ISSN: 2454-9940

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT

E-Mail :
editor.ijasem@gmail.com
editor@ijasem.org

www.ijasem.org

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT

ISSN2454-9940

www.ijasem.org

Vol 18, Issue 3, 2024

FORWARD PRIVACY PRESERVATION IN IOT-ENABLED HEALTHCARE SYSTEMS

[1]A. NAGARAJU, [2] M. SABHIHA BHANU

[1](Assistant Professor), MCA, **DANTULURI NARAYANA RAJU COLLEGE(A) PG COURSES, BHIMAVARAM ANDHRA PRADESH**

[2]MCA, scholar, **DANTULURI NARAYANA RAJU COLLEGE(A) PG COURSES, BHIMAVARAM ANDHRA PRADESH**

Abstract

In recent years, Internet of things (IoT)-enabled health monitoring wearable devices have become a trend in healthcare systems, regularly collecting vital sign data from patients and uploading them to the cloud. Through on-demand search queries, data are shared with third-party healthcare service providers (HSPs) to monitor patients' health status and provide timely diagnoses. To ensure privacy and security, patient health data should be encrypted before being uploaded to the cloud. The cloud can give search encryption services. However, current searchable encryption technologies still have problems with forward privacy security and verifiability. This paper proposes an IoT-cloud-enabled healthcare data system incorporating a searchable encryption method with forward privacy and verifiability. By designing a trapdoor permutation function, we render the resulting output indistinguishable from meaningless random data to the adversary. Thus, the adversary cannot judge the relationship between a newly inserted record and a past search token, and therefore, the system realizes forward privacy or forward secrecy. We propose a multi-keyword search verification mechanism based on a pseudo-random function (PRF). Our approach solves verifying the correctness of search results in the top-k search scenario with partial search results. A formal security analysis proves that our scheme achieves forward privacy preservation, which can help guarantee healthcare data privacy. Additionally, a performance evaluation shows that our method is efficient and effective, providing an information security system to preserve patient privacy in IoT-enabled healthcare systems.

1. INTRODUCTION

THE combination of the Internet of things (IoT) and cloud computing has become a

ISSN2454-9940
www.ijasem.org
Vol 18, Issue 3, 2024

technological trend in healthcare systems. When collected data from IoT devices are stored in the cloud and integrated into a coherent system, continuous remote monitoring and intelligent treatment of personal health problems become possible, improving patient healthcare outcomes. Such systems enable people with limited access to hospitals or limited mobility to remotely access excellent healthcare services. It allows parents to monitor their children's health and caregivers to ensure that elderly patients receive treatment as needed. For instance, in this application, a set of wearable devices periodically collects critical vital signs from a data owner (i.e., a patient). The system aggregates this information into personal health information (PHI) files and stores it on cloud servers. These PHI files are generally shared with third-party health service providers (HSPs), including doctors, through on-demand queries to monitor patients' health status and provide timely diagnoses. The combination of cloud computing and IoT wearable devices in the healthcare industry is beneficial for saving data storage space, reducing information technology (IT) costs, and improving patient treatment efficiency. However, issues of data security and personal privacy remain critical concerns in medical information systems.

Before PHI files are uploaded to cloud storage, encryption can support privacy protection functions in an e-healthcare system, but this also touches on other challenges. When third-party HSPs send on-demand queries to the cloud storage, the cloud is expected to return logically related query results rather than irrelevant results. Concurrently, encryption renders regular use of remote search in PHI files particularly challenging. Searchable encryption (SE) technology provides a promising solution to the problem of encrypted file search by adding an encrypted search index. The data owner first constructs an encrypted document index and uploads it to the cloud with the encrypted document. Any legitimate user can generate a search token, sometimes called a trapdoor. According to the received search token, the server searches the encrypted data and finally returns the search results to the user. Throughout the process, the document, search index, and search token all remain encrypted. The server can complete the search without obtaining the unencrypted plaintext information, and data privacy is effectively protected.

However, in a real environment, the data is dynamic and subject to users' change over time. Therefore, searchable encryption should support dynamic updates to protect

the stored data and search for privacy. Also, the system is allowed to modify the security index and encrypted documents themselves dynamically. Nevertheless, this modification of encrypted data causes a forward security problem; that is, the insert operation reveals the inserted data's content. The server can match the index corresponding to the newly inserted data using a legitimate search token generated by past users. Using this access, a user can distinguish data containing previous keyword searches, which still can result in a healthcare data privacy violation through unauthorized information disclosure. Moreover, considering that the third-party storage server is usually regarded as a semi-trusted entity, it may deliberately return wrong search results to mislead users. To save computing resources, the server may also submit empty sets as search results to users. Therefore, searchable encryption schemes should be port users' verification of the correctness of the results.

Forward privacy and verifiability, or forward secrecy, has received recent attention in the field of searchable encryption (SE). The purpose of forward security is to prevent the server from judging whether the updated content contains keywords from previous user search requests. It also helps verifiability consider the malicious modification of search data on the server, which requires an additional authentication mechanism to ensure that users can judge whether search results are correct.

However, few studies have been conducted on SE schemes that satisfy both forward security and verifiability. It remains necessary to design appropriate verification mechanisms to provide a Défense for SE schemes' forward security properties against potential attack.

Searchable symmetric encryption (SSE), first introduced by Song et al. [1], is designed to protect remote data privacy, with a search time linear to documents' length. Considering the need to update data on remote servers, Kamara et al. [2] proposed a dynamic, searchable symmetric encryption (DSSE) with an optimal search time to allow the data owner to dynamically modify the encrypted data, i.e., to perform an insert or delete operation.

Key-value (KV) store systems [3,4] with high performance and scalability have become popular recently. Yuan et al. [5] proposed a distributed DSSE scheme based on Redis KV, and the authors in [6] subsequently proposed an encrypted and distributed KV store with an EncKV scheme. These methods provide a range-match search model hiding order relations and partial information with ciphertexts and order-revealing encryption (ORE). The

ISSN2454-9940
www.ijasem.org
Vol 18, Issue 3, 2024

search time for an exact-match model is optimal, while the search time for a range-match model is linear to the number of records.

2. EXISTING SYSTEM

The present article throws light on advancement in ICTs. It is an evident that highly intelligent and smart IoT based use cases are possible with the advent in ICTs like Internet of Things, 5G Cellular Technology and Cyber- Physical Systems (CPS). For an instance, people spend considerable amount of their earning towards health in the present scenario. In view of this, there is high- impact- on society use case in Healthcare as IoT enables Ambient Assisted Living (AAL), Mobile Health (mHealth) and Electronic Health (eHealth).

The conventional healthcare services are prone to delay, wastage of time and money, besides causing death of people. With intelligence and prediction capabilities of IoT, Remote Patient Monitoring (RPM) on regular basis (home/office/in-hospital), for those who deliberately need it, can be exploited to overcome challenges thrown by conventional healthcare units. IoT based RPM with wearable devices, sensor network and other digital infrastructure form an early warning system for impending emergencies that lead to severe health issues and even death of patients is left untreated or even treatment is delayed. It is proposed that a secure and privacy preserving IoT integration with healthcare units for realizing a reliable, available and secure RPM system at the conclusion.

An existing system provides secure RFID based authentication, end-to-end secure communications and privacy protection. The system includes MOTO 360 watch (biosensor | body sensor) with Android wearable OS, server with REST framework and a smart phone application to monitor and detect fall, blood pressure and heart rate. This motivating scenario is enriched with security and privacy. The empirical evaluation revealed that the proposed RPM has potential to help improve quality of life and healthcare services.

Disadvantages

- The system is not implemented Machine Learning Algorithms to optimize datasets.
- The support vector machine (SVM) algorithm is a supervised classifier that is not applied widely to solve classification and regression problems.

3. PROPOSED SYSTEM

We propose a scheme called FEncKV, based on a trapdoor permutation and a status count.

ISSN2454-9940
www.ijasem.org
Vol 18, Issue 3, 2024

We prove that FEncKV has the feature of forward privacy, meaning that an adversary is unable to determine the relationship between a previous search query and a newly added record.

Forward privacy and verifiability, or forward secrecy, has received recent attention in the field of searchable encryption (SE). The purpose of forward security is to prevent the server from judging whether the updated content contains keywords from previous user search requests. It also helps verifiability consider the malicious modification of search data on the server, which requires an additional authentication mechanism to ensure that users can judge whether search results are correct. However, few studies have been conducted on SE schemes that satisfy both forward security and verifiability. It remains necessary to design appropriate verification mechanisms to provide a defense for SE schemes' forward security properties against potential attack.

Advantages

1. We improve on EncKV to satisfy the condition of forward privacy. This approach ensures that an adversary cannot learn the relationship between an inserted record and a previous search query.
2. The main contribution of this system is used machine learning algoriths to predict the threats and to categories the threats.

4. MODULES

Service Provider

In this module, the Service Provider has to login by using valid user name and password. After login successful he can do some operations such as Login,Browse IOT Datasets and Train & Test Data Sets, View Trained and Tested Accuracy in Bar Chart, View Trained and Tested Accuracy Results, View Prediction Of Threat Detection Status, View Threat Detection Status Ratio, Download Predicted Data Sets, View Threat Detection Ratio Results, View All Remote Users..

View and Authorize Users

In this module, the admin can view the list of users who all registered. In this, the admin can view the user's details such as, user name, email, address and admin authorizes the users.

Remote User

In this module, there are n numbers of users are present. User should register before doing any operations. Once user registers, their details will be stored to

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT
ISSN2454-9940
www.ijasem.org
Vol 18, Issue 3, 2024

the database. After registration successful, he has to login by using authorized user name and password. Once Login is successful user will do some operations like REGISTER AND LOGIN, PREDICT THREAT DETECTION, VIEW YOUR PROFILE.

5. OUTPUT SCREENS

=

6. CONCLUSION

In this study, we designed a trapdoor permutation method and proposed a verifiable forward searchable encryption scheme. After each insertion update, the corresponding state counter is transformed by the trapdoor replacement function and a private key to replace the incrementing method each time in the original scheme. Because the trapdoor permutation function's output is indistinguishable from

random numbers to the adversary, the adversary cannot judge the relationship between a newly inserted record and a past search token FEncKV has forward private security or a forward private secrecy cryptographic feature. Besides, we proposed a multi-keyword search verification mechanism based on a pseudo-random function. Our approach solved the problem of verifying the correctness of search results in the top-K search scenario with only partial search results. The experimental results show that the proposed FEncKV scheme is suitable for IoT-enabled healthcare systems.

7. REFERENCES

[1] D. X. Song, D. Wagner, and A. Perrig, "Practical Techniques for Searches on Encrypted
Data," in IEEE Symposium on Security & Privacy, 2002.

[2] S.Kamara,C.PapamanthouandT.Roeder,Dynamicsearchablesymmetricencryption,in computer and communications security, 2012, pp. 965-976.

[3] Ma W, Zhu Y, Li C, et al. BiloKey: A Scalable Bi-Index Locality-Aware In-Memory
Key-Value Store, in IEEE Transactions on Parallel and Distributed Systems, 30(7), 2019:1528 - 1540.

[4] Anwar A, Cheng Y, Huang H, et al. Customizable Scale-Out Key-Value Stores, in IEEE
Transactionson Parallel and Distributed Systems, 2020, 31(9):2081-2096.

[5] X. Yuan, X. Wang, C.Wang, C. Qian, and J. Lin, Building an Encrypted, Distributed, and
Searchable Key-value Store, incomputer and communications security, 2016.

[6] Guo Y, Yuan X, Wang X, et al. Enabling Encrypted Rich Queries in Distributed
Key-value Stores, in IEEE Transactions on Parallel and Distributed Systems, 2018, 30(6):
1283 -1297.

[7] Li H, Yang Y, Dai Y, et al. Achieving Secure and Efficient Dynamic Searchable Symmetric Encryption over Medical Cloud Data, in. IEEE Transactions on Cloud Computing, 2017:1-1.

[8] Wang Q, He M, Du M, et al. Searchable Encryption over Feature-Rich Data, in IEEE
Transactions on Dependable & Secure Computing, 2018:1-1.

[9] Li H, Yang Y, Dai Y, et al. Achieving Secure and Efficient Dynamic Searchable Symmetric Encryption over Medical Cloud Data, in IEEE Transactions on Cloud Computing, 2017:1-1.

ISSN2454-9940
www.ijasem.org
Vol 18, Issue 3, 2024

[10] Chen B, Wu L, Kumar N, et al. Lightweight Searchable Public-key Encryption with
ForwardPrivacy overIIoT Outsourced Data,in IEEETransactionsonEmerging Topicsin
Computing, 2019, PP (99):1-1.

[11] Li H, Yang Y, Dai Y, et al. Achieving Secure and Efficient Dynamic Searchable Symmetric Encryption over Medical Cloud Data, in IEEE Transactions on Cloud Computing, 2020, 8(2):484-494.

[12] Song X, Dong C, Yuan D., et al. Forward Private Searchable Symmetric Encryption with
Optimized I/O Efficiency, in IEEE Transactions on Dependable & Secure Computing,
2017, 17(5): 912-927.

[13] Chen B, Wu L, Wang H, et al. A Blockchain-Based Searchable Public-Key Encryption
with Forward and Backward Privacy for Cloud-Assisted Vehicular Social Networks, in
IEEE Transactions on Vehicular Technology, 2020, 69(6):5813-5825.

[14] Xiong H, Mei Q, Zhao Y, et al. Scalable and Forward Secure Network Attestation with
Privacy-Preserving in Cloud-Assisted Internet of Things, in IEEE Sensors Journal, 2019,
19 (18): 8317-8331.

[15] Li H, Liu L, Lan C, et al. Lattice-Based Privacy-Preserving and Forward-Secure Cloud
Storage Public Auditing Scheme, in IEEE Access, 2020, 8: 86797-86809.