International Journal For Advanced Research In Science & Technology
A peer reviewed international journal www.ijarst.in
ISSN: 2457-0362

HMAC-SHA-1HRS Deduplication Scheme in Cloud

Madhav Polavarapu Venkata Lakshmi [1], Ramesh PL[2]
[1]Student, Computer Science (Honors), KLU, Vijayawada, Andhra Pradesh, India.
klucse2000030810@gmail.com
[2] Vice-Principal, K.B.N. College (A), Vijayawada.

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 duplicateEMRs would be generated numerously only in the case that the patients consult doctors in the same department. We then proposethe 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.

Keywords: -Admin, Doctor, Appointment, De-duplication, Cloud Storage.

1. INTRODUCTION

Applying Internet of Things (IoT) technologies withthe integration of cloud computing in various industrieshas already shown great potential in improving the quality ofservices in these industry systems [1], [2], [3], [4]. One of themost prominent manifestations is the cloud-assisted electronichealth (eHealth) systems [5], [6]. Such systems provide amore efficient, less error-prone, and more reliable way tomanage electronic medical records (EMRs) for both healthcareproviders and patients, compared with traditional paper basedsystems. Specifically, cloud-assisted eHealth systems not onlyallow medical institutions to outsource EMRs to the storageserver and access them flexibly without incurring substantialstorage and maintain costs in practice [7], but also make agreat contribution to the judgement and dispute resolution inmedical malpractice [8].Generally, the storage server needs to store the outsourcedEMRs, such as prescriptions, for a prolonged period of time tosatisfy several government regulations or hospital requirementson EMRs archiving. With the volume of EMRs generated fromeHealth systems grows over time, the costs of storing EMRsare persistently increase in practice. Actually, the storagecosts can be reduced significantly after deduplication, wherethe storage server checks duplicate EMRs and deletes theredundant ones. For example, as shown in Fig. 1(a) and1(b), both two patients (one is diagnosed with coronary heartdisease and stable angina pectoris, and the other one isdiagnosed with hypertension) need to use "Aspirin EntericciatedTablets", "Metoprolol Tartrate Tablets", and "NifedipineSustained-release Tablets" with the same usage and dosage.Table I shows the savings of storage costs that performingdeduplication on prescriptions from an actual eHealth system,these prescriptions are selected randomly from 10000 prescriptionsgenerated by doctors from Department of Cardiologyduring 2013-2017. The results demonstrate that the storagecosts can be reduced by more than 66% in the case of 500prescriptions. However, from the perspective of data ownersincluding both medical institutions and patients, the content ofEMRs should not be leaked for security reasons. Therefore,privacy protection of the EMRs' content against anyone whodoes not own the EMRs should be guaranteed. This canbe achieved by conventional encryption, but its randomness(i.e. for the same message, different users produce differentciphertexts) makes deduplication impossible.

2. RELATED WORK

Existing System

Generally, the storage server needs to store the outsourcedEMRs, such as prescriptions, for a prolonged period of time tosatisfy several government regulations or hospital requirementson EMRs archiving. With the volume of EMRs generated fromHealth systems grow over time, the costs of storing EMRsare persistently increased in practice. Actually, the storage costs can be reduced significantly after de-duplication, where the storage server checks duplicate EMRs and delete the redundant ones.

Proposed System:

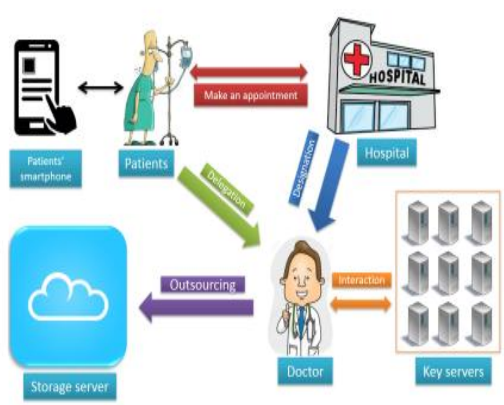
In this paper, we propose the first efficient and secure encrypted EMRs deduplication scheme for cloud-assisted eHealth systems, and realize it in a system called HealthDep.In HealthDep, multiple dedicated key servers are introducedto assist in

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal www.ijarst.in
ISSN: 2457-0362

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. 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.

3. IMPLEMENTATION

System Architecture



Appointment

Now we illustrate the procedure when a patient consultsa doctor in HealthDep. First, the patient registers with ahospital, and the hospital determines that the patient is subjectto which department. Then the hospital designates a doctorfor diagnosing, and the patient makes an appointment withthe hospital to obtain the diagnosing information (e.g. timeand place).

Delegation

At the corresponding time, the patient delegatesto the doctor, and is diagnosed and treated. Then the doctorgenerates the EMRs for the patient, performs a server-aidedMLE to encrypt the EMRs, and outsources the ciphertextsto storage server.

De-duplication

This algorithm enables the doctor to generate and encrypt EMRs for each patient and outsource the ciphertexts to the storage server, and allows the storage server to perform ciphertext de-duplication to reduce the storage overhead.

Methodology

• **TokenGen(Tag, UserID)** - It loads the associatedprivilege keys of the user and generate the token with HMAC-SHA-1 algorithm.

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
IJARST
ISSN: 2457-0362

•**ShareTokenGen(Tag, {Priv.})** - It generatesthe share token with the corresponding privilegekeys of the sharing privilege set with HMAC-SHA-1algorithm.

Public Server (Storage Server):

Our implementation of the Storage Server providesdeduplication and data storage with following handlersand maintains a map between existing files and associated token with Hash Map.

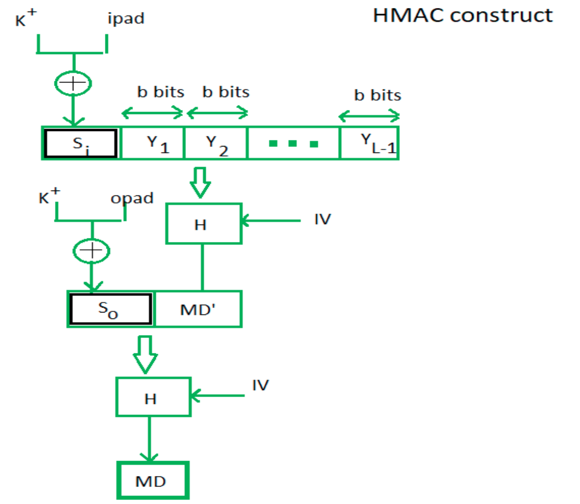
• **DupCheck(Token) -** It searches the File to Token Map for Duplicate and

• **FileStore(FileID, File, Token) -** It storesthe File on Disk and updates the Mapping**.**

HMAC-SHA-1 algorithm

The working of HMAC starts with taking a message M containing blocks of length b bits. An input signature is padded to the left of the message and the whole is given as input to a hash function which gives us a temporary message digest MD'. MD' again is appended to an output signature and the whole is applied a hash function again, the result is our final message digest MD.

Here is a simple structure of HMAC:



Here, H stands for Hashing function,

M is original message

Si and So are input and output signatures respectively,

Yi is the ith block in original message M, where i ranges from [1, L)

L = the count of blocks in M

K is the secret key used for hashing

IV is an initial vector (some constant)

The generation of input signature and output signature Si and So respectively.

$S_i = K^+ \oplus ipad$ where K^+ is nothing but K padded with zeros on the left so that the result is b bits in length

$S_0 = K^+ \oplus opad$ where ipad and opad are 00110110 and 01011100 respectively taken b/8 times repeatedly.

$$MD' = H(S_i \,||\, M)$$

$$MD = H(S_0 \,||\, MD') \quad \text{or } MD = H(S_0 \,||\, H(S_i \,||\, M))$$

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362

4. EXPERIMENTAL RESULTS

Fig: -2 Application Dashboard

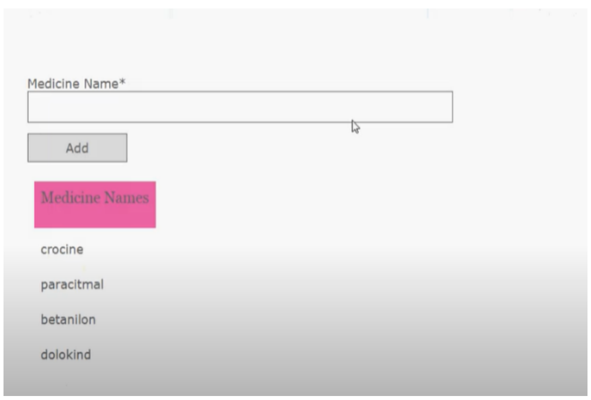


Fig: -3 Updating Medicine Information

Fig:-4 HMAC-SHA-1 algorithm Results

5. CONCLUSION

In this paper, we have proposed the first secure and efficient encrypted EMRs deduplication scheme for cloud-assistedeHealth systems, namely HealthDep. HealthDep is able toresist brute-force attacks without suffering from the singlepoint-of-failure problem; the patients in HealthDep make useof their smartphones to secure delegation and MLE keys.We have analyzed EMRs in actual eHealth systems andpointed out that patients consulted the doctors with the samedepartment would generate numerous duplicate EMRs, whilepatients consulted the doctors with the different departmentswould generate few duplicate EMRs, which is integrated intoHealthDep to improve the performance that the storage serverchecks duplicate EMRs. We have provided implementationto demonstrate the feasibility of HealthDep, and conducted acomprehensive performance comparison between HealthDepand the existing schemes, which has shown that HealthDepprovides a strong security guarantee with a high efficiency.

6. 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 ofthings 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 efficientand 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 collaborationsfor software defined vehicular networks," IEEE CommunicationsMagazine, vol. 55, no. 8, pp. 80–86, 2017.

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

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

[7] Y. Zhang, C. Xu, X. Liang, H. Li, Y. Mu, and X. Zhang, "Efficientpublic verification of data integrity for cloud storage systems fromindistinguishability obfuscation," IEEE Transactions on InformationForensics 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 secureand efficient dynamic searchable symmetric encryption over medicalcloud data," IEEE Transactions on Cloud Computing, 2017, to appear.

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

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