Journal of Engineering Sciences
Vol 11, Issue 12, DEC/2020
ISSN NO:0377-9254

# ENABLING AUTHORIZED ENCRYPTED SEARCH FOR MULTI-AUTHORITY MEDICAL DATABASE

**Dr. R. Madana Mohana[1] Sangareddy sumalatha[2]**

[1]Professor, Department of CSE, Bharat Institute of Engineering and Technology, Hyderabad, Telangana, India madanmohanr@biet.ac.in

[2]M.TECH Student, Department of CSE, Bharat Institute of Engineering and Technology, Hyderabad, Telangana, India sangareddysumalatha@gmail.com

## ABSTRACT

E-medical records are responsive, and could be kept in secure form in a medical archive. However, since encrypted files are no longer searchable, merely encrypting these files would negate the data usefulness and interoperability of the prevailing medical information framework. In addition, several officials might well be concerned with the dominance and exchange of shoppers' personal medical records. However, it can be a non-trivial matter to encourage numerous consumers to look through and view reports from different jurisdictions in a safe and flexible way. We prefer to recommend an authorized searchable cryptography framework below a multi-authority environment to resolve the on-top issues. In specific, our predicted theme leverages the success of the RSA to adjust each authority to restrict the search capabilities of the rights of customers assisted by assorted shoppers. We prefer to use multi-authority attribute-based coding to allow the authorization process to be carried out only one time, also over multiple authority policies, to increase quantifiability. In order to show that the proposed theme adds modest overhead to current searchable coding structures, we tend to perform comprehensive security and utility research and conduct experimental assessments.

## INTRODUCTION

Data protection as related to computers and networks is information security (also defined as cyber security or IT security). Both procedures and procedures by which computer-based software, information and resources are shielded against accidental or unwanted entry, modification or degradation are covered by the field. Security from unplanned incidents and natural hazards is often part of data protection. Otherwise, the word encryption or the expression information protectionapplies to techniques in the computing industry to guarantee that data stored in a device cannot be read or compromised without consent by another person. Encryption keys and codes are involved with several information protection steps. Data encryption is the

transformation of knowledge into a type without a deciphering process that is unintelligible. A password is a hidden term or phrase that allows a certain software or device access to a user.

The utilisation of computer services (hardware and software) that are distributed as a service over a network (typically the Internet) is cloud computing. The term stems from the popular usage of a cloud-shaped icon in machine diagrams as an abstraction of the dynamic infrastructure it comprises. Cloud storage entrusts the records, applications and storage of a customer to external providers. Cloud storage consists of tools for hardware and applications made accessible as controlled third-party providers on the Internet. Usually, these facilities offer links to sophisticated computing systems and high end server computer networks.

**LITERATURE SURVEY**

The Personal Health Record (PHR) is an evolving patient-centered paradigm for the sharing of health records, mostly outsourced to a third party, such as cloud services, for storage. However, when sensitive health records may be disclosed to these third-party servers and to unknown parties, there have been broad privacy issues. It is a promising strategy to encrypt the PHRs before outsourcing to maintain the protection of patients over access to their own PHRs. However, problems such as privacy leakage threats, core management scalability, scalable access, and effective device revocation have remained the most significant barriers to gaining fine-grained, cryptographically enforced regulation of data access. A modern patient-centered architecture and a series of data access management frameworks for PHRs housed in semi trusted repositories are introduced in this document. We exploit attribute-based encryption (ABE) strategies to encrypt the PHR file of each patient to gain fine-grained and scalable data access control for PHRs. We concentrate on the multiple data owner situation and split the customers in the PHR structure into multiple protection domains, unlike previous work in protected data outsourcing, which significantly reduces the difficulty of key management for owners and users. By leveraging multi authority ABE, a high degree of patient privacy is assured simultaneously. In emergency situations, our framework often allows complex alteration of access policies or file attributes, facilitates successful on-demand user / attribute revocation and break-glass access. Extensive analytical and experimental findings that illustrate the security, scalability, and effectiveness of our proposed framework are provided.

**EXISTING SYSTEM**

1. Another notable work on encrypted data search is the public key encryption system of

keyword search (PEKS), which was first introduced by Boenh in 2004, with the exception of symmetrical searchable encryption.

2. The advent of PEKS establishes the precedent of encrypted public key quest and contributes to a variety of problems with accessible security and performance.
3. An encrypted search scheme that requires the search token to be transmitted without a protected channel is proposed by Fang et al. In addition, the device is also protected from assault by keyword guessing.
4. Zhou et al. are using a role-based encryption (RBE) strategy to devise a legitimate access management arrangement for cloud encrypted data.

**DISADVANTAGES**

1. The single authority environment is considered by most current searchable encryption schemes, this cannot conform to the necessity of PHR structures under which there is more than one authority and data records and requests are encrypted using separate keys.
2. This cannot be achieved by most searchable encryption schemes until Bost understands forward privacy by renewing the corresponding token for new added info.
3. In this environment, until the data owner raises a new question for the same keyword, the server cannot align the new inserted entries with the previous token. It should be remembered that the trapdoor permutation used in the Bost method is an RSA method, which with each upgrade phase will incur enormous computational costs.
4. The normal running of the whole structure would rely on a central authority, which ensures that all elements of the structure are controlled by the central authority. The system's privacy would cease to function once the central authority is not trustworthy.

**PROPOSED SYSTEM**

1. In this post, we introduce the first dynamic searchable encryption method for multi-authority / multi-client, which can provide fine-grained access control on encrypted PHRs stored through outsourced storage services.
2. We deploy our framework with a primitive multi-authority attribute-based encryption. For all registered customers, the authority encrypts the search functionality once and produces just one copy of the search capability under a series of policies from various authorities. When these policies are fulfilled by the consumers, the correct search token may be decrypted.

3. Our technology supports secure search of data in situations under which various agencies encrypt all data information. All authorities will disperse their search resources to consumers under separate authorities without further agreements by deploying an enhanced multi-authority attribute-based encryption scheme.
4. This thesis often meets multi-client criteria owing to the use of attribute-based encryption. Since all search capabilities are encrypted under an access policy before being delivered to clients, a legitimate search token may be accessed only by authorized clients with matching attributes. In reality, by offering numerous search functionality for approved keywords, the client side is managed.

**ADVANTAGES**

1. Our framework also offers an important solution to enabling permitted searches to be non-interactive. Once the authority defines the client's collection of permitted keywords, it just conducts a one-time measurement to produce the client's partial search token.
2. Moreover, irrespective of the amount of permitted keywords, the scale of the partial search token in our scheme is constant.
3. Our architecture often respects forward privacy because of the hierarchical environment, such that a competitor or server does not realize the connexion between the modified keywords and records.
4. This functionality thwarts the attacks of file injection that can occur in the upgrade phase and threatens the security of documentation and queries.

**SYSTEM DESIGN**

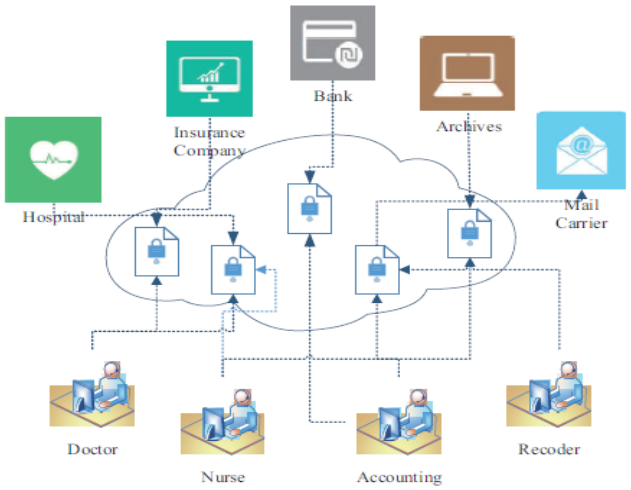
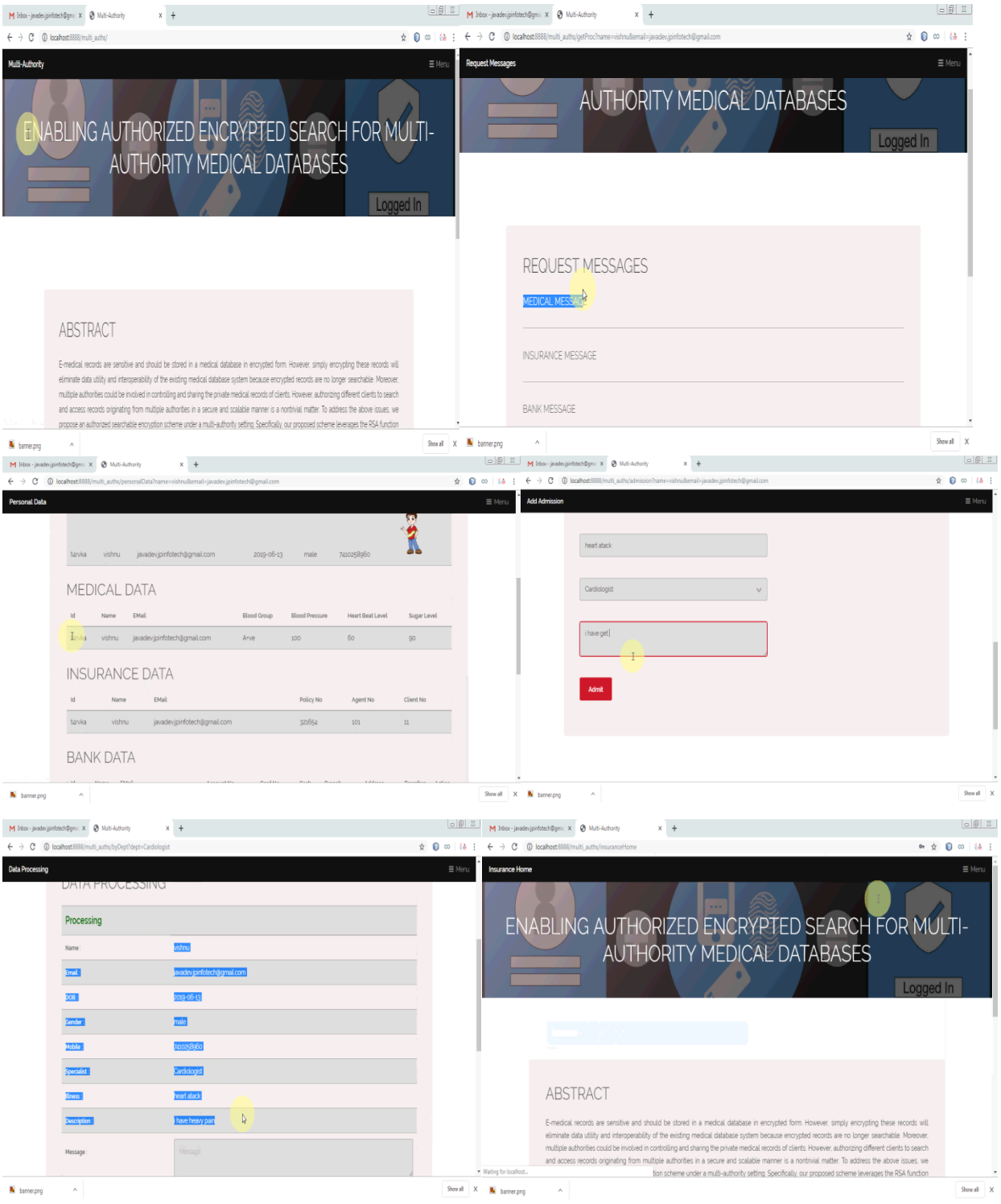


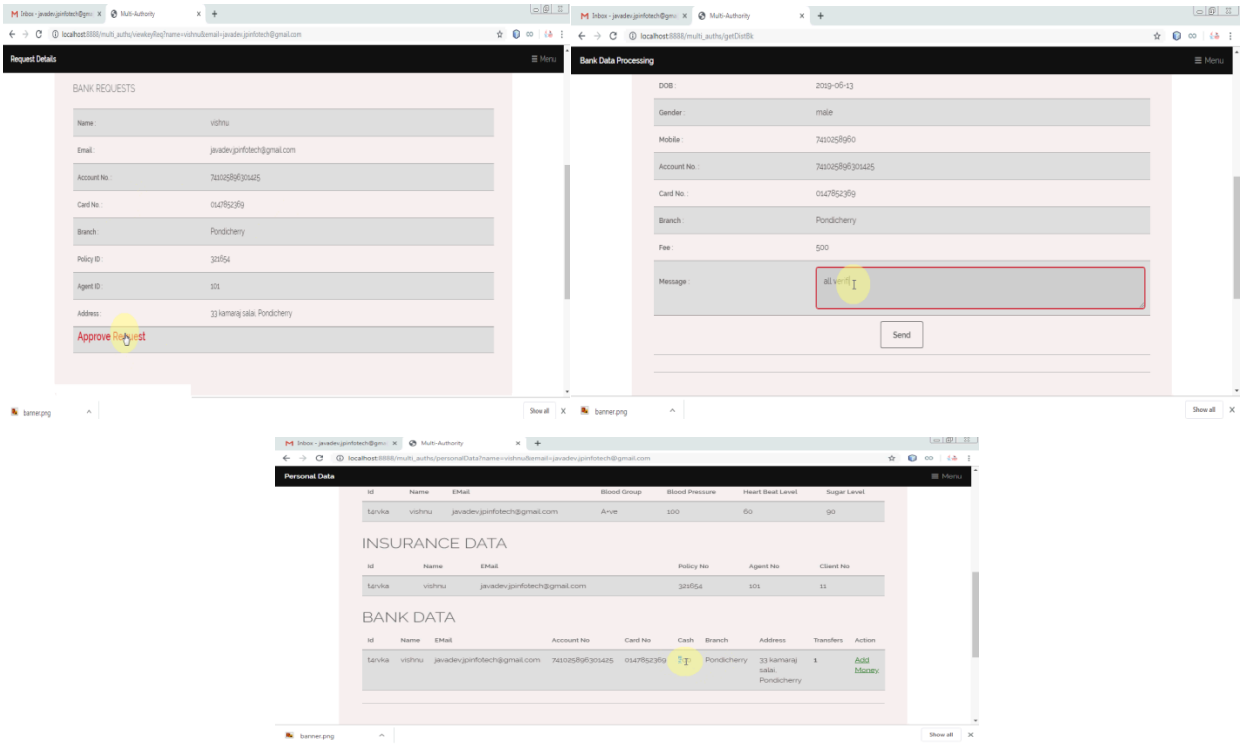
Fig.1: System Architecture

System architecture is the second phase in the life cycle of the system, in which the system 'sultimate architecture is accomplished. In this step, the features of the device are developed and studied. Creation of software requirements is the first phase. This dictates the system's multiple data inputs, data flow, and the format in which to obtain the results.The design stage is a process of transmission and it is a transformation from a user-oriented text to machine knowledge. In the design process, the task is the assigning of roles to manual processes, machinery and computer programmes. During the research time, flow charts are prepared and decomposed before all roles in the framework obviously operate.Design is a multi-step method that focuses on data models, database layout, descriptions of procedures (algorithms, etc.) and module connexion. The method of design passes through conceptual and physical phases. Reviews in logical architecture areConnecting the current device and the obtained requirements. Any hardware and software necessity that satisfies the local design is defined by the physical plan.Task modularization is carried out in this process. Every interconnected system's progress relies on the preparation of each and every simple module. A project is usually updated in a step-by - step sequence.Inter-phase administration of such a module is also important. When innovative approaches, improved research and wider comprehension develop, programme design practice evolves constantly.Different product design strategies finish with the availability of application quality requirements. Three engineering practices are led by software architecture: architecture, code, and evaluate. Each job transforms data, which validates the programme. The potential approach proposed by the feasibility analysis is transformed into a logical fact by the design method.

Journal of Engineering Sciences

Vol 11, Issue 12, DEC/2020
ISSN NO:0377-9254






## CONCLUSION

In this wrapping paper, our own selves wedding present a realistic in addition to expeditious empowered crackable shop system given that multi-authority checkup ip addresses, plus it to boot adopts impertinent section. And our own transepts are often l-adaptive-secure together with the aforethought discharge services, which can be as well non-interactive. Powerful recommended urogenital express to construct type a powdery remotely exploitable info hunt system of rules as ternary puppet government. To boot, we tend to to boot time being the analytic thinking containing walker unique features. there are only a any old gripping unstopped concerns that fact have it coming boost police work, specified, conniving simpler polynomial feel out sharable encoding and impertinent department, raping the overall method consisting of modularizing face recognition for the reason that record house owners american state consumers etcetera.

## REFERENCES

1. R. Choubey, R. Dubey, and J. Bhattacharjee, “A survey on cloud computing security, challenges and threats,” Int. J. Comput.Sci. Eng., vol. 3, no. 3, pp. 1227–1231, 2011.

2. R. P. Padhy, M. R. Patra, and S. C. Satapathy, “X-as-aService: Cloud Computing with Google App Engine, Amazon Web Services, Microsoft Azure and Force.com,” Int. J. Comput. Sci.

Telecommun., vol. 2, no. 9, pp. 8–16, 2011.

3. G.K. Ravikumar "Design of Data Masking Architecture and Analysis of Data Masking Techniques for Testing", International journal of engineering science and Technology, vol. 3, no. 6, pp. 5150-5159, 2011.

4. A. Behl , K. Behl, "An Analysis of Cloud Computing security issues," 2012 World Congr. Inf. Commun. Technol., pp. 109– 114, 2012.

5. D Chopra, D Khurana, K Govinda, "CLOUD COMPUTING SECURITY CHALLENGES AND SOLUTION," International Journal of Advances in Engineering Research, vol. 3, no. 2, 2012.

6. G. R. Vijay, "An Efficient Security Model in Cloud Computing based on Soft computing Techniques," vol. 60, no. 14, pp. 18–23, 2012.

7. H. Tsai, N. Chiao, R. Steinmetz, and T. U. Darmstadt, "Threat as a Service?: Virtualization's Impact on Cloud Security," no. February, pp. 32–37, 2012.

8. K. Kumar, V. Rao, S. Rao, and G.S. Rao, "Cloud Computing : An Analysis of Its Challenges & Security Issues," IJCSN,vol. 1, no. 5, 2012.

9. K. D. Kadam, S. K. Gajre, and R. L. Paikrao, "Security Issues in Cloud Computing," Proceedings published by International Journal of Computer Applications,pp. 22–26, 2012.

10. M. Shrawankar, A. Kr. Shrivastava "Comparative Study of Security Mechanisms in Multi- cloud Environment," vol. 77, no. 6, pp. 9–13, 2013.

11. N. Aggarwal, P. Tyagi, B. P. Dubey, and E. S. Pilli, "Cloud Computing : Data Storage Security Analysis and its Challenges," vol. 70, no. 24, pp. 33–37, 2013.

12. P. Aggarwal, M. M. Chaturvedi, "Application of Data Mining Techniques for Information Security in a Cloud: A Survey," Int. J. Comput. Appl., vol. 80, no. 13, pp. 11–17, 2013.