A SECURE AND EFFICIENT BLOCKCHAIN-BASED MULTI- CLOUD MEDICAL FILE SHARING

[1]J. RAHUL,[2]N. HARSHVARDHAN,[3]K. NITISH REDDY,[4]T. AISHWARYA,[5]Mrs. E. ARUNA

[1234] Students, [5] Assistant Professor

Department Of Information Technology

Teegala Krishna Reddy Engineering College, Meerpet, Balapur, Hyderabad-500097

ABSTRACT

The blockchain-powered scheme for sharing medical files in a practical manner decentralized quality based encryption is a secure and efficient approach for sharing sensitive medical information among healthcare providers. The system utilizes blockchain technology to store and handle the framework for restricting entry to specific areas and permissions for medical files, providing a tamper-proof and transparent mechanism for managing access to the data. Additionally, the use of decentralized attributes- based encryption ensures that patient data remains confidential and only accessible to those with the appropriate permissions. The scheme enables data owners to define granular access control policies based on specific attributes such as the type of data, patient information, and the role of the requesting party, enabling better collaboration and decision-making while ensuring data privacy and confidentiality.

I. INTRODUCTION

The traditional system of keeping medical records in particular based on manuscripts they have many problems such as random Sequence of events, information, insufficient data, broken record, data repetition, inconsistency with handwriting also sometimes it does not work well. In modern times, victory this shortcoming the healthcare industry is changing the Electronic system based on the electronic and currently known better known as Electrical Health Records (EHR). Major projects in the healthcare sector can be considered with an EHR program that starts with a patient medical record, Doctor Appointments and appointments, clinical and laboratory tests report, doctor's note, payment and accounts, and future Patient follow-up. The main purpose of the EHR is to provide order, sufficient without restriction, and not required medical, Consistent, and effective medical record participants. The advantage of the system is that it is better efficiency, accuracy.

A common phenomenon in healthcare in most Arab countries is the lack of optimal utilization of human and material resources available to provide integrated healthcare to prevent diseases and treat diseases after they occur. Statistics indicate that Arab countries suffer from high rates of health problems, such as diabetes, liver disease, and parasitic diseases, such as histosomiasis and malaria. These health problems could be prevented before they occur or their complications prevented by early detection. This is due to a combination of factors: planning, operational, and technical. If we were able to overcome them, this would lead to significant progress in the level of health care.

In addition, there is a weakness and lack of available hospital information systems, which is some of the most advanced software that directly serves all technical and administrative healthcare activities, ensuring that the medical institution has full control over all its activities and resources. The successes of these advanced systems do not depend on the exact selection of equipment and software for storage. Rather, their success depends on their suitability for different users—from healthcare providers, such as doctors, nurses, technicians, and even administrators—where the vision and priorities of each of these categories differ, and their information needs vary, as do the benefits of each of these systems. The traditional health system (paper) has been replaced by an electronic health information system because

the traditional system has been found to be ineffective due to a number of issues, including low storage capacity, high operating and maintenance costs, and system integration. The computerized health system was then replaced by cloud computing because it relies on a more efficient infrastructure, as well as the many benefits of cloud computing in IT, such as cost, scalability, flexibility, and other features. The use of cloud computing in electronic health records reduces costs in the provision of health services, maintenance costs, networks, licensing fees, and infrastructure in general, and this will therefore encourage developers to adopt the cloud in healthcare.

Motivation

Blockchain-based systems are a decentralized technology that is used in several industries such as logistics, supply chain management, finance applications, and the Internet of Things (IoT). Blockchain provides a secure distributed database and queries to the database can be made without any intervention of unauthorized identities. It is highly efficient in the case when various participants want to access the same database. Thus, Blockchain can minimize a lot of resources and costs to access the same database securely. The critical issue in electronic health/medical records (EHR/EMR) is maintaining the interoperability among various involved identities. This issue may cause obstacles in the data transaction among each other. There is a lack of data management and sharing mechanism among the identities which leads to fragmentation of the healthcare information. Apart from interoperability, data security and privacy are also challenges in the current ways of data storing and sharing data through EHR/EMR systems. Sharing and storing patients' data has a lot of liabilities due to data leakage and potential shortcoming in security mechanisms. Blockchain for healthcare can ensure the security of the personal and medical information of the patients and can make sure that only authorized identities can access/edit the data using features that enable specific features among various identities in the system. Therefore, there is a clear need for a distributed way of sharing and storing data where patients are surer about their data security and privacy and in addition, all the involved identities can see the holistic view of overall transactions and interactions.

Problem Statement

In this project, we will create an EHR system using the concept of blockchain. We will be deploying the project using web technologies like HTML, CSS, and JavaScript and serverside technologies like java and SQL for database management. To manage the medical records of patients, need to map EHR components to the requirements of the systems. All hospitals act as organizations in the network. Patient data has been treated as assets that are stored in the ledger. It is also possible to store the reference of the EHR data in the ledger but since the application is not managed by real data and for that it will be necessary to maintain a separate database that will have patient data.

This can be a good solution when it is integrated with production or real hospitals' EHR data. For now, the patient record has a few fields like personal and medical details like age, address, allergies, symptoms, treatment, follow-up, etc. When a doctor is medicating a patient, patient history data will be available which helps doctors to assign appropriate treatment. To improve the privacy of records, it is designed to provide extra steps in an application for patients. The patient can decide to have permission to access his/her data from a particular doctor. A doctor can view limited fields of assent means patient data like all medical fields along with age and allergies, whereas the patient can view all the fields but edit only the personal field.

Objectives

The objective of this project is to design and implement a secure, efficient system for sharing medical files across multiple cloud platforms using blockchain technology. It aims to ensure patient data privacy, integrity, and accessibility without relying on a single cloud provider. The system will utilize blockchain to

create a decentralized, tamper-proof ledger of file transactions and access logs. Smart contracts will automate access control, ensuring that only authorized parties can view or modify medical records. Multiple cloud storage providers will be integrated to enhance redundancy, availability, and load balancing.

Data will be encrypted before uploading to the cloud, ensuring confidentiality even if a provider is compromised. The project seeks to reduce trust dependencies on centralized authorities or single service providers. Patients will retain ownership and control over their medical data through blockchain identity management. Healthcare providers will have streamlined, secure access to necessary files, improving care coordination. The system will incorporate efficient file-sharing protocols to minimize latency and overhead costs. Blockchain consensus mechanisms will be optimized for high transaction throughput and low energy consumption.

II. LITERATURE SURVEY

Smart healthcare realizes the interaction between patients and medical staff, medical institutions, and medical devices by building a health archive regional medical information platform and using the most advanced Internet of things technology so that the medical industry gradually achieves information. Sharing medical data is an important step to making the medical system more intelligent and improving the quality of medical service. However, the sharing of patient data among institutions is not yet fully realized, and the blockchain is a great way to solve this problem right now. Blockchain is distributed data system involving multiple independent nodes, which is an emerging technology for decentralized and transactional data sharing among large networks of entrusted participants. It features decentralization, timestamps, collective maintenance, programmability, and tamper-proofing Blockchain has relatively few applications in medical treatment, and the existing research mainly focuses on combining blockchain 2 Journal of Healthcare Engineering with a certain information technology to build a single application platform, such as using blockchain technology to build a medical transaction sheet verification system; using etheric blockchain to build a medical information sharing platform MedRec which combines blockchain with big data, and using Blockchain technology.

owever, the application of blockchain technology in the whole intelligent medical industry lacks systematic research. Based on this, the study will build a customer-centered Blockchain smart healthcare application system based on stakeholder theory to explore its development path. After sorting out and analyzing all the stakeholders of the system, we get the application system based on ten aspects including 22 criteria.

Description: This technology has been said can solve many problems of the healthcare system such as increase the storage capacity and add new capability on the existing healthcare system. Cloud computing offers cost effective, increase interoperability and accessibility, optimize resources and integrate the healthcare information systems. It becomes a solution for solving the current issues, which lead to enhance functionality and features of the healthcare information systems. Therefore, the aim of this study is to explore the cloud computing technology as solution for healthcare information system issues. Issues such as data transmission, data storage, cost and maintenance issues are presented and described. The implications of this study then discussed.

Description: he computerized health system was then replaced by cloud computing because it relies on a more efficient infrastructure, as well as the many benefits of cloud computing in IT, such as cost, scalability, flexibility, and other features [2]. The use of cloud computing in electronic health records reduces costs in the provision of health services, maintenance costs, networks, licensing fees, and infrastructure in general, and this will therefore encourage developers to adopt the cloud in healthcare.

We present a descriptive literature review and classification scheme for cloud computing research. This includes 205 refereed journal articles published since the inception of cloud computing research. The articles are classified based on a scheme that consists of four main categories: technological issues, business issues, domains and applications, and conceptualizing cloud computing. The results show that although current research is still skewed towards technological issues, new research themes regarding social and organisational implications are emerging. This review provides a reference source and classification scheme for IS researchers interested in cloud computing, and to indicate under-researched areas as well as future directions.

As a result the aim of this paper is twofold; firstly to evaluate cloud security by identifying unique security requirements and secondly to attempt to present a viable solution that eliminates these potential threats. This paper proposes introducing a Trusted Third Party, tasked with assuring specific security characteristics within a cloud environment. The proposed solution calls upon cryptography, specifically Public Key Infrastructure operating in concert with SSO and LDAP, to ensure the authentication, integrity and confidentiality of involved data and communications. The solution, presents a horizontal level of service,

available to all implicated entities, that realizes a security mesh, within which essential trust is maintained. It remains to be seen how cloud computing will impact the healthcare business since it is very diverse and complex, it presents several challenges such as protecting members health records in addition to following HIPAA guidelines set by federal compliance regulations Efforts are being made to decrease the costs for consumers and it will play a big role in achieving it and also improving clinical and quality outcomes for patients.

EXISTING SYSTEM

1. Reliance on Paper Records**:** Many healthcare institutions in developing countries still rely on paperbased files for patient medical record documentation.
2. Limited Access to Previous Records: When patients visit a new healthcare facility, they must provide their health information again, as the new facility cannot access their previous medical records.
3. Challenges of Paper-Based Systems: The paper-based method has various shortcomings, including issues with organization, accessibility, and security of patient records.
4. Service-Oriented Architecture (SOA) Model: The paper uses the SOA software development model to create a framework for an electronic health records (EHR) system designed to solve realworld healthcare challenges. The system allows access through a web portal over a private network, ensuring secure interactions between patients, doctors, nurses, and medical assistants via various devices

In many developing countries however, most healthcare institution still relies on paper-based files as the method for patients' medical record documentation. In this method, patients' medical records are stored on paper-based files and registers. If for any reason a patient needs to visit a new healthcare facility, the patient would need to provide his/her health information to the new facility without reference to the previous medical records of such a patient. Aside this limitation, this method also suffers from many attendant shortcomings earlier mentioned in this Section of the paper. Furthermore, in some few healthcare institutions that operates automated health records, various units or departments in these healthcare institutions operate as independent entities and they suffer from the inability to transfer patient health information and records amongst themselves most of the architectures proposed by the authors are for contextual scenarios where there are no constraints in ICT resources and there exist already deployed legacy systems for different tasks within healthcare facilities. A large majority of these reviewed works proposed

architectures that integrate already deployed legacy systems into an EHR system and rather than develop an EHR system from the scratch. In this paper, a framework for a cloud-based electronic health records system that is capable of automating storage, retrieval, updating and maintaining of patients medical records from the scratch in developing countries is proposed.

PROPOSED SYSTEM

1. Security Measures: Patient data security is ensured using a public key cryptosystem and steganography. Medical records are saved and transferred to a network server via Secure File Transfer Protocol (FTPS) for future use, protecting sensitive information from unauthorized access.
2. Data Access and Communication: Medical practitioners with valid credentials can access patient data to analyze medical history, medication reactions, and provide recommendations. Physicians can also communicate with patients through the web portal, allowing patients to access their personal medical records.
3. Multi-layered Architecture: The proposed system follows a multitiered approach, including the Presentation, Application, Middle, and Data tiers. The Presentation tier is the user interface, independent of other layers, ensuring compatibility with different devices.
4. Functionality of Each Tier: The Application tier processes user inputs, while the Middle tier, composed of web services, addresses integration issues, data structure discrepancies, and technical conflicts. The Data tier supplies the patient data required by the EHR application for effective management and received. An essential of devising model solutions to identified problems is defining apposite research methodologies .This paper employed the Service Oriented Architecture (SOA) software development model to derive a framework for an electronic health records system that would solve a real life problem. The EHR system can be accessed through a web portal over a private network by patients, doctors, nurses and medical assistants with valid credentials using various devices that include Smartphones, laptop and desktop computers.

The security of patient information and data is to be by a public key cryptosystem and steganography. Recorded patient's data are routinely saved and transferred to the network server via Secure File Transfer Protocol (FTPS) for future referencing. Patients' medical data accessed by medical practitioners with valid credentials can be used by them to analyze and manage patients' medical history, reaction to medication, evolution and possibly send to patients, a medical recommendation.

Also, physicians can communicate with patients through the web portal while patients too can access their personal medical records. The implementation view of the proposed framework is a multi-layered approach consisting of the Presentation, Application, Middle and Data tiers. The foremost layer is the Presentation tier which is a web portal that facilitates the exchange of information between users and the system and among various users.

It is a layer that is independent of other layers underneath it since it was to be implemented for a variety of devices. Next to the Presentation tier is the Application tier. The Application tier collates users' inputs (data and information) and process them. Beneath the Application tier is the Middle tier.

The Middle tier is essentially made up of services layer that handles issues bothering on integration of different applications, problems arising from disparity in data structures implemented, technical conflict in connectivity to different protocols and so on. This layer is composed by web services. The last of the layers is the Data tier. The patient data requests by the EHR application is supplied by the data tier.

III. OUTPUT SCREENS

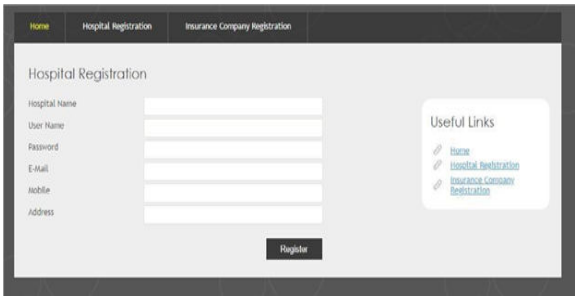

Fig 1: Hospital Registration

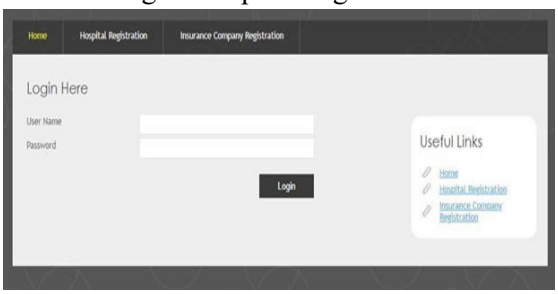

Fig2: Hospital Login

Fig 3: View Treatments

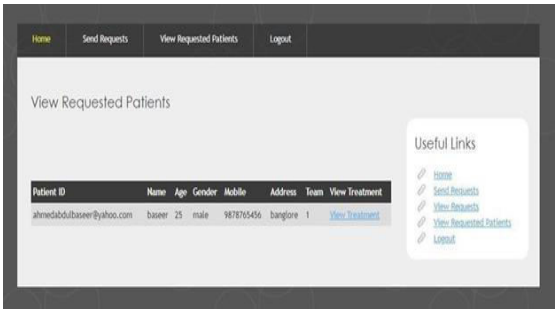

Fig 4: view Request

Fig 5: Send Request

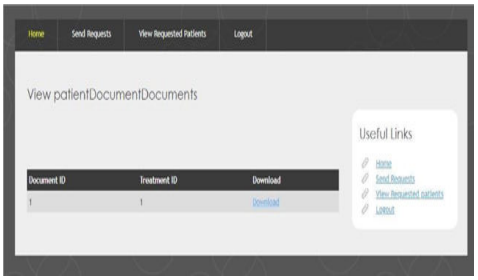

Fig 6 : Patient Document

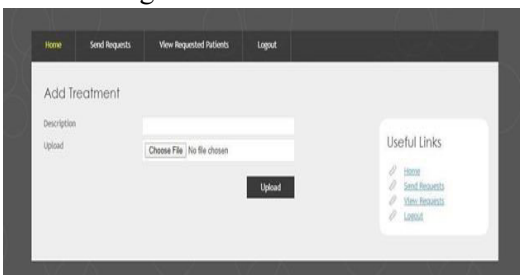

Fig 7:Add Treatment

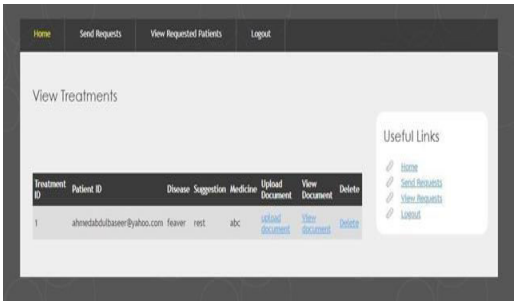

Fig 8: View Treatment

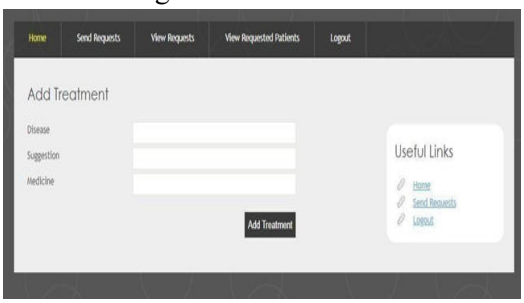

Fig 9: Add Treatment

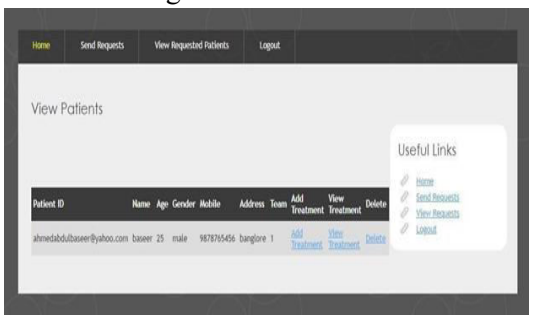

Fig 10 : View Treatment

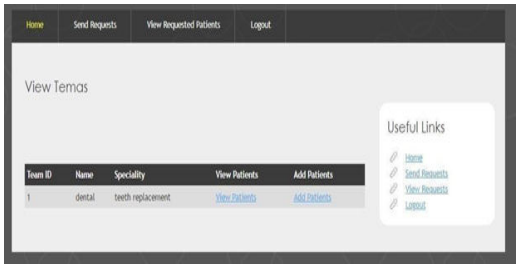

Fig 11: View teams

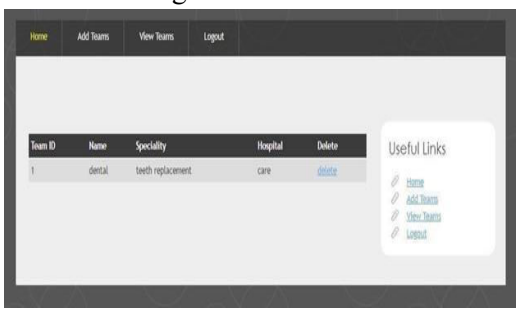

Fig 2: Home Page

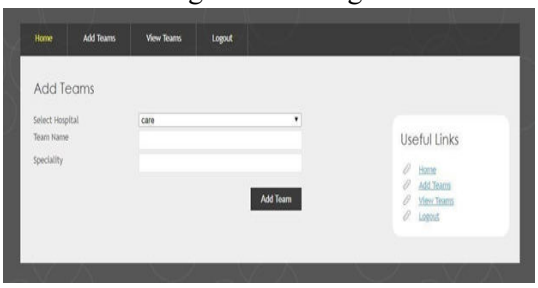

Fig13: Add Team

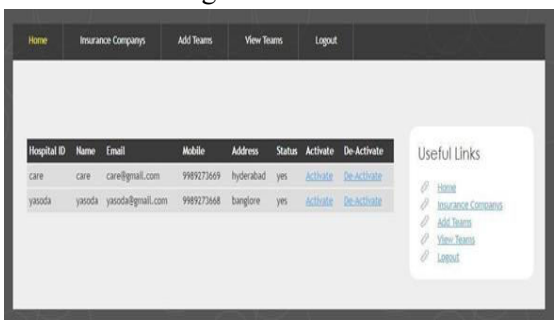

Fig 14: Home Page

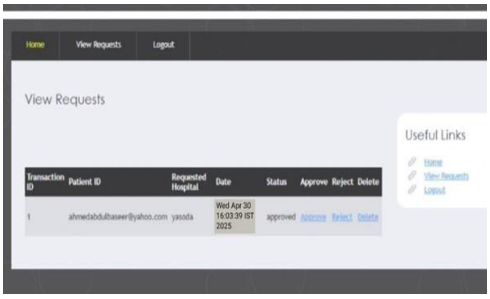

Fig 15: View Requests

IV. CONCLUSION

In this paper, we have proposed a blockchain-based approach to give patients control over their medical records in a decentralized, traceable, reliable, trustful, and secure manner. we have created an architecture for the Electronic Health Record using blockchain technology and we have proposed framework for the block chain and create a block to store the patients data in a decentralized healthcare network for secure sharing. We were able to deploy a block chainbased EHR network and implement basic functionalities in the network. We successfully achieved the main objective of this research by using the primary features of blockchain that is hashing and decentralization. We conclude that blockchain technology is an innovative technology for implementing EHRs and also it has the potential to help in the research and progress of healthcare in the near future.

The overarching benefit In multi-cloud storage, the identity-based distributed provable data possession scheme has been revisited to ensure that data remains in storage. The server can still produce a valid proof to show that data is still stored, ensuring data integrity. To enhance the security of multi- cloud storage, a general model for ID-PDP protocols. This was introduced, which utilizes regular signature schemes and usual PDP protocols. This mechanism was found to be secure, and a new public auditing mechanism was proposed, which allows for data sharing with effective user deletion in the cloud

REFERENCES

1. J. S. Ancker, M. Silver, and R. Kaushal, “Rapid growth in use of personal health records in newyork, 2020–2021,” J. Gen. Internal Med., vol. 29, no. 6, pp. 850–854, Jun. 2019.EHRs Have Made it Easy for Cardiologists to Treat Their Patients. Accessed: Jul. 8, 2020. [Online].Available: http://tbrcinfo.blogspot.com/ 2018/12/ehrs-have-made-it-easy-for.html

2. A. Bhardwaj, S. B. H. Shah, A. Shankar, M. Alazab, M. Kumar, and T. R. Gadekallu, “Penetration testing framework for smart contract blockchain,” Peer-to-Peer Netw. Appl.,pp. 1–16, Sep.2020, doi: 10.1007/s12083-020-00991-6.

3. Y. Sharma and B. Balamurugan, “Preserving

the privacy of electronic health records using blockchain,"Procedia Comput. Sci., vol. 173, pp. 171–180, Jan. 2020.

4. M. Qazi, D. Kulkarni, and M. Nagori, "Proof of authenticity-based electronic medical records storage on blockchain," in Smart Trends in Computing and Communications. Singapore: Springer,2019, pp. 297–306.
5. T. McGhin, K.-K. R. Choo, C. Z. Liu, and D. He, "Blockchain in healthcare applications: Research challenges and opportunities," J. Netw. Comput. Appl., vol. 135, pp. 62–75, Jun. 2019. [Online].
6. Hamlen, Kevin, Murat Kantarcioglu, Latifur Khan, and Bhavani Thuraisingham. "Security issues for cloud computing." Optimizing Information Security and Advancing Privacy Assurance: New Technologies: New Technologies 150 (2012).
7. Omachonu, Vincent K., and Norman G. Einspruch. "Innovation in healthcare delivery systems: a conceptual framework." The Innovation Journal: The Public Sector Innovation Journal 15, no. 1 (2010): 1–20.
8. Reddy, B. Eswara, TV Suresh Kumar, and Gandikota Ramu. "An efficient cloud framework for health care monitoring system." In Cloud and Services Computing (ISCOS), 2012 International Symposium on, pp. 113-117. IEEE, 2012.
9. Parekh, Maulik, and B. Saleena. "Designing a cloud based framework for healthcare system and applying clustering techniques for region wise diagnosis." Procedia Computer Science 50 (2015): 537–542.
10. Botta, Alessio, Walter De Donato, Valerio Persico, and Antonio Pescapé. "Integration of cloud computing and internet of things: a survey." Future Generation Computer Systems 56 (2016):684– 700. [15] Stergiou, Christos, Kostas E. Psannis, Byung-Gyu Kim, and Brij Gupta. "Secure integration of IoT and cloud computing." Future Generation Computer Systems 78,(2018):964–975.
11. Zhiwei Yu, Chaokun Wang, Clark Thomborson, Jianmin Wang, Shiguo Lian and Athanasios V. Vasilakos, A novel watermarking method for software protection in the cloud, SOFTWARE – PRACTICE AND EXPERIENCE, 42:409–430, 2012. https://www.yesser.gov.sa/en/Pages/default.aspx
12. Huang, Jie, Mohamed Sharaf, and Chin-Tser Huang. "A hierarchical framework for secure and scalable ehr sharing and access control in multi-cloud." In Parallel Processing Workshops (ICPPW), 2012 41st International Conference on, pp. 279–287. IEEE, 2012.
13. Huang, Qinlong, Yixian Yang, and Mansuo Shen. "Secure and efficient data collaboration with hierarchical attribute-based encryption in cloud computing." Future Generation Computer Systems72 (2017): 239–249.
14. Goyal, Vipul, Omkant Pandey, Amit Sahai, and Brent Waters. "Attribute-based encryption for fine-grained access control of encrypted data." In Proceedings of the 13th ACM conference on Computer and communications security, pp. 89–98. Acm, 2006.
15. Bethencourt, John, Amit Sahai, and Brent Waters. "Ciphertextpolicy attribute-based encryption." In Security and Privacy, 2007. SP'07. IEEE Symposium on, pp. 321–334. IEEE, 2007.
16. Li, Qinyi, Hu Xiong, Fengli Zhang, and Shengke Zeng. "An expressive decentralizing kp- abe scheme with constant-size ciphertext." IJ Network Security 15, no. 3 (2013): 161–170.
17. Li, Qi, Jianfeng Ma, Rui Li, Ximeng Liu, Jinbo Xiong, and Danwei Chen. "Secure, efficient and revocable multi-authority access control system in cloud storage." Computers & Security
59 (2016): 45–59.
18. Sekhar, B. Raja, B. Sunil Kumar, L. Swathi Reddy, and V. Poorna Chandar. "CP-ABE based encryption for secured cloud storage access." International Journal of Scientific & Engineering Research 3, no. 9 (2012): 1–5.