ISSN: 2321-2152

IJMECE

International Journal of modern electronics and communication engineering

E-Mail
editor.ijmece@gmail.com
editor@ijmece.com

www.ijmece.com

ISSN2321-2152
www.ijmece .com
Vol 12, Issue.1Jan 2024

PUBLICLY VERIFIABLE SHARED DYNAMIC ELECTRONIC HEALTH RECORD DATABASES

Geetha Prathibha[1],M.Saineha[2],M.Sri Laxm[i3] ,P.S. Mani Deepthi[4]

ABSTRACT :

The Electronic Health Record (EHR) system serves as a pivotal tool for collecting and sharing patients' digital health information among healthcare providers through cloud-based infrastructure. Given the substantial and sensitive nature of patient data within the EHR, ensuring both response correctness and storage integrity is imperative. The integration of Internet of Things (IoT) devices into the ecosystem has introduced low-performance terminals for transmitting patient data to the server, adding computational and communication burdens to the EHR systems. To address these challenges, a verifiable database (VDB) model has been proposed, enabling users to outsource large databases to a cloud server and query specific data when needed, particularly catering to resource-constrained users. While existing VDB schemes leverage proof reuse and updating techniques to verify query result correctness, they often overlook the "real-time" aspect of proof generation. This oversight results in an additional overhead, compelling users to perform supplementary processes, such as auditing schemes, to validate storage integrity. This article introduces a novel approach by presenting a publicly verifiable shared updatable EHR database scheme. The proposed scheme not only supports privacy-preserving measures but also facilitates batch integrity checking, minimizing user communication costs. The modification of the existing functional commitment (FC) scheme for VDB design is a key contribution, constructing a concrete FC under the computational l-BDHE assumption. Furthermore, the incorporation of an efficient verifier-local revocation group signature scheme enhances the scheme's capabilities, supporting dynamic group member operations while offering desirable features like traceability and non-frameability. This comprehensive scheme addresses the intricacies of EHR systems, ensuring robust privacy, integrity, and efficiency in a cloud-based healthcare infrastructure.

I. INTRODUCTION

In the realm of healthcare, Electronic Health Record (EHR) systems play a crucial role in digitalizing and sharing patients' health information among various healthcare providers, leveraging cloud-based infrastructure for seamless collaboration. The sensitivity and significance of patient data mandate the need for robust mechanisms ensuring both response correctness and storage integrity within EHR systems. With the proliferation of the Internet of Things (IoT), the integration of low-performance terminals for data transmission to servers introduces computational and

[1]assistant professor, geethaprathibha2023@gmail.com
[2,3,4]UG Students, Department of CSE, Malla Reddy Engineering College, Hyderabad, TS, India.

communication challenges for EHR systems. This project addresses these complexities by proposing a Publicly Verifiable Shared Dynamic Electronic Health Record Databases scheme, aimed at providing efficient, secure, and privacy-preserving storage solutions for resource-constrained users.

II.LITERATURE REVIEW :

Publicly Verifiable Shared Dynamic Electronic Health Record Databases With Functional Commitment Supporting Privacy-Preserving Integrity Auditing,Ye Su; Jiameng Sun; Jing Qin; Jiankun Hu Electronic health record (EHR) is a system that collects patients' digital health information and shares it with other healthcare providers in the cloud. Since EHR contains a large amount of significant and sensitive information about patients, it is required that the system ensures response correctness and storage integrity. Meanwhile, with the rise of IoT, more low-performance terminals are deployed for receiving and uploading patient data to the server, which increases the computational and communication burden of the EHR systems. The verifiable database (VDB), where a user outsources his large database to a cloud server and makes queries once he needs certain data, is proposed as an efficient updatable cloud storage model for resource-constrained users. To improve efficiency, most existing VDB schemes utilize proof reuse and proof updating technique to prove correctness of the query results. However, it ignores the “real-time” of proof generation, which results in an overhead that the user has to perform extra process (e.g., auditing schemes) to check storage integrity. In this article, we propose a publicly verifiable shared updatable EHR database scheme that supports privacy-preserving and batch integrity checking with minimum user communication cost. We modify the existing functional commitment (FC) scheme for the VDB design and construct a concrete FC under the computational l -BDHE assumption. In addition, the use of an efficient verifier-local revocation group signature scheme makes our scheme support dynamic group member operations, and gives nice features, such as traceability and non-frameability.

III.EXISTING SYSTEM

Current EHR systems face challenges in ensuring real-time response correctness and storage integrity, especially with the increasing use of low-performance IoT terminals. While Verifiable Database (VDB) models have been proposed to alleviate some of these challenges, existing schemes often neglect the real-time aspect of proof generation. This oversight results in additional overhead, requiring users to perform supplementary processes, such as auditing schemes, to validate storage integrity. These limitations underscore the need for an improved and dynamic approach to EHR database systems.

IV.PROPOSED SYSTEM

The proposed Publicly Verifiable Shared Dynamic Electronic Health Record Databases scheme addresses the shortcomings of existing systems by introducing a novel approach. This scheme not only supports privacy-preserving measures but also facilitates batch integrity checking, thereby minimizing user communication costs. Key modifications include the adaptation of the Functional Commitment (FC) scheme for VDB

ISSN2321-2152
www.ijmece .com
Vol 12, Issue.1Jan 2024

design, constructing a concrete FC under the computational l-BDHE assumption. Additionally, the scheme incorporates an efficient verifier-local revocation group signature scheme to support dynamic group member operations, providing desirable features like traceability and non-frameability. This innovative approach aims to enhance the efficiency and security of EHR databases, particularly catering to the challenges posed by resource constraints and the dynamic nature of healthcare data.

V. MODULES

Data Collection and Integration:

- Module for collecting patient health records from various sources and integrating them into a unified database.
- Implement data collection mechanisms that adhere to privacy regulations and standards.

Data Preprocessing:

- Module for cleaning and preparing the collected data for storage and analysis.
- Techniques may include data anonymization, de-identification, and handling missing values.

Real-Time Data Processing:

- Module to handle real-time updates and queries efficiently.
- Implement streaming data processing techniques or in-memory databases for instantaneous data analytics.

User Interface (UI):

- Module for designing an intuitive and user-friendly interface for healthcare professionals and administrators.
- Focus on accessibility, ease of navigation, and visualization of relevant health data.

Admin login requires secure credentials, including a username and password, with potential for two-factor authentication.

Admins utilize role-based access control for managing user accounts, overseeing system analytics, and ensuring security measures.

User login involves secure username and password credentials, leading to a patient portal for accessing health records. Privacy measures, notification features, and account management functionalities enhance the user experience while adhering to healthcare regulations.

ISSN2321-2152
www.ijmece .com
Vol 12, Issue.1Jan 2024

Continuous monitoring and user support contribute to a secure and user-friendly Electronic Health Record system.

VI.CONCLUSION

In conclusion, the Publicly Verifiable Shared Dynamic Electronic Health Record Databases project presents a comprehensive solution to the evolving challenges in EHR systems. By addressing the real-time aspects of proof generation, ensuring privacy preservation, and minimizing user communication costs, the proposed scheme offers an advanced and efficient approach to managing healthcare data. The integration of dynamic group member operations, traceability, and non-frameability further enhances the scheme's capabilities, making it a promising advancement in the realm of EHR database systems. This project holds the potential to significantly contribute to the efficiency, security, and adaptability of electronic health record management in contemporary healthcare settings.

VII.REFERENCES :

1. L. Wei, C. Wu and S. Zhou, "efficient verifier-local revocation group signature schemes with backward unlinkability", *Chin. J. Electron.*, vol. e90-a, no. 2, pp. 379-384, 2009.
2. B. Dan and H. Shacham, "Group signatures with verifier-local revocation", *Proc. ACM Conf. Comput. Commun. Secur.*, pp. 168-177, 2004.
3. C. David and T. P. Pedersen, "Wallet databases with observers", *Proc. Int. Cryptol. Conf. Adv. Cryptol.*, pp. 89-105, 1992.
4. B. Dan, X. Boyen and E. J. Goh, "Hierarchical identity based encryption with constant size ciphertext", *Proc. Int. Conf. Theory Appl. Cryptographic Techn.*, pp. 440-456, 2005.
5. A. Kate, G. M. Zaverucha and I. Goldberg, "Constant-size commitments to polynomials and their applications", *Proc. Adv. Cryptol. - ASIACRYPT 2010 Int. Conf. Theory Appl. Cryptol. Inf. Secur. Proc.. DBLP*, pp. 177-194, 2010.
6. J. Hu, H. H. Chen and T. W. Hou, "A hybrid public key infrastructure solution (HPKI) for HIPAA privacy/security regulations", *Comput. Standards Interfaces*, vol. 32, no. 5–6, pp. 274-280, 2010.
7. S. Benabbas, R. Gennaro and Y. Vahlis, "Verifiable delegation of computation over large datasets" in Proc. Conf. Adv. Cryptol., pp. 111-131, 2011.
8. D. Catalano and D. fiore, "vector commitments and their applications" in Public-Key Cryptography – PKC 2013, Berlin, Germany:Springer, pp. 55-72, 2013.
9. X. Chen, J. Li, X. Huang, J. Ma and W. Lou, "New publicly verifiable

databases with efficient updates", *IEEE Trans. Depend. Secure Comput.*, vol. 12, no. 5, pp. 546-556, Sep./Oct. 2015.
10.X. Chen et al., "Verifiable computation over large database with incremental updates", *Proc. Eur. Symp. Res. Comput. Secur.*, pp. 148-162, 2014.
11.M. Miao et al., "Publicly verifiable databases with efficient insertion/deletion operations", *J. Comput. Syst. Sci.*, vol. 86, pp. 49-58, 2017.
12.T. Jiang, X. Chen and J. Ma, "Public integrity auditing for shared dynamic cloud data with group user revocation", *IEEE Trans. Comput.*, vol. 65, no. 8, pp. 2363-2373, Aug. 2016.
13.B. Libert, S. C. Ramanna and M. Yung, "Functional commitment schemes: From polynomial commitments to pairing-based accumulators from simple assumptions (full version)", *Proc. ICALP*, vol. 50, pp. 30:1-30:14, 2016.
14.Y. Zhan et al., "HealthDep: An efficient and secure deduplication scheme for cloud-assisted ehealth systems", *IEEE Trans. Ind. Inf.*, vol. 14, no. 9, pp. 4101-4112, Sep. 2018.
15.X. Yao, Y. Lin, Q. Liu and J. Zhang, "Privacy-preserving search over encrypted personal health record in multi-source cloud", *IEEE Access*, vol. 6, pp. 3809-3823, 2018.
16.S. Roy, A. K. Das, S. Chatterjee, N. Kumar, S. Chattopadhyay and J. J. P. C. Rodrigues, "Provably secure fine-grained data access control over multiple cloud servers in mobile cloud computing based healthcare applications", *IEEE Trans. Ind. Informat.*, vol. 15, no. 1, pp. 457-468, Jan. 2019.
17.K. Belyaev et al., "On the design and analysis of protocols for personal health record storage on personal data server devices", *Future Gener. Comput. Syst.*, vol. 80, pp. 467-482, 2018.
18.G. Ateniese et al., "Provable data possession at untrusted stores", *Proc. 14th ACM Conf. Comput. Commun. Secur.*, pp. 598-609, 2007.
19.T. T. Tomson and R. Passman, "The reveal LINQ insertable cardiac monitor", *Expert Rev. Med. Devices*, vol. 12, no. 1, pp. 7-18, 2015.
20.J. Sun, B. Zhu, J. Qin, J. Hu and Q. Wu, "Confidentiality-preserving publicly verifiable computation", *Int. J. Found. Comput. Sci.*, vol. 28, no. 6, pp. 799-818, 2018.
21.H. Shacham and B. Waters, "Compact proofs of retrievability", *J. Cryptol.*, vol. 26, no. 3, pp. 442-483, 2013.
22.S. Li et al., "Public auditing with privacy protection in a multi-user model of cloud-assisted body sensor networks", *Sensors*, vol. 17, no. 5, 2017.
23.M. Sookhak, R. Yu and A. Zomaya, "Auditing big data storage in cloud computing using divide and conquer tables", *IEEE Trans. Parallel Distrib. Syst.*, vol. 29, no. 5, pp. 999-1012, May 2018.
24.W. Shen, J. Yu, H. Xia, H. Zhang, X. Lu and R. Hao, "Light-weight and privacy-preserving secure cloud auditing scheme for group users via the third party medium", *J. Netw. Comput. Appl.*, vol. 82, pp. 56-64, 2017.
25.J. Yuan and S. Yu, "Efficient public integrity checking for cloud data sharing with multi-user modification", *Proc. IEEE Conf. Comput. Commun.*, pp. 2121-2129, 2014.