aderval S Luna 2020, ‗εultivariate regression models obtaine d from near-infrared spectros copy data for prediction of the physical properties of biodiesel and its blends‘, Fuel, vol. 261, p.116344.

22. Chen, ε, Hao, Y, Hwang, K, Wang, δ & Wang, δ 2017, ‗Disease Prediction by Machine Learning Over Big Data From Healthcare Communities‘, in IEEE Access, vol. 5, pp. 8869-8879.