

Authenticating Insurance Documents Using Ciphertext-Policy Based Attribute Signcryption

G.Princiya^[1], G.Rubini^[2], B.Santhana Lakshmi^[3], Kavitha Subramani^[4]

U.G.Scholar^{[1],[2],[3]} Associate Professor^[4]

Department Of Computer Science and Engineering, Panimalar Engineering College
Chennai – India

ABSTRACT

With regards to Information Societies, a colossal measure of data is day by day traded or discharged. Among different data discharge cases, therapeutic archive discharge has increased huge consideration for its potential in improving medicinal services administration quality and adequacy. 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. Data editing, a simple tool for protecting privacy, is to delete sensitive data from the text. Redactable signatures allow any party to delete pieces of an authenticated document while guaranteeing the origin and integrity authentication of the resulting (released) subdocument. In our Construction we introduced a new entity called Authenticator. The Authenticator does the process of verifying the user-specified details and proceeds further. We also analyses the performance of our constructions in terms of security, efficiency and functionality. The analysis results indicates the performance of our construction has major advantages over others, from the aspects of security and efficiency.

Keywords:- *Authenticator, Privacy, Redactable Signatures.*

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 delete confidential details 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 tremendous publicity among practitioners as well as in the culture of scientists. 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 efficiency 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. Relevant to this, yet another important requirement regarding subsequent 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's critical 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.

II. RELATED WORK

Ashish Kundu Elisa et al (2013) have introduced an authentication scheme is used to verify accuracy of data and that the claimed owner is in fact the authorized owner of the data. Specific authentication requirements and techniques depend on the structure according to which data are organized. Since tree and graph structures are widely used data organization structures, the development of techniques specifically suited for data organized according to such tree structures is crucial. When addressing the problem of authentication of tree structures, it is important to notice that each node may contain some content

and that the structural nodal relationships may establish some relationships between the contents in these nodes. These relationships can be characterized by properties such as the indexing of the temporal orientation and content sensitivity. The integrity of these relationships is called structural integrity while material integrity is referred to as software integrity.

Dan Boneh et al (2003) have stated the sanitizable signature until now to several Sanitizable Signature Schemes. Existing signature sanitizable schemes however face the dishonest sanitizer or additional sanitizing issue because the sanitizer will unrestrictedly change the signed document. This paper will therefore propose a scalable, Signature Sanitizing Scheme based on a bilinear mapping. According to our safety review this proposed scheme is not just to preserve the safety requirement of sanitizable signature but also to boost the disadvantage of related schemes. The requirement that all messages in an aggregate be distinct is naturally satisfied for the applications to certificate chains and SBGP we have in mind. The implicit prefix need not be transmitted with the signature, so signature and message length is unaffected.

Jianghua Liu et al (2019) have proposed 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 when at a party 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.

Jinhua Ma et al (2017) have proposed Redactable signatures, a branch of malleable homomorphic signatures for editing have wide applications in online privacy interactions to bandwidth savings. Nonetheless, most current systems are vulnerable to unlicensed arbitrariness wording or further redaction. Redaction control is a key mechanism for restricting behavior that legitimate users can take in sensitive systems and for restricting unauthorized abuse by any user. We suggest a new and widespread approach to creating a redactable

signature scheme with fine-grained redaction control.

Josh Benaloh et al (1994) have emphasized that the advantage of this approach over the naïve “save everything you see” approach is simply one of storage. In terms of storage, this practice is comparable with that of holding a central authority's public key and using it to check that it was signed with the central authority. Use the one-way accumulator, but implementations accumulators shall be of one sort provided in the section for central authority. The First is a method for creating a time-stamping system in which participants can store and time-stamp their documents in such a way that time-stamped documents can be revealed to others later. Second Application demonstrates how a membership testing program can be developed needless to say maintain membership lists of both applications.

Kai Samelin et al (2012) have stated the “digital document sanitization problem”, as proposed by Miyazaki, the process of signing cannot be altered by itself. This may happen, where the signer is no longer reachable or does not know what portions of the contract are passed on to third parties. Consider the following two examples clarifying why one needs to be able to redact structure, in a university the exam results are published in a list. We only want a signed list of all the students' name who took part in the exam. We therefore need to write all the grade details from this list, a redactable scheme allows the deletion of grades using a clear RSS to eliminate the trace that any pieces have been removed. However, the original ordered relationship of the remaining subdocuments still invades privacy, so we must also write the ordering between them. Present schemes cannot edit this information because they allow that the order cannot be changed or only operate on structureless sets.

Kunihiko Miyazaki et al (2006) have introduced existing digital signature systems cannot guarantee a document's confidentiality and integrity. This is called the digital document sanitizing problem, and one proposed solution is to use sanitizing schemes that verify the authenticity of the unmasked portions of a sanitized document. This solution is essentially the same as the content extraction signature (CES) scheme developed by Steinfeld, Bull and Zheng if we regard a sanitizer in the digital document sanitizing scheme as a document owner in the CES scheme. A CES requires structured documentation to the owner, such as birth or marriage certificates signed by a trusted authority to generate an extracted signature on selected extracted portions from the original documents and enables any third party to verify

that those portions were in the signed original documents.

Kunihiko MIYAZAK et al (2005) have explained to deal with our proposed scheme, the major difference between that model and the extended model is the existence of multiple sanitizers. In our template may be assigned by could sanitizer disclosure condition for the document and other subsequent sanitizer may change the condition under the condition assigned by the previous sanitizer .The signer produces a digital signature that guarantees the original document's validity without knowing the parts of the document will be sanitized . A sanitizer assigns to the portion, for which the condition “disclosed and additional sanitizing is allowed” has been assigned, one of the conditions “sanitized,” “disclosed and additional sanitizing is allowed,” or “disclosed and additional sanitizing is prohibited” and send the document to other sanitizers or to the verifier. A sanitizer does not know which blocks of a paper will be disclosed before the signer generates a digital signature for the document.

Laurence Bull et al (2004) have proposed Content Extraction Signatures (CES) were originally designed for use in multiparty interactions to overcome privacy concerns by enabling the selective verifiable disclosure document content. CES allow the owner bob of a document signed by a signatory Alice to create an (original subdocument with less material removed) that can be verified by any third party carol without transparency the contents of the removed portions of the original document. The production of the sub-document may involve either extracting or blinding content from the original document. An essential and integral component of CES is the extraction policy, since it requires the signer to decide the fragments or blinded extraction policy can be extracted. Extraction Policy validation is a requirement for CES validation. In short, these enable verifiable selective disclosure information through the use of a salt to provide protection for blinded information and let the signer define the material that the owner of the document can extract or blind.

Vipul Goyal et al (2006) have stated one way to improve problems some of these problems is to store data in encrypted form so if the database is compromised the amount of information loss is reduced. One downside to encrypting data is because it strongly restricts users' ability to selectively share their encrypted data at a fine grained level. The user must either serve as a mediator and decode all related party entries or provide the party with its private key for decryption thus granting it access to all entries .A major environment where these issues cause serious

problems is the audit logs. Fine-grained access control systems facilitate granting differential access rights to a set of users and allow flexibility in specifying the access rights of individual users. Several techniques are known for implementing command of fine grained exposure. Access control is based on software checks such that a person should access only one piece of data if he is allowed to do.

III.METHODOLGY

A new scheme with sanitizing condition control based on bilinear maps as the solution the first authenticated record with sanitization scheme with redaction condition control another authenticated document sanitizing scheme based on bilinear maps. Nonetheless, the computation cost of the framework is relatively high security properties in terms of enforceability, privacy and transparency. The security properties are proved in a reduction mode two RSSs-FRC as well as their security in security, accountability, unforgivable. The correctness of our constructions have been distinctly presented in their respective verification. 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 future work, we plan to explore RSSs with redactor accountability for privacy-preserving release of authenticated medical documents. RSSs with Flexible Release Control (Signcryption) a flexible and modular control for a modular production system with the ability to use manufacturer-independent functions and modules is proposed. A new approach is developed to standardize the description and an open interface for functions and modules. The analysis results show security and efficiency. It uses Redactable Signature.

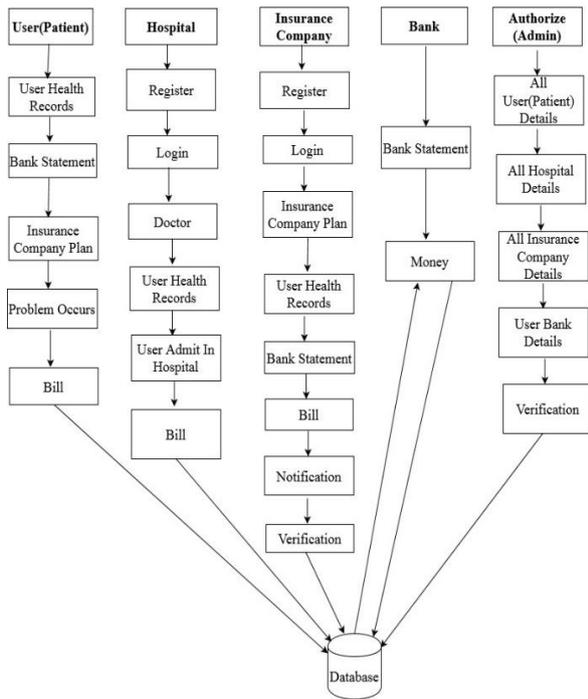


Fig1. System Architecture

IV.SYSTEM IMPLEMENTATION

System Implementation is the process of defining how the system should be built ensuring that the system is operational and used. The proposed system comprises of modules such as

1. USER INTERFACE DESIGN
2. INSURANCE COMPANY PLAN
3. VERIFICATION OF BANK STATEMENT
4. USERS PLAN
5. EMERGENCY OCCURS
6. PROVIDING BILL TO INSURANCE COMPANY
7. VERIFICATION FROM INSURANCE COMPANY

1. USER INTERFACE DESIGN

This is the first module of our project. The important role for the user is to move login window to user window. This module has created for the security purpose. In this login page we have to enter login user id and password. It will verify your username and password is match or not (valid user id and valid password). If we enter any invalid username or password we can't enter into login window to user window it will shows error message as 'please contact your authenticator'. So we are preventing from unauthorized user entering into the login window to user window. It will provide a good security for our project. So server contain password and user ID server also check the authentication of the user. It enhances safety well and prevents unauthorized users from accessing the network in our project that we use JSP to build architecture and server authentication.

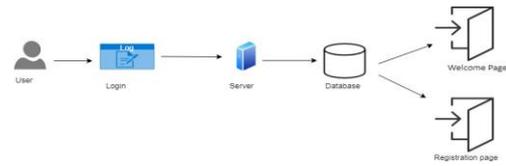


Fig2. User Interface

2. INSURANCE COMPANY PLAN

Insurance Company targets on several users and make them to take insurance. Insurance Company ask users to get insurance from their company through online. In this module the insurance plan details are stored. Here we use JSP page to get information from user through online. Then the document will be shown to the user. User verifies and sign the document. The Advanced Encryption Standard (AES) algorithm is used in this module to generate a random key for that particular document. The key is used in decrypting a particular document.



Fig3. Insurance Plan

3. VERIFICATION OF BANK STATEMENT

Here Insurance Company will verify the bank statements of particular user. The reason for verifying a bank statement is to ensure that the particular user has a monthly income or whether the user is able to pay the corresponding insurance plan. After checking the bank Statement Company will provide a insurance for them. In this module we have to upload the *signature file*. This ensures that the signature is from a valid user or not. This provides an additional security in our project through internet.

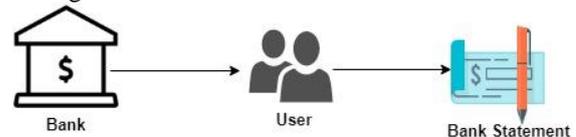


Fig4. Bank Verification

4. USERS PLAN

In this module, user will get a full health insurance from the assured company, there they will get some offers like free health checkup etc., The health records information is sent to insurance company by the health care. The insurance company collects all the information regarding the user health and also the bank statement. Both the documents are encrypted and signed by using and the Redactable Signature Scheme (RSS) and key is generated in this module.

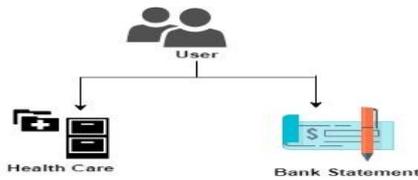


Fig5. User Plan

5. EMERGENCY OCCURS

In this module, if the user is affected by some severe disease or an accident they will be admitted in nearby hospitals. After getting all the necessary treatment in their specified hospital and the bill will be issued by the hospital to the user.

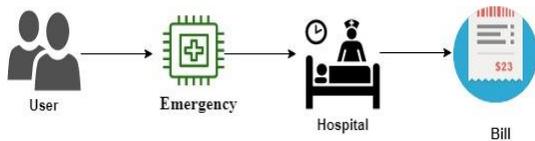


Fig6. Emergency Occurs

6. PROVIDING BILL TO INSURANCE COMPANY

After getting the treatment, if the user wishes to claim the insurance, he has to submit the bill provided by hospital. The user gives the bill to insurance company for verification and claiming process.

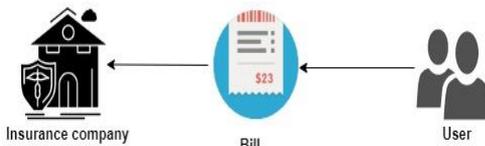


Fig7. Bill

7. VERIFICATION FROM INSURANCE COMPANY

Insurance company will verify the bill provided by the hospital. It will then verifies the encrypted files of bank statement and health records of a particular user. Insurance company asks the Authenticator to verify the particular hospital, user documents and bank statement. The Authenticator in turn verifies and provides permission to claim. Then the Insurance Company will credit the amount to the user’s account.



Fig8. Insurance Company Verification

SYSTEM TECHNIQUES

1. REDACTABLE SIGNATURE SCHEME-FLEXIBLE RELEASE CONTROL

Redactable Signature Schemes-Flexible Release Control RSS-FRC permit to remove parts from signed documents, while the signature remains valid. Some RSS-FRC for trees allow to redact non-leaves. Then, new edges have to be added to

the tree to preserve its structure. This alters the position of the nodes' children and may alter the semantic meaning encoded into the tree's structure. A security model, Redactable Signatures allow any party to delete parts of an authenticated document while maintaining the origin and validity of the resulting subdocument. And much of the established Redactable Signature Schemes-Flexible Release Control (RSS-FRCs) is open to dishonest editors or identification of unauthorized redactions. Redactable Signature Schemes-Flexible Release Control for trees with signer enabled and non-leaf edits.

- **Setup:** On input of a security parameter, it outputs a public key PK and a secret key SK.
- **Sign (SK, t, M):** On input of a SK and a document with message blocks, it outputs a signature on M.
- **Redact (PK, t, M,σ, M'):** On input of a PK, documents and a valid signature on M, it outputs a signature on M'. In this case, we say that (M', σ') is a redaction of(M, σ).
- **Verify (PK, t, M, σ):** On input of a PK, a document and a signature, it outputs 0 (reject) or 1 (accept).

2. ADVANCED ENCRYPTION STANDARD

Advanced Encryption Standard (AES) is a cipher, meaning that it is a method or process used to change raw information (usually human readable) into something that cannot be read. This part of the process is known as encryption. The method uses a known, external piece of information, called a key, to uniquely change the data. An example might be your computer login password, or the password to your account on a bank machine. Further, the process is reversible, meaning that it can be applied again to put the information back to original form. This part is known as decryption.

- **KeyExpansion:** Round keys are derived from the cipher key, AES requires a separate 128-bit round key block for each round plus one more.
- **Initial round key addition:** AddRoundKey, each byte of the state is combined with a byte of the round key using bitwise xor.
- **9, 11 or 13 rounds:**

- ✓ **SubBytes:** A non-linear substitution step where each byte is replaced with another according to a lookup table.
- ✓ **ShiftRows:** A transposition step where the last three rows of the state are shifted cyclically a certain number of steps.

- ✓ **MixColumns:** A linear mixing operation which operates on the columns of the state, combining the four bytes in each column.
- ✓ AddRoundKey

➤ **Final round (making 10, 12 or 14 rounds in total):**

- ✓ SubBytes.
- ✓ ShiftRows.
- ✓ AddRoundKey.

V. RESULTS AND DISCUSSION

The proposed system is implemented using J2EE (JSP, Servlets) JavaScript, My SQL 5.5, IDE: Eclipse in Windows Operating System.

Fig11. Patient Registration

Fig9. Hospital Login

Fig12. Authenticator Login

Fig10. Insurance Plan

S.NO	HOSPITAL NAME	MAIL ID	MOBILE NUMBER	ADDRESS	PH	STATUS	UPDATE
4	xps	xps@gmail.com	123523619	heyyl	54632	activate	Activate
5	saveetha	saveetha@gmail.com	1489055498	sripurumbudur	466256	activate	Activate
6	ramachandra	ram@gmail.com	4057583221	adayar	24833	activate	Activate
7	xyyy	xyyy@gmail.com	234567890	adayar	12345	activate	Activate

Fig13. Hospital Activity Status

IC	IC Name	Insurance Plan	Insurance Status				
INSURANCE COMPANY STATUS							
Hospital Name	Doctor Name	Patient Name	Insurance Company	File Size	File Name	File Type	Status
xyyy	rsd	kurnat	ic	4106	application.pdf	application/pdf	on
xyyy	rsd	rs	ic	932	0nd new ren 2278.pdf	application/pdf	on

Fig14. Insurance Company Status

IC	IC Name	Insurance Plan	Insurance Status	Patient Name	IC	IC Name	Insurance Plan	Insurance Status
DOCTOR SEND TO INSURANCE COMPANY								
Hospital Name	Doctor Name	Patient Name	Insurance Company	File Size	File Name	File Type		
abc	rsd	kurnat	ic	5030	Patient Register Details Success Full 1.pdf	application/pdf		

Fig15. Application to Insurance Company

The image shows a web form titled "PATIENT DETAILS" with a light green header. The form has a yellow background and contains several input fields:

- Hospital Name:** A text box containing "abc".
- Doctor Name:** A text box containing "ram".
- Date:** A text box containing "03-04-2020".
- Bill Copy:** A file selection area with a "Choose File" button and the text "Patient Register Details Success Full1.pdf".
- Bill Key:** A text box containing "92703".

 At the bottom of the form is a red "Send" button.

Fig16. Key Generation

VI. CONCLUSION AND FUTURE ENHANCEMENT

Presented two developments of RSSs-FRC with an alternate adaptability of discharge control systems to determine the security conservation and discharge control issues in discharging confirmed medicinal reports. The RSSs-FRC1 development enables the endorser to indicate a base number of subdocument hinders that the redactor needs to discharge, while the RSSs-FRC2 development additionally engages underwriter to direct the reliance of reveal able subdocument squares. Our developments not just keep the untrustworthy discharge from redacting report freely yet in addition can identify unlawful redaction by the verifier. Moreover, the two proposed RSSs-FRC additionally bolster numerous redaction controls giving the discharged subdocument is approved by the endorser. At last, we exhibited the security confirmation and effectiveness investigation for our RSSs-FRC. For future work, we intend to investigate RSSs with redactor responsibility for security saving arrival of verified therapeutic archives.

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 we except what to do, we plan to explore RSSs with redactor accountability for privacy-preserving release of authenticated medical documents.

REFERENCES

- [1] Ashish Kundu ,Elisa Bertino , "Privacy-preserving authentication of trees and graphs", Published online: 26 May 2013© Springer-Verlag Berlin Heidelberg 2013.
- [2] Dan Boneh, Craig Gentry, Ben Lynn, and Hovav Shacham,"Aggregate and Verifiably Encrypted Signatures from Bilinear Maps", E. Biham (Ed.): EUROCRYPT 2003, LNCS 2656, pp. 416–432, 2003.
- [3] Jianghua Liu, Jinhua Ma, Yang Xiang, Wanlei Zhou and Xinyi Huang, "Authenticated Medical Documents Releasing with Privacy Protection and Release Control", IEEE Transactions on Dependable and Secure Computing,DOI 10.1109/TDSC.2019.2892446.
- [4] Jinhua Ma, Jianghua Liu, Xinyi Huang, Yang Xiang, and Wei Wu," Authenticated Data Redaction with Fine-Grained Control", 2168-6750 (c) 2017 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission.
- [5] Josh Benaloh and Michael de Mare," One-way Accumulators: A Decentralized Alternative to Digital Signatures" , T. Hellesteth (Ed.): Advances in Cryptology - EUROCRYPT '93, LNCS 765, pp. 274-285, 1994.
- [6] Kai Samelin, Henrich C. P'ohls, Arne Bilzhaue,Joachim Posegga, and Hermann de Meer, "Redactable Signatures for Independent Removal of Structure and Content" , ISPEC 2012, LNCS 7232, pp. 17–33, 2012.Springer-Verlag Berlin Heidelberg 2012.
- [7] Kunihiko Miyazaki, Goichiro Hanaoka, Hideki Imai, " Digitally Signed Document Sanitizing Scheme Based On Bilinear maps" , ASIACCS'06, March 21–24, 2006, Taipei, Taiwan Copyright 2006 ACM 1-59593-272-0/06/0003.
- [8] Kunihiko MIYAZAKI, Tsutomu MATSUMOTO, Ryoichi SASAKI, Hiroshi YOSHIURA," Digitally Signed Document Sanitizing Scheme with Disclosure Condition Control" , Ieice Trans. Fundamentals, Vol.E88–A, No.1 January 2005.
- [9] Laurence Bull1, David McG. Squire, Yuliang Zheng,"A Hierarchical Extraction Policy for content extraction signatures", Published online: 20 October 2004 – Springer-Verlag 2004.
- [10] Vipul Goyal, Omkant Pandey, Amit Sahai and Brent Waters, "Attribute-Based Encryption for

Fine-Grained Access Control of Encrypted Data” , CCS’06, October 30–November 3, 2006, Alexandria, Virginia, USA. Copyright 2006 ACM 1-59593-518-5/06/0010 ...\$5.00.