Cloud Based Privacy Preserving Data Encryption

Akash Kumar[1], Dr. Bhuvana J[2]

[1]Professor, School of CS & IT, Jain University, Bangalore, India.
[2]MCA, School of CS & IT, Jain University, Bangalore, India.

Abstract – *The purpose of this paper is to improve Data Security which will be uploaded by the data owner in encrypted format and will later be converted to encrypted form. In this paper, we consider multi-file system encryption where multiple data providers such as hospitals and physicians are authorized by individual data owners to upload their personal health data to a trusted public cloud. Health data is sent in encrypted form to ensure data security, and each data provider also sends encrypted data references to enable queries to encrypted data. We propose a Multi-Source Order-Preserving Symmetric Encryption (MOPSE) novel system where the cloud can integrate encrypted data tracks for multiple data providers without knowing the content of the index. MOPSE enables effective query processing and confidentiality where a data user can send a single data query that they can process to encrypted data from all related data providers without knowing the content of the query. We also propose an advanced scheme, MOPSE +, to effectively support data queries by successive data providers. Extensive analysis and real-world site testing demonstrates the effectiveness and efficiency of MOPSE and MOPSE +.*

Key words: AWS, Cloud Based, MySQL, Database, Javascript, HTML, CSS, AES

1. INTRODUCTION

New revolving technologies in hardware, middleware, virtual machine and distributed systems are needed to meet the growing needs of the information . Such technology should meet the need for all types of clients from individuals and organizations. All of these services can be provided by cloud computing as they provide platform, infrastructure and software as a service using the technologies mentioned above. This is a payment model as you go. As these technologies require resources, network, hardware and virtualization on a larger scale than the integration of all technical issues leads to a complete loop in the systems. Among all the problems associated with cloud computing we focus on issues of user privacy and data securities. Cloud computing emerges as a new computer paradigm in the field of healthcare among other business domains. Many health care companies have begun to transform electronic health information into a cloud. Introducing cloud services in the health sector is not just a matter of exchanging electronic medical records. In addition, switching to cloud-based environment rehabilitates a health care organization with tedious infrastructure management activities and reduces the cost of development and preservation. However, maintaining patient privacy concerns should be considered important when designing safety and confidentiality guidelines. Various methods have been used to protect the privacy of health information in the cloud environment. This study aims to integrate sophisticated privacy protection techniques used in e-health clouds. In addition, privacy sensitive methods are classified as encryption and cryptographic methods, and are assigned to the category categories. Additionally, the strengths and weaknesses of the provided methods are reported and some open issues are highlighted.

2. PROBLEM STATEMENT

In this project, we aim to identify effective schemes for storing patient information. In this case the owner will upload the files in encrypted format and can be accessed later. That data will be sent to the cloud and can be accessed by hospitals and even cell phones we can access. Later uploaded files will be encrypted. We can create flexible patient requests to complete through schemes:

MOPSE enables effective query processing and confidentiality where a data user can submit a single data query that they can process to encrypted data from all related data providers without knowing the content of the query.

We also propose an advanced scheme, MOPSE +, to effectively support data queries by successive data providers.

Extensive analysis and evaluation of the actual database demonstrates the effectiveness and efficiency of MOPSE and MOPSE +.

3. LITERATURE WORK

[1] Assisted Cloud Health Care Surveillance System For compression, wireless nerves are increasingly being used to record / collect information on health care organisation . To get the right resource data, one big practice today is to use compression sensitivity, as it involves sampling normal data and congestion. Despite growing popularity, the ever-present way of processing data of health care and protecting data privacy at the same time, while maintaining low sensitivity, remains a challenge. To solve the problem, we propose a cloud-based healthcare monitoring system using a pressure sensor, which combines different domain strategies with

the following advantage. By design, sensitive data samples never leave the nerves in an unsafe state. Protected samples are then sent to the cloud, to be stored, processed, and distributed and recycled data to recipients. The system ensures privacy when the cloud does not see real samples or basic data. Handles small and standard data, as well as audio-interrupted data. Visual and visual inspections indicate that the system gains privacy verification, efficiency, efficiency, and time-saving services.

[2] HCPP: The Cryptography Based Secure EHR System for Patient Confidentiality and Emergency Medical Care is undoubtedly a major obstacle to the delivery of electronic health records (EHR) records that are considered to be highly efficient, less prone to errors, and additionally accessible than standard paper recording systems. Patients are unwilling to accept an EHR system unless their protected health information (PHI) containing highly confidential data is guaranteed for proper use and disclosure, which cannot be easily achieved without controlling the patient in his or her PHI. However, caution should be exercised when dealing with emergencies where a patient may not be able to regain a controlled PHI in order to receive emergency treatment. In this paper, we propose a secure EHR system, HCPP (Patient Privacy Care Program), based on cryptographic design and existing wireless network infrastructure, to provide privacy protection to patients under any circumstances while allowing timely PHI detection for treatment. which saves lives. for emergencies. Additionally, our HCPP system limits PHI access to authorized physicians (not negligently), who may not be tracked and accountable if the diagnosed PHI is found to be inappropriate disclosure. Lastly, HCPP uses wireless network access to support the confidentiality / access of PHI, which is under a secure and feasible EHR system.

[3] Search Cloud Computing Records Keyword Records Your Health Recently, uploaded data has emerged as a patient-centered model for exchanging health information, which includes keeping all records in one place, as a single person. cloud service provider. While this is very helpful in managing and sharing patient health information (PHI), there has been considerable concern about whether these service providers can be fully relied upon to manage a critical patient PHI. To ensure patients' control over their privacy, data encryption has been proposed as a promising solution. However, important service functions such as keyword search by many users are especially challenging with encrypted data. Basically, user queries should be done in a confidential manner that hides both keywords in the queries and documents. More importantly, in order to prevent unnecessary exposure of patients' PHI to unlimited questioning power, each user's questionnaire needs to be authorized and controlled in a straightforward manner, which will be achieved with a high level of systematic assessment. Available search encryption functions cannot meet the above requirements simultaneously.

In this paper, we create and address a keyword search (APKS) encrypted on cloud computing sites. We present a downtime and an encrypted search framework, in which users derive the power of queries from trusted local authorities based on their attributes, which are very high in the user rating. We then propose two APKS novel solutions based on the latest cryptographic primitive encryption, hierarchical predicate (HPE) encryption, one of which is highly efficient and the other encrypted. In addition to the privacy of the text and the privacy of the queries, other notable features of our programs include: multi-sided keyword support that works, with a variety of simple queries, allowing for the submission and acquisition of search capabilities. We use our system in a modern work environment, and test results show its suitability for practical use.

[4] Eliver Control Encryption: Ensuring the Privacy of Electronic Medical Records. We argue that security in such systems should be exercised by encryption and access control. In addition, we oppose systems that allow patients to generate and store encryption keys, so that patient privacy is protected in the event that the host data center is compromised. A common argument against such a method is that encryption would interfere with system performance. However, it does show that we can create an effective system that allows patients to share partial access rights with others, and to conduct searches through their records. We have officially implemented the requirements of the Patient-Managed Encryption System, and provided a few presentations, based on available hidden resources and agreements, each receiving a different set of properties.

[5] Effective and Secure Sharing of Health Records in Cloud Computing using Quality-Based Encryption.

A personal health record is kept in one place for the keeping of personal information and patient diagnosis. The health record is a growing model that focuses on patient exchange of health information, which is often released to be stored on an external company, such as cloud providers. However, there have been widespread privacy concerns as personal health information may be disclosed to those third-party servers and to unauthorized persons. Security schemes are used to protect data from public access. Ensuring patient control of access to their information, is a promising way to encrypt before removing Servers. However, problems such as risks of privacy disclosure, downtime in critical management, flexible access and effective user withdrawal, remain the most important challenge in achieving well-designed, privately enforced data access control. In order to obtain well-analyzed and measurable data access controls, we use attribute-based (ABE) encryption techniques to encrypt each patient's file. The data owner updates personal data into third-party cloud

data centers. Many data owners can access the same data values. It differs from previous functions in secure data extraction, focuses on the status of multiple data holders, and separates users from a system with multiple security domains that significantly reduce the administrative complexity that is important for owners and users. A high level of patient privacy is guaranteed at the same time with strong ABE. Our system also enables flexible modification of accessibility policies or file attributes, support for user extensions / active identifiers and glass access under emergencies.

4. DISCUSSION

In our paper, here we have created a cloud-based app to load that data in an efficient way to tackle the health recording system. Cloud provides us with a flexible feature, using a computer cloud is essential in helping businesses and individuals identify and deliver the promise of digital change.

Using HTML, cascade, and java script I created my own interactive app. and we can use the loping feature in HTML because we can use long slide code or any module we have to repeat. MySQL provides data storage on the website.

The final user flow of my model cover i.e., user / customer. Here the owner can upload the files in encrypted format and they will be deleted from encrypted users.

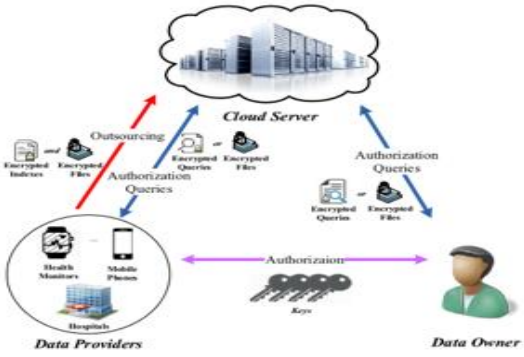

Figure: 1.1 Performance Model

Data will flow as the owner begins to upload the file to the cloud in encrypted format where authorization questions will be collected. Later that data will be provided to hospitals, Cell Phones.

5. Conclusion

In this paper, we explore the problem of encrypting multiple choice questions in the cloud-based PHR environment. Unlike previous functions, our MEIM proposed method allows a certified data holder to access secure, relevant, and effective query data for multiple data providers. To address the practical question, we introduced MDBT as a data framework. To reduce the productivity question of the data owner, and allow the cloud server to ask securely, we recommend a novel symmetric encryption system for mass storage (MOPSE). To make our model more efficient, we propose a very sophisticated symmetric encryption system (MOPSE +) to satisfy a statistically valid question. In addition, we use strong security evidence to prove that our systems are secure. Finally, we demonstrate that the MEIM method works best on a computer by using our schemes and operating on virtual storage.

Although our work only focuses on Encrypting and clearing data system encryption, it can be expanded by looking at various scenarios, mobile data collection, recommendation system, and so on. However, devices, such as cell phones, have limited memory and memory function. In all of this, we will discuss low-cost schemes in our future work.

REFERENCES:

[1] C. Wang, B. Zhang, K. Ren, J. Roveda, C. Chen, Z. Xu, "A health care monitoring system assisted in the recognition of privacy and oppressive behavior," at INFOCOM'14, Toronto, Canada, 2014.

[2] J. Sun, X. Zhu, C. Zhang, Y. Fang, "HCPP: A Cryptography based secureehr system for patient privacy and emergency medical care," at ICCDCS'11, Minneapolis, Minnesota, 2011.

[3] M. Li, S. Yu, N. Cao, W. Lou, "Private data search keywords are enabled in cloud computing," at ICCDCS'11, Minneapolis, Minnesota, 2011.

[4] J. Benaloh, M. Chase, E. Horvitz, K. Lauter, "Patient Management: Ensuring the Privacy of Electronic Medical Records," at: ACM CCS'09 Workshop, New York, NY, 2009.

[5] M. Li, S. Yu, Y. Zheng, K. Ren, W. Lou. 24, no. 1, pages 131 - 143, 2013.

[6] M. Li, S. Yu, K. Ren, W. Lou, "Protecting personal health records from cloudcomputing: Managing patient access to fine and refined data in multiple owner settings," at SecureComm'10, Singapore, 2010 .

[7] X. Ma, Y. Zhu, X. Li, "An efficient and secure ridge regression outsourcingscheme for wearable devices," Computer & Electrical Engineering, 2017, DOI: 10.1016 / j.compeleceng.2017.07.019.

[8] J. Liu, X. Huang, J. Liu, "Secure sharing of personal health records in incloud computing: a signature-based signature-based policy," FutureGener Comp Sy. , Vol. 52, pages 67-76, 2015.

[9] P. Scheuermann, M. Ouksel, "Multidimensional B-trees for associativesearch in the data system," Inform Syst., Vol. 7, no. 2, pages 123 - 137,1982.

[10] K. Xue, J. Hong, Y. Xue, D. Wei, N. Yu, P. Hong, "CABE: A NewComparable Attribute-based Encryption Construction with 0-Encodingand 1-Encoding," IEEE Trans Comput. , vol. 66, nxa. 9, pages 1491 - 1503,2017.