

STREAMLINED AND SECURED DATA DEDUPLICATION METHOD FOR HEALTH RECORDS

R.Deepika, Assistant Professor CSE, Vaagdevi College of Engineering (Autonomous), India
Mohammed Khaja Ali, UG Student, CSE, Vaagdevi College Of Engineering (Autonomous), India
Rakkireddy Vinod, UG Student, CSE, Vaagdevi College Of Engineering (Autonomous), India
Thakur Adithya Singh, UG Student CSE, Vaagdevi College Of Engineering (Autonomous), India
Akuthota Bunny, UG Student CSE, Vaagdevi College Of Engineering (Autonomous), India

ABSTRACT

In this project, we analyze the inherent characteristic of electronic medical records (EMRs) from actual electronic health (eHealth) systems, where we found that (1) multiple patients would generate large amounts of duplicate EMRs and (2) cross patient duplicate EMRs would be generated numerous only in the case that the patients consult doctors in the same department. We then propose the first efficient and secure encrypted EMRs deduplication scheme for cloud-assisted eHealth systems (HealthDep). With the integration of our analysis results, HealthDep allows the cloud server to efficiently perform the EMRs deduplication, and enables the cloud server to reduce storage costs by more than 65% while ensuring the confidentiality of EMRs. Security analysis shows that HealthDep is more secure than the Marforio et al.'s scheme (NDSS 2014) and Bellare et al.'s scheme (USENIX Security 2013). Algorithm implementation and performance analysis demonstrate the feasibility and high efficiency of HealthDep.

INTRODUCTION

APPLYING Internet of Things (IoT) technologies with the integration of cloud computing in various industries has already shown great potential in improving the quality of services in these industry systems [1], [2], [3], [4]. One of the most prominent manifestations is the cloud-assisted electronic health (eHealth) systems [5], [6]. Such systems provide a more efficient, less error-prone, and more reliable way to manage electronic medical records (EMRs) for both healthcare providers and patients, compared with traditional paper-based systems. Specifically, cloud-assisted eHealth systems not only allow medical institutions to outsource EMRs to the storage server and access them flexibly without incurring substantial storage and maintain costs in practice [7], but also make a great contribution to the judgement and dispute resolution in medical malpractice [8].

Generally, the storage server needs to store the outsourced EMRs, such as prescriptions, for a prolonged period of time to satisfy several government regulations or hospital requirements on EMRs archiving. With the volume of EMRs generated from health systems grows over time, the costs of storing EMRs are persistently increase in practice. Actually, the storage costs can be reduced significantly after deduplication, where the storage server checks duplicate EMRs and deletes the redundant ones. For example, as shown in Fig. 1(a) and 1(b), both two patients (one is diagnosed with coronary heart disease and stable angina pectoris, and the other one is diagnosed with hypertension) need to use "Aspirin Enteric-coated Tablets", "Metoprolol Tartrate Tablets", and "Nifedipine Sustained-release Tablets" with the same usage and dosage. Table I shows the savings of storage costs that performing deduplication on prescriptions from an actual eHealth system, these prescriptions are selected randomly from 10000 prescriptions generated by doctors from Department of Cardiology during 2013-2017. The results demonstrate that the storage costs can be reduced by more than 66% in the case of 500 prescriptions. However, from the perspective of data owners including both medical institutions and patients, the content of EMRs should not be leaked for security reasons. Therefore, privacy protection of the EMRs' content against anyone who does not own the EMRs should be guaranteed. This can be achieved by conventional encryption, but its randomness (i.e. for the same message, different users produce different ciphertexts) makes deduplication impossible.

Message-locked encryption (MLE) is a cryptographic primitive that supports encrypted data deduplication, where the key used for encryption and decryption is itself derived from the data [9]. However, EMRs are inherently low entropy. For example, a list of most existing antibiotics can be found in [10], the list only involves about 100 items. Actually, most EMR candidates can be enumerated quickly by adversaries, this problem is further exacerbated by the fact that an adversary has sufficient contextual information (e.g. patients' symptoms). As a consequence, the outsourced EMRs protected by MLE is vulnerable to brute-force ciphertext recovery. Recently, Bellare et al. [10] proposed the first encrypted data deduplication scheme with resistance against brute-force attacks, namely DupLESS. In DupLESS, a dedicated key server is introduced to assist users in generating MLE keys. Each user requests to the key server for the MLE key in an oblivious way such that the user can obtain a message-derived key from the key server without leaking any information about his/her data to it. Integrating DupLESS with cloud-assisted eHealth systems can achieve both EMRs' privacy protection and encrypted EMRs deduplication, however, there are two problems in this mechanism:

DupLESS as well as some subsequent schemes [9], [6] bears a strong assumption: the generation of MLE keys requires a fully trusted entity (e.g. the key server in [3], and the dealer in [2]), and thereby are vulnerable to brute-force attacks when the trusted entity is compromised; As the number of EMR fields is huge, checking duplicate EMRs requires the storage server to scan the entire EMR database and check the EMR fields one by one. Consequently, employing existing schemes to check duplicate EMRs incurs a huge delay and becomes a bottleneck in applications.

LITERATURE SURVEY

Cloud computing represents today's most exciting computing paradigm shift in information technology. However, security and privacy are perceived as primary obstacles to its wide adoption. Here, the authors outline several critical security challenges and motivate further investigation of security solutions for a trustworthy public cloud environment.

Problem Statements :

Identification of Critical Security Challenges in Public Cloud Computing:

What are the primary security challenges faced by users and providers of public cloud services, and how do these challenges impact the adoption and trustworthiness of cloud computing environments?

Analysis of Perceived Security and Privacy Obstacles in Public Cloud Adoption:

How are security and privacy concerns perceived by stakeholders in the context of public cloud computing, and what strategies can be developed to address these obstacles and promote wider adoption of cloud technologies?

Exploration of Security Solutions for Trustworthy Public Cloud Environments:

What are the key security solutions and technologies that can be implemented to enhance the trustworthiness of public cloud environments, and how can these solutions effectively mitigate security risks and vulnerabilities?

Evaluation of Existing Security Measures in Public Cloud Services:

How effective are current security measures implemented by public cloud providers in addressing security challenges, and what areas require further investigation and improvement to ensure the integrity, confidentiality, and availability of cloud-based data and services?

Development of Comprehensive Security Frameworks for Public Cloud Infrastructure:

What frameworks and methodologies can be developed to establish a comprehensive security architecture for public cloud environments, considering factors such as data protection, access control, encryption, and compliance with regulatory requirements?

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. We describe our cryptographic schemes [7] 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 presented are simple, fast (for a document of length n , the encryption and search algorithms only need $O(n)$ stream cipher and block cipher operations), and introduce almost no space and communication overhead, and hence are practical to use today.

Problem Statements :

Enhancing Data Security in Storage Servers Through Encryption:

How can data storage servers such as mail servers and file servers effectively utilize encryption techniques to mitigate security and privacy risks associated with storing sensitive data, without sacrificing functionality?

Developing Cryptographic Schemes for Searching Encrypted Data:

What cryptographic schemes and techniques can be developed to enable searches on encrypted data stored on untrusted servers, while ensuring provable secrecy, query isolation, controlled searching, and support for hidden queries?

Ensuring Provably Secure Encryption and Search Mechanisms:

What methods can be employed to provide provable secrecy for encryption, preventing untrusted servers from learning anything about the plaintext from the ciphertext, and ensuring query isolation to restrict the server's access to plaintext beyond search results?

Supporting Controlled Searching and Hidden Queries:

How can cryptographic algorithms be designed to support controlled searching, allowing users to authorize specific search queries while preventing arbitrary searches by untrusted servers, and enabling hidden queries where the server searches for a secret word without revealing it to the server?

Optimizing Efficiency and Practicality of Cryptographic Algorithms:

What approaches can be taken to develop cryptographic algorithms that are simple, fast, and practical for use in today's data storage environments, with minimal space and communication overhead, while still providing robust security guarantees.

A secure index is a data structure that allows a querier with a "trapdoor" for a word x to test in $O(1)$ time only if the index contains x ; The index reveals no information about its contents without valid trapdoors, and trapdoors can only be generated with a secret key. Secure indexes are a natural extension of the problem of constructing data structures with privacy guarantees such as those provided by oblivious and history independent data structures. In this paper, we formally define a secure index and formulate a security model for indexes known as semantic security against adaptive chosen keyword attack (ind-cka). We also develop an efficient indcka secure index construction called z -idx using pseudo-random functions and Bloom filters, and show how to use z -idx to implement searches on encrypted data. This search scheme is the most efficient encrypted data search scheme currently known; It provides $O(1)$ search time per document, and handles compressed data, variable length words, and boolean and certain regular expression queries. The techniques developed in this paper can also be used to build encrypted searchable audit logs, private database query schemes, accumulated hashing schemes, and secure set membership tests.

Development of Efficient Secure Indexes:

How can secure indexes be efficiently constructed to allow a querier with a "trapdoor" for a word x to test in $O(1)$ time if the index contains x , while revealing no information about its contents without valid trapdoors and ensuring trapdoors can only be generated with a secret key. [8]

Formulation of Security Models for Secure Indexes:

What security models can be formulated to ensure semantic security against adaptive chosen keyword attacks (ind-cka) for secure indexes, providing robust privacy guarantees while allowing efficient keyword searches?

Exploration of Efficient Construction Techniques for Secure Indexes:

How can pseudo-random functions and Bloom filters be effectively utilized to develop efficient ind-cka secure index constructions, such as z-idx, for implementing searches on encrypted data with $O(1)$ search time per document and support for compressed data, variable-length words, boolean queries, and certain regular expression queries?

Application of Secure Index Techniques in Encrypted Data Searches:

How can the techniques developed for secure indexes be applied to implement efficient searches on encrypted data, enabling applications such as encrypted searchable audit logs, private database query schemes, accumulated hashing schemes, and secure set membership tests?

Evaluation and Comparison of Secure Index Schemes:

What methodologies can be employed to evaluate and compare the efficiency, security, and practicality of different secure index schemes, and how do these schemes perform compared to existing encrypted data search schemes in terms of search time, space complexity, and query handling capabilities.

Searchable symmetric encryption (SSE) allows a party to outsource the storage of his data to another party in a private manner, while maintaining the ability to selectively search over it. This problem has been the focus of active research and several security definitions and constructions have been proposed. In this paper we begin by reviewing existing notions of security and propose new and stronger security definitions. We then present two constructions that we show secure under our new definitions. Interestingly, in addition to satisfying stronger security guarantees, our constructions are more efficient than all previous constructions. Further, prior work on SSE only considered the setting where only the owner of the data is capable of submitting search queries. We consider the natural extension where an arbitrary group of parties other than the owner can submit search queries. We formally define SSE in this multi-user setting, and present an efficient construction

Development of Efficient Secure Indexes:

How can secure indexes be efficiently constructed to allow a querier with a "trapdoor" for a word x to test in $O(1)$ time if the index contains x , while revealing no information about its contents without valid trapdoors and ensuring trapdoors can only be generated with a secret key.

Formulation of Security Models for Secure Indexes:

What security models can be formulated to ensure semantic security against adaptive chosen keyword attacks (ind-cka) for secure indexes, providing robust privacy guarantees while allowing efficient keyword searches?

Exploration of Efficient Construction Techniques for Secure Indexes:

How can pseudo-random functions and Bloom filters be effectively utilized to develop efficient ind-cka secure index constructions, such as z-idx, for implementing searches on encrypted data with $O(1)$ search time per document and support for compressed data, variable-length words, boolean queries, and certain regular expression queries?

Application of Secure Index Techniques in Encrypted Data Searches:

How can the techniques developed for secure indexes be applied to implement efficient searches on encrypted data, enabling applications such as encrypted searchable audit logs, private database query schemes, accumulated hashing schemes, and secure set membership tests?

Evaluation and Comparison of Secure Index Schemes:

What methodologies can be employed to evaluate and compare the efficiency, security, and practicality of different secure index schemes, and how do these schemes perform compared to existing encrypted data search schemes in terms of search time, space complexity, and query handling capabilities.

PROBLEM STATEMENT

In the proposed system, Data deduplication techniques play an important role in cloud storage systems, it enables storage server to delete duplicate data and store only a single copy of the data to reduce storage costs. To support encrypted data deduplication, Douceur et al. [8] proposed convergent encryption (CE), which requires that the data is encrypted by using a symmetric encryption, in which the encryption key is the hash of the data. Following the Douceur et al.'s work, researchers proposed many CE variants.

- Bellare et al. [9] first formalized CE and its variants under the name of message-locked encryption (MLE). Essentially, an MLE scheme is a symmetric encryption scheme, where the encryption/decryption key is derived from the data itself. As such, an MLE-based deduplication scheme cannot thwart brute-force dictionary attacks [9].
- Bellare et al. [10] first proposed the DupLESS, which introduces a dedicated key server to generate MLE keys for users (i.e., hash values protected under the key server's secret). The users interact with the key server through an oblivious protocol, which protects the data information from the key server, and guarantees that the users who own the same data would obtain the same MLE key. This mechanism is able to resist brute-force attacks and has been attractive enough to see significant usage, with server aided deduplication deployed in [9]. Nevertheless, these schemes require that the generation of MLE key needs a fully trusted entity and thereby the trusted entity (e.g., the key server in the DupLESS and the dealer in [10] becomes the single point of failure. A more comprehensive survey on secure data deduplication can be found in .

DISADVANTAGES OF EXISTING SYSTEM

- Dependency on Fully Trusted Entities: Existing systems, such as DupLESS, require a fully trusted entity (e.g., key server or dealer) for the generation of message-locked encryption (MLE) keys. This dependency introduces a single point of failure, as the compromise of the trusted entity could lead to security breaches or data loss.
- Single Point of Failure: The reliance on a single trusted entity as the key server or dealer poses a significant risk to the overall security and reliability of the system. If the trusted entity experiences a failure or is compromised, it could disrupt the entire deduplication process and compromise the confidentiality of the stored data.
- Limited Resistance Against Brute-Force Attacks: Message-locked encryption (MLE) schemes, including those proposed by Bellare et al., are susceptible to brute-force dictionary attacks. Since the encryption/decryption key is derived from the data itself, adversaries could potentially guess the key by iterating through possible data values, compromising the security of the deduplication process.
- Complexity of Implementation: Systems like DupLESS, which introduce a dedicated key server and utilize oblivious protocols for interaction, may involve complex implementation requirements. Managing and securing the communication between users and the key server adds complexity to the system architecture and increases the risk of implementation errors or vulnerabilities.
- Risk of Data Exposure: While systems like DupLESS aim to protect data information from the key server through oblivious protocols, there remains a risk of data exposure or leakage in case of

protocol vulnerabilities or misconfigurations. Adversaries could exploit weaknesses in the communication protocol to gain access to sensitive data or MLE keys.

PROPOSED SYSTEM

- In the proposed system, the system proposes the first efficient and secure encrypted EMRs deduplication scheme for cloud-assisted e- Health systems, and realize it in a system called HealthDep. In HealthDep, multiple dedicated key servers are introduced to assist in generating MLE keys, where these key servers share a secret via a distributed protocol and the MLE key is generated by the EMR itself and the secret jointly through an oblivious protocol. This guarantees that the confidentiality of outsourced EMRs cannot be violated by brute-force attackers when one or more key servers are compromised, and therefore provides a stronger security guarantee compared with existing schemes [10].

- We also analyze the medical data existing in actual eHealth systems. The key observation from the analysis is that patients consulted the doctors with the same department would generate numerous duplicate EMRs, while patients consulted the doctors with the different departments would generate few duplicate EMRs. As such, the storage server is able to quickly determine whether to perform duplicate checking when given two patients' EMRs, which significantly improves the efficiency of checking duplicate EMRs. Furthermore, as most persons already have equipped with smartphones, current cloud-assisted eHealth systems always assume that the patients are only equipped with mobile devices and deployment of the smartphone on the patient side is practical. HealthDep makes use of system-wide Trusted Execution Environments (TEEs) , such as ARM TrustZone , to handle the patients' tasks on their smartphones. Specifically, the contributions of this work are as follows.

- The system analyzes the inherent characteristic of EMRs from actual eHealth systems. The results show that (a) EMRs are inherently low entropy and (b) cross-patient duplicate EMRs would be generated numerous in the case that the patients consult in the same department.

- The system proposes the first efficient and secure encrypted EMRs deduplication for eHealth systems, namely HealthDep, where the patients store MLE keys in the secure storage of their smartphones' TEEs. HealthDep provides a stronger security guarantee compared with existing schemes [11], [13], due to its resistance against bruteforce attacks in the case that one or more key servers are compromised. We also present security analysis to demonstrate that HealthDep is secure against more powerful adversaries (compared with [16]) that can additionally control cellular network communications.

- The system implements the algorithm running in the patient smartphone on the Open Virtualization's SierraVisor and SierraTEE [7], which demonstrates the feasibility of HealthDep, and shows that HealthDep can be easily deployed; We also conduct a comprehensive performance analysis, which shows the high efficiency of HealthDep in terms of MLE keys' generation.

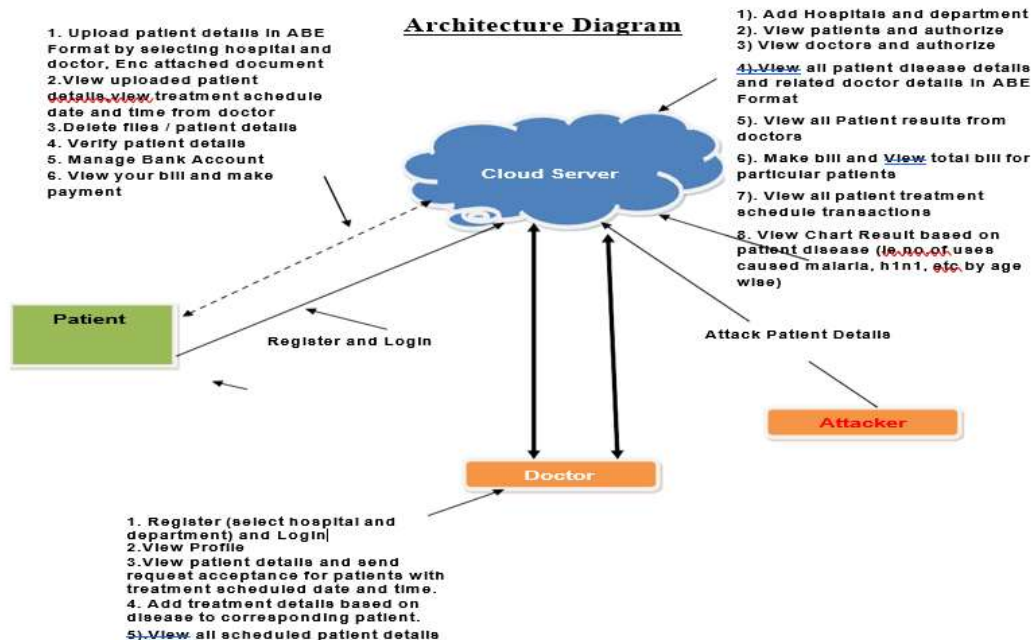
ADVANTAGES OF PROPOSED SYSTEM

- Stronger Security Guarantee: HealthDep introduces multiple dedicated key servers and utilizes distributed protocols to generate message-locked encryption (MLE) keys. This approach enhances security by ensuring that the confidentiality of encrypted electronic medical records (EMRs) cannot be violated even if one or more key servers are compromised. Compared to existing schemes, HealthDep provides a stronger security guarantee against brute-force attacks.

- Efficient Duplicate EMR Checking: The system analyzes the inherent characteristics of EMRs from actual eHealth systems and observes that cross-patient duplicate EMRs are generated numerous in cases where patients consult in the same department. HealthDep leverages this insight to efficiently determine whether to perform duplicate checking when given two patients' EMRs, significantly improving the efficiency of duplicate EMR detection.

- Utilization of Trusted Execution Environments (TEEs): HealthDep leverages system-wide Trusted Execution Environments (TEEs), such as ARM TrustZone, to handle patient tasks on their smartphones. This approach ensures the security and integrity of patient data by executing critical operations within secure environments, enhancing the overall security posture of the system.
- Resistance Against Powerful Adversaries: The security analysis demonstrates that HealthDep is secure against more powerful adversaries that can control cellular network communications, providing robust protection against various attack vectors and scenarios.
- Feasibility and Ease of Deployment: The implementation of HealthDep running on Open Virtualization's SierraVisor and SierraTEE demonstrates the feasibility of the system and its ease of deployment. This indicates that HealthDep can be readily integrated into existing eHealth systems without significant infrastructure changes or operational overhead.

SYSTEM ARCHITECTURE



IMPLIMENTATION

6.1 Patient Module:

Patients register and wait for admin approval. Upon approval, they access their accounts to view profiles, search hospitals, view doctor details, check bed availability, and access medicine details.

6.2 Cloud Server Module:

The central storage and processing hub of the system. It securely stores and manages encrypted health records, facilitates communication between modules, implements data deduplication, and ensures data integrity, confidentiality, and availability.

6.3 Doctor Module:

Doctors register and wait for admin approval. Upon approval, they access their accounts to manage appointments, access patient records, prescribe medications, update treatment plans, communicate with peers, access medical resources, and collaborate with hospitals.

EXPERIMENTAL RESULTS



RECORDS

Health Care
 Doctor
 Hospital
 Pharmacist
 Nurse
 Dentist
 First Aid
 Surgeons
 Emergency

MEDICAL
 Hi mohan !! (Doctor)
 Logout

MEDICAL

All Scheduled Patients !!!

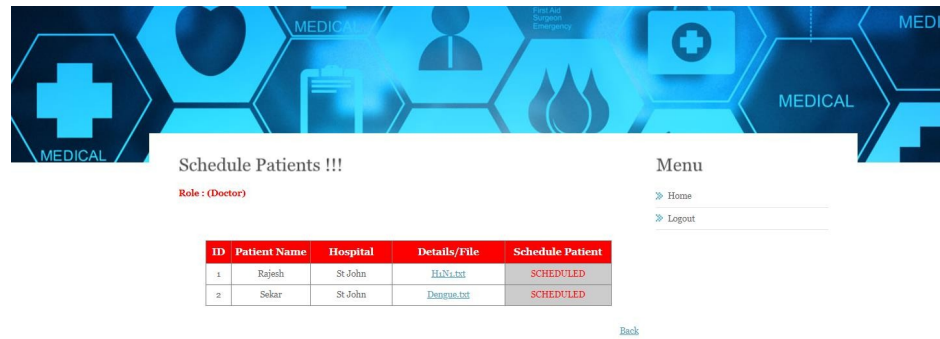
Role : (Doctor)

ID	Patient Name	Hospital	Scheduled Date	Scheduled Time	Details/File
1	Rajesh	St John	2018-12-28	13:00	HiN.txt
2	Sekar	St John	2018-12-14	13:00	Dengue.txt

Menu

- » Home
- » Logout

[Back](#)



MEDICAL

MEDICAL

MEDICAL

Schedule Patients !!!

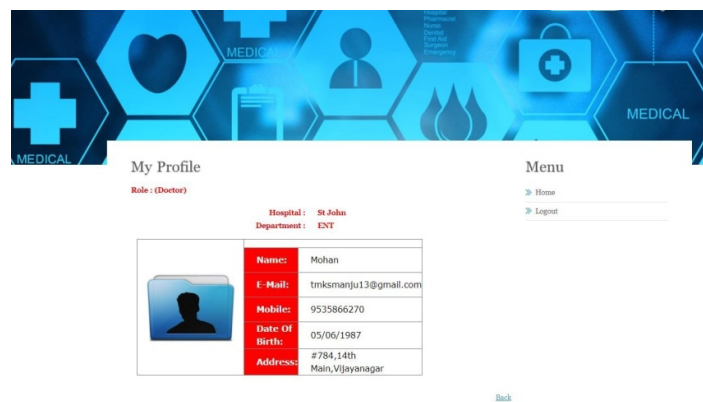
Role : (Doctor)

ID	Patient Name	Hospital	Details/File	Schedule Patient
1	Rajesh	St John	HiN.txt	SCHEDULED
2	Sekar	St John	Dengue.txt	SCHEDULED

Menu

- » Home
- » Logout

[Back](#)



MEDICAL


MEDICAL

MEDICAL

My Profile

Role : (Doctor)

Hospital : St John
 Department : ENT

	Name: Mohan
	E-Mail: tmksmanju13@gmail.com
	Mobiles: 9535866270
	Date Of Birth: 05/06/1987
	Address: #784,14th Main,Vijayanagar

Menu

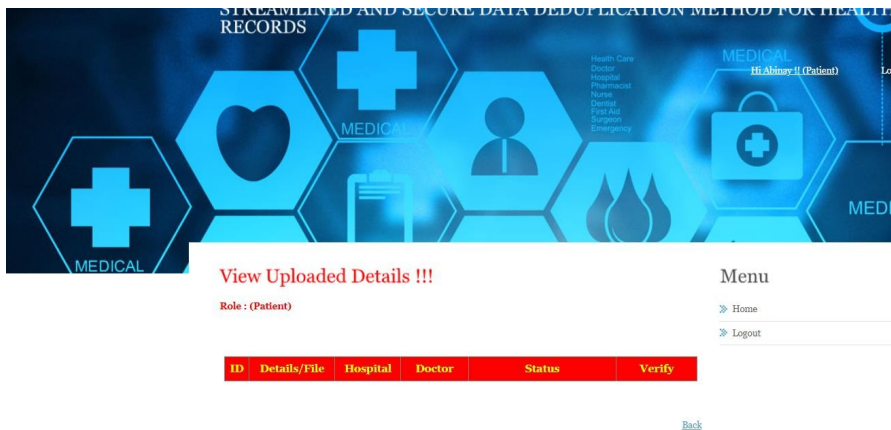
- » Home
- » Logout

[Back](#)





1.





Patient Register !!!

Menu

- » Home
- » Patient
- » Doctor
- » Cloud

Name (required) :

Password (required) :

Email Address (required) :

Mobile Number (required) :

Your Address :

Date of Birth (required) :

Select Gender (required) :

Enter Pincode (required) :

Enter Location (required) :

Select Profile Picture (required) : No file chosen



Hi Abinay !!

Role : (Patient)



Menu

- » Home
- » Upload Details
- » View Details
- » Delete Details
- » Bank Account
- » Make Payment
- » Logout

In this paper, we analyze the inherent characteristic of electronic medical records (EMRs) from actual electronic health (eHealth) systems, where we found that (1) multiple patients would generate large amounts of duplicate EMRs and (2) cross-patient duplicate EMRs would be generated numerously only in the case that the patients consult doctors in the same department. We then propose the first efficient and secure encrypted EMRs deduplication scheme for cloud-assisted eHealth systems (HealthDep). With the integration of our analysis results, HealthDep allows the cloud server to efficiently perform the EMRs deduplication, and enables the cloud server to reduce storage costs by more than 65% while ensuring the confidentiality of EMRs. Security analysis shows that HealthDep is more secure than the Starfotis et al.'s scheme (NDSS 2014) and Bellare et al.'s scheme (USENIX security 2012). Algorithm implementation and performance analysis demonstrate the feasibility and high efficiency of HealthDep.



Patient Login !!!

Menu

- » Home
- » Patient
- » Doctor
- » Cloud

Name (required)

Password (required)

New User? click here to [Register](#)

MEDICAL

Upload Patient Details !!!

Role : (Patient)

Menu
» Home
» Logout

Patient Name :	Abinay
File Name :	
Patient Disease :	
Enter Age :	
Blood Group :	
Gender :	Male
E-mail :	brksmanju13@gmail.com
Mobile No :	9535899270
Select Hospital :	-Select-
Select File :	Choose File No file chosen



Introduction



In this paper, we analyze the inherent characteristic of electronic medical records (EMRs) from actual electronic health (eHealth) systems, where we found that (1) multiple patients would generate large amounts of duplicate EMRs and (2) cross-patient duplicate EMRs would be generated numerously only in the case that the patients consult doctors in the same department. We then propose the first efficient and secure encrypted EMRs deduplication scheme for cloud-assisted eHealth systems (HealthDep). With the integration of our analysis results, HealthDep allows the cloud server to efficiently perform the EMRs deduplication and enables the cloud server to reduce storage costs by

Menu

- » Home
- » Patient
- » Doctor
- » Cloud Server

Concepts

- » Cloud-assisted eHealth systems,
- » secure deduplication,
- » ARM TrustZone



Authorize Doctors !!!

ID	Doctor Name	Status
1	Mohan	Authorized
2	Suresh	Authorized

Menu

- » Home
- » Logout

[Back](#)



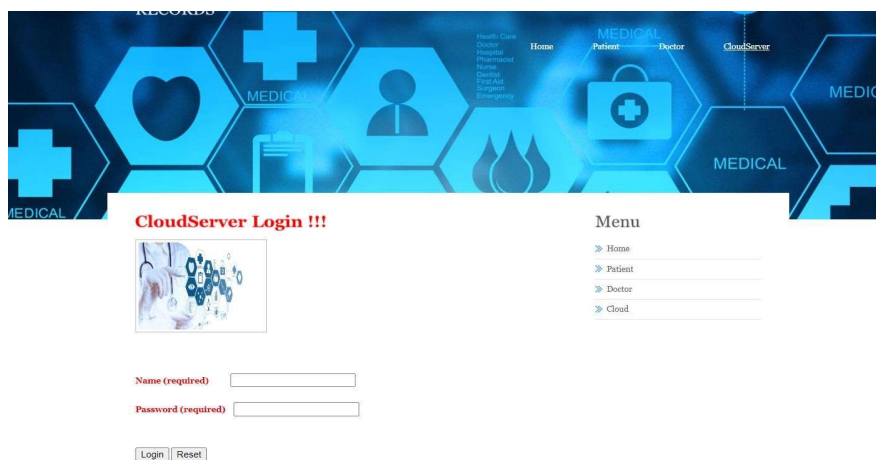
Welcome Cloud Server !!!



In this paper, we analyze the inherent characteristic of electronic medical records (EMRs) from actual electronic health (eHealth) systems, where we found that (1) multiple patients would generate large amounts of duplicate EMRs and (2) cross-patient duplicate EMRs would be generated numerously only in the case that the patients consult doctors in the same department. We then propose the first efficient and secure encrypted EMRs deduplication scheme for cloud-assisted eHealth systems (HealthDep). With the integration of our analysis results, HealthDep allows the cloud server to efficiently perform the EMRs deduplication, and enables the cloud server to reduce storage costs by more than 65% while ensuring the confidentiality of EMRs. Security analysis shows that HealthDep is more secure than the Marforio et al.'s scheme (NDSS 2014) and Bellare et al.'s scheme (USENIX Security 2013). Algorithm implementation and performance analysis demonstrate the feasibility and high efficiency of HealthDep.

Menu

- » Home
- » View and Authorize Doctors
- » View and Authorize Patients
- » Add Hospital
- » View Transactions
- » View and Generate Bill
- » View Patient Results
- » View Patient Details
- » View Result
- » Logout



CONCLUSION

In this project, we have proposed the first secure and efficient encrypted EMRs deduplication scheme for cloud-assisted eHealth systems, namely HealthDep. HealthDep is able to resist brute-force attacks without suffering from the singlepoint-of-failure problem; the patients in HealthDep make use of their smartphones to secure delegation and MLE keys. We have analyzed EMRs in actual eHealth systems and pointed out that patients consulted the doctors with the same department would generate numerous duplicate EMRs, while patients consulted the doctors with the different departments would generate few duplicate EMRs, which is integrated into HealthDep to improve the performance that the storage server checks duplicate EMRs. We have provided implementation to demonstrate the feasibility of HealthDep, and conducted a comprehensive performance comparison between HealthDep and the existing schemes, which has shown that HealthDep provides a strong security guarantee with a high efficiency.

FUTURE SCOPE

The future scope for HealthDep encompasses several key avenues for advancement. Firstly, there is a continual need for enhancing its security mechanisms to keep pace with evolving threats in cloud environments. Scalability improvements are essential to ensure HealthDep can efficiently handle the increasing volume of EMRs and users. Exploring interoperability with existing eHealth systems and standards will facilitate seamless integration and data exchange. Enhancing the user experience, particularly in smartphone-based security measures, will promote widespread adoption among both patients and healthcare providers. Real-world deployment and adoption studies will provide valuable insights into HealthDep's feasibility and impact on healthcare delivery. Lastly, ongoing research into optimization techniques and emerging technologies will further refine HealthDep's capabilities, ensuring it remains at the forefront of secure and efficient encrypted EMRs deduplication in cloud-assisted eHealth systems.

REFERENCES

- 1.K. Ren, C. Wang, and Q. Wang, "Security challenges for the public cloud," IEEE Internet Computing, vol. 16, pp. 69–73, Jan. 2012.
- 2.D. X. Song, D. Wagner, and A. Perrig, "Practical techniques for searches on encrypted data," in Security and Privacy, 2000. SandP 2000. Proceedings. 2000 IEEE Symposium on, pp. 0–44, 2002.
- 3.E. J. Goh, "Secure indexes," Cryptology ePrint Archive, <http://eprint.iacr.org/2003/216>, 2003.

4.R. Curtmola, J. Garay, S. Kamara, and R. Ostrovsky, "Searchable symmetric encryption: improved definitions and efficient constructions," in ACM Conference on Computer and Communications Security, pp. 79–88, 2006.

5.J. Li, Y. Shi, and Y. Zhang, "Searchable ciphertext-policy attribute-based encryption with revocation in cloud storage," International Journal of Communication Systems, vol. 30, no. 1, 2017.

6.Y. Miao, J. Ma, X. Liu, X. Li, Q. Jiang, and J. Zhang, "Attributebased keyword search over hierarchical data in cloud computing," IEEE Transactions on Services Computing, vol. PP, no. 99, pp. 1–1, 2017.

7.A. Swaminathan, Y. Mao, G. M. Su, H. Gou, A. L. Varna, S. He, M. Wu, and D. W. Oard, "Confidentiality-preserving rank-ordered search," in ACM Workshop on Storage Security and Survivability, Storagess 2007, Alexandria, Va, Usa, October, pp. 7–12, 2007.

8.C. Wang, N. Cao, K. Ren, and W. Lou, "Enabling secure and efficient ranked keyword search over outsourced cloud data," IEEE Transactions on Parallel and Distributed Systems, vol. 23, pp. 1467–1479, Aug. 2012.

9.S. Zerr, D. Olmedilla, W. Nejdl, and W. Siberski, "Zerber +r :topk retrieval from a confidential index," in International Conference on Extending Database Technology: Advances in Database Technology, pp. 439–449, 2009.

10. P. Golle, J. Staddon, and B. Waters, "Secure conjunctive keyword search over encrypted data," Lecture Notes in Computer Science, vol. 3089, pp. 31–45, 2004.