As per UGC guidelines an electronic bar code is provided to seure your paper

International Journal for Modern Trends in Science and Technology, 8(09): 104-107, 2022
Copyright © 2022 International Journal for Modern Trends in Science and Technology
ISSN: 2455-3778 online
DOI: https://doi.org/10.46501/IJMTST0809019
Available online at: http://www.ijmtst.com/vol8issue09.html

Privacy Protection Authenticated Medical Document Releasing and Release Control

K.Harshini [1] | P. Srinivasa Reddy[2]

[1]PG Scholar, Department of Computer science, SVKP &Dr K S Raju Arts & Science College(A), Penugonda, W.G.Dt., A.P, India
[2]Associate Professor in Computer science, SVKP &Dr K S Raju Arts & Science College(A), Penugonda, W.G.Dt., A.P, India

To Cite this Article
K.Harshini and P. Srinivasa Reddy. Privacy Protection Authenticated Medical Document Releasing and Release Control. International Journal for Modern Trends in Science and Technology 2022, 8(09), pp. 104-107. https://doi.org/10.46501/IJMTST0809019

Article Info
Received: 22 August 2022; Accepted: 12 September 2022; Published: 17 September 2022.

ABSTRACT

A huge volume of information is released or shared every day in the context of information societies. Medical document release is one of several information-release examples that has drawn a lot of interest due to its potential to increase the effectiveness and quality of healthcare services. However, in later applications, the integrity and origin authentication of released medical documents take precedence. Additionally, the sensitive nature of much of this data creates a serious privacy risk when medical records are uncontrollably made accessible to unreliable third parties. Any party can remove portions of an authenticated document with redactable signatures, and the resulting (released) subdocument will still be able to be validated for its origin and integrity. Nevertheless, most of existing redactable signature schemes (RSSs) are vulnerable to dishonest redactors or illegal redaction detection.

1. INTRODUCTION

Steinfeld et al. 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. The digital data that businesses, public agencies, and governments have gathered has greatly expanded the possibilities for knowledge-based applications. These advantages have led to a significant increase in the demand for publishing and exchanging collected data among various parties. However, sensitive information about users is typicall contained in the original documents, and the privacy would be violated if such data is released without being processed. Redacting a document means removing sensitive information, which is an easy way to protect privacy. 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.

The fact that the released data can be manipulated is another danger to the sharing of medical data. Providing an authentication mechanism for data users is a pertinent requirement regarding the secondary use of medical data. For the reason that researchers or any other party should be given guarantees that the data they are accessing or receiving are real and unaltered. It should go without saying that medical data is a valuable resource for data owners. It is essential to constantly verify the integrity and source of the relevant data in order to ensure that the quality of the data is adequate. In the worst case, if medical data authentication is not guaranteed, the public may lose trust in healthcare systems.

A healthcare provider (the signer) creates a redactable signature for a medical document using the framework for implementing RSSs in medical documents. The healthcare provider then sends the signed medical documents and the associated redactable signatures to a different party (redactor), such as patients or hospitals, who are the subject or administrator of the documents. The second party is later permitted to publicly redact any information from the legally binding medical records that they do not wish made available to outside parties. Any recipient (verifier) can confirm the origin and integrity of the released medical document after obtaining the redacted document-signature pair

2. LITERATURE SURVEY

Steinfeld et al. 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. 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. Proposed another authenticated document sanitizing scheme based on bilinear maps. Nonetheless, the computation cost of this scheme is relatively high.

Ma et al. Also presented a secure and efficient design of RSSs with subdocument redaction condition control.

Liu et al. Proposed a novel and efficient redactable signature scheme for trees with finegrained redaction control mechanism.

In 2015,Pohls et al. 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.

3. PROBLEM STATEMENT

In the past few decades, a large number of researchers have thoroughly investigated the fundamentals of data verification [1]–[7]. For the integrity and authenticity verification, the majority of the earlier research was on generic solutions. While they safeguard data from hostile attackers, they also prohibit data from being processed, which limits the flexibility and effectiveness of the data's future uses. They may also conflict with data confidentiality in specific circumstances. Therefore, looking for appropriate procedures for data verification with confidentiality makes sense.

The privacy protection of patient health data in healthcare systems is the redactable signature's most widespread application [14]. In order to address privacy concerns, RSSs have also been used in social networks [15] and the smart grid [16]. The redaction problem of several data structures, including lists [12], [17], sets [13], [18], graphs [19], and trees [20], has been addressed by RSSs as a result of the diversity of data structures in various practical applications.

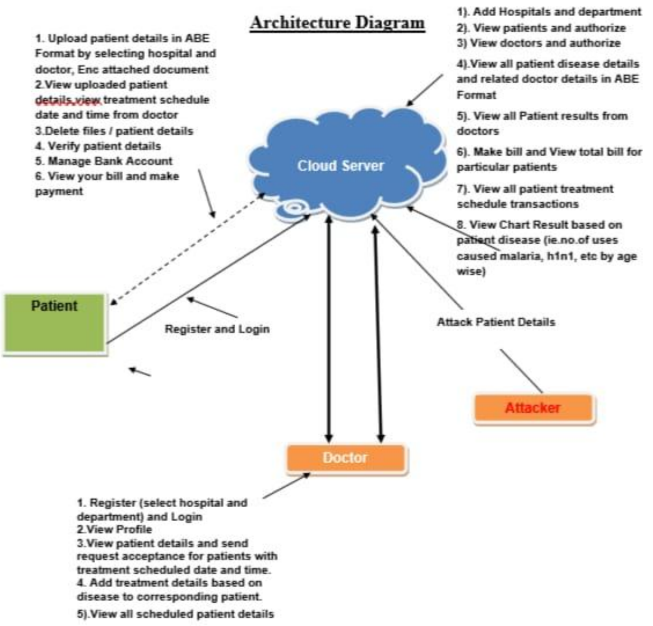
However, the security concepts used by RSSs for various data formats vary. A greater privacy feature that most of the existing systems lack is transparency [21], in particular. Derler et al. presented a general framework to avoid the need to build numerous models for various data structures.

Disadvantages:

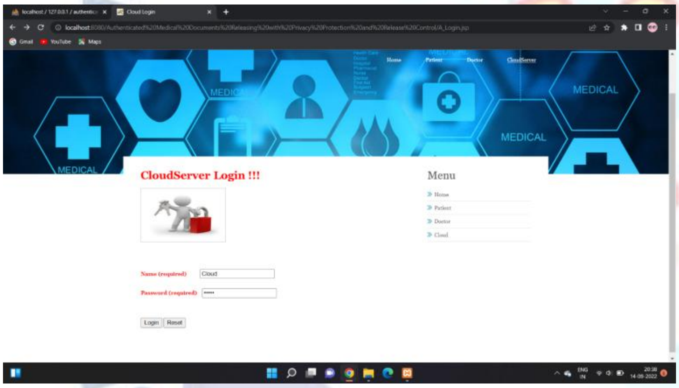
1.In the current work, the system uses the redactable signature scheme (RSS) that was developed in this work and is based on the Merkle hash tree and GGM tree. This design's most notable flaw is that the signature is rather brief when using the Merkle hash tree.

2.The current system added a new hierarchical redaction control scheme with a much reduced encoding.

4. ARCHITECTURE:


Architecture Diagram
1. Upload patient details in ABE Format by selecting hospital and doctor, Enc attached document
2.View uploaded patient details,view treatment schedule date and time from doctor
3.Delete files / patient details
4. Verify patient details
5. Manage Bank Account
6. View your bill and make payment
1). Add Hospitals and department
2). View patients and authorize
3) View doctors and authorize
4).View all patient disease details and related doctor details in ABE Format
5). View all Patient results from doctors
6). Make bill and View total bill for particular patients
7). View all patient treatment schedule transactions
8. View Chart Result based on patient disease (ie.no.of uses caused malaria, h1n1, etc by age wise)
Cloud Server
Patient
Register and Login
Attack Patient Details
Attacker
Doctor
1. Register (select hospital and department) and Login
2.View Profile
3.View patient details and send request acceptance for patients with treatment scheduled date and time.
4. Add treatment details based on disease to corresponding patient.
5).View all scheduled patient details

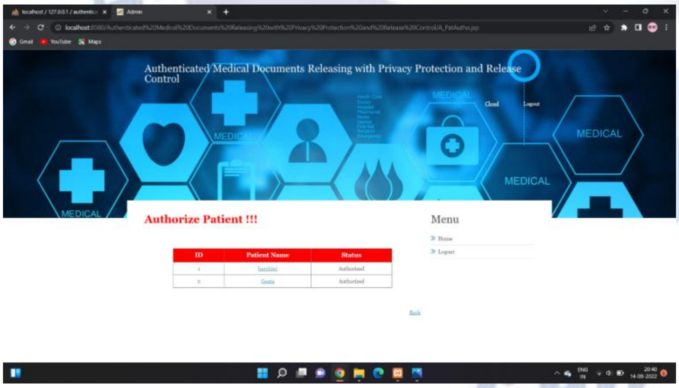
5.RESULTS


localhost / 127.0.0.1 / authentic
Cloud Login
localhost:8080/Authenticated%20Medical%20Documents%20Releasing%20with%20Privacy%20Protection%20and%20Release%20Control/A_Login.jsp
Gmail
YouTube
Maps
Home
Patient
Doctor
CloudServer
MEDICAL
MEDICAL
MEDICAL
MEDICAL
Menu
Home
Patient
Doctor
Cloud
Login
Reset
ENG
IN
20:38
14-09-2022

CloudServer Login !!!

Name (required) Cloud

Password (required) •••••


localhost / 127.0.0.1 / authentic
Admin
localhost:8080/Authenticated%20Medical%20Documents%20Releasing%20with%20Privacy%20Protection%20and%20Release%20Control/A_PatAutho.jsp
Gmail
YouTube
Maps
Cloud
Logout
MEDICAL
MEDICAL
MEDICAL
MEDICAL
Menu
Home
Logout
Back
ENG
IN
20:40
14-09-2022

Authenticated Medical Documents Releasing with Privacy Protection and Release Control

Authorize Patient !!!

ID	Patient Name	Status
1	harshini	Authorized
2	Geeta	Authorized

6. CONCLUSION

In order to address the privacy preservation and release control difficulties associated with publishing authenticated medical data, we developed two constructions of RSSs-FRC in this article, each of which had a distinct flexibility of release control methods. While the RSSs-FRC2 construction likewise gives the signer the ability to control the dependence of revealable subdocument blocks, the RSSs-FRC1 construction allows the signer to designate a minimum number of subdocument blocks that the redactor must release. Our designs are able to both identify unlawful redaction by the verifier and stop dishonest releases from redacting documents without restriction. Furthermore, provided the published subdocument has the signer's consent, the two suggested RSSs-FRC also permit repeated redaction operations. Finally, we presented the efficiency analysis and security proof for our RSSs-FRC.

Conflict of interest statement

Authors declare that they do not have any conflict of interest.

REFERENCES

[1] X. Chen, J. Li, J. Weng, J. Ma, and W. Lou, "Verifiable computation over large database with incremental updates," IEEE transactionson 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 onDependable 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 Transactionson 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 transactionson 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 Transactionson 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 Fundamentalsof 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 ofthe 2006 ACM Symposium on Information, computer and communicationssecurity. 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 Practiceand 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 EmergingTopics in Computing, 2017.

[19] A. Kundu and E. Bertino, "Privacy-preserving authenticationof trees and graphs," International journal of information security,vol. 12, no. 6, pp. 467–494, 2013.

[20] S. Hirose and H. Kuwakado, "Redactable signature scheme fortree-structured data based on merkle tree," in Security and Cryptography(SECRYPT), 2013 International Conference on. IEEE, 2013,pp. 1–8.

[21] C. Brzuska, H. Busch, O. Dagdelen, M. Fischlin, M. Franz,S. Katzenbeisser, M. Manulis, C. Onete, A. Peter, B. Poetteringet al.,"Redactable signatures for tree-structured data: definitions andconstructions," in International Conference on Applied Cryptography and Network Security. Springer, 2010, pp. 87–104.

[22] D. Derler, H. C. Pöhls, K. Samelin, and D. Slamanig, "A general framework for redactable signatures and new constructions," in International Conference on Information Security and Cryptology. Springer, 2015, pp. 319,

[23] L. Bull, D. McG. Squire, and Y. Zheng, "A hierarchical extraction policy for content extraction signatures," International Journal onDigital Libraries, vol. 4, no. 3, pp. 208–222, 2004

Authors Biography

K.Harshini currently pursuing MCA in SVKP & Dr.K.S Raju Arts & Science College affiliated to Adikavi Nannayya University, Rajamahendravaram, Her research include Web technologies ,Java script, Java.

P.Srinivasa Reddy is working as Associate Professor in SVKP &Dr K S Raju Arts & Science College, Penugonda, A.P. He received Masters Degree in Computer Applications from Andhra University. His research interests include Operational, Research ,Probability and Statistics , Design and Analysis of algorithm , Big Data Analytics