Turkish Online Journal of Qualitative Inquiry (TOJQI)
Volume 12, Issue 7, July 2021: 2552 – 2559

Medical Data Security and Privacy using Released Signature Schemes- Flexible Release Control

B.Vedika and D.Rajeswara Rao

Department of Computer Science and Engineering,
Velagapudi Ramakrishna Siddhartha Engineering College, Vijayawada, Andhra Pradesh, India.
ammuvedika7@gmail.com, hodcse@vrsiddhartha.ac.in

ABSTRACT

At the global level, various enterprises, public agencies, and governments have amassed vast amounts of digital data, thereby creating humungous amounts of knowledge-based applications. In view of the enormous potential thrown up by such innovative applications, the global business has witnessed a surge in demand in data collection. When huge amounts of data that are varied and sensitive in nature, are published and exchanged among various persons and entities, maintaining data security and personal privacy becomes a really challenging task. In particular, the patient information and health data leaks are highly potential for pharma companies for targeted marketing. It is very essential to provide security to the collected medical document. In this research article, we propose a novel technique called Released Signature Schemes and Flexible Release Control (RSS-FRC) to safeguard the documents both in transit and in rest. The document data is encrypted using image-based steganography technique and stored in cloud for effective retrieval process.

1. INTRODUCTION

The specialized data obtained by businesses, non-profit organization, and government agencies around the world has created enormous opportunities for developing applications that are based on information or data. Such developments have made the distribution and exchange of acquired information among multiple parties more productive and mutually-beneficial. However, sensitive client information is usually found in the initial entries, and there is chance for abuse or misuse of such protected data if such information was released without being safeguarded. In such a scenario, archive redaction may be applied as a direct security method to remove very sensitive data from a report, thereby preventing its potential misuse. For example, as a fundamental approach for enterprises, record redaction helps them to avoid unintended or even malicious disclosure of proprietary information when providing information to redistribution activities. In recent years, the safe exchange of clinical data has come to gain a lot of traction from both professionals and even expert researchers. As such a concept has great promise for fostering a coordinated effort

within the medical services network and other groups, such as pharmaceutical companies, insurance companies, and research organizations; it may help better clinical treatment methods in qualitative as well as quantitative terms. Digital signals may now be sent via the internet with ease thanks to recent and rapid improvements in communication technologies [1]. These improvements have brought numerous benefits, but they have also brought with them a number of hazards and concerns that must be considered. As new technologies emerge, such as telemedicine, guaranteeing medical data security is getting more difficult [2]. Medical data theft has recently emerged as a serious cybercrime activity. When any sensitive information gets hacked or stolen, there is a strong possibility of unauthorized persons or entities trying to breach the fundamental rights of a patient. To maintain trust between patients and health-care facilities, medical report confidentiality must be maintained. In medical centers huge databases are installed to store Electronic health records (EHR) so that it becomes possible to keep patient's health records in secure manner [3]. Usually, the patient-related sensitive records comprise his/her personal data, vital signs, reports from diagnostic labs, and any other medical information. Such comprehensive and vital medical data can help both the medical professionals as well as the patient, which is also supported really well by using advanced ICT applications like internet-based networks like LAN or WAN for real time sharing of such medical data. Medical imaging account for around 90 percent of all medical data stored in EHRs. The Digital Imaging and Communications in Medicine (DICOM) standard is used to store, process, and transmit medical pictures such as X-rays, endoscopic images and video, MR (magnetic resonance) images, and so on. To avoid tampering with patient data, unauthorized copying, and to ensure copyright protection, patient information in DICOM files must be kept confidential [3]. Medical data must be protected in every way feasible to maintain confidentiality.

2. LITERATURE SURVEY

As reported in their research work entitled, "Verifiable computation over large database with incremental updates," IEEE transactions on Computers, vol. 65, no. 10, pp. 3184–3195, 2016X, Chen, J. Li, J. Weng, J. Ma, and W. Lou stated that the large presence of cloud services have enabled the scientific community to search for ways to develop techniques to achieve secure outsourcing of the costly critical computational tasks. It means that clients having problems with resources get the chance to transfer some critical computing tasks to unknown cloud servers to get the usage in exchange for some specified fees known as pay-per-use method. Because cloud servers may occasionally produce erroneous results, while assigning tasks to outsourcing agencies, clients demand that the outsourced computational task is open to quick validation of the legitimacy of the computation result. Many researchers have spent decades studying the basic concept of verifiable computation [9], [13], [14].The majority of previous researches have concentrated on developing generic solutions for any function (encoded as a Boolean circuit). Alt hough the challenge of verifiable computation has been resolved in theory, there is still some question marks over the efficiency of the offered solutions in real-world applications. As a result, there is still some possibility of exploring efficient protocols that could make computation of certain functions easily and effectively verifiable. To address the challenge of verifiable outsourcing storage, Benabbas et al. [15] developed a concept of the verifiable database (VDB). In other words,

when a resource-constrained client wants to keep a very big database on a server, he/she should be able to obtain a database record and effect some modifications or updates in future by assigning a new value later. Any tampering effort by the server in the database has a high probability of being noticed by the client. Furthermore, the client's investment in compute and storage resources must be independent of the database's size (excluding initial setup phase). With the rise of cloud computing, clients with low resources are increasingly turning towards the cloud server for assigning tasks requiring heavy computation. In spite of the obvious advantages of the outsourced computing model for the clients as well as the outsourcing cloud servers, there can still be some security risks and cyber threats. In the present work, the primary tasks is on analyzing and understanding a significant aspect like the outsourcing computation of matrix multiplication; and also, propose a novel computation scheme for batch matrix multiplication that can be publicly verified. Unlike previous matrix computing outsourcing models, our scheme's outsourcing task involves computation of MXiMXi for a clientele, by employing XiXi as a private matrix that a client chooses himself, while M represents a public matrix that a data centre assigns prior to the task. Our scheme can protect the secrecy of the client's private matrix XiXi and drastically lower the computation expense while generating keys as well as in the computing phases by combining the two techniques of privacy-preserving matrix transformation and matrix digest. Under the co-CDH assumption, the suggested method can also accomplish the requisite security features as indicated by security analysis. Many businesses and organizations are keen on outsourcing their data to third-party cloud service providers (CSPs) due to the emergence of cloud computing avenues that help them in enhancing the storage limits of local devices. Amazon's basic storage service (S3) on-line data backup services and Google Drive [2], Dropbox [3], Mozy [4], Bitcasa [5], and Memopal [6] are new age commercial cloud storage systems developed specifically for delivering cloud applications. In some instances, when such servers yield unfavourable and inaccurate results due to hardware/software malfunction or any problem caused by human handling of tasks, or any hostile assault [7], new types of data integrity and accessibility assurance are needed to defend the security and privacy of the user data. Measures such as simple replication and protocols like Rabin's data dispersion method [8] do not offer any concrete solution to tackle the significant security challenges that cloud storage services are experiencing these days. In fact, the above methods do not seem feasible in application in this regard as a recent IDC analysis suggests that data production is fast surpassing storage availability [9]. When a quorum of repositories, such as k-out-of-n of shared data gets assigned, the more recent protocols prove their worth in the maintenance of data availability. But, such protocols fail to guarantee their clientele as far as steady availability of each repository is concerned, thus limiting their potential to provide effective assurance to their clients.

3. PROBLEM STATEMENT.

Though past researchers have largely dealt with primitive of data verification during the last few decades, yet a majority of such works have only concentrated on developing generic solutions to prove the integrity and authenticity of such verification processes. Apart from protecting data from getting exploited by unscrupulous attackers, they also ensure that data

does not get processed by the unauthorised players. In fact, while getting in such exercises their flexibility and efficiency with data processing gets compromised. Furthermore, in some cases, some incompatibility issues with data secrecy crop up. As a result, it's important to look for proper data verification protocols that are also confidential. Johnson et al. explicitly presented the concept of redactable signatures as an illustration of a wide class of homomorphic signatures. The Merkle hash tree and GGM tree are the foundations of the redactable signature system (RSS) that is proposed in this paper.

The most notable benefit of this approach is that the signature is reasonably small for Merkle hash tree application. Johnson et al. created a situation in which only a small portion of a document is censored and the rest is made public. The term "Content Extraction Signature" (CES) was coined by Steinfeld et al. in 2001. Here, the holder of a signed document creates redacted signatures even for parts contained in the original authenticated document. The idea behind redactable signatures is very much like the concept of CES. The “Content Extraction Access Structure” (CEAS) was suggested by Steinfeld et al. so as to encode subdocument indexes in original documents, which is the evident difference between RSSs and CES. In such an approach, the signer defines subdocuments that can be extracted by subsequent users.

Ever since the introduction of the redactable signature concept, there has been numerous applications of this concept in varied practical situations, whether while protecting privacy of audit-log data or in releasing old classified government documents and , more recently, in sharing medical data, among others. To overcome the document sanitising problem, Miyazaki et al. introduced the first redactable signature technique that prevents occurrence of further sanitising assaults. As a follow up, they developed such a different system having a bilinear maps based sanitising condition control as a solution to this issue, pointing out flaws in the previous solution that could potentially expose the number of cleaned regions.

4. METHODOLOGY

A cloud server receives the outsourced documents from a patient, after which it is ensured that the data is easily and securely accessed by the designated search doctor. The patient applies attribute-based encryption to convert the original records into a suitable encrypted format under an access policy in order to maintain data privacy. She also produces some keywords for each outsourced document to boost search efficiency. The secure KNN scheme's secret key is then used to construct the corresponding index based on the keywords. The encrypted files are then sent by the patient to the cloud server along with the associated indexes, while submitting the secret key to the searched doctor.

The encrypted records and indexes received from patients are stored on a cloud server, which subsequently enables data access and search services to approve search doctors and authorise them. When the cloud server is sent a trapdoor by the search doctor, while in turn, it returns a host of relevant records segregated on the basis of a few specific parameters.

The secret key can be obtained from the patient by a designated doctor, who can then use it to create trapdoors. He will create a search keyword set when there is a need to search the outsourced files that the cloud server has already stored. Then, a trapdoor is generated when the doctor applies the secret key, which is then transmitted to the cloud server after inputting

the keyword set. In the end, the corresponding records are retrieved from the cloud server and decrypted by applying the ABE key that the trusted authority provides. The medical reports can also be outsourced to the cloud server when the patient's health information is accessed or received In our case, we have considered the one-way communication only for the sake of simplicity.

Database Schema

Field	DataType
Patient_Id	Number
First_Name	String
Last_Name	String
Email	String
Mobile	Number
Scans	BLOB

PROCUDER

Image encryption using chaos based hybrid AES algorithm

1. Let the source image be I and the size is denoted with I_m *I_n.
2. Generate a set of pseudorandom numbers P =$\{p_1, p_2, \ldots\ldots, p_n\}$.
3. Find the minimum and maximum in the sequence $\{p_{min}, p_{max}\} \in P$.
4. For i=1 to P=$\{\emptyset\}$
5. $b_i = \{p_{min}, p_{max}\}$
6. $P = P/\{p_{min}, p_{max}\}$
7. b_i= $\{b_1, b_2, \ldots\ldots, b_{p/2}\}$be the generated chaos sequence such that the pairs of{ $b_1 < b_2 < \cdots < b_{p/2}\}$
8. Divide the image I into J blocks such that each of the block consists of 16 pixels.
9. J=Int($I_m * I_{n/16}$)
10. Rearrange the source image such that the resolution become $I_r = I_{mn} * I$.
11. Permute each block in J and place it with the pseudorandom numbers P.
12. Input the permuted block of image in AES encryption
    For i=1 to j
    Chipher(i)=Encrypt_AES(I,key)
    End for
13. Reshape the resultant matrix $I_r = I_{mn} * 1\ to\ I = I_m * I_n$

The suggested method aims to create safe and efficient RSSs having flexible release control (RSSs-FRC) that helps in preserving privacy and guarantees flexibility in release control in case of authorized health record release systems. The following key contributions that our study seeks to make in this regard. In medical records releasing systems, the system presents two novel RSSs-FRCs that satisfy distinct release control needs. The threshold secret sharing mechanism applied in RSSs-FRC1 helps in achieving minimal release control. RSSs-FRC2 implements hybrid release control via an access tree that regulates not just minimum release number, it also regulates dependency of releasable subdocument blocks.

The proposed RSSs-FRCs are formally defined, besides defining the security features that are associated with unforgeability, privacy, and transparency. In a reduction mode, the security attributes are clearly demonstrated. Moreover, while applying theoretical and practical approaches, the efficiency and usefulness of our structures are evaluated by the system to demonstrate their applicability in the form of efficiency and functionality. In order to ensure designing of secure and efficient RSSs- FRCs on the basis of universal approaches, the suggested system makes use of generalized constructs. Such a design will prove itself as most efficient while dealing with unauthorized redaction and privacy leakage problems that occur in varying conditions under which authenticated records are released.

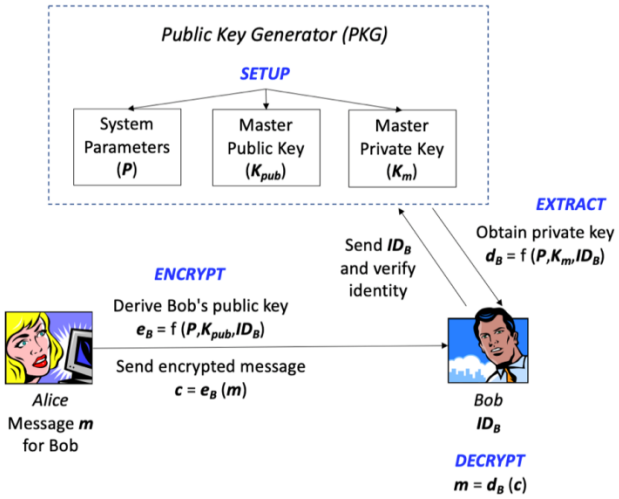
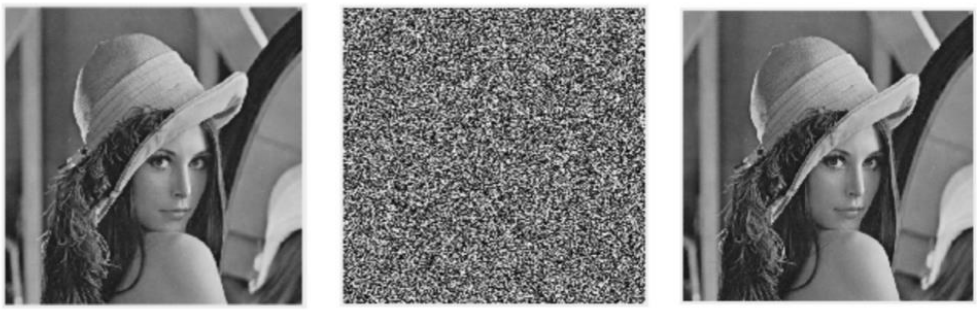


Fig 1: Illustration of the encryption process

Other than the release control mechanism, there is much similarity between the building elements of the proposed RSSs-FRCs, which results in presenting in universal formats the algorithm descriptions and formal security definitions associated with the suggested RSSs-FRC. In order to avoid duplication in the above definitions, which are already done in case of trees, we have attempted suitable alterations in order to attain the stated objectives set in case of data-structure, release control, and security. The RSSs-FRC has a similar unforgeability definition as that of a typical conventional DSS. However, as it is computationally impossible for an attacker to create a valid message-signature pair (M,σ) without any access to the secret key, it is made mandatory for them to pass the verification test, and M is neither (A) a submessage of any message queried to the signing oracle i.e.,(M* M_j)or (B) is a submessage of a message queried to the signing oracle, but skips the validation of the release control policy, i.e M($M_j \cup P_j$ 6 = 1). In RSSs-FRC systems, transparency is more deemed more valuable than privacy, thus making the message signature remain an enigma for all the verifiers, who are clueless whether they were directly derived from the Sign or Redact algorithms or not. As a result, every redactable signature scheme having transparency is also private.In a digital signature scheme (DSS), the secret key S_K, is used by signer S to “sign” a message in order to enable the person knowing the associated public key P_k, to verify whether the message has ever been modified in transit or not, thus validating its origin from *S*. A DSS comprises three polynomial-time algorithms ($D_{Gen}, D_{Sign}, D_{Verify}$) such

that:$D_{Gen}(1\gamma)$ The input of this probabilistic algorithm is a security parameter 1γ and the output is a key pair(P_k, S_k),$D_{sign}(P_k, M)$ The input of this algorithm is a secret key S_k and a message M. It outputs a signature σ of this message, which is represented as $\sigma \leftarrow D_{sign}(S_k, M)$. $D_{verify}(P_k, M, \sigma)$: The input of this deterministic algorithm includes a message M, public key P_k, and a signature σ. The output is a bit $b \in \{0,1\}$, with $b = 0$indicating invalid and $b = 1$ meaning valid. This is denoted as $b \leftarrow D_{verify}(P_k, M, \sigma)$.

Experimental Results



(a1)Original Lena (a2)Encrypted Lena (a3)Decrypted Lena

Fig 2: Illustration of the encrypted steganographic image

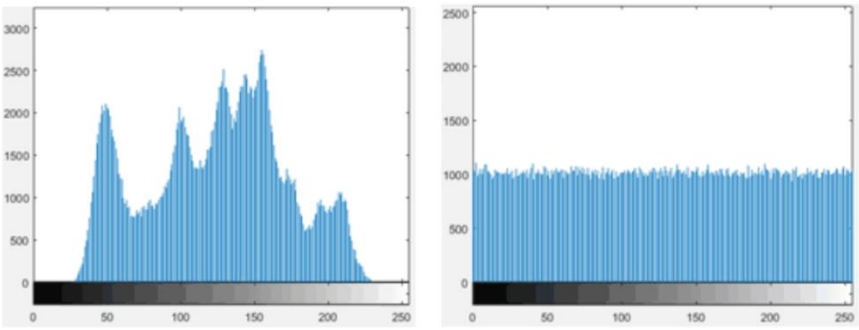


Fig 3: Histogram of original image and decrypted image

Conclusion

Medical data can be easily stolen or intercepted or exploited while it is stored, transmitted, or received through a network or over the internet. With proper security protocols, medical data can be securely stored, transmitted and processed, thereby preventing a host of cybercrimes. In this paper, a novel image steganography approach has been proposed to securely encrypt the medical or health data of patients while ensuring that the quality and imperceptibility in stego images are adequately maintained. Using the proposed construction model, we have demonstrated that doctors and patients can easily and securely share medical records between themselves. Further, the results prove that such shared information can't be directly accessed by any unauthorized person(s), thus making our system safe and secure for transaction of 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 publiclyverifiable 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, “Newalgorithms for secure outsourcing of large-scale systems of linearequations,” 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 forsecure 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, “Verifiableauditing 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 shareddynamic 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, “Newpublicly verifiable computation for batch matrix multiplication,”Information Sciences, 2017.

[8] R. Johnson, D. Molnar, D. Song, and D. Wagner, “Homomorphicsignature schemes,” in Cryptographers’ Track at the RSA Conference.Springer, 2002, pp. 244–262.

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

[10] O. Goldreich, S. Goldwasser, and S. Micali, “How to constructrandom 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 withdisclosure 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 documentsanitizing 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, “Sanitizablesigned privacy preferences for social networks,” DICCDI, LNI. GI,2011.

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