WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Medical Confidentiality And Data Privacy Using Homomorphism Encryption

Pavan Kalyan VR[1], Nagarjum KR[2], Y.Pranay[3], Suhas DP[4]

[1,2,3,4] Dept. of Computer Science and Engineering, SJC Institute of Technology, Chickballapur, India

ABSTRACT:

Secure data transmission and storage can be made possible by homomorphic encryption in computer systems. Cloud computing & cloud storage have brought about a huge transformation in how data is processed and utilized. Cloud computing has lead to a decrease in the number of staff and material resources required, thus making available a lot of them for use in other sectors. Outsourced applications are highly popular during this of cloud computing revolution. Clients upload data to the cloud anthem process it through its services.Though it has numerous advantages for customers, there is also the downside of their personal information being exposed to external service providers. Patient health records, electronic documents storing an individual's medical history, are usually managed and upheld by hospitals or other healthcare establishments within the healthcare industry. By letting patients be monitored out the clinical environment, personal health monitoring devices like commercially available wireless ECG patches can significantly reduce health care costs. Cloud storage is used by these devices to transmit important healthcare information that doctors find essential. The privacy laws that regulate patients' health information have made it difficult for medical cloud computing to be widely accepted despite its potentiality in transforming the healthcare industry. We propose a newmethod of medical cloud computing which eliminates the privacy concerns of cloud providers. Our technique uses homomorphic encryption, hence enabling operation on hidden health data without visualization of underlying data. We present an implementation for a feasibility study.

Keywords: Authorization, Privacy ,Dataprivacy ,Taxonomy ,Transforms,Homomorphic Encryption.

Introduction

This study aims to ensure the privacy of healthcare application data computations on public servers and improve the security of data produced by medical devices. Swift decision-making is critical in healthcare systems, especially for high-risk individuals dealing with post-diagnosis effects. However, many studies currently rely on cloudbased computations due to the abundance of processing and storage resources. This dependence on cloud processing can cause delays in returning results to devices, affecting prompt decision-making. With frequent medical data processing and exchange, communication overhead between the cloud and devices increases as data volume grows. When data is encrypted, homomorphicencryption stops hackers from reading. A lot of data and apps may be stored and shared online and on distant servers thanks to the useful technology known as cloud computing. Everyone wants to protect their data, but while using the cloud to store data, consumers must put their trust in other parties. Clients must rely on the cloud when their hardware for data storage is restricted. Clients must first download the data from the cloud before they can process it or do any computational operations on it. Therefore, our methodology offers a homomorphic method for carrying out computations on encrypted data. Since every patient wants their medical records to be shared between them and their doctor, we used a sample as medical data in our scheme.

Literature survey

Paper 1

Title: Challenges in Maintaining Patient Data Privacy   :
Author : Johnson, A., White, B., & Martinez, D.
Published on : 2020.
Description : The paper places significant emphasis on the challenges healthcare systems encounter in adapting to evolving privacy regulations and standards.

Paper 2

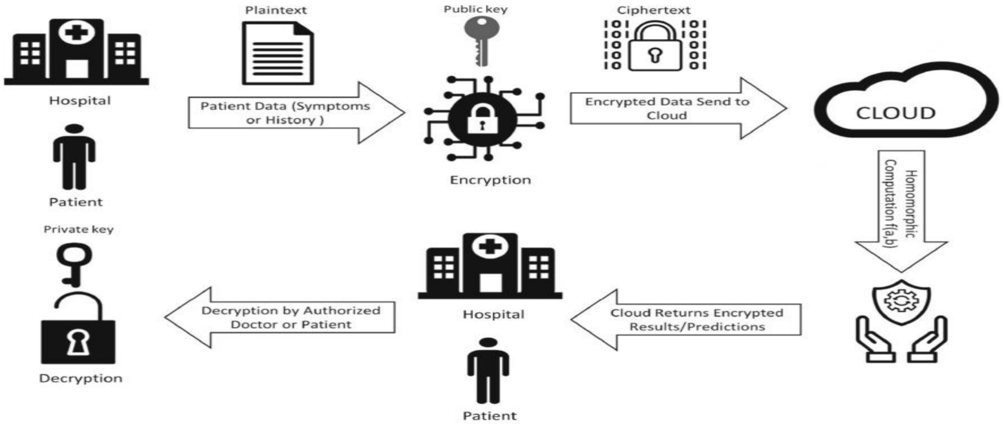
Title: Legal and Ethical Implications of Using Homomorphic Encryption in Healthcare
Author: : Anderson, M., Smith, P., & Jones, R.Author
Published on : 2017.
Description : This paper discusses the promises and challenges associated with targeted drug delivery systems, including those based on nanotechnology.

Paper 3

Title : “A Comparative Analysis of Privacy-Preserving Technologies in Healthcare”. Author : : Liu, Y., Zhang, X., & Wang, S.
Published on : 2020
Description : The paper begins with a thorough exploration of the privacy concerns prevalent in healthcare settings, highlighting the critical need for robust solutions.

DESIGN AND METHODOLOGY

One way to think of the systematic review process is a vehicle for addressing a specific research problem. No systematic review has yet been conducted on homomorphic cryptosystems in healthcare and bioinformatics; hence, the adoption of this particular research approach. Moreover, I undertook this systematic review so as to fill this crucial gap. Kitchenham and Brereton’s recommendations are selected to evaluate and explain every research question about homomorphic encryption. This work is led by Craig Gentry’s groundbreaking work. Additionally, it offers motivation that fully homomorphic encryption will be important for the healthcare sector since it can keep patients’ health data completely private. A simple understanding of the processes outlined above will help us understand the systematic review process Different research questions were identified. Develop an evaluation process: Determine in advance the type of research that will be included, as well as the data collection, evaluation, and analysis procedures Research ID Following Gentry's groundbreaking work on homomorphic encryption, several homomorphic encryption methods in healthcare Numerous works on computational biology, as it is sometimes referred to, have been published. Despite the abundance of studies on homomorphic encryption, there has not been any review that evaluates the quality of research in this field. Extracts: Articles considered were restricted only to relevant ones while all irrelevant papers were disqualified from inclusion. Data synthesis: This step graphical form and involves presenting data in descriptive. By doing so, an overview of the results may be done with ease. Research Quality Rating: Homomorphic encryption was used as a keyword to search for basic homomorphic approaches among research articles downloaded from popular repositories. Application of Knowledge: The results and information about Exam will be disseminated to appropriate parties such as target groups through different Medial Security aspects are most important when it belongs to cloud computing


Hospital
Patient
Plaintext
Patient Data (Symptoms or History)
Public key
Encryption
Ciphertext
Encrypted Data Send to Cloud
CLOUD
Homomorphic Computation f(a,b)
Private key
Decryption
Decryption by Authorized Doctor or Patient
Hospital
Patient
Cloud Returns Encrypted Results/Predictions

3.1 Architecture of Homomorphic encryption in healthcare

The major challenge is that third-party service providers become able to access data for processing and automation purposes every day. Each corporation or agency wants to know what personal and sensitive data their consumers have got .Every company Policies are developed by various organizations that may be government, business, healthcare and academic institutions based on data. collected. Cloud computing is mostly concerned with safety. That problem arises because third parties can access and analyze the data. Every company or organization in existence wants to understand its users’ private and sensitive information. Data is essential for organizations across various sectors, including government, private enterprise, healthcare, and academia, serving purposes such as policy-making, research, and strategic planning. Privacy concerns, particularly in healthcare, are paramount, highlighted by a survey conducted by Acumen Research and Consulting, forecasting that the healthcare cloud computing market will surpass. Healthcare cloud computing enhances efficiency and cost-effectiveness, offering swift operations while safeguarding sensitive patient data remains crucial. This protection not only instills confidence among patients but also contributes to economic growth. Electronic Medical Records (EMR) hold the potential for delivering superior quality care at reduced costs by enhancing care coordination and minimizing errors. However, patient's files contain much crucial information pertaining to their health life styles etcetera Thus they should have an easy way of allowing a few trusted organizations within the health care system to get hold of such protected health information promptly without any unnecessary steps involving more than simple yet effective security measures that are reliable too. The remainder of this article is organized as follows: the evaluation methods, planning, inclusion and exclusion criteria, and motivated research questions are presented in the next sections. Comparing homomorphic encryption techniques beginning with partially homomorphic encryption method followed by partially and fully homomorphic encryption methods respectively is done in the next section. There are four types of fully homomorphic encryption techniques that have been classified and compared using important approaches in each category.

Advantages and Applications

1.1 Advantages

1. Privacy preservation.
2. Data security .
3. Compliance.
4. Secure collaboration.
5. Trust building
6. versatility.

1.2 Applications

1. Medical research.
2. Healthcare analytics.
3. telemedicine.
4. Genomic data analysis.
5. Healthcare billing and administration.

Conclusion

There has been a great deal of study in computational sciences on Homomorphic Encryption because it is an important computing topic. This forms the basis for why it is an important concept. It can be noted that all three techniques, that is, fully, somewhat and partially homomorphic encryption enables secure communication, storage, and processing of encrypted data without compromising the confidentiality of information. The impact of this technology can be witnessed in various sectors within the financial industry being one of several cases in point. They have adopted homomorphic encryption as they conduct their researches which will go down well with them in utilizing it to their advantages in coming years. For data privacy is more necessary than ever in this internet world. Cloud computing revolution has necessitated a high demand for outsourcing applications. To use the service, customers upload their data to the cloud and it is evaluated to give results. This helps consumers and exposes some of those valuable data to third parties' service providers. Nevertheless, the trouble with encrypted information is that it must be decrypted before it can be used. Being decrypted, it becomes susceptible to any security measures put in place. Moving forward, homomorphic encryption could potentially serve as a proper solution for this challenge whereby data can be computed on yet remain secure at all times. Homomorphic Encryption (HE) was an idea that came into existence about 30 years ago but since then there have been rapid improvements in the field of HE that has seen Gentry's groundbreaking research turning into workable implementations we see today. The digitization of patient medical records is expected to improve the quality of care while reducing its costs and enhancing efficiency. On the other hand, Electronic Health Records (EHRs) contain a large volume of sensitive information that can be accessed by not only physicians but also other entities such as insurance companies and employees among others. EHR administration plays important role in addressing issues related to data security. What are the crucial elements needed for successful implementation of homomorphic encryption Four different divisions have been made with regard to homomorphic encryption technique and the significant techniques in each division are compared . To end, HE methods in health and foremost bioinformatics have been accessed, looking at LQTC, cancer, average heart rate, cardiovascular problems and secured query generation systems. safety in medicine field. Generally speaking, homomorphic encryption will be useful for healthcare industry as its efficiency and effectiveness improve.

REFERENCES

[1] Javed, A.R.; Sarwar, M.U.; Beg, M.O.; Asim, M.; Baker, T.; Tawfik, H. A collaborative healthcare framework for shared healthcare plan with ambient intelligence. Hum.-Cent. Comput. Inf. Sci. 2020, 10, 1–21

[2] Sun, Y., Liu, Q., Chen, X., & Du, X. (2020). An adaptive authenticated data structure with privacy1preserving for big data stream in cloud. IEEE Transactions on Information Forensics and Security, 15, 3295-3310

[3] Chenthara, S., Ahmed, K., Wang, H., & Whittaker, F. (2019). Security and privacy-preserving challenges of e-health solutions in cloud computing. IEEE access, 7, 74361-74382

[4] Paillier, P. Public-key cryptosystems based on composite degree residuosity classes. In Proceedings of the International conference on the theory and applications of cryptographic techniques, Prague, Czech Republic, 2–6 May 1999; pp. 223–238

[5] Singh, V.K.; Chandna, H.; Kumar, A.; Kumar, S.; Upadhyay, N.; Utkarsh, K. IoT-Q-Band: A low cost internet of things based wearable band to detect and track absconding COVID-19 quarantine subjects. EAI Endorsed Trans. Internet Things 2020, 6