DOI: 10.17148/IJARCCE.2023.12311

Enhancing Security of E-Healthcare on Cloud with Advanced Encryption Standard (AES)

Dr. Rengarajan A[1], B Keerthana[2]

Professor, Department of CS & IT, Jain (Deemed-to-be) University, Bengaluru, India[1]

Student, Department of CS & IT, Jain (Deemed-to-be) University, Bengaluru, India [2]

Abstract: Securing e-healthcare involves encrypting sensitive patient data, such as medical records, in a way that allows for search operations to be performed on the encrypted data without compromising the security of the patient's information. One way to accomplish this is through the use of homomorphic encryption, which allows computations to be performed on ciphertext, resulting in an encrypted output that can be decrypted to the same plaintext as if the computation was performed on the plaintext. Another way is through the use of searchable encryption, which uses a combination of encryption and data structures such as inverted indexes to enable keyword searches on encrypted data. These methods can be used to create secure systems for e-healthcare that allow authorized personnel to search patient data while ensuring that the data remains confidential and protected from unauthorized access. E-Healthcare systems are increasingly popular due to the introduction of wearable healthcare devices and sensors. Personal health records (PHRs) are collected by these devices and stored in a remote cloud. Due to privacy concern, these records should not be accessible by any unauthorized party, and the cloud providers should not be able to learn any information from the stored records. To address the above issues, one promising solution is to employ attribute-based encryption (ABE) for fine-grained access control and searchable encryption for keyword search on encrypted data. However, most of existing ABE schemes leak the privacy of access policy which may also contain sensitive information. On the other hand, for users' devices with limited computing power and bandwidth, the mechanism should enable them to be able to search the PHRs efficiently. Unfortunately, most existing works on ABE do not support efficient keyword search on encrypted data. In this work, we propose an efficient hidden policy ABE scheme with keyword search. Our scheme enables efficient keyword search with constant computational overhead and constant storage overhead. Moreover, we enhance the recipient's privacy which hides the access policy. As of independent interest, we present a trapdoor malleability attack and demonstrate that some of previous schemes may suffer from such attack.

Keywords: Advance Encryption Standard, E-healthcare, Security, Cloud Security, Attribute Based Encryption, Fine Grained Access Control.

I. INTRODUCTION

E-Healthcare systems are increasingly popular due to the introduction of wearable healthcare devices and sensors. Personal health records (PHRs) are collected by these devices and stored in a remote cloud. Due to privacy concern, these records should not be accessible by any unauthorized party, and the cloud providers should not be able to learn any information from the stored records. To address the above issues, one promising solution is to employ attribute-based encryption (ABE) for fine-grained access control and searchable encryption for keyword search on encrypted data.

Attribute Based Encryption: Attribute-based encryption is a generalisation of public-key encryption which enables fine grained access control of encrypted data using authorisation policies. The secret key of a user and the ciphertext are dependent upon attributes (e.g., their email address, the country in which they live, or the kind of subscription they have). In such a system, the decryption of a ciphertext is possible only if the set of attributes of the user key matches the attributes of the ciphertext. A crucial security aspect of attribute-based encryption is collusion-resistance: An adversary that holds multiple keys should only be able to access data if at least one individual key grants access.

Fine Grained Access Control: Fine-grained access control is the ability to grant or deny access to critical assets, such as resources and data, based on multiple conditions and/or multiple entitlements to a single data resource. Fine-grained access control is important because it changes the rules of static authorization and enables secure sharing of many more sensitive information assets. Fine-grained authorization allows rich business rules and authorization policies to be enforced. Policy writers can create complex rules and policies that contain multiple conditions relating to time, location, role, action, and more, and these will be enforced. Rich, fine-grained controls can also be applied within a single resource.

DOI: 10.17148/IJARCCE.2023.12311

II. PROBLEM STATEMENT

The confidentiality of information and its visibility are extremely important in a scenario with various owners and users. When uploading the data to the cloud, it should be encrypted. Access to data must be managed by the owner. Due to the complexity of this phenomena, shared data management should be streamlined, resulting in straightforward key management.

III. LITERATURE REVIEW

[1] Ostrovsky. R et al., (2013) has mentioned in his paper that software protection is one of the most important issues concerning computer practice. There exist many heuristics and ad-hoc methods for protection, but the problem as a whole has not received the theoretical treatment it deserves. In this paper we provide theoretical treatment of software protection. We reduce the problem of software protection to the problem of efficient simulation on oblivious RAM. A machine is oblivious if the sequence in which it accesses memory locations is equivalent for any two inputs with the same running time. For example, an oblivious Turing Machine is one for which the movement of the heads on the tapes is identical for each computation. (Thus, it is independent of the actual input.) What is the slowdown in the running time of any machine, if it is required to be oblivious? In 1979 Pippenger and Fischer showed how a two-tape oblivious Turing Machine can simulate, on-line, a one-tape Turing Machine, with a logarithmic slowdown in the running time. We show an analogous result for the random-access machine (RAM) model of computation. In particular, we show how to do an on-line simulation of an arbitrary RAM input by a probabilistic oblivious RAM with a poly-logarithmic slowdown in the running time. On the other hand, we show that a logarithmic slowdown is a lower bound.

[2] Boneh, Dan et al., (2004) has studied the problem of searching on data that is encrypted using a public key system. Consider user Bob who sends email to user Alice encrypted under Alice's public key. An email gateway wants to test whether the email contains the keyword "urgent" so that it could route the email accordingly. Alice, on the other hand does not wish to give the gateway the ability to decrypt all her messages. We define and construct a mechanism that enables Alice to provide a key to the gateway that enables the gateway to test whether the word "urgent" is a keyword in the email without learning anything else about the email. We refer to this mechanism as Public Key Encryption with keyword Search. As another example, consider a mail server that stores various messages publicly encrypted for Alice by others. Using our mechanism Alice can send the mail server a key that will enable the server to identify all messages containing some specific keyword, but learn nothing else. We define the concept of public key encryption with keyword search and give several constructions.

[3] It is desirable to store data on data storage servers such as mail servers and file servers in encrypted form to reduce security and privacy risks. But this usually implies that one has to sacrifice functionality for security. For example, if a client wishes to retrieve only documents containing certain words, it was not previously known how to let the data storage server perform the search and answer the query without loss of data confidentiality. In this paper, we describe our cryptographic schemes for the problem of searching on encrypted data and provide proofs of security for the resulting crypto systems. Our techniques have a number of crucial advantages. They are provably secure: they provide provable secrecy for encryption, in the sense that the untrusted server cannot learn anything about the plaintext when only given the ciphertext; they provide query isolation for searches, meaning that the untrusted server cannot learn anything more about the plaintext than the search result; they provide controlled searching, so that the untrusted server cannot search for an arbitrary word without the user's authorization; they also support hidden queries, so that the user may ask the untrusted server to search for a secret word without revealing the word to the server. The algorithms we present are simple, fast (for a document of length, the encryption and search algorithms only need stream cipher and block cipher operations), and introduce almost no space and communication overhead, and hence are practical to use today as mentioned by Wagner, D et al., (2000).

[4] As Cloud Computing becomes prevalent, more and more sensitive information are being centralized into the cloud. Although traditional searchable encryption schemes allow a user to securely search over encrypted data through keywords and selectively retrieve files of interest, these techniques support only exact keyword search. In this paper, for the first time we formalize and solve the problem of effective fuzzy keyword search over encrypted cloud data while maintaining keyword privacy. Fuzzy keyword search greatly enhances system usability by returning the matching files when users' searching inputs exactly match the predefined keywords or the closest possible matching files based on keyword similarity semantics, when exact match fails. In our solution, we exploit edit distance to quantify keywords similarity and develop two advanced techniques on constructing fuzzy keyword sets, which achieve optimized storage and representation overheads. We further propose a brand-new symbol-based trie-traverse searching scheme, where a multi-way tree structure is built up using symbols transformed from the resulted fuzzy keyword sets. Through rigorous security

DOI: 10.17148/IJARCCE.2023.12311

analysis, we show that our proposed solution is secure and privacy-preserving, while correctly realizing the goal of fuzzy keyword search. Extensive experimental results demonstrate the efficiency of the proposed solution as studied by Aswani, P. et al., (2012)

[5] As so much advantage of cloud computing, more and more data owners centralize their sensitive data into the cloud. In this paper, we propose a semantic keyword ranked search scheme over the encrypted cloud data, which simultaneously meets a set of strict privacy requirements. Firstly, we utilize the “Latent Semantic Analysis” to reveal relationship between terms and documents. The relationship between terms is automatically captured. Secondly, our scheme employs secure “k-nearest neighbour (k- NN)” to achieve secure search functionality. The proposed scheme could return not only the exact matching files, but also the files including the terms latent semantically associated to the query keyword. Finally, the experimental result demonstrates that our method is better than the original MRSE scheme as mentioned by Xia, Z. et al., (2013).

IV. EXISTING SYSTEM

In existing system, they have the multi-keyword ranked search allows users to input multiple query keywords for personalized queries. Proposed the first secure multi-keyword ranked search scheme over encrypted cloud data (MRSE), and the documents are ranked by the “inner product” between file vectors and query vectors. However, they do not consider the weight of different keywords. They Proposed multi-keyword fuzzy search scheme aimed at the tolerance of both slight typos and format inconsistencies for users’ input.

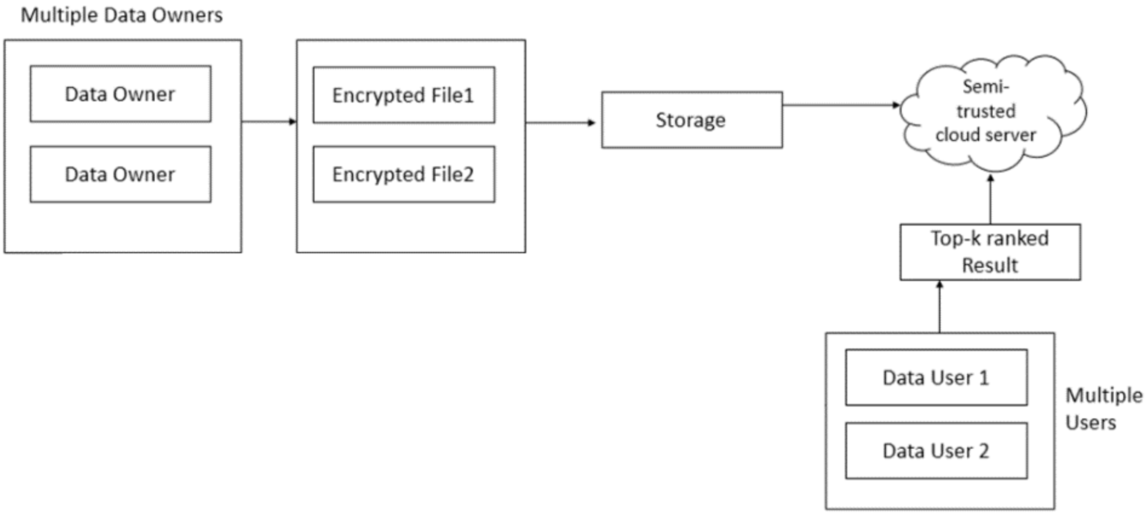

Fig. 1 Architecture of Existing System

V. PROPOSED SYSTEM

Here we focus on a special type of multi-keyword ranked search, namely the multi-keyword top-k search, which has been a very popular database operator in many important applications, and only needs to return the k documents with the highest relevance scores. For supporting multi-keyword search, we introduce the vector space model which represents documents and queries as vectors. In order to support top-k search, the relevance scores between documents and queries should be calculated, therefore, the TF_IDF (term frequency _ inverse document frequency) model is introduced as a weighting rule to compute the relevance scores for ranking purposes. To improve the query efficiency for better user experiences, we propose a group multi-keyword top-k search scheme (GMTS), which is based on partition and supports top-k similarity search over encrypted data. In this scheme, the data owner divides the keywords in the dictionary (suppose that the dictionary contains all the keywords that could be extracted from all documents) into multiple groups and establishes a searchable index for each group. We use random traversal algorithm (RTRA) to strengthen the data security, where the data owner builds a binary tree as searchable index and assigns a random switch to each node, so the data user can assign a random key to each query. Therefore, the data user can change the results and visiting paths of queries by using different keys, which maintains high accuracy of queries. Finally, we combine the GMTS and the RTRA together into an efficient and secure solution to our proposed problem.

DOI: 10.17148/IJARCCE.2023.12311

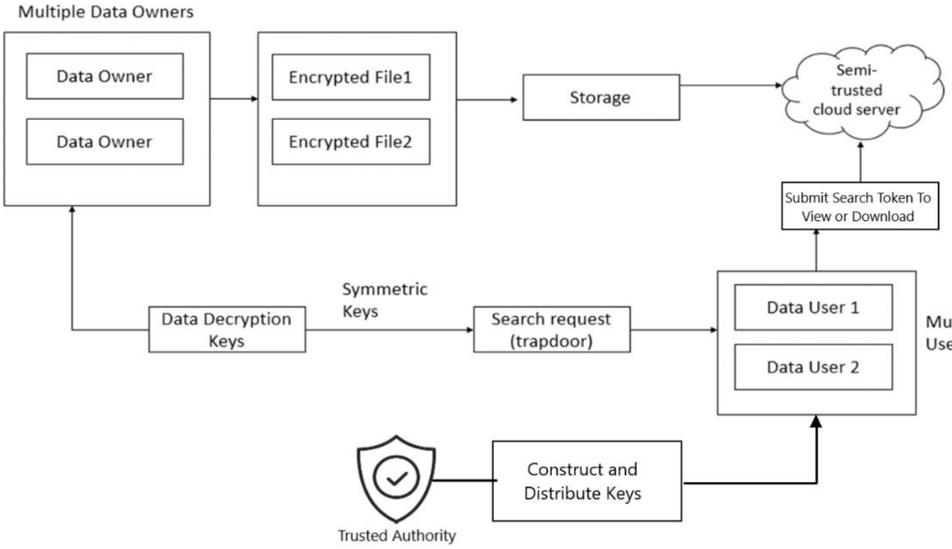

Fig. 2 Architecture of Proposed Syatem

VI. METHODOLOGY

The important concept is that both patients and physicians would register. Only doctors who have the patient ID can view the general information profile for a patient. Patients have the option of sharing their Patient ID with others. The medical history of a patient includes a variety of information on numerous specialties, including dentistry, cardiology, cancer, etc. Each area's data may also be of a variety of forms, such as test results, medical records, discharge summaries, and so on. These files are all based on various attributes. The owner will use Advanced Encryption Standard to upload these files. Moreover, this framework encrypts the data that is stored in the database. So that even if hackers get access to the database, they are unable to view the data within. Only those who are permitted inside the framework, such as data owners and doctors, are able to view the data. Only doctors have access to all of these patient facts. As a result, they may search using the patient ID anytime the information is needed.

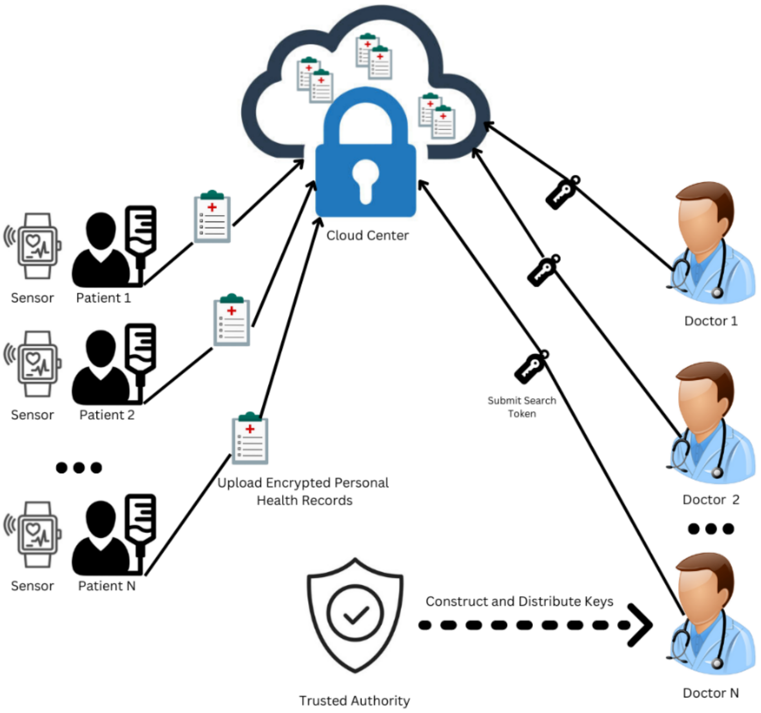

Fig. 3 System Model

DOI: 10.17148/IJARCCE.2023.12311

VII. ADVANTAGES

7.1. ADVANTAGES

- Virtual machine allocation may Differ.
- A secure ranked multi-keyword search scheme in a multi-owner model (PRMSM) that not only allows the cloud server to perform a multi-keyword search without knowing any sensitive information, but also enable the data owner to flexibly change the encryption key.
- Time Delay.
- However, these schemes rarely focus on query efficiency.
- Response time is high.

7.2. OBJECTIVE

To secure and make digital health records accessible and conveniently available for both the doctors as well as the patients at any given time. Secure the data that is uploaded so no one can have direct access to the data. This also helps efficiently manage the medical records of person without the hassle of carrying around various reports with them.

VIII. SECURITY ISSUES

On the cloud, data may be tampered with and changed. Data privacy is guaranteed by utilizing AES. There are three possible key sizes in the AES algorithm. The quantity of turns is decided by the key size. With this method, data may be both en- and re- encrypted. AES is used to transmit encrypted data in a safe manner.

IX. SOLUTIONS

Many cryptographic techniques can be used to encrypt data. Both symmetric and asymmetric algorithms are possible. Whereas RSA and ECC are asymmetric, DES as well as AES are symmetric. The effectiveness of these algorithms is displayed in the following table.

	DES	**AES**	**RSA**
Contributing Factors	IBM 75	Rijman, Joan	Rivest, Shamir
Key Length	56 - bits	128, 192, and 256	Based on No of bit in N=p*q
Block Size	64- bits	128- bits	Variant
Security	Not Good	Excellent	Good
Execution Time	Slow	Faster	Slowest

Tabel. 1 Comparison of Algorithms against AES

AES Algorithm is the strongest among these.

Although AES is less costly than ABE, it is thought to be extremely suited. The majority of data is typically encrypted using symmetric keys, whereas brief key values can be encrypted using asymmetric keys like ABE. Here, the information is secured using AES utilizing one of three different key sizes: 128 bits, 192 bits, or 256 bits. As a result, the AES algorithm key is initially used to symmetrically encrypt the data file. Afterwards, the cloud server is used to store the encrypted data. The users have access to the data by using the allocated keys that the owner has supplied.

DOI: 10.17148/IJARCCE.2023.12311

X. CONCLUSION

Given that the current healthcare system is becoming increasingly digital, it is safe to assume that e-healthcare will become more and more common in our Internet-connected culture. While this is a fairly recent field of study, building a safe and privacy-preserving system\sthat is viable for implementation remains a research problem. The article examines the two essential components of managing personal health records: data access control and security.

Here, the data is grouped according to attributes to make access control easier, and it is encrypted with AES to safeguard the record.

Future work will involve implementing the system in a practical setting (such as a small hospital) with the goal of analyzing and improving the current system to add new functions without sacrificing security and effectiveness.

REFERENCES

[1]. Ostrovsky,R et al., (2013). Distributed oblivious RAM for secure two-party computation. In Theory of Cryptography Conference (pp. 377-396). Springer, Berlin, Heidelberg.

[2]. Boneh, D., et al., (2004). Public key encryption with keyword search. In International conference on the theory and applications of cryptographic techniques (pp. 506-522). Springer, Berlin, Heidelberg.

[3]. Wagner, D., et al., (2000, May). Practical techniques for searches on encrypted data. In Proceeding 2000 IEEE symposium on security and privacy. S&P 2000 (pp. 44-55). IEEE.

[4]. Aswani, P. N., et al., (2012). Fuzzy keyword search over encrypted data using symbol-based Trietraverse search scheme in cloud computing. arXiv preprint arXiv:1211.3682.

[5]. Xia, Z., et al., (2013). An efficient and privacy-preserving semantic multi-keyword ranked search over encrypted cloud data. Advanced Science and Technology Letters, 31, 284.