INTERNATIONAL JOURNAL · ENGINEERING RESEARCH ·

International Journal for Innovative Engineering and Management Research

A Peer Revieved Open Access International Journal

www.ijiemr.org

IJIEMR Transactions, online available on 2nd Jan 2021. Link :http://www.ijiemr.org/downloads.php?vol=Volume-09&issue=ISSUE-12

DOI: 10.48047/IJIEMR/V09/I12/160

Title: **AUTHENTICATED MEDICAL DOCUMENTS RELEASING WITH PRIVACY PROTECTION AND RELEASE CONTROL**

Volume 09, Issue 12, Pages: 934-940

Paper Authors

JATOTHU GOWTHAMI, SAMALA SPANDANA, UNDAM HEMALATHA, Y.DHANANJAY

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

AUTHENTICATED MEDICAL DOCUMENTS RELEASING WITH PRIVACY PROTECTION AND RELEASE CONTROL

JATOTHU GOWTHAMI[1], SAMALA SPANDANA[2], UNDAM HEMALATHA[3], Y.DHANANJAY[4]

[1,2,3,] B TECH Students, Department of CSE, Princeton Institute of Engineering & Technology For Women, Hyderabad, Telangana, India.

[4] Assistant Professor, Department of CSE, Princeton Institute of Engineering & Technology For Women, Hyderabad, Telangana, India.

ABSTRACT: With regards to Information Societies, a huge measure of data is every day traded or delivered. Among different data discharge cases, clinical report discharge has picked up huge consideration for its potential in improving medical care administration quality and viability. Notwithstanding, respectability and beginning verification of delivered clinical archives is the need in resulting applications. In addition, the delicate idea of a lot of this data likewise offers ascend to a genuine security danger when clinical records are wildly made accessible to untrusted outsiders. Redactable marks permit any gathering to erase bits of a verified report while ensuring the birthplace and trustworthiness verification of the subsequent (delivered) subdocument. In any case, a large portion of the current redactable mark plans are powerless against untrustworthy redactors or unlawful redaction identification. To address the above issues, we propose two unmistakable RSS with adaptable delivery control (RSS-FRC). We additionally break down the exhibition of our developments regarding security, effectiveness and usefulness. The examination results show that the exhibition of our development has critical favorable circumstances over others, from the parts of security and proficiency.

Index Terms: Medical document release, privacy preservation, data authentication, release control.

I. INTRODUCTION

The digital information collected by enterprises, public administrations, and governments has created enormous opportunities for knowledge-based applications. Driven by these benefits, there exists a high demand for the publication and exchange of collected data among numerous parties. However, sensitive information about users is typically contained in the original documents, and the privacy would be violated if such data is released without being processed. Document redaction, a straightforward method for privacy-preserving, is to remove sensitive information from the document. For example, document redaction is a critical approach for companies to prevent inadvertent or even malicious disclosure of proprietary formation while sharing data with outsourced operations. 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

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

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. Redactable signatures, a straightforward approach, inherently solve the above theoretical incompatibility and practical requirements of privacy information redaction in authenticated medical document releasing. In the definition of redactable signature schemes (RSSs), parts of a signed document are allowed to be removed by any party while preserving the source and integrity verifiability of the remaining subdocument. Another outstanding advantage of the redactable signature is that the reserved subdocument and its signature of the original document do not reveal any content information about deleted parts. Therefore, RSSs are such a useful primitive that comes in handy in scenarios where only parts of the authenticated data are releasable or required for privacy-preserving, but the origin and integrity authentication of these data must still hold. 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 redactable 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.

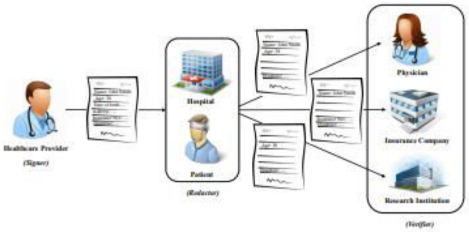

Figure 1: Authenticated medical documents releasing under RSSs

II. Related review

The primitive of data verification has been well studied by plenty of researchers in the past decades [1]–[7]. Most of the prior work focused on generic solutions for the integrity and authenticity verification. While they protect data from alteration by malicious attackers, they also prevent data from being processed and thus hinder the further flexible and efficient use of data. Moreover, in some situations they are incompatible with the confidentiality of the data. Therefore, it is meaningful to seek for appropriate protocols for data verification with confidentiality. 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 and trees. 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.

III. Minimal Release Control Construction (RSSsFRC1)

This construction is designed to resolve the issue where a patient might not be willing to release sufficient medical document content for a service in releasing their medical documents authenticated by healthcare providers. The outline of RSSs-FRC1 is shown in Fig. 2. To sign an original medical document M, a healthcare provider divides it into n subdocument blocks according to the granularity of document content. A seed is shared among n parts through a TSSS [32], and each share is appended to a subdocument before accumulating. After the short digest of this concatenation is generated, healthcare provider signs the concatenation of the short digest, the seed, a threshold value, and some other associated parameters. Redacting a subset of subdocument blocks is simply removing these blocks from the original signed document and updating the signature accordingly. Finally, the third party checks the validity of the concatenated parameters using DVerify algorithm of a fixed DSS. This construction consists of four algorithms: KeyGen, Sign, Verify and Redact.

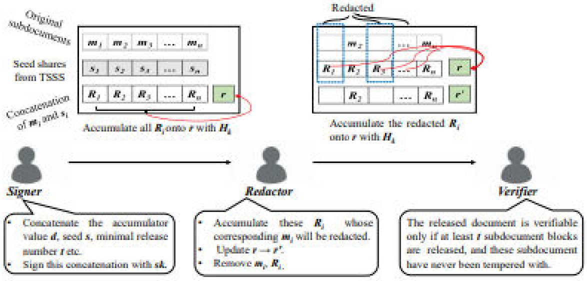
Original subdocuments
Seed shares from TSSS
Concatenation of m_i and s_i
m_1 m_2 m_3 ... m_n
s_1 s_2 s_3 ... s_n
R_1 R_2 R_3 ... R_n r
Accumulate all R_i onto r with H_k
Redacted
m_2 ... m_n
R_1 R_2 R_3 ... R_n r
R_2 ... R_n r'
Accumulate the redacted R_i onto r with H_k
Signer
Redactor
Verifier
Concatenate the accumulator value d, seed s, minimal release number t etc.
Sign this concatenation with sk.
Accumulate these R_i whose corresponding m_i will be redacted.
Update $r \rightarrow r'$.
Remove m_i, R_i.
The released document is verifiable only if at least t subdocument blocks are released, and these subdocument have never been tempered with.

Figure 2: Outline of RSSs-FRC1.

KeyGen(1λ): This algorithm fixes a DSS and chooses a quasi-commutative accumulator Hk. Then, the key generation algorithm (pk, sk) ← DGen(1λ) of DSS is run. Sign(sk,M,P): The input of this algorithm includes a signing secret key sk, a document M = {m1, m2, · · · , mn}, and a release control policy P. P is built upon the TSSS allows signer to control the minimal number of subdocument blocks that a patient has to release. The signer chooses a seed value s ∈ Zρ and defines a threshold value t which is the minimal number of blocks that a patient must reserve, where ρ is a safe prime and ρ > n. This also means the maximal number of removal blocks is n − t. To share the seed value s, signer chooses t − 1 random numbers a1, . . . , at−1 ∈ Zρ independently and randomly as the coefficients of a polynomial function. These coefficients, the threshold value and seed value define a polynomial function of degree t − 1, i.e., P(x) = s + Pt−1 i=1 aix i . Then, the signer shares the seed value s into n shares with P(x), and each share is si = P(xi), where xi ∈ Zρ.

Hybrid Release Control Construction (RSSs-FRC2): We develop RSSs-FRC2 with an advanced release control which achieves the combination of minimal release and dependent release control of subdocument blocks. This hybrid release control grants patients a more flexible redaction right for different subdocument blocks. Thus, this scheme is an improvement of RSSs-FRC1. The outline of RSSs-FRC2 is shown in Fig. 3. To sign an original medical document M, a healthcare provider divides it into n subdocument blocks as in the previous construction. An access tree [28] is constructed according to the number and dependence of subdocument blocks. A seed is shared through this access tree in a top-down manner. Thus, each leaf node of this tree is allocated a seed share which is associated with a subdocument block. We also consider the situation where some subdocument blocks may appear more than once, which could be solved by associating with different seed shares. Then, the concatenation of each seed share and subdocument block is accumulated. After a short digest of these concatenations is generated, healthcare provider signs the concatenation of the short digest, seed, access tree, and other parameters. Redaction of a subset of subdocument blocks is simply removing this subset from the original signed document and updating the signature accordingly. Finally, the third party checks the validity of the concatenation using DVerify algorithm of the fixed DSS. This construction consists of four algorithms: KeyGen, Sign, Verify and Redact.

The Comparison of RSSs-FRC2 and [18]: Although it seems that the design of RSSs-FRC2 is analogous to [18], the redaction control mechanisms are quite different. In our previous work [18], we proposed a generalized approach for constructing redactable signature scheme with fine-grained redaction control (RSS-FGRC). The redaction control policy provides a mechanism for signers to avoid arbitrary redaction operations by specifying which fragment or group of subdocuments can be legally redacted. The redaction control design in RSS-FGRC is based on monotone span program (MSP) and linear secret sharing scheme (LSSS) which realizes the fine-grained redaction control. It specifies the dependency and combination of subdocument blocks. For instance, a fine-grained redaction policy P 0 : “(m1 OR m2) AND (m3 OR (m4 AND m5))" which can be converted into a binary tree: every interior node is either AND or OR gate and each leaf node corresponds to subdocument blocks. In order to satisfy the redaction control policy, any remaining subdocument should contain at least one of the following combination: {m1, m4, m5}, {m2, m4, m5}, {m1, m3}, {m2, m3}. That is to say any unauthorized combination such as {m1, m2}, {m3, m5}, etc., are forbidden to release. Despite regulating the combination of released subdocuments, the signer in [18] is unable to control the number of released subdocuments. RSSs-FRC2 achieves hybrid release control through access tree which controls not only the minimal number but also the dependency of releasable subdocument blocks. In the access tree, each non-leaf node is described by a threshold value and its child nodes. Assume that tx is the threshold value of a node x, and numx is the number of children, then $0 < tx \leq numx$. The threshold gate is an AND gate when tx = numx and when tx = 1, it means that x is an OR gate. Besides, it indicates that x has a general threshold value if $1 < tx < numx$. As for the leaf node of this tree, each of them is associated with a subdocument block. Thus, the inner node with threshold value tx = 1 or tx = numx has the similar redaction control function in [18]. However, the inner node with threshold value $1 < tx < numx$ has no regulation about the combination of child nodes, but only the number of child node retained.

IV. Conclusion and Feature Work

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.

V. 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.

[15] H. C. Pöhls, A. Bilzhause, K. Samelin, and J. Posegga, "Sanitizable signed privacy preferences for social networks," DICCDI, LNI. GI, 2011.

[16] H. C. Pöhls and M. Karwe, "Redactable signatures to control the maximum noise for differential privacy in the smart grid," in International Workshop on Smart Grid Security. Springer, 2014, pp. 79–93.

[17] K. Samelin, H. C. Pöhls, A. Bilzhause, J. Posegga, and H. De Meer, "Redactable signatures for independent removal of structure and content," in International Conference on Information Security Practice and Experience. Springer, 2012, pp. 17–33.

[18] J. Ma, J. Liu, X. Huang, Y. Xiang, and W. Wu, "Authenticated data redaction with fine-grained control," IEEE Transactions on Emerging Topics in Computing, 2017.