IARJSET

ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 11, Issue 7, July 2024

DOI: 10.17148/IARJSET.2024.11754

Openly Verifiable Shared Dynamic Medical Records with Privacy-Preserving Integrity Checks

Chethan K[1], Dr. T Vijaya Kumar[2]

Student, Department of MCA, Bangalore Institute of Technology, Karnataka, India[1]

Professor & Head, Department of MCA, Bangalore Institute of Technology, Karnataka, India[2]

Abstract: Electronic Health Record EHR might be a system that gathers digital health information from patients and exchanges it via the cloud with other providers of healthcare services. Given that EHRs include a large amount of sensitive and important patient data, the framework must ensure accuracy and capacity in responses and astuteness . In interim , because of the rise of IoT, more low performance terminals are sent for accepting and uploading quiet info to the server, which increments the computational and communication burden of the EHR frameworks . The unquestionable database VDB , where a client outsources his huge database to a cloud server and queries it whenever he wants certain data; this is suggested as a useful updatable cloud capacity demonstrate for resource constrained clients . To move forward productivity, the majority of current VDB designs use verification upgrade and reuse strategies to show that the question is correct. It ignores the real-time proof era, resulting in an overhead where the customer must carry out extra preparation work, such as reviewing blueprints to verify capacity judgement. We provide a freely verifiable shared updatable EHR database plot in this work that supports privacy-preserving and bunch judgment checking with least client communication fetched . We adjust the existing utilitarian commitment FC plot for the VDB plan and develop a concrete FC beneath the computational l BDHE suspicion . In expansion , the utilize of an productive verifier local denial bunch signature plot makes our conspire back energetic bunch part operations, and gives pleasant highlights , such as traceability and non frameability.

Key Words: VDB, FC, EHR FRAMEWORK

I. INTRODUCTION

In the rapidly evolving landscape of healthcare, Nowadays, electronic health records, or EHRs, are essential for gathering, storing, and exchanging patient digital health data across different healthcare providers. EHR system adoption is fueled by the need for seamless information flow, which enhances the quality of care, improves patient outcomes, and streamlines administrative processes. However, the sensitive nature of the data contained within EHRs necessitates stringent measures to ensure the correctness of responses and the integrity of storage. As healthcare data grows exponentially, so do the challenges associated with managing it, particularly with the integration of Internet of Things (IoT) devices that often come with limited computational and communication capabilities.

The introduction of IoT into healthcare brings a plethora of low-performance terminals tasked with collecting and uploading patient data to central servers. This influx of data intensifies the computational and communication demands on EHR systems, highlighting the need for scalable and efficient data management solutions. To address these challenges, the concept of an undeniable database (VDB) has been proposed, where users can outsource large databases to a cloud server and retrieve information as needed. VDBs offer a promising model for resource-constrained environments by leveraging verification reuse and enhanced authentication techniques to ensure the correctness of query results. However, existing VDB schemes often overlook the real-time aspects of proof generation, imposing additional burdens on users who must perform extra processes, such as scheme verification, to ensure storage correctness.

II. LITERATURE SURVEY

Dynamic collaborative databases of Health Records accessible by the public are revolutionizing healthcare by enhancing the accessibility and management of patient data. These systems must balance the dual imperatives of data integrity and patient privacy. This literature survey examines existing methodologies and technologies that ensure the integrity and privacy of public EHR databases, focusing on functionally committed systems supporting integrity audits. Key areas reviewed include cryptographic techniques, blockchain applications, functional commitment schemes, and verifier-local revocation group signature schemes. The survey identifies the strengths and limitations of these approaches, emphasizing their role in maintaining data accuracy while protecting sensitive information. By evaluating recent advancements and pinpointing areas needing further research, this survey aims to provide a detailed understanding of current solutions and make recommendations for future paths to enhance the security and reliability of public EHR databases.

This study explores a range of cryptographic techniques designed to secure Electronic Health Records (EHRs) while maintaining accessibility for authorized users. The paper discusses symmetric and asymmetric encryption methods, digital signatures, and advanced cryptographic protocols such as homomorphic encryption and zero- knowledge proofs. Homomorphic encryption allows privacy-preserving calculations on encrypted data without decryption data processing. Zero- knowledge proofs enable verification of data integrity without revealing the data itself. The research highlights the benefits of these techniques in ensuring data integrity and confidentiality, particularly in publicly accessible EHR systems. It also addresses the computational challenges and performance trade-offs associated with implementing robust cryptographic solutions. The authors suggest that combining these cryptographic methods can create a secure framework for EHRs, supporting integrity audits and maintaining patient privacy. Among the objectives for further study is enhancing these techniques for real- time processing and exploring their integration with other security measures.

This paper investigates the application of blockchain technology to manage Electronic Health Records (EHRs) securely and transparently. Blockchain's decentralized nature and immutable ledger make it an ideal solution for ensuring the integrity and traceability of medical data. The study reviews various blockchain architectures, including public, private, and consortium blockchains, and their suitability for EHR systems. Smart contracts are highlighted as a mechanism to automate data access controls and integrity audits. The paper also discusses the scalability challenges of blockchain systems and potential solutions such as sharding and off-chain storage. The writers provide case examples that show successful implementations of blockchain in healthcare, showcasing improved data integrity, patient consent management, and interoperability across different healthcare providers. The research concludes that while blockchain offers significant advantages for EHR management, issues such as regulatory compliance, integration with existing systems, and scalability need further exploration. Potential work should focus on developing hybrid blockchain models that balance security and performance for large-scale EHR deployment.

This study delves into functional commitment (FC) schemes as a method to ensure the integrity and verifiability of Electronic Health Records (EHRs) in dynamic databases. FC schemes allow the commitment of a function's input and output, enabling verifiable data audits without revealing the actual data. The paper examines the application of FC in public EHR systems, emphasizing its role in maintaining data integrity while preserving patient privacy. Various cryptographic constructs, including bilinear pairings and computational Diffie-Hellman assumptions, are discussed as foundations for FC schemes. The authors highlight the efficiency of FC in supporting real-time integrity audits, reducing the computational burden on resource-constrained devices such as IoT terminals. Case studies of FC implementation in healthcare demonstrate its potential to enhance data security and trustworthiness. However, challenges such as key management, scalability, and the complication of cryptographic operations are noted. The paper suggests future research should aim at optimizing FC schemes for practical deployment and integrating them with other cryptographic protocols to bolster EHR system security comprehensively.

This paper explores verifier-local revocation (VLR) group signature schemes to enhance seclusion and safety in publicly accessible Electronic Health Record (EHR) systems. VLR group signatures allow users to sign data anonymously while enabling verifiers to revoke malicious users without updating public keys. The study reviews the cryptographic foundations of VLR schemes, such as bilinear pairings and the computational Diffie-Hellman assumption. The authors demonstrate how VLR group signatures can support dynamic group member operations, including adding and revoking users, while maintaining system integrity and user privacy. The paper highlights the applicability of VLR schemes in EHR methods to guarantee that access is restricted to authorised parties modify records, thus supporting privacy-preserving integrity audits. Case studies indicate that VLR group signatures effectively balance security and efficiency, providing robust protection against Unlicensed entry and breaches of data. Among the objectives for further study is optimising VLR schemes for large-scale EHR systems and integrating them with other security protocols to enhance overall system resilience.

This paper examines the incorporation of Internet of Things (IoT) devices with Electronic HealthRecord (EHR) systems to facilitate real-time data collection and processing. The study addresses the challenges of ensuring data integrity, privacy, and security in such an interconnected environment. IoT devices, often resource- constrained, pose significant challenges with respect to computational and communication capabilities. The paper reviews various security protocols, including lightweight cryptography and mechanisms for secure communication that are intended to safeguard privacy and data integrity in IoT-integrated EHR systems. The writers also go over using edge computing and fog computing to offload processing tasks from central servers, enhancing the system's scalability and efficiency. Case studies of IoT- EHR

DOI: 10.17148/IARJSET.2024.11754

integration highlight the benefits of real-time health monitoring, improved patient outcomes, and more efficient healthcare delivery. However, the research underscores strong security measures are required to shield private patient information from cyber threats. Future research should focus on developing comprehensive security frameworks that combine cryptographic techniques, access control mechanisms, and real-time auditing capabilities to safeguard IoT-integrated EHR systems.

III. EXISTING MODEL

Benabbas et al. proposed the unquestionable database VDB as a secure and effective updatable cloud capacity show for resource limited clients. In a VDB plot, a client can outsource the capacity of a collection of information things to an untrusted server. Afterward, the client can inquiry the server for an thing a message at position i, the server returns the put away message at this position in conjunction with a verification that it is the right reply. Nevertheless, the safety of as it were verifying the server reaction rightness is far from sufficient for the EHR framework, it's unclear if adequately stored information that is not regularly accessed is still kept. In the unlikely event that this knowledge is devastated and not found in time, it can cause colossal misfortunes within the occasion of an emergency.

Jiang et al.'s plot proposed to utilize vector commitment conspire to develop the review plot. Although the reduction of labels has been accomplished, their scheme fails to attain the anticipated security due to the disregard of the genuine time execution of verification era. There is still no great way to play down the communication for moo execution users.

- **DISADVANTAGES OF EXISTING SYSTEM**

The essential issue confronted by the EHR framework is on how to confirm that the server reactions accurately each time.
The existing VLR bunch signature conspire does not have in reverse unlikability BU, which suggests that in fact, in the unlikely event that a part is repudiated at a certain time, the signature some time recently that time remains mysterious. It postures a danger to client personality privacy.

In the existing system, due to the reality that their programme did not consider a idea of real time verification, the utilize of these methods makes their review plot and other VDB plans incapable of checking capacity astuteness. In this case, as it where the questioned information is included within the confirmation prepare. This leads to confirmation, so to speak, of the data being questioned, whereas capacity judgment of other cloud information is not checked. On the off chance that the cloud information which is not questioned is harmed, it will not be recognized in time. When the harmed information is required, there resolve be shifting degrees of loss.

3. PROPOSED MODEL

Our inquire about centers on the security and effectiveness of huge database capacity, such as EHR. Concurring to the characteristics of EHR framework, two perspectives of security merit our consideration, to be specific, the server reaction rightness and the data capacity astuteness. In arrange to bargain with over issues, we utilize a modern device called useful commitment FC and plan a freely unquestionable updatable database conspire based on utilitarian commitment supporting privacy preserving keenness inspecting and energetic gather operation.

We adjust the existing useful commitment plot in arrange to operate the work official of useful commitment to plan an auditable VDB conspire. We point out security issues with existing plot and propose a freely unquestionable updatable VDB conspire based on the utilitarian commitment and gather signature without bringing about as well much computational overhead and capacity taken a toll. In addition, our plot is appropriate for large scale information capacity with least client communication fetched.

Our proposed conspire not as it remained jam all the properties of the initial VDB plot, but moreover actualizes productive privacy preserving astuteness reviewing, non frameability and traceability.

- **ADVANTAGES OF PROPOSED SYSTEM**

The plot jam information protection from the evaluator by employing a arbitrary concealing procedure and the meagre vector is utilized for testing inspecting.

Our plot underpins energetic bunch part operations which incorporate connect and denial. In expansion, our VDB bolsters group inspecting and it bolsters multi cloud server, multiuser and multi storage vector scenarios.

Security investigation and experimental comparison with existing plans are given and it appears that our VDB is secure and efficient.

Our VDB plot can safely and efficiently query, and renew database stored contained by the cloud and freely review information capacity judgment.

IV. SYSTEM ARCHITECTURE

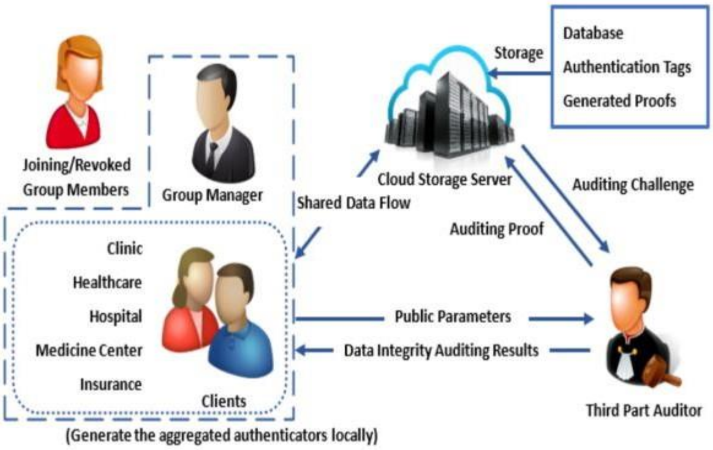

Fig1 system architecture

V. MODULE DESCRIPTION

- **Member**

The part, counting patients, clinic, clinic, pharmaceutical centre, protections, etc., can outsource huge databanks to the server. Not at all like most inspecting plans, the client produces the amassed confirmation labels transfers them to the cloud locally. At that moment, the customer has the option to inquire, update the database, and assess the accuracy of the information. Any group member may upload their own databases to the cloud and share them with other group members in our dynamic group sharing scenario. Additionally, a dependable group manager is careful while accepting or rejecting a customer. Within the part module, we create the module, such that when the part logged into, at that point the part has the choices of Transfer record My records Review confirmation Get to Record Asked record Download record and Take off Bunch functionalities.

- **Group Manager**

In this module, we create the Gather Chief. Gather Supervisor is like an admin of the framework. Once after logged into the framework, the Gather Chief has the choices of seeing the Individuals subtle elements and access Repudiated Clients. Within the Part points of interest, the Bunch Chief can see the points of interest of a particular member is dynamic state or take off state additionally the Gather Chief can able to deny the specific

part. Within the Revoked users portion, the bunch director can able to see the list of disavowed clients additionally the gather supervisor has the get to of actuating the specific part once more. The bunch chief could be a effective substance. It can be seen as an chairman of the gather. When a client clears out the bunch, the director is in charge of repudiating this user. The denied client cannot transfer data to the cloud any more.

- **TPA**

Third Party Inspector which can be anybody within the framework, checks the information capacity astuteness of client outsourced database. The TPA can use open key in order to verify the information capacity astuteness of the often-updated database. an effective way. Within the TPA module, it has the options of Examining Ask and Inspecting Points of interest. The TPA is capable for inspecting the keenness of cloud information on sake of gather clients. When the TPA needs to review the information judgment, it will send an examining challenge to the clouds. After receiving the examining challenge, the cloud will react to the TPA with a verification of information ownership. At last, the TPA will

IARJSET

ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 11, Issue 7, July 2024

DOI: 10.17148/IARJSET.2024.11754

confirm the information judgment by checking the rightness of the verification. TPA might be capable party and it is honest.

- **Cloud**

The cloud capacity server gives inaccessible information capacity administrations for the clientcustomer. The cloud gives colossal capacity space and computing assets for gather clients. Through the cloud capacity, gather clients can appreciate the information sharing benefit. Cloud Server gives a open stage for data proprietors to store and share their scrambled information. The cloud supplier does not conduct information get to control for proprietors. The scrambled data can be downloaded unreservedly by any information clients. We have utilized DriveHQ cloud benefit supplier for the capacity of records in the cloud portion. multi-storage vector scenarios. It makes the auditing process more efficient. Furthermore, we prove that our functional commitment scheme with updates and VDB scheme can achieve the required security properties. The performance of our scheme is more efficient compared with other different algorithms.

VI. RESULT

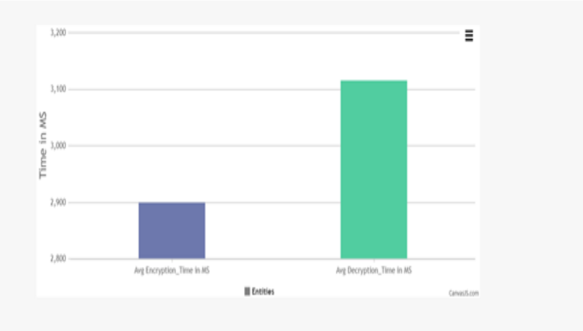

Fig 2. Graph

The concept of irrefutable database could be a awesome device for unquestionable EHR capacity. In any case, verification reclaim and the method of verification overhauling by the server to make strides framework productivity falls flat to realize information astuteness checking. In this work, we provide a new VDB graphic that is updatable, based on the utilitarian commitment that bolsters privacy preserving judgment reviewing and bunch part operations, counting connect and denial. Two security prerequisites of HER are actualized the server response rightness and the information capacity astuteness. Our VDB conspire accomplishes the specified security objectives without causing as well much computational increment.

VII. CONCLUSION

For verified EHR storage, the idea of a verifiable databases is a very useful tool. However, data integrity verification is not achieved via proof reuse or the server-updated proof approach, which is intended to increase system performance. In this work, we offer a unique updatable VDB method that allows group member activities, such as join and revocation, and privacy-preserving integrity audits based on the functional commitment.The server response accuracy and the data storage integrity are the two security criteria of HER that are put into practice. Our VDB approach avoids excessive computational overhead while achieving the intended security objectives. Furthermore, our VDB method offers the terminal with restricted performance the lowest possible connection cost. To create a functional commitment scheme that applies to our program, two algorithms are added to make the FC scheme updatable. A practical improved concrete VDB scheme under computational l −BDHE assumption is presented. In addition, batch auditing for our VDB scheme supports multi-cloud server, multi-user and multi-storage vector scenarios. It makes the auditing process more efficient. Furthermore, we prove that our functional commitment scheme with updates and VDB scheme can achieve the required security properties. The performance of our scheme is more efficient compared with other different algorithms

REFERENCES

[1]. Wei L, Wu C, Zhou S. efficient verifier-local revocation group signature schemes with backward unlinkability. Chinese Journal of Electronics, 2009, e90- a(2):379-384.

[2]. Dan B, Shacham H. Group signatures with verifier- local revocation. Acm Conference on Computer & Communications Security. 2004.

[3]. Chaum, David, and T. P. Pedersen. Wallet Databases with Observers. International Cryptology Conference on Advances in Cryptology 1992.

DOI: 10.17148/IARJSET.2024.11754

[4]. B. Dan, X. Boyen, E. J. Goh, “Hierarchical identity based encryption with constant size ciphertext”, International Conference on Theory and Applications of Cryptographic Techniques. Springer-Verlag, pp. 440- 456, 2005.

[5]. A. Kate, G. M. Zaverucha, I. Goldberg, “Constant-Size Commitments to Polynomials and Their Applications”, Advances in Cryptology - ASIACRYPT 2010 -, International Conference on the Theory and Application of Cryptology and Information Security, Singapore, December 5-9, 2010. Proceedings. DBLP, pp. 177-194,2010.

[6]. B. Libert, S. C. Ramanna and M. Yung. Functional Commitment Schemes: From Polynomial Commitments to Pairing-Based Accumulators from Simple Assumptions (Full Version). In ICALP 2016, to ap-pear, 2016.

[7]. J. Hu, H.H. Chen, T.W. Hou, "A hybrid public key infrastructure solution (HPKI) for HIPAA privacy/security regulations", Computer Standards & Interfaces vol. 32, No. 5-6, pp. 274-280, 2010.

[8]. S. Benabbas, R. Gennaro, Y. Vahlis, “Verifiable Delegation of Computation over Large Datasets”, Conference on Advances in Cryptology. Springer-Verlag,pp. 111-131, 2011

[9]. D. Catalano, D. Fiore. “Vector Commitments and Their Applications”, Public-Key Cryptography – PKC 2013. Springer Berlin Heidelberg, pp. 55-72, 2013.

[10]. X. Chen, J. Li, X. Huang, et al. “New Publicly Verifiable Databases with Efficient Updates”. IEEE Operations on Dependable & Secure Computing, vol. 12, no.5, pp. 546-556, 2015.

[11]. T. Jiang, X. Chen, J. Ma. “Public Integrity Auditing for Shared Dynamic Cloud Data with Group User Revocation”, IEEE Transactions on Computers, vol. 65, no. 8, pp. 2363-2373, 2016.