International Journal of Trendy Research in Engineering and Technology
Volume 4 Issue 3 June 2020
IJTRET
ISSN NO 2582-0958

AUTHENTICATED MEDICAL DOCUMENTS RELEASING WITH PRIVACY PROTECTION AND RELEASE CONTROL

G.MUTHUKUMAR[1], S.ASWIN[2], S.SANTHOSH KUMAR[2], S.BARATHAN[2]
[1]Assistant Professor, [2]Finalyear Student, Dept. of Computer Science & Engineering
Sriram Engineering College, Chennai – 602024, Tamil Nadu, India.

ABSTRACT

In the context of Information Societies, 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 untrusted 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:

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 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.

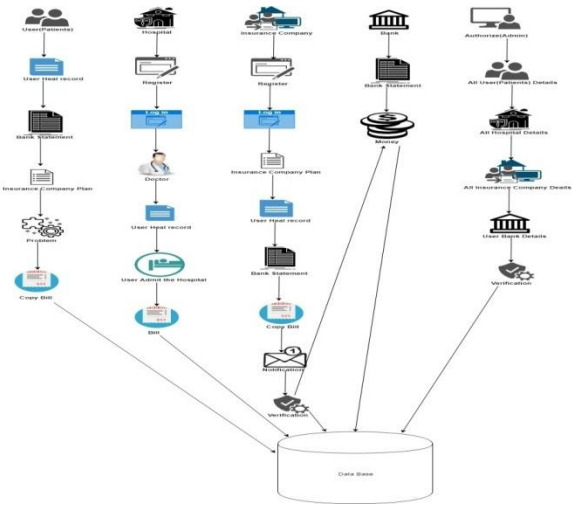
RELATED WORK:

Redactable signature schemes (RSSs) are vulnerable to dishonest redactors or illegal redaction detection. To address the above issues. Over the years, RSSs are also applied in social networks and smart grid 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 This sort of design is efficient in solving the unauthorized redaction and privacy leakage issues in other scenarios of authenticated documents release.

PROPOSED METHODOLOGY:

A new scheme with sanitizing condition control based on bilinear maps as the solution the first authenticated document sanitizing scheme with redaction condition control another authenticated document sanitizing scheme based on bilinear maps. Nonetheless, the computation cost of this scheme is relatively high. security properties in terms of unforgeability, privacy and transparency. The security properties are proved in a reduction mode. two RSSs-FRC as well as their security in unforgeability, privacy and transparency. The correctness of our constructions have been distinctly presented in their respective verification.

ARCHITECTURE:

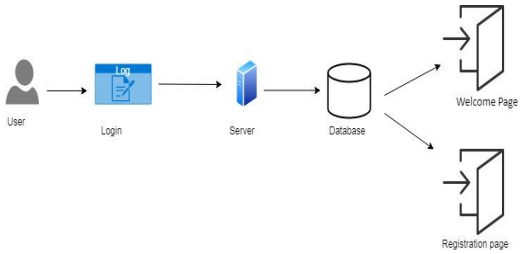


OBJECTIVE MODULES:

- User Interface Design.
- Insurance Company Plan.
- Verification of Bank Statement.
- Users Plan.
- If Emergency Occurs.
- Providing Bill to Insurance Company.
- Verification from Insurance Company.

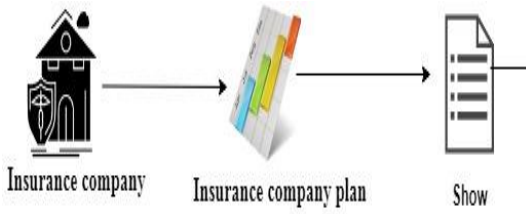
USER INTERFACE DESIGN:

This is the first module of our project. Theimportant 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 check 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. 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 user id and password server also check the authentication of the user. It well improves the security and preventing from unauthorized user enters into the network. In our project we are using JSP for creating design. Here we validate the login user and server authentication.



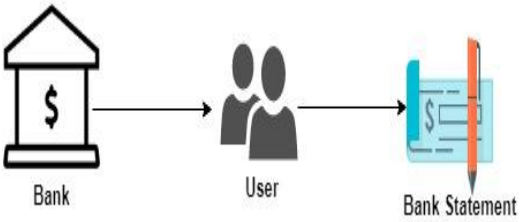
INSURANCE COMPANY PLAN:

Insurance Company Targets On Several Users And Verify Them, Insurance Company Ask Users To Get Insurance From Their Company Through Online.



VERIFICATION OF BANK STATEMENT:

Here insurance company will verify the bank statements of particular user. After checking the statement company will provide a insurance for them.



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.,After That User Will Claim Insurance Here.

IF EMERGENCY OCCURS:

In This Module, If User Is Affected By Some Severe Disease Or An Accident They Will Get A Treatment In Their Specified Hospital And The Bill Will Be Issued By The Hospital After Getting Full Treatment.

PROVIDING BILL TO INSURANCE COMPANY:

After Getting The Treatment,User Will Buy The Bill And Gives The Bill To Insurance Company For Verification And Claiming Process

VERIFICATION FROM INSURANCE COMPANY:

Insurance company will verify the bill provided by the hospital. if it is original means they will claim the amount to the particular user.

CONCLUSION:

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 revealable 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.

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. 23
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.