Shodhshauryam, International Scientific Refereed Research Journal
Available online at : www.shisrrj.com
OPEN ACCESS
© 2024 SHISRRJ | Volume 7 | Issue 2
ISSN : 2581-6306
doi : https://doi.org/10.32628/SHISRRJ

An Approach for Protected Exchange of Individual Medical Data in the Cloud Environment

Prof. Mrs. B. Rupa Devi[1], B. Madhuri Deekshitha[2]

[1]Associate Professor, Department of MCA, Annamacharya Institute of Technology & Sciences, Tirupati, Andhra Pradesh, India

[2]Post Graduate, Department of MCA, Annamacharya Institute of Technology & Sciences, Tirupati, Andhra Pradesh, India

Article Info

Publication Issue :
March-April-2024
Volume 7, Issue 2

Page Number : 195-203

Article History
Received : 15 March 2024
Published : 30 March 2024

ABSTRACT

The wide relinquishment of cloud- grounded results in the healthcare sphere has paved the way for cost-effective and accessible exchange of Personal Health Records(PHRs) among colorful realities involved ine-Health systems. still, storing sensitive medical data on cloud servers exposes it to implicit exposure or theft, challenging the development of methodologies that guard the sequestration of PHRs. Accordingly, we propose an approach called SeSPHR for secure sharing of PHRs in the cloud terrain. The SeSPHR scheme ensures patient- centric control over PHRs and maintains the confidentiality of these records. Cases store translated PHRs on untrusted cloud servers and widely grant access to different types of users for specific portions of the PHRs. Asemi-trusted conciliator, nominated the Setup andRe-encryption Garçon(SRS), is introduced to induce public/ private key dyads and producere-encryption keys. likewise, the methodology is secure against bigwig pitfalls and tools forward and backward access control.

Keywords: Personal Health Records,E-Health, Cloud, Key

I. INTRODUCTION

While the cloud offers scalable, nimble, cost-effective, and ubiquitous services, enterprises related to the sequestration of health data also . A major reason for cases' apprehensions regarding the confidentiality of PHRs is the essential nature of the cloud to partake and store these records [10]. Storing private medical information on cloud servers managed by third- party realities makes it susceptible to unauthorized access. Particularly, the sequestration of PHRs stored in public shadows operated by marketable service providers is extremely vulnerable. The confidentiality of PHRs can be compromised in several ways, similar as theft, loss, and leakage[7]. The PHRs, either in cloud

storehouse or in conveyance from the case to the cloud or from the cloud to any other stoner, may be exposed to unauthorized access due. likewise, there are also implicit pitfalls from licit interposers to the data[6].

For case, the PHRs, either in cloud storehouse or in conveyance, may be susceptible to unauthorized access because of the external realities. individualities employed by the cloud service provider can act virulently. A notable illustration of this is an incident where an hand of theU.S. Department of Veterans Affairs carried home sensitive particular health information of around26.5 million individualities without authorization. The Health Insurance Portability and Responsibility Act(HIPAA) authorizations that the integrity and confidentiality of electronic health information stored by healthcare providers must be defended by conditions of use and exposure, and with the authorization of cases. also, while PHRs are stored on third- party cloud storehouse, they should be translated in such a way that neither the cloud garçon providers nor unauthorized realities can pierce them. rather, only realities or individualities with the' right - to- know' honor should be suitable to pierce the PHRs. also, the medium for granting access to PHRs should be administered by the cases themselves to help any unauthorized variations or abuse of data when it's transferred to other stakeholders in the health cloud terrain[8].

Unlike the approach presented in[5] that proposes the operation of multiple keys by the PHR possessors, leading to charges at their end, the SeSPHR methodology avoids this outflow by delegating the task of setting up public/ private key dyads and producing decryption keys to the authorized users only to a Setup andRe-encryption Garçon(SRS). Considering the cloud servers as untrusted realities, the methodology introduces a semi-trusted garçon, the SRS, as a deputy. A deputyre-encryption-based approach is employed by the SRS to inducere-encryption keys for secure sharing of PHRs among users. The PHRs are translated by the cases or PHR possessors, and only the authorized users enjoying keys issued by the SRS can decipher them. likewise, users are granted access to specific portions of PHRs supposed important by the PHR proprietor.

II. LITERATURE SURVEY

In [1], The contemporary rapid-fire expansion of Internet- grounded technologies has sparked a revolution in network- centric operations. An connected terrain farther energies the confluence of colorful ways, similar as edge computing, cloud computing, and the Internet of effects(IoT). sequestration enterprises have surfaced throughout the data transmission process, some of which stem from insecure communication protocols. In practice, high- security protection protocols generally bear advanced computing coffers due to increased computational loads and communication manipulations. The perpetration of secure dispatches becomes grueling when dealing with large data volumes. This work addresses the conflict between sequestration safekeeping and effectiveness, proposing a new approach for enabling advanced-position secure transmissions throughmulti-channel dispatches.

In [7], The recent preface of the" Health Insurance Marketplace" conception, designed to grease the purchase of health insurance by enabling comparisons among different plans in terms of price,

content benefits, and quality, assigns a pivotal part to health insurance providers. presently, the web-grounded tools available for searching health insurance plans are deficient in offering individualized recommendations grounded on content benefits and cost. thus, anticipating users' requirements, propose a cloud- grounded frame that provides individualized recommendations about health insurance plans. employMulti-attribute Utility Theory(MAUT) to help users in comparing different health insurance plans grounded on content and cost criteria, similar as(a) decoration,(b)co-payment,(c) deductibles,(d)co-insurance, and(e) maximum benefit offered by a plan. To overcome implicit issues arising from miscellaneous data formats and different plan representations across providers, we present a standardized representation for health insurance plans. The plan information of each provider is recaptured using Data as a Service(DaaS). The frame is enforced as Software as a Service(SaaS) to offer tailored recommendations by applying a ranking fashion to the linked plans according to stoner- specified criteria.

In [8], Mobile bias have limited computational capabilities, exploration associations and academia to concentrate on computationally secure schemes that can discharge computationally ferocious data access operations to the cloud or a trusted reality for prosecution. utmost being security schemes, similar as deputyre-encryption, director- grounded re-encryption, and cloud- grounded re-encryption, are grounded on the El- Gamal cryptosystem for unpacking computationally ferocious data access operations to the cloud or a trusted reality. still, the resource-empty pairing- grounded cryptographic operations

In recent times, healthcare providers are more likely to shift their electronic medical record systems to the cloud, as mentioned in [9] of Modern healthcare environments. Instead of building and managing separate data centers, this approach enables them to reduce operational expenses and improve compatibility with other healthcare providers. However, the implementation of cloud computing in healthcare systems may bring about different security difficulties linked to verifying one's identity, managing identities, controlling access, managing trust, and more. This article discusses the problems related to controlling access in cloud-based electronic medical record systems. We suggest implementing a structured method for controlling access to composite electronic health records (EHRs) in the cloud. This mechanism will enable the selective sharing of EHRs that are combined from different healthcare providers. Our method guarantees that privacy issues are taken into consideration during the processing of patients' healthcare information access requests.

In[10], In the field of healthcare, as well as other industries, cloud computing is becoming a new and innovative way of computing. Many health organizations have started moving their electronic health information to the cloud environment. Introducing cloud services in the healthcare industry not only simplifies the sharing of electronic medical records between medical facilities, but also allows the cloud to function as a storage system for medical records. Additionally, shifting to the cloud environment alleviates healthcare organizations from the burdensome responsibilities of overseeing infrastructure and reduces expenses related to development and upkeep. However, there are significant risks to data privacy when patient health data is stored on

servers owned by third-party entities. When designing security and privacy mechanisms, it is crucial to prioritize patients' privacy concerns, as there is a risk of medical records stored and shared in the cloud being exposed. Different methods have been used to protect the confidentiality of medical data in the cloud setting. This survey seeks to cover the latest methods used to protect privacy in e-Health clouds. Furthermore, the methods of preserving privacy can be divided into two categories: cryptographic and non-cryptographic techniques. Additionally, a classification system for these approaches is also provided. Furthermore, the article includes an analysis of the advantages and disadvantages of the approaches discussed, and brings attention to several unresolved matters.

III. PROPOSED SYSTEM

The system being suggested or put forth for consideration. In comparison to other constructions, the suggested method is considered secure because the proposed framework ensures that the Setup and Re-encryption Server (SRS) never obtains the Personal Health Record (PHR) data. However, the role of the SRS is to handle the management of keys. Encryption tasks are performed by the owners of the PHR, and the process of decryption is undertaken by authorized users who possess the appropriate decryption keys. The suggested method also compels control over both forward and backward access. Newly added individuals in a specific user community receive access keys from the SRS. The data that is being shared is protected by encryption, and only the owner of the data can access it using their own keys. New members are given access to the data once the owner of the PHR approves it. Likewise, a user who is leaving is taken off the ACL (Access Control List), and the relevant keys for that user are erased. When the user keys are deleted and their access is removed from the ACL, any unauthorized attempts to access the PHR will be denied after the user has left. We also carried out a comprehensive assessment of the suggested plan through the utilization of High-Level Petri Nets (HLPN) and the Z language. HLPN is used for two purposes - to imitate the system and to explore the system's behavior using mathematical properties. The SMT-Lib and Z3 solver are used to conduct the verification process.

The process of verification using SMT involves converting the Petri net model and its specific properties into SMT format. This is followed by using the Z3 solver to check if the properties are true or false.

Here are the main contributions of the proposed work:

- We introduce a technique known as SeSPHR, which enables patients to manage the distribution of their personal health records (PHRs) on the cloud. The use of El-Gamal encryption and proxy re-encryption in the SeSPHR methodology guarantees the confidentiality of personal health records (PHR).
- The method enables PHR owners to choose which users can access certain parts of their PHRs, depending on the specified access level in the ACL for different groups of users.
- A partially trusted proxy known as SRS is used to guarantee access control and create re-encryption keys for various user groups, eliminating the need for the PHR owner to handle key management tasks.

- The proposed methodology includes the implementation of both forward and backward access control.
- We conduct formal analysis and verification of the suggested approach to ensure that it operates effectively in line with the given specifications.

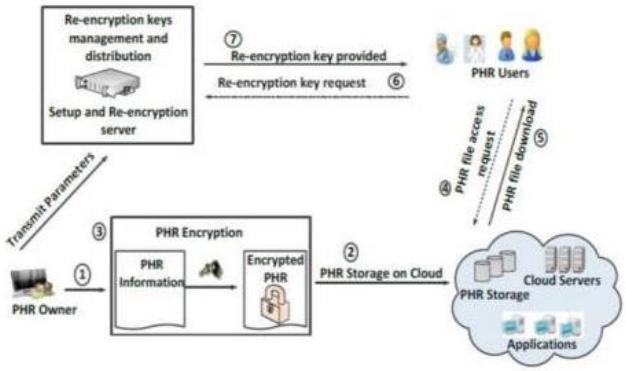

Fig 1. Proposed System Architecture

IV. RESULTS AND DISCUSSION

The outcome and analysis of the research findings are presented in this section. The effectiveness of the SeSPHR methodology, which allows for secure sharing of personal health records (PHRs) among various users, was assessed through the creation of a Java-based client application. The entities included in the proposed SeSPHR methodology consist of the cloud, the SRS, and the users. The task of generating public/private key pairs and re-encryption keys is carried out by a third-party server, known as the SRS. The PHR data was encrypted using the JPBC library for Java-based Pairing Based Cryptography. Unlike the usual pattern of longer key generation time as the number of users increases, it is noticeable that the rise in key generation time is not consistent as the number of users grows.

For example, it takes 0.6 seconds to generate keys for 10 users, but the key generation time increases to 0.97 seconds when generating keys for 100 users. In comparison, it is found that generating keys for 10,000 users takes approximately 2.16 seconds, which is a reasonable amount of time considering the large number of users. The time taken to generate keys for new members who are joining occasionally is very short and efficient, as it only needs to be done for one user at a time.

The researchers also assessed the amount of time it took to encrypt and decrypt data files of different sizes using the SeSPHR methodology. For the experimentation, different file sizes were used, including 50 KB, 100 KB, 200 KB, 500 KB, 800 KB, 1024 KB, 1500 KB, and 2048 KB. The amount of time taken for both the encryption and decryption processes for the mentioned file sizes is indicated. According to our observations, when the size of the PHR file increases, the time it takes for encryption also increases. For instance, it takes 0.13 seconds to encrypt a file of 50 KB, while it takes 1.289 seconds to encrypt a file of 2 MB.

Data encryption for users on public domains as well as those on personal/private domains is the owners' responsibility. Users in the public domain include doctors, researchers, pharmacists, and any other users approved by the PHR owner; users in the personal/private domain, on the other hand, are usually more numerous than those in the public domain. In the personal domain, users are limited to the patients' families or friends. For users in the personal domain, the key distribution complexity of SeSPHR is O(1), the same as other comparison approaches; for users in the public domain, it is O(PuG/p). While the methodologies given depend on the universe of role attributes and data attributes

for various users, the public and private key sizes utilized in SeSPHR are fixed. The product determines the level of decryption complexity for SeSPHR.

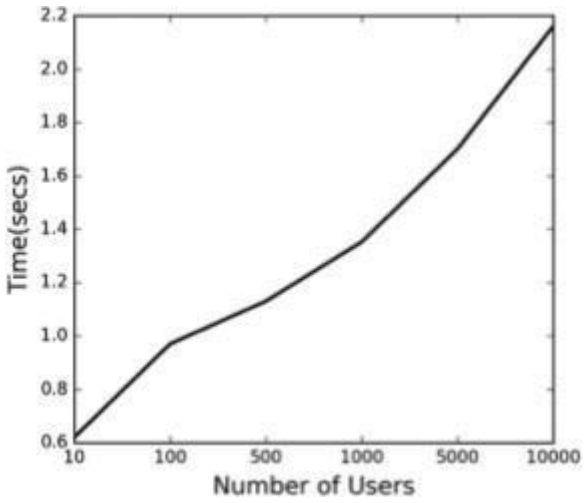

Fig 2. Result Analysis

The results of this paper are as follows :

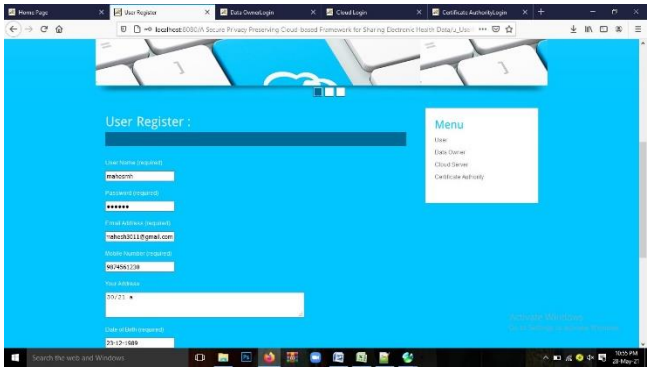

Fig 3. User registration

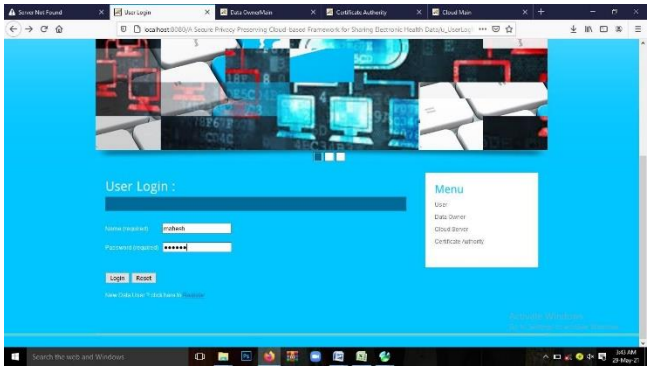

Fig 4. Data user login page

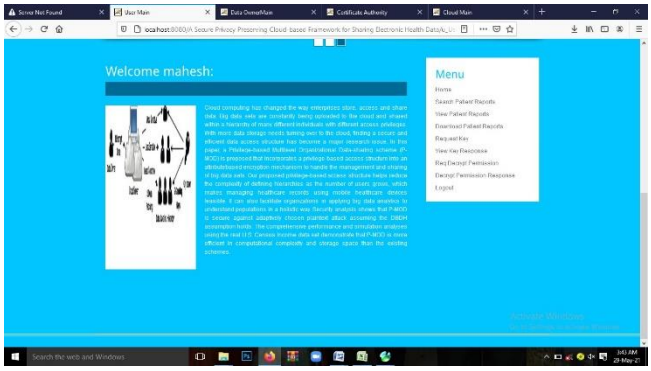

Fig 5. Home page data user

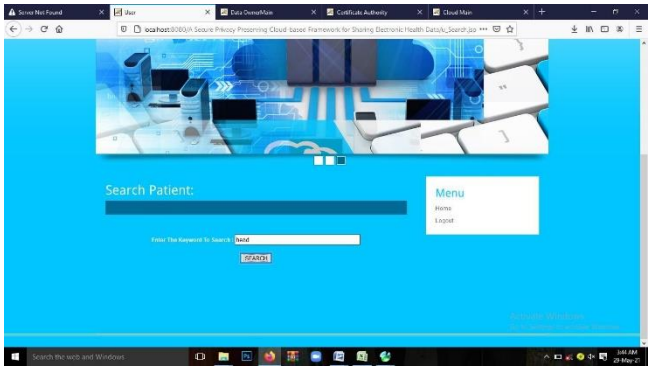

Fig 6. Search patient

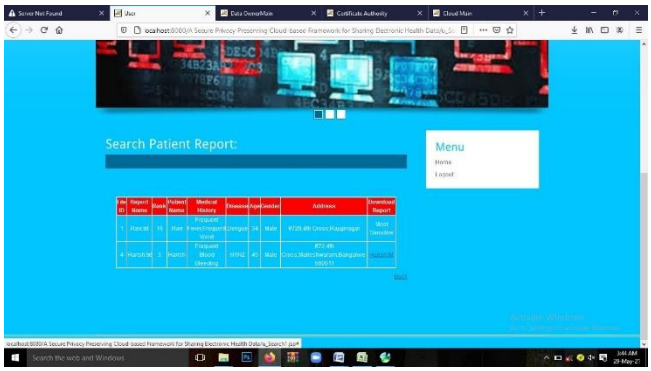

Fig 7. Search patient list

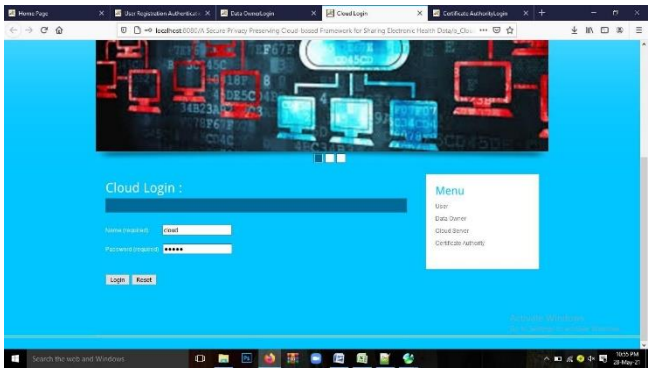

Fig 8. Cloud server login

Fig 9. Cloud server home page

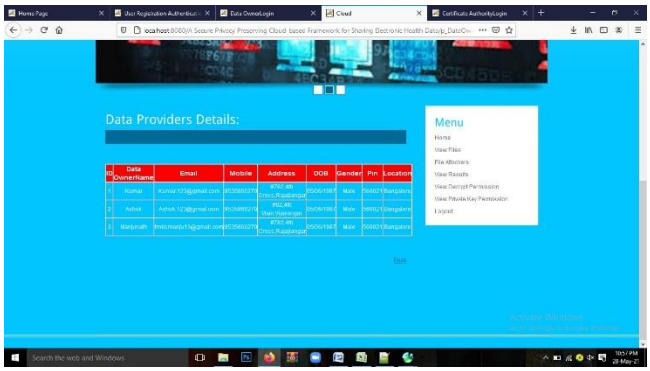

Fig 10. Data provides

Fig 11. View patient

Fig 12. View private key

Fig 13. View decrypt

Fig 14. View private key

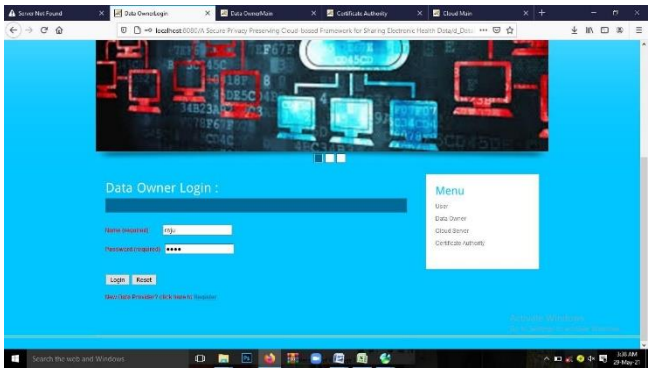

Fig 15. Data owner login page

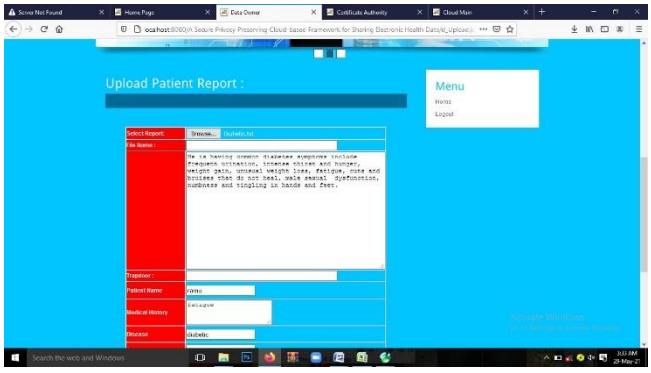

Fig 16. Uploaded patient report

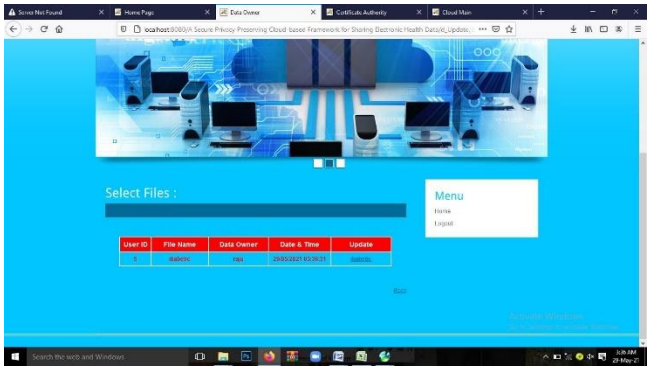

Fig 17. Update patient details

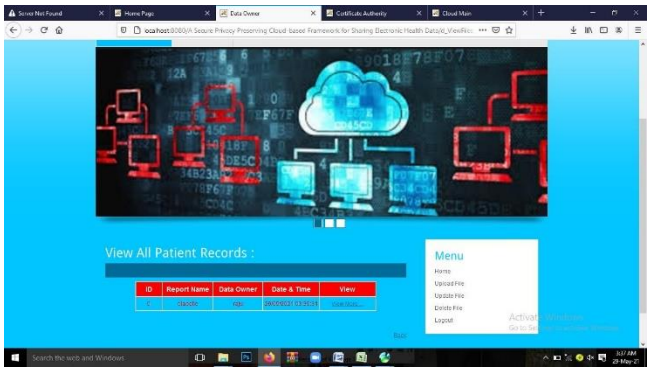

Fig 18. view patients list

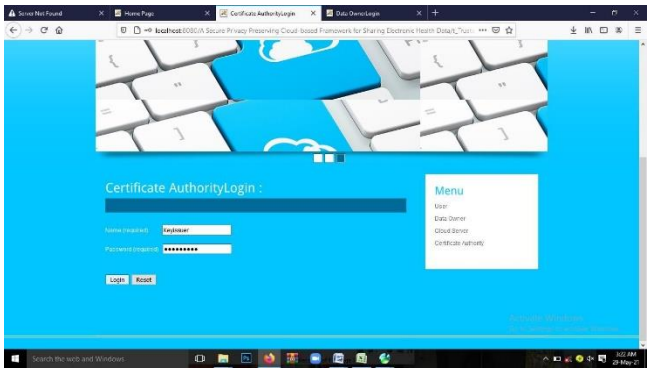

Fig 19. authority login

Fig 20. View all private key

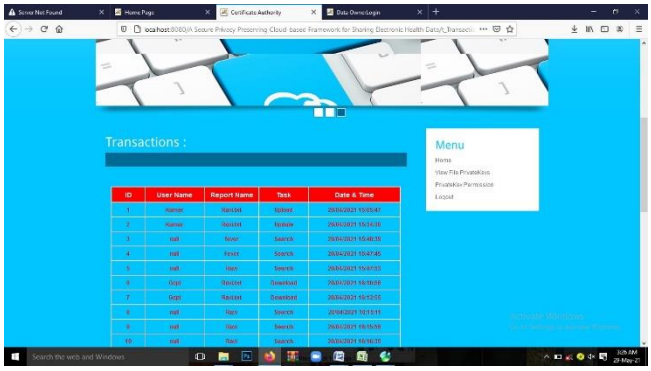

Fig 21. View all transaction

V. CONCLUSION AND FUTURE WORK

Suggested a way for safely transferring and storing Personal Health Records (PHRs) on the cloud to approved organizations. By enforcing patient-centric access control across various PHR sections based on access authorized by the patients themselves, the technique protects PHR confidentiality. Our fine-grained access control mechanism prevents even authorized system users from accessing PHR sections they are not permitted to access. PHR owners store their encrypted data in the cloud, and the only people who may decrypt the PHRs are authorized users who have valid re-encryption keys that have been granted by a semi-trusted proxy. The semi- trusted proxy's job is to create and maintain public/private key pairs for system users.

In addition, we used the Z3 solver, the Satisfiability Modulo Theories Library (SMT- Lib), and High-Level Petri Nets (HLPN) to formally examine and validate the SeSPHR methodology's performance. The time spent on key creation, encryption and decryption processes, and turnaround times was used to evaluate performance. The experimental findings show that securely exchanging PHRs in a cloud setting using the SeSPHR approach is feasible.

II. REFERENCES

[1]. K. Gai, M. Qiu, Z. Xiong, and M. Liu, "Privacy-preserving multi-channel communication in Edge-of-Things," Future Generation Computer Systems, 85, 2018, pp. 190-200.

[2]. K. Gai, M. Qiu, and X. Sun, "A survey on FinTech," Journal of Network and Computer Applications, 2017, pp. 1-12.

[3]. A. Abbas, K. Bilal, L. Zhang, and S. U. Khan, "A cloud based health insurance plan recommendation system: A user centered approach, "Future Generation Computer Systems, vols. 43- 44, pp. 99-109, 2015.

[4]. A. N. Khan, ML M. Kiah, S. A. Madani, M. Ali, and S. Shamshirband, "Incremental proxy re-encryption scheme for mobile cloud computing environment," The Journal of Supercomputing, Vol. 68, No. 2, 2014, pp. 624-651.

[5]. R. Wu, G.-J. Ahn, and H. Hu, "Secure sharing of electronic health records in clouds," In 8th IEEE International Conference on Collaborative Computing: Networking, Applications and Work-sharing (CollaborateCom), 2012, pp. 711-718.

[6]. A. Abbas and S. U. Khan, "A Review on the State-of-the-Art Privacy Preserving Approaches in E-Health Clouds," IEEE Journal of Biomedical and Health Informatics, vol. 18, no. 4, pp. 1431-1441, 2014.

[7]. M. H. Au, T. H. Yuen, J. K. Liu, W. Susilo, X. Huang, Y. Xiang, and Z. L. Jiang, "A general framework for secure sharing of personal health records in cloud system," Journal of Computer and System Sciences, vol. 90, pp, 46-62, 2017.

[8]. J. Li, "Electronic personal health records and the question of privacy," Computers, 2013, DOI: 10.1109/MC.2013.225.

[9]. D. C. Kaelber, A. K. Jha, D. Johnston, B. Middleton, and D. W. Bates, "A research agenda for personal health records (PHRs)," Journal of the American Medical Informatics Association, vol. 15, no. 6, 2008, pp. 729-736.

[10]. S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving secure, scalable and fine-grained data access control in cloud computing," in Proceedings of the IEEE INFOCOM, March 2010, pp. 19.