SECURITY AND EFFICIENCY OF AUTHENTICATED MEDICAL DOCUMENTS RELEASE CONTROL

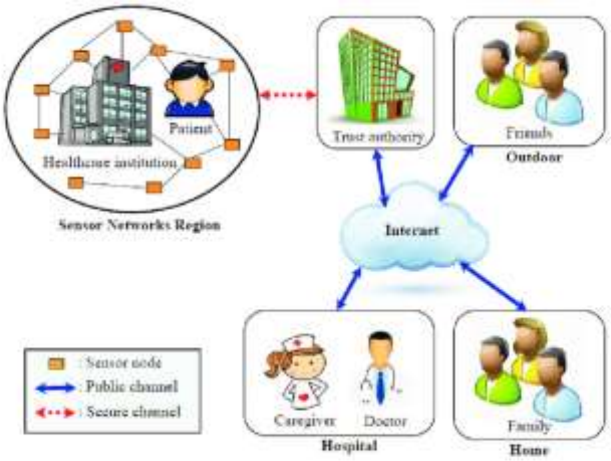
SIVA PRASUNA KOLLI Student, M.Tech (CSE), MVR College of Engineering & Technology, A.P., India.

Dr.D.SRINIVAS Professor & HOD, Dept. of Computer Science & Engineering, MVR College of Engineering & Technology, A.P., India.

Abstract — In this paper, a tremendous amount of information is daily exchanged or released. Among various information-release cases, medical document release has gained significant attention for its potential in improving healthcare service quality and efficacy. However, integrity and origin authentication of released medical documents is the priority in subsequent applications. Moreover, sensitive nature of much of this information also gives rise to a serious privacy threat when medical documents are uncontrollably made available to un trusted third parties. Redactable signatures allow any party to delete pieces of an authenticated document while guaranteeing the origin and integrity authentication of the resulting (released) subdocument. Nevertheless, most of existing redactable signature schemes (RSSs) are vulnerable to dishonest redactors or illegal redaction detection. To address the above issues, we propose two distinct RSSs with flexible release control (RSSs-FRC). We also analyse the performance of our constructions in terms of security, efficiency and functionality. The analysis results show that the performance of our construction has significant advantages over others, from the aspects of security and efficiency.

INTRODUCTION

In recent years, effective sharing of medical data has gained significant attention among practitioners as well as in the scientific community. Because this concept holds great potential for fostering the collaboration within the health-care community and other parties, such as pharmaceutical companies, insurance companies and research institutes, so as to enhance the quality and efficacy of medical treatment processes. For example, a hospital may need to release medical data to a research institute in an attempt to evaluate a new therapy or develop a new drug. The medical data ranges from general information such as gender, social security number, name, date of birth, and home address to payment information such as credit card expiration dates and card numbers. Therefore, it is obligatory to protect patients' privacy when their medical data is used for secondary use such as clinical studies and medical research. Another threat for medical data sharing is that the released data are vulnerable to be tempered with. Relevant to this, yet another important requirement regarding the secondary use of medical data is to provide an authentication mechanism for data users. Because researchers or any third party should be provided assurances that the data they are accessing or have received are authentic and have not been falsified. It is quite obvious that medical data is a valuable asset to data holders. In order to guarantee an adequate quality of data, it is crucial to check the origin and integrity of involved data at any time. In the worst case, failure to guarantee authentication of medical data could result in the public losing faith in healthcare systems, which could lead to severe restrictions on the development of healthcare service. Even though there are relevant laws or regulations concerning ownership rights, effective technical approaches are also indispensable to protect the holders' rightful possession of data and data authenticity. The framework for applying RSSs in medical documents releasing system is shown in Fig. 1. As shown in the figure, a healthcare provider (signer) generates a redact able signature for a medical document. Then, the healthcare provider forwards the medical documents and the corresponding redactable signatures to another party (redactor) such as patients or hospitals who are the subject or administrator of the signed medical documents. Later, the second party is allowed to publicly redact parts of the signed medical documents that they do not want to release to third parties. Upon receiving the redacted document-signature pair, any recipient (verifier) is able to verify the source and integrity of the released medical document.



LITERATURE SURVEY

Steinfeld et al. [1] introduced CEAS with which signers specify which portions of the authenticated document is redactable. However, the encoding length of any CEAS is exponential in the number of subdocument blocks which is compactly not encodable.

Bull et al. [2] introduced a new hierarchical redaction control policy whose encoding is dramatically smaller.Yet, this kind of redaction policy is only applicable to hierarchically structured documents.

Miyazaki et al. [3] proposed another authenticated document sanitizing scheme based on bilinear maps. Nonetheless, the computation cost of this scheme is relatively high.

Ma et al. [4] also presented a secure and efficient design of RSSs with subdocument redaction condition control.

Liu et al. [5] proposed a novel and efficient redactable signature scheme for trees with fine-grained redaction control mechanism.

In 2015,Pohls et al. [6] introduced the notion of accountable RSSs and presented a generic construction which regulates other parties' redaction operation. At present, although there exist a number of related works that have introduced different methods to prevent unauthorized redaction manipulation, some significant characteristics are still unsatisfied, such as a lack of flexibility in selecting releasable blocks by the redactor or inability to detect illegal redaction by verifiers. Even worse, Some release control designs are achieved with the compromise of performance or security.

PROPOSED METHOD

- ❖ The concept of redactable signatures was formally introduced by Johnson et al. in [8] as an example of a large class of homomorphic signatures. The redactable signature scheme (RSS) designed in this work is based on Merkle hash tree [9] and GGM tree [10]. The outstanding advantage of this design is that signature is relatively short for the application of Merkle hash tree. Johnson et al. described a scenario where a small part of a document is redacted, with the majority released. In 2001, Steinfeld et al. [11] first put forward the definition of "Content Extraction Signature" (CES) in which the holder of a signed document is allowed to generate redacted signatures for portions of the original authenticated document. The notion of redactable signatures is quite similar to the concept of CES. However, the obvious distinction between RSSs and CES is that Steinfeld et al. [11] introduced the "Content Extraction Access Structure" (CEAS) as an encoding of subdocument indexes in the original document. This mechanism allows the signer to specify extractable subdocuments by the subsequent users.
- ❖ Since the concept of redactable signature introduced [8], [11], it has been applied in many practical scenarios, including privacy protection of audit-log data, the release of previously classified government documents, health data sharing, etc. Miyazaki et al. [12] proposed the first redactable signature scheme to solve the document sanitizing problem, which prohibit the additional sanitizing attack. Subsequently, their another work [13] pointed out that the previous solution could expose the number of sanitized portions and proposed a new scheme with sanitizing condition control based on bilinear maps as the solution to this issue.
- ❖ The most extensive application of redactable signature is the privacy protection of patients' health data in medical healthcare systems [14]. Over the years, RSSs are also

applied in social networks [15] and smart grid [16] for dealing with privacy issues. Due to the varieties of data-structure in distinct practical applications, RSSs have been extended to address the redaction problem of different data structures, such as lists [12], [17], sets [13], [18], graphs [19], and trees [20].

- However, RSSs for different data structures have distinct security models. In particular, transparency [21] is a stronger privacy property that most of the present constructions do not possess. In order to eliminate the necessity to construct different models for distinct data structures, Derler et al. presented a general framework for the construction of RSSs in this system.

Disadvantages

- In the existing work, the system implements the redactable signature scheme (RSS) designed in this work is based on Merkle hash tree and GGM tree. The outstanding disadvantage of this design is that signature is relatively short for the application of Merkle hash tree.
- The existing system introduced a new hierarchical redaction control policy whose encoding is dramatically smaller..

PROPOSED SYSTEM

- The proposed system is to design secure and efficient RSSs with flexible release control (RSSs-FRC) so as to provide privacy preservation and flexible release control guarantee for authenticated medical documents release systems. The main contributions of our work are summarized as follows.
- The system proposes two novel RSSs-FRC satisfying different release control requirements in medical document releasing systems. The minimal release control in RSSs-FRC1 is realized by employing the threshold secret sharing scheme. RSSs-FRC2 achieves hybrid release control through access tree which control not only the minimal release number but also the dependency of releasable subdocument blocks.
- The system formally define the proposed two RSSs-FRC and the security properties in terms of unforgeability, privacy and transparency. The security properties are proved in a reduction mode. Furthermore, the system analyses the performance of our constructions in terms of theoretical and practical methods to show their practicality in the aspects of efficiency and functionality.
- The proposed system generalized constructions provide a universal approach for the design of secure and efficient RSSs-FRC. This sort of design is efficient in

solving the unauthorized redaction and privacy leakage issues in other scenarios of authenticated documents release.

Advantages

- In order to preserve the privacy information in the authenticated medical document as much as possible, dishonest patients might not be willing to release a sufficient number of signed medical subdocument blocks to third parties for some services.
- The system is more secured since Redactable signatures, a straightforward approach, inherently solve the authentication theoretical incompatibility and practical requirements of privacy information redaction in authenticated medical document releasing.

RELATED WORK

MODULES DESCRIPTION:

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.

SAMPLE RESULTS

Authenticated Medical Documents Releasing with Privacy Protection and Release Control
Welcome Research Cloud Server !!!
Research Cloud Menu
MEDICAL
Pause (k)

Authenticated Medical Documents Releasing with Privacy Protection and Release Control
Control
Authorize Patient !!!
Menu
MEDICAL

CONCLUSION& FUTURE SCOPE

In this paper, we introduced two constructions of RSSs-FRC with a different flexibility of release control mechanisms to resolve the privacy preservation and release control issues in releasing authenticated medical documents. The RSSs-FRC1 construction allows the signer to specify a minimum number of subdocument blocks that the redactor has to release, while the RSSs-FRC2 construction also empowers signer to regulate the dependence of revealable subdocument blocks. Our constructions not only prevent the dishonest release from redacting document unrestrictedly but also have the ability to detect illegal redaction by the verifier.

Furthermore, the two proposed RSSs-FRC also support multiple redaction manipulations providing the released subdocument is authorized by the signer. Finally, we presented the security proof and efficiency analysis for our RSSs-FRC. For future work, we plan to explore RSSs with redactor accountability for privacy-preserving release of authenticated medical documents.

REFERENCES

[1] X. Chen, J. Li, J. Weng, J. Ma, and W. Lou, "Verifiable computation over large database with incremental updates," IEEE transactions on Computers, vol. 65, no. 10, pp. 3184–3195, 2016.

[2] X. Chen, J. Li, X. Huang, J. Ma, and W. Lou, "New publicly verifiable databases with efficient updates," IEEE Transactions on Dependable and Secure Computing, vol. 12, no. 5, pp. 546–556, 2015.

[3] X. Chen, X. Huang, J. Li, J. Ma, W. Lou, and D. S. Wong, "New algorithms for secure outsourcing of large-scale systems of linear equations," IEEE transactions on information forensics and security, vol. 10, no. 1, pp. 69–78, 2015.

[4] X. Chen, J. Li, J. Ma, Q. Tang, and W. Lou, "New algorithms for secure outsourcing of modular exponentiations," IEEE Transactions on Parallel

and Distributed Systems, vol. 25, no. 9, pp. 2386–2396,2014.

[5] J. Wang, X. Chen, X. Huang, I. You, and Y. Xiang, "Verifiable auditing for outsourced database in cloud computing," IEEE transactions on computers, no. 1, pp. 1–1, 2015.

[6] T. Jiang, X. Chen, and J. Ma, "Public integrity auditing for shared dynamic cloud data with group user revocation," IEEE Transactions on Computers, vol. 65, no. 8, pp. 2363–2373, 2016.

[7] X. Zhang, T. Jiang, K.-C. Li, A. Castiglione, and X. Chen, "New publicly verifiable computation for batch matrix multiplication," Information Sciences, 2017.

[8] R. Johnson, D. Molnar, D. Song, and D. Wagner, "Homomorphic signature schemes," in Cryptographers' Track at the RSA Conference.Springer, 2002, pp. 244–262.

[9] G. Becker, "Merkle signature schemes, merkle trees and their cryptanalysis," Online im Internet: http://imperia.rz.rub.de, vol. 9085, 2008.

[10] O. Goldreich, S. Goldwasser, and S. Micali, "How to construct random functions," Journal of the ACM (JACM), vol. 33, no. 4, pp. 792–807, 1986.

[11] R. Steinfeld, L. Bull, and Y. Zheng, "Content extraction signatures," in International Conference on Information Security and Cryptology.Springer, 2001, pp. 285–304.

[12] K. Miyazaki, M. Iwamura, T. Matsumoto, R. Sasaki, H. Yoshiura,and S. Tezuka, "Digitally signed document sanitizing scheme with disclosure condition control," IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, vol. 88, no. 1,pp. 239–246, 2005.

[13] K. Miyazaki, G. Hanaoka, and H. Imai, "Digitally signed document sanitizing scheme based on bilinear maps," in Proceedings of the 2006 ACM Symposium on Information, computer and communications security. ACM, 2006, pp. 343–354.

[14] J. L. Brown, "Verifiable and redactable medical documents," Ph.D.dissertation, Georgia Institute of Technology, 2012.