International Journal of Multidisciplinary Research and Growth Evaluation.

Privacy-preserving integrity auditing on electronic health records using elliptic curve cryptography

Abinaya D [1*], Mubena M [2], Swetha S [3], K Rajammal [4]
[1-4] Computer Science and Engineering, EGS Pillay Engineering College, Nagapattinam, Tamil Nadu, India

* Corresponding Author: **Abinaya D**

Article Info

ISSN (online): 2582-7138
Volume: 04
Issue: 03
May-June 2023
Received: 26-03-2023;
Accepted: 19-04-2023
Page No: 62-67

Abstract
Electronic health records possess the patient's medication details and health history. To secure health records using a distributed and decentralized ledger called Blockchain. Blockchain is an append-only list of sets of cryptographically signed records or transactions called blocks that a number of parties want to update. Provide Different Identity-based authentication for medical data access. Implement ECC (Elliptic Curve Cryptography) algorithm to provide security parameters to encrypt the data before it a store on the cloud. Blockchain technology can be used in many different areas of the healthcare system. Provides efficient access control policy based on user's different identity and also implements secure encryption using ECC encryption algorithm. The proposed Access Control with Encryption model efficiently performs user revocation and decryption operations. Access control is a fundamental component of security compliance programs that ensures security technology and access control policies are in place to protect confidential information, such as customer data. The owner can set different access policies based on the data user's role. Uploaded data are encrypted using the ECC encryption algorithm. Encrypted data are stored based on blockchain technology. File access keys will be shared with specific data users based on their role-based access permission. Time control implements to verify the access pattern of the data user. Implement a secure user revocation process with a key update system. Modify the existing functional commitment (FC) scheme for the VDB design and construct a concrete FC under the computational BDHE assumption. In addition, the use of an efficient verifier-local revocation (VLR) group signature scheme makes our scheme support dynamic group member operations and gives nice features, such as traceability and non-flammability.

Keywords: verifiable database, cloud storage, functional commitment, blockchain, user revocation

1. Introduction
Electronic health record (EHR) is a system that collects patients' digital health information and shares it with other healthcare providers in the cloud. The cloud service industry has been developing unprecedentedly. Many cloud service providers are rushing to launch cloud service platforms and products, such as Amazon, GOOGLE, Alibaba, Microsoft, Huawei, etc. People start to outsource their large data storage tasks to cloud service providers (CSPs). It makes them no longer constrained by limited local storage and computing resources. As a concrete and high-quality application example of cloud storage, the cloud-based electronic health record (EHR), which is a system that collects the patients' digital health information, is being vigorously promoted by many organizations, such as the Office of the National Coordinator for Health Information Technology (ONC) [1] in the United States and Canada Health Info way [2]. The patient EHRs are written on the workstation or mobile device and can be accessed and modified later. The patient EHRs uploaded to the cloud can be shared among different medical institutions to help patients get better treatment, help scientific researchers to carry out disease analysis and research, and help public health departments predict, detect, and potentially prevent the outbreak of epidemic diseases, etc.

Since the cloud service provider (CSP) is an independent management entity, users actually give up ultimate control over their EHRs. This brings security challenges for outsourcing tasks. For example, the cloud servers may return incorrect results for various reasons, such as malfunctioning cloud equipment and a hacker's attack. The incorrect returned values can have serious consequences for every part of the medical system. Therefore, the primary problem faced by the EHR system is how to verify that the server responds correctly each time.

Benabbas *et al*. [3]. Proposed the verifiable database (VDB) as a secure and efficient updatable cloud storage model for resource-limited users. In a VDB scheme, a client can outsource the storage of a collection of data items to an untrusted server. Later, the client can query the server for an item (a message) at position I, and the server returns the stored message at this position along with proof that it is the correct answer. However, the security of only verifying the server response correctness is far from enough for the EHR system, and it is not clear whether data that is not frequently accessed is still stored correctly. If these data are destroyed and not discovered in time, it can cause huge losses in the event of an emergency.

Many audit schemes [4, 5, 6, 13, 14, 15] exist to check the data storage integrity. A simple idea to realize the server response correctness and the data storage integrity of the EHR system is to use the VDB scheme and an audit scheme respectively. But there will be a lot of authentication tags generated and transmitted for verification At present, with the development of the Internet of things, emerging wearable devices are also deployed for receiving and uploading users' EHR information. For example, a smartwatch can upload information about a user's heartbeat and breathing, and an insertable cardiac monitor called Reveal LINQ [12] provides long-term heart monitoring. Similarly, mobile terminals with limited performance are used in such applications.

The biggest feature of the EHR system is that patients' health information is shared in a group, including clinics, healthcare, hospital, medicine center, insurance, and so on. Anyone in the group can upload, download, and modify the database. In most cases, the members in such groups are not fixed. And a group manager (GM) is appointed to control members' joining or quitting. The scheme [15] provided an efficient audit scheme for group members to share cloud data, but only GM can upload the database. Jiang *et al*. [17] scheme involved the dynamic problem of group members, but their scheme can only realize the revocation, and the case of users joining the group is not considered. They used the group signature scheme with verifier-local revocation (VLR)

[13] Proposed by Boneh *et al*. to make group members revocable. However, their VLR group signature scheme does not have backward unlinkability (BU), which means that even if a member is revoked at a certain time, the signature before that time remains anonymous. It poses a threat to user identity privacy.

2. Related Works

Zhang, Cheng, Yang Xu, Yupeng Hu, *et al* [7] proposed a scheme that can handle multiple security threats. Network storage services have benefited countless users worldwide due to the notable features of convenience, economy, and high availability. Since a single service provider is not always reliable enough, more complex multi-cloud storage systems are developed for mitigating the data corruption risk. While a data auditing scheme is still needed in multi-cloud storage to help users confirm the integrity of their outsourced data. Unfortunately, most of the corresponding schemes rely on trusted institutions such as the centralized third-party auditor (TPA) and the cloud service organizer, and it is difficult to identify malicious service providers after service disputes. Therefore, I present a blockchain-based multi-cloud storage data auditing scheme to protect data integrity and accurately arbitrate service disputes. I'm not only introducing the blockchain to record the interactions among users, service providers, and organizers in the data auditing process as evidence but also employing the smart contract to detect service disputes, so as to enforce the untrusted organizer to honestly identify malicious service providers. I also use the blockchain network and homomorphic verifiable tags to achieve low-cost batch verification without TPA. Theoretical analyses and experiments reveal that the scheme is effective in multi-cloud environments and the cost is acceptable.

Rajput, Ahmed Raza, Qianmu Li, and Milad Taleby Ahvanooey, *et al* [8] assures the secret data sharing of the PHR by considering the immutability, auditing, and emergency access control policies. Blockchain technology is the most trusted all-in-one cryptosystem that provides a framework for securing transactions over networks due to its irreversibility and immutability characteristics. Blockchain network, as a decentralized infrastructure, has drawn the attention of various startups, administrators, and developers.

This system preserves transactions from tampering and provides a tracking tool for tracing past network operations. A personal health record (PHR) system permits patients to control and share data concerning their health conditions with particular people. In the case of an emergency, the patient is unable to approve the emergency staff access to the PHR. Furthermore, a history record management system of the patient's PHR is required, which exhibits hugely private personal data (e.g., modification date, name of the user, last health condition, etc.). In this, I suggest a healthcare management framework that employs blockchain technology to provide a tamper protection application by considering safe policies. These policies involve identifying extensible access control, auditing, and tamper resistance in an emergency scenario. Our experiments demonstrated that the proposed framework affords superior performance compared to state-of-the-art healthcare systems concerning accessibility, privacy, emergency access control, and data auditing.

Li, Jiaxing, Jigang Wu, Guiyuan Jiang, Thambipillai Srikanthan *et al* [9] To reduce the overhead of computation and communication for integrity verification. In the proposed scheme, different from the existing works that involve three participatory entities, only two predefined entities (i.e. data owner and cloud service provider) who may not trust each other are involved, and the third-party auditor for data auditing is removed. Security analysis shows that the proposed scheme can defend against malicious entities and the 51% attack. Data integrity verification becomes an essential part of the security strategy of cloud storage, as it enables cloud users to check the integrity of their outsourced data efficiently.

Shen, Jian, Huijie Yang, Pandi Vijayakumar, and Neeraj Kumar *et al* [10] It prevents malicious user collusion with other users. By employing the proxy re-encryption algorithm and oblivious random-access memory (ORAM), a privacy-preserving and untraceable scheme is proposed to support

multiple users in sharing data in cloud computing. On the one hand, group members and a proxy use the key exchange phase to obtain keys and resist multiparty collusion if necessary. The ciphertext obtained according to the proxy re-encryption phase enables group members to implement access control and store data, thereby completing secure data sharing. On the other hand, this article realizes data untraceability and a hidden data access pattern through a one-way circular linked table in a binary tree (OCLT) and obfuscation operation. Additionally, based on the designed structure and pointer tuple, malicious users are identified and data tampering is prevented. The security analysis shows that the protocol designed in this article can meet the security requirements of proxy re-encryption and ORAM. Both theoretical and experimental analyses demonstrate that the proposed scheme is secure and efficient for group data sharing in cloud computing.

Shen, Jian, Jun Shen, Xiaofeng Chen, Xinyi Huang, *et al* [11] Proposed protocol performs better both in terms of efficient dynamic support and reduced overhead. Proposed an efficient public auditing protocol with global and sampling block less verification as well as batch auditing, where data dynamics are substantially more efficiently supported than is the case with the state of the art. Note that, the novel dynamic structure in our protocol consists of a doubly linked info table and a location array. Moreover, with such a structure, computational and communication overheads can be reduced substantially. Security analysis indicates that our protocol can achieve the desired properties. Moreover, numerical analysis and real-world experimental results demonstrate that the proposed protocol achieves a given efficiency in practice.

3. Working Methodology

Blockchain is majorly used to perform cryptocurrency transactions securely. Blockchain is used in healthcare to secure the healthcare information of patients. The healthcare information includes EHR, insurance details of the patient, research information of biomedical, drug supply chain info, and medical education

One of the most important problems in using a group signature scheme in practice is group member revocation. Boneh *et al*. [13] introduced the verifier-local revocation group signature scheme. In their scheme, the method of revocation is to send the information about the revoked members to the signature verifier. When the verifier checks the signature, he/she checks whether or not the signer of the signature has been revoked. However, their VLR group signature scheme does not have backward unlinkability. Another important property of group signatures is non- flammability, which is to make sure no one, including the group manager, can sign a message on behalf of other group members. Then, an efficient verifier-local signature scheme with these properties is constructed in [1]. As shown in fig1.

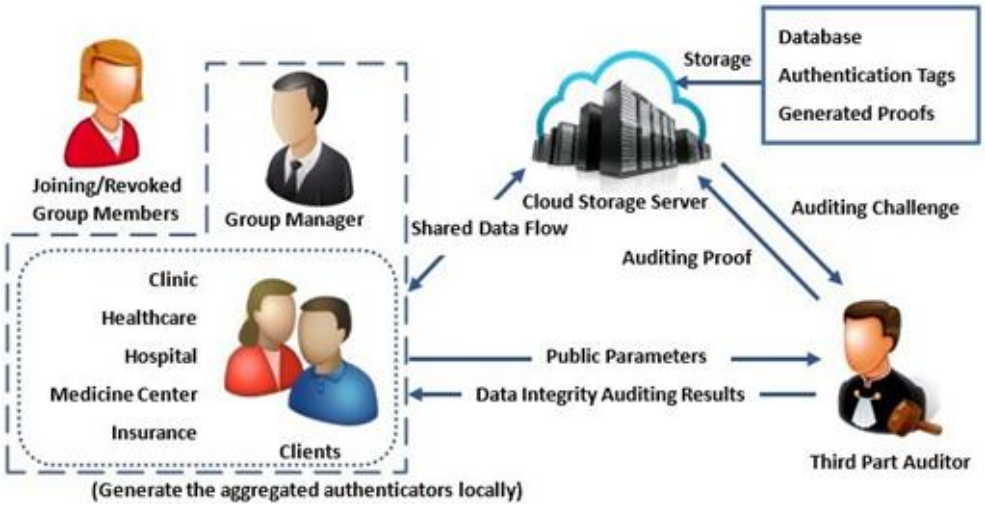

Fig 1: Outline of proposed system

Similar to ordinary digital signatures, a group signature means anyone can verify the correctness of a group signature. The difference is that after verifying the group signature, the verifier can only confirm that the message is signed and issued by a member of a group, but it does not know who signed and issued it, which protects the anonymity of the signer. When a dispute arises, there is a trusted group manager (GM) who can identify the member who actually signs the message.

Like the VC scheme, the FC scheme allows a vector to be committed to generating a commitment value. After that, the commitment value happened as a specified linear reaction in an FC. They provided a concrete FC scheme for linear combinations under subgroup decision assumption. Their scheme satisfies two properties, called perfectly hiding and computational binding. However, in order to design the scheme under well-studied assumptions, their construction uses Composite order bilinear groups, which have a number of parameters and are less efficient. And the scheme does not focus on the update algorithm.

4. Implementation

A. Functional Commitment Algorithm

A functional commitment scheme enables a user to concisely commit to a function from a specified family, then later concisely and verifiably reveal values of the function at desired inputs. Useful special cases, which have seen applications across cryptography, include vector commitments and polynomial commitments. The FC scheme allows a vector to be committed to generating a commitment value. After that, the commitment value is opened as a specified linear function, for public coefficients. They provided a concrete FC for linear combinations under subgroup decision assumption in composite order bilinear groups. Their FC

satisfies two properties which are perfectly hiding and function binding. Meanwhile, the functional commitment is concise. However, the scheme has more parameters and is less efficient. In this section, for the design of the VDB scheme, two algorithms for updating are added based on the original FC scheme in [18]. And a modified concrete FC with updates under the computational l −BDHE assumption is presented.

Definition of FCs for Linear Functions with Updates

In this section, I present a concrete FC for linear functions with updates under computational l −BDHE assumption.

i. FC. Setup

$$TK := g_{n+1} = h^{\alpha^{n+1}} \quad (1)$$

ii. FC.Com

$$\vec{m} = (m_1, m_2, \ldots, m_n) \in Z_q^n \quad (2)$$

iii. FC. Open

$$P_i = g_{n-i+1}^{\gamma} \cdot \prod_{j=1, j\neq i}^{n} g_{n+1+j-i}^{m_j}, \quad \forall i \in \{1, \ldots, n\} \quad (3)$$

iv. FC. Ver

$$e\left(C, \prod_{i=1}^{n} g_{n-i+1}^{x_i}\right) = e(g_1, g_n)^{y} \cdot e(h, P_y). \quad (4)$$

A functional commitment scheme enables a user to concisely commit to a function from a specified family, then later concisely and verifiably reveal values of the function at desired inputs. Useful special cases, which have seen applications across cryptography, include vector commitments and polynomial commitments. To date, functional commitments have been constructed (under falsifiable assumptions) only for functions that are essentially linear, with one recent exception that works for arbitrarily complex functions. However, that scheme operates in a strong and non-standard model, requiring an online, trusted authority to generate special keys for any opened function inputs. In this work, I give the first functional commitment scheme for nonlinear functions indeed, for all functions of any bounded complexity under a standard setup and a falsifiable assumption. Specifically, the setup is "transparent," requiring only public randomness (and not any trusted entity), and the assumption is the hardness of the standard Short Integer Solution (SIS) lattice problem. Our construction also has other attractive features, including stateless updates via generic composability; excellent asymptotic efficiency for the verifier, and also for the committer in important special cases like vector and polynomial commitments, via pre-processing; and post-quantum security, since it is based on SIS.

B. Verifiable database algorithm

The security goal of the verifiable database in [19, 20, 21, 22, 17] is every time a user accesses the database, the data returned by the cloud not only verify the correctness of this query but also indirectly checks the storage integrity of the overall database. However, the proof reuse and the technique of proof updating by the server to improve system efficiency make their security goal impossible. It means there is no guarantee that the data which is not queried is securely stored in a cloud server. Such data storage integrity auditing is not secure enough for the storage of large databases, such as electronic health records. In order for the existing VDB to regain its defined security, additional procedures (such as auditing schemes) are required to verify the storage integrity. In this section, Our VDB scheme is designed to combine storage and auditing into one, which is more efficient than executing two schemes separately. In addition, constrained by the construction techniques of the current vector commitment scheme, these VDBs cannot aggregate the proofs to achieve the integrity auditing of the data storage. FC scheme can work this out. In this section, by using functional commitment with updates and random masking techniques. Our scheme in this section aims to provide better security for the traditional three-party VDB schemes.

A VDB scheme with updates supporting privacy-preserving integrity auditing allows a client with a constrained resource to outsource the storage of their large database to the cloud. After that, the user can query and update the database stored on the cloud. Besides, any damage to records by the untrusted cloud will be found when the user queries the database and the TPA privacy-preserving audits the data which the client saves in the cloud server every time. The formal definition is given as follows:

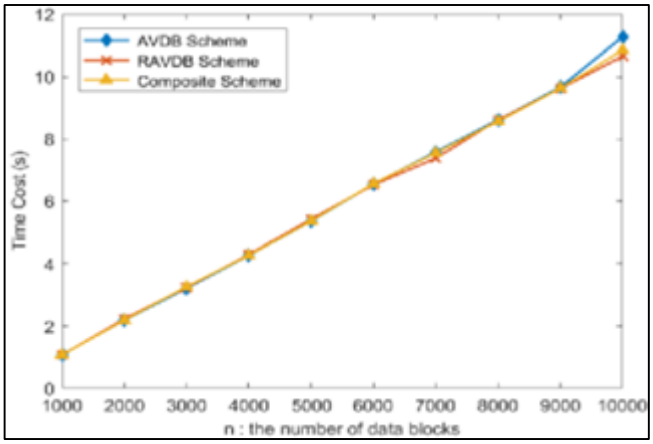

Fig 2: VDB query time cost

As shown in fig2, in the Setup algorithm, the computation overhead for all four schemes increases as the total number of data blocks N. Compared with the composite scheme, our scheme does not need to compute VDB proofs and audit authentication tags separately, so it is more efficient. Compared with the scheme [15], our scheme only needs to generate one signature for n data blocks, which has a big advantage in the computation. In the Query algorithm, the server only needs to generate the proof once for each data block. As the SVer algorithm of the RAVDB scheme shown in Table contains the verification of queried data correctness and user revocation, the computation amount is larger than that of the AVDB scheme and composite scheme. However, if I can reduce the security requirements so that the SVer algorithm only verifies the correctness of the data being queried, and check the user revocation during the audit stage, I can significantly reduce the user computation overhead. In the Update algorithm of our schemes, the user only needs to update the signature once to update w data blocks and For the Revocation algorithm, both our RAVDB and scheme [15] are

affected by the number of revoked users, and scheme [15] is additionally affected by the number of blocks that are last updated by the revoked user.

C. Elliptic curve cryptography algorithm

Elliptical curve cryptography (ECC) is a public key encryption technique based on elliptic curve theory that can be used to create faster, smaller, and more efficient cryptographic keys. ECC is an alternative to the Rivest-Shamir-Adleman (RSA) cryptographic algorithm and is most often used for digital signatures in cryptocurrencies, such as Bitcoin and Ethereum, as well as one-way encryption of emails, data and software. An elliptic curve is not an ellipse or oval shape, but it is represented as a looping line intersecting two axes, which are lines on a graph used to indicate the position of a point. The curve is completely symmetric, or mirrored, along the x-axis of the graph. Public key cryptography systems, like ECC, use a mathematical process to merge two distinct keys and then use the output to encrypt and decrypt data. One is a public key that is known to anyone, and the other is a private key that is only known by the sender and receiver of the data. ECC generates keys through the properties of an elliptic curve equation instead of the traditional method of generation as the product of large prime numbers. From a cryptographic perspective, the points along the graph can be formulated using the following equation:

$$y^2=xt + ax + b$$

Public-key cryptography is based on the intractability of certain mathematical problems. Early public-key systems based their security on the assumption that it is difficult to factor a large integer composed of two or more large prime factors. For later elliptic-curve-based protocols, the base assumption is that finding the discrete logarithm of a random elliptic curve element with respect to a publicly known base point is infeasible: this is the "elliptic curve discrete logarithm problem" (ECDLP). The security of elliptic curve cryptography depends on the ability to compute a point multiplication and the inability to compute the multiplicand given the original and product points. The size of the elliptic curve, measured by the total number of discrete integer pairs satisfying the curve equation, determines the difficulty of the problem.

ECC is like most other public key encryption methods, such as the RSA algorithm and Diffie-Hellman. Each of these cryptography mechanisms uses the concept of a one-way, or trapdoor, function. This means that a mathematical equation with a public and private key can be used to easily get from point A to point B. But, without knowing the private key and depending on the key size used, getting from B to A is difficult, if not impossible, to achieve. ECC is based on the properties of a set of values for which operations can be performed on any two members of the group to produce a third member, which is derived from points where the line intersects the axes as shown with the yellow line and three blue dots in the above diagram labelled A, B and C. Multiplying a point on the curve by a number produces another point on the curve (C). Taking point C and bringing it to the mirrored point on the opposite side of the x-axis produces point D. From here, a line is drawn back to our original point A, creating an intersection at point E. This process can be completed n number of times within a defined max value. The n is the private key value, which indicates how many times the equation should be run, ending on the final value that is used to encrypt and decrypt data. The maximum defined value of the equation relates to the key size used.

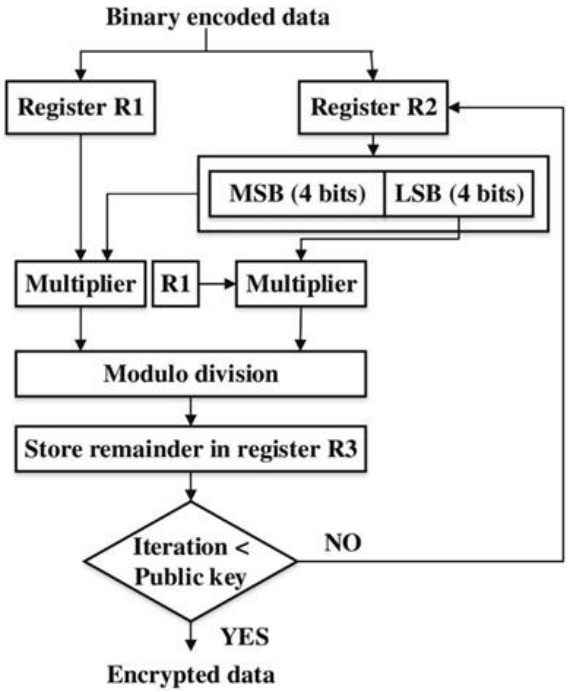

Fig 3: Concept of ECC

D. Blockchain Algorithm

Blockchain is the world's most trusted service. It serves as a ledger that allows transaction to take place in a decentralized manner. There are so many applications based on blockchain technology, including those covering numerous fields like financial services, non-financial services, internet of things (IoT), and so on. Blockchain combines a distributed database and decentralized ledger without the need of verification by central authority. This chapter surveys the different consensus algorithms, blockchain challenges, and their scope. There are still many challenges of this technology, such as scalability and security problems, waiting to be overcome. The consensus algorithms of blockchain are proof of work (POW), proof of stake (POS), ripple protocol consensus algorithm (RPCA), delegated proof of stake (dPOS), stellar consensus protocol (SCP), and proof of importance (POI). This chapter discusses the core concept of blockchain and some mining techniques, consensus problems, and consensus algorithms and comparison algorithms on the basis of performance.

5. Result Analysis

The below table represents the accuracy rate provided by the functional commitment, verifiable database, and elliptic curve cryptography algorithm

Table 1

Model Performance	
Algorithm	**Accuracy**
Functional commitment	70. 8543%
Verifiable database	83. 9542%
Elliptic curve cryptography	96.8934%

From the table, it is analyzed that functional commitment produced the least amount of 70% of accuracy among the three algorithms. The verifiable database algorithm is the data returned by the cloud not only verify the correctness of this query but also indirectly checks the storage integrity of the overall database It produced 83% of accuracy which is comparatively acceptable as compared to the elliptic curve cryptography algorithm. It is analyzed that has produced around 96% of accuracy, which is the highest among these three algorithms.

6. Conclusion

The proposed solution for privacy-preserving integrity auditing on electronic health records using elliptic curve cryptography. The owner can set different access policy based on the data user's role. Uploaded data are encrypted using the ECC encryption algorithm. Encrypted data are stored based on blockchain technology. File access keys will be shared with specific data users based on their role-based access permission. Compared with the previous research results, the proposed system, offering security with an outer-connection facility without consuming the hardware resources of the portable device, allows the facility to share its hardware resources to process other requested tasks, rather than just reserving its computation capabilities to the mentioned security issues. To rapidly and securely transmit health information in a wireless network, the ECC-based Secure EHR system (ESEMR), which utilizes the ECC security scheme to effectively encrypt EHRs is proposed.

7. References

1. Official Website of the Office of the National Coordinator for Health Information Technology (ONC), 2004. Available: https://www.healthit.gov/
2. Canada Health Infoway, 2001. Available: https://www.infoway-inforoute.ca/en/
3. S Benabbas, R Gennaro, Y Vahlis. Verifiable Delegation of Computation over Large Datasets, Conference on Advances in Cryptology. Springer-Verlag, 2011, 111-131.
4. H Shacham, B Waters. Compact Proofs of Retrievability. Journal of Cryptology. 2013; 26(3):442-483
5. S Li, J Cui, H Zhong. *et al*. Public Auditing with Privacy Protection in a Multi-User Model of Cloud-Assisted Body Sensor Networks. Sensors. 2017; 17(5):1032.
6. M Sookhak, R Yu, A Zomaya. Auditing Big Data Storage in Cloud Computing Using Divide and Conquer Tables. IEEE Transactions on Parallel & Distributed Systems, 2017, 99(1-1), 2018.
7. Zhang Cheng, Yang Xu, Yupeng Hu, Jiajing Wu, Ju Ren, Yaoxue Zhang. A blockchain-based multi-cloud storage data auditing scheme to locate faults, 2021.
8. Rajput, Ahmed Raza, Qianmu Li, Milad Taleby Ahvanooey. A blockchain-based secret-data sharing framework for personal health records in emergency condition, 2021.
9. Li Jiaxing, Jigang Wu, Guiyuan Jiang, Thambipillai Srikanthan. Blockchain-based public auditing for big data in cloud storage, 2020.
10. Shen, Jian, Huijie Yang, Pandi Vijayakumar, Neeraj Kumar. A privacy-preserving and untraceable group data sharing scheme in cloud computing, 2021.
11. Li, Yannan, Yong Yu, Bo Yang, Geyong Min, Huai Wu. Privacy-preserving cloud data auditing with efficient key update, 2018.
12. Tomson TT, Passman R. The Reveal LINQ insertable cardiac monitor". Expert Rev Med Devices, 2015.
13. W Shen, J Yu, H Xia, H Zhang, X Lu, R Hao. Light-weight and privacy-preserving secure cloud auditing scheme for group users via the third party medium, Journal of Network and Computer Applications. 2017; 82:56-64.
14. J Shen, T Zhou, *et al*. Anonymous and Traceable Group Data Sharing in Cloud Computing. IEEE Transactions on Information Forensics and Security. 2018; 13(4):912-925.
15. J Yuan, S Yu. Efficient public integrity checking for cloud data sharing with multi-user modification. IEEE INFOCOM 2014-IEEE Conference on Computer Communications. IEEE, 2014.
16. Tomson TT, Passman R. The Reveal LINQ insertable cardiac monitor. Expert Rev Med Devices, 2015.
17. T Iang, X Chen, J Ma. Public Integrity Auditing for Share Dynamic Cloud Data with Group User Revocation, IEEE Transactions on Computers. 2016; 65(8):2363- 2373.
18. B Libert, SC Ramanna, M Yung. Functional Commitment Schemes: From Polynomial Commitments to Pairing-Based Accumulators from Simple Assumptions (Full Version). In ICALP 2016, to appear, 2016.
19. D Catalano, D Fiore. Vector Commitments and Their Applications, Public-Key Cryptography – PKC 2013. Springer Berlin Heidelberg, 2013, 55-72.
20. X Chen, J Li, X Huang. *et al*. New Publicly Verifiable Databases with Efficient Updates. IEEE Transactions on Dependable & Secure Computing. 2015; 12(5):546-556.
21. X Chen, J Li, J Weng, *et al*. Verifiable Computation over Large Database with Incremental Updates, European Symposium on Research in Computer Security. Springer, Cham, 2014, 148-162.
22. M Miao, J Wang, J Ma, *et al*. Publicly verifiable databases with efficient insertion/deletion operations, Journal of Computer & System Sciences, vol. 86, pp. 49-58, 2017.