International Journal For Recent Developments in Science & Technology
2581-4575
Crossref
A Peer Reviewed Research Journal

An efficient and secure scheme for cloud E-healthcare System

Ms.A.Mamatha[1], A.Swathi Likhitha [2], A.Srinitha [3], B.Samatha[4], B.Spandana[5]

[2,3,4,5] UG Scholars, Department of CSE, ***MALLA REDDY ENGINEERING COLLEGE FOR WOMEN***, Hyderabad, Telangana, India.

[1]Assistant Professor, Department of CSE, ***MALLA REDDY ENGINEERING COLLEGE FOR WOMEN***, Hyderabad, Telangana, India.

ABSTRACT

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.

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 eHealth 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 Entericciated 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. [11] 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:

1) DupLESS as well as some subsequent schemes [12], [13] bears a strong assumption: the generation of MLE keys requires a fully trusted entity (e.g. the key server in [13], and the dealer in [12]), and thereby are vulnerable to brute-force attacks when the trusted entity is compromised;

2) 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.

BUSINESS CONTINUITY PLAN :

Cloud services may include analytics, applications, databases, storage, servers, and networking. Services tend to be available on demand, which means you can easily increase capacity. Though the cloud presents some challenges, it also offers these advantages:

- Uses load balancing to deliver processing and storage resources where your company needs them
- Charges only for services you use and quickly scales up or down
- Eliminates costs related to hardware that you must maintain and secure
- Reduces your electric bill because you don't need to power servers and the air conditioning to cool them

- Reduces the latency of the fixed company-owned data center through global data center networks
- Increases availability because storage is decentralized; if one center fails, another should be available
- Helps control company expenses, increase efficiency, and reduce vulnerabilities

Read our article on cloud collaboration best practices to learn more about the benefits of the cloud.

How Cloud-Based Systems Support Business Continuity

The cloud is a key part of business continuity for transaction- and data-focused companies that can't afford downtime. Cloud services protect continuous availability and offer fast, reliable continuity support.

Cloud Benefits for Business Continuity

The cloud offers timely and error-free data recovery for business continuity. The cloud offers a secure, seamless alternative when you cannot access your main offices. Home offices, satellite offices, or recovery sites can continue working as normal.

Traditional recovery solutions often took hours to transfer data from on-premise tape or flash drives or servers to recovery hardware. The on-premise model could stall an entire company if the main servers crash.

SaaS and cloud offerings typically include more redundancy and resiliency against potential outages than an individual company can afford to establish and maintain. Large-scale remote work and continued trade through online shopping was impossible in the early 2000s, before the advent of cloud computing.

Here is a summary of how cloud computing supports business continuity:

- Provides regular backups and easy failover (equipment that assumes the work when primary systems fail)
- Reduces downtime
- Provides better network and information security management
- Scales to suit your business needs; for example, keep critical data on-premise and back up the rest to the cloud
- Helps reduce impact in disruption of service (DoS) attacks
- Removes the need to stand up and maintain a costly physical mirror site of your infrastructure
- Eliminates the need to sync software on two sites
- Reduces recovery time to as little as a few minutes — potentially
- Eliminates the need to travel to a remote site in potentially difficult or dangerous circumstances

For smaller organizations, cloud services for business continuity center on SaaS. Small companies should still evaluate a provider's end-to-end setup and analyze strengths and weaknesses as they would for their own functions.

Businesses in regulated industries need to remember they always bear the onus for doing their part to ensure availability and security. Furthermore, it is easier to build in continuity buffers when you first build and implement an IT or communications environment than in a mature system. If you are starting a business, now is the time to consider business continuity.

Consider these issues when looking for cloud-computing resources for business continuity:

- **Backups:** Does the vendor back up your data or is that your responsibility? How do they back up data?

Continuity:

- Sharing data seamlessly across programs makes work easier. “Organizations don't want to move a few workloads that are on-premise. They want to have it all in the cloud because then they don't have to worry about where their employees work,” says the CEO and Chief Architect of Refactr, Michael Fraser. “But in doing so, they have to think about the impact of how their users are going to connect.”
- **Compatibility:** Consider vendor-neutral tools and applications. Look for solutions that are broadly compatible with your hardware and software systems.
- **Cost:** Price and preserving cash are paramount concerns for small businesses, especially in a crisis. Can you get a service for free that provides the same quality of output as a paid version?“We don't choose tools with a price premium for features and functions we aren't yet ready to use,” explains Bombacino. “We try to use best-in-breed when it makes sense if they have versions aligned with small-business needs.”
- **Data Extraction:** Can you get your data if you change providers? Cloud companies can shut down, too — what happens to your data then? Don’t choose a vendor that either won’t let you take your data or can’t provide a way to extract it. “If the answer is no, and there's no way to get your data out of it whatsoever in any form, then you have to determine if that's okay with you. And for a lot of organizations, that may be fine,” says Fraser.
- **Data Ownership:** Some free platforms retain rights to your work. Find out who owns the data you add to a cloud resource.
- **Data Segregation:** Find out exactly how a vendor segregates and protects your data. Also ask who has access to it and how they verify users.
- **Distributed Platform:** Ensure you can connect your complete platform. For example, users should be able to access internal cloud services only from inside a company network, behind a firewall. In that scenario, you might need to provide a VPN setup to remote workers.
- **Functionality:** Does the tool do the job the way you want it?
- **Location:** Avoid a recovery data center co-located at or near your original site. If you need to establish a redundant site, set it up 30 to 100 miles from the primary cloud provider location.
- **Remote Access:** By their nature, most cloud-based tools permit remote working. You’ll want to ensure the applications are robust and flexible enough to serve a distributed workforce that uses a range of devices, including mobile.
- **Security:** “Security is still not top of mind for the florist and the baker,” says Brelsford. “They don't wake up thinking about security, so the platform must be secure. For example, in a collaboration tool, can I have a private conversation with you and know that I'm not being overheard?” At the very least, ask the vendor how they plan to handle a hack or breach.
- **Service-Level Agreement (SLA):** Do the vendor’s guarantees of availability and return to service fit your needs? Also, what is the protocol if your contract ends?
- **Support:** A cloud services provider may not share your time zone or even reside in the same country. Find out if support is available during

your working hours. Ask if there's access to user forums and a robust online help center.

- **Usability:** "Not everybody in a company has the same level of tech savvy, so we choose things that everybody can learn fairly quickly," explains Bombacino. "It's a giant waste of money to invest in all of this technology if people can't or won't use it."
- **Vendor Reputation:** You could lose all your data if a vendor suddenly goes out of business. Do some research to see the number and quality of patches and upgrades a company provides, as well as its security history. Consider whether the company is old and stable, with a large user base. "For example, nobody ever got fired for buying an IBM product," notes Brelsford.
- **Vendor Business Continuity:** Your cloud services provider needs a business continuity plan, too. Understand how they will protect your data if they experience a disaster or other crisis. Learn about their backup and restore processes, along with how they test recovery plans.
- **Literature Survey**

  ❖ In the proposed system,Date 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 [30], [31]. To support encrypted data deduplication, Douceur et al. [32] 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 [33], [34], [35].

  ❖ 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 [36].

  ❖ Bellare et al. [11] 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 [20], [12], [13]. 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 [12]) becomes the single point of failure. A more comprehensive survey on secure data deduplication can be found in [37].

PROPOSED Mthod:

❖ 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 [11], [12], [13].

- 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) [14], such as ARM TrustZone [15], 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 numerously 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 [17], 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.

International Journal For Recent Developments in Science & Technology
2581-4575
Crossref
A Peer Reviewed Research Journal

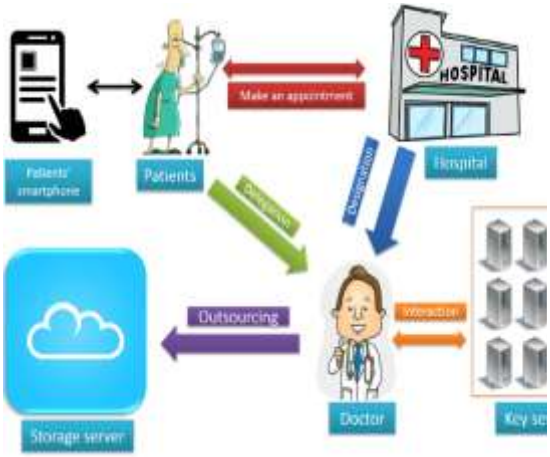

Fig : Architecture

IMPLEMENTATION

Patient:

A patient outsources her documents to the cloud server to provide convenient and reliable data access to the corresponding search doctors. To protect the data privacy, the patient encrypts the original documents under an access policy using attribute-based encryption. To improve the search efficiency, she also generates some keyword for each outsourced document. The corresponding index is then generated according to the keywords using the secret key of the secure kNN scheme. After that, the patient sends the encrypted documents, and the corresponding indexes to the cloud server, and submits the secret key to the search doctors.

Cloud server:

A cloud server is an intermediary entity which stores the encrypted documents and the corresponding indexes received from patients, and then provides data access and search services to authorized search doctors. When a search doctor sends a trapdoor to the cloud server, it would return a collection of matching documents based on certain operations.

Doctor:

An authorized doctor can obtain the secret key from the patient, where this key can be used to generate trapdoors. When she needs to search the outsourced documents stored in the cloud server, she will generate a search keyword set. Then according to the keyword set, the doctor uses the secret key to generate a trapdoor and sends it to the cloud server. Finally, she receives the matching document collection from the cloud server and decrypts them with the ABE key received from the trusted authority. After getting the health information of the patient, the doctor can also outsource medical report to the cloud server by the same way. For simplicity, we just consider one-way communication in our schemes.

CONCLUSION

In this paper, 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 smatphones 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.

REFERENCES

[1] L. D. Xu, W. He, and S. Li, "Internet of things in industries: A survey," IEEE Transactions on Industrial Informatics, vol. 10, no. 4, pp. 2233–2243, 2014.

[2] H. Ren, H. Li, Y. Dai, K. Yang, and X. Lin, "Querying in internet of things with privacy preserving: Challenges, solutions and opportunities," IEEE Network, 2018, to appear.

[3] G. Xu, H. Li, C. Tan, D. Liu, Y. Dai, and K. Yang, "Achieving efficient and privacy-preserving truth discovery in crowd sensing systems," Computers & Security, vol. 69, pp. 114–126, 2017.

[4] W. Quan, Y. Liu, H. Zhang, and S. Yu, "Enhancing crowd collaborations for software defined vehicular networks," IEEE Communications Magazine, vol. 55, no. 8, pp. 80–86, 2017.

[5] V. Casola, A. Castiglione, K. R. Choo, and C. Esposito, "Healthcarerelated data in the cloud: Challenges and opportunities," IEEE Cloud Computing, vol. 3, no. 6, pp. 10–14, 2016.

[6] M. S. Hossain and G. Muhammad, "Cloud-assisted industrial internet of things (iiot) - enabled framework for health monitoring," Computer Networks, vol. 101, no. 4, pp. 192–202, 2016.

[7] Y. Zhang, C. Xu, X. Liang, H. Li, Y. Mu, and X. Zhang, "Efficient public verification of data integrity for cloud storage systems from indistinguishability obfuscation," IEEE Transactions on Information Forensics and Security, vol. 12, no. 3, pp. 676–688, 2017.

[8] H. Li, Y. Yang, Y. Dai, J. Bai, S. Yu, and Y. Xiang, "Achieving secure and efficient dynamic searchable symmetric encryption over medical cloud data," IEEE Transactions on Cloud Computing, 2017, to appear.

[9] M. Bellare, S. Keelveedhi, and T. Ristenpart, "Message-locked encryption and secure deduplication," in Proceedings of EUROCRYPT. Springer, 2013, pp. 296–312.

[10] "List of antibiotics," https://en.wikipedia.org/wiki/List of antibiotics.

[11] M. Bellare, S. Keelveedhi, and T. Ristenpart, "Dupless: Server-aided encryption for deduplicated storage," in Proceedings of USENIX Security

Symposium. USENIX, 2013, pp. 179–194.

[12] Y. Duan, "Distributed key generation for encrypted deduplication achieving the strongest privacy," in Proceedings of CCSW, 2014, pp. 57–68.

[13] Y. Zheng, X. Yuan, X. Wang, J. Jiang, C. Wang, and X. Gui, "Enabling encrypted cloud media center with secure deduplication," in Proceedings of ASIACCS. ACM, 2015, pp. 63–72.

[14] J. Ekberg, K. Kostiainen, and N. Asokan, "Trusted execution environments on mobil devices," in Proceedings of CCS. ACM, 2013, pp. 1497–1498.

[15] ARM, "Building a secure system using trustzone technology," http://www.arm.com.

[16] C. Marforio, N. Karapanos, C. Soriente, K. Kostiainen, and S. Cˇ apkun, "Smartphones as practical and secure location verification tokens for payments," in Proceedings of NDSS. Internet Society, 2014, pp. 1–15.

[17] "Openvirtualization," www.openvirtualization.org.

[18] Y. Zhang, C. Xu, H. Li, and X. Liang, "Cryptographic public verification of data integrity for cloud storage systems," IEEE Cloud Computing, vol. 3, no. 5, pp. 44–52, 2016.

[19] Y. Zhang, C. Xu, S. Yu, H. Li, and X. Zhang, "Sclpv: Secure certificateless public verification for cloud-based cyber-physical-social systems against malicious auditors," IEEE Transactions on Computational Social Systems, vol. 2, no. 4, pp. 159–170, 2015.

[20] F. Armknecht, J. Bohli, G. O. Karame, and F. Youssef, "Transparent data deduplication in the cloud," in Proceedings of CCS. ACM, 2014, pp. 831–843.