PUBLICLY VERIFIABLE SHARED DYNAMIC ELECTRONIC HEALTH RECORD DATABASES

[1]*S. Sunitha*, [2]*Eedhula Charan*, [3]*Didugu Peeyusha Lakshmi*, [4]*Sudam Koundinya*, [5]*Y. Ojasvi Mani Chandana*

Assistant Professor in Department of CSE Sreyas Institute Of Engineering And Technology

[1]sunithasurarapu@sreyas.ac.in

[2.3.4,5]UG Scholar in Department of CSE Sreyas Institute Of Engineering And Technology

[2]prabhucharan533@gmail.com, [3]peeyushadidugu@gmail.com,[4] sudamkoundinya@gmail.com ,

[5]yenumulaojasvi246@gmail.com

Abstract

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 paper, 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 features, such as traceability and non-frame ability.

I INTRODUCTION

With the explosive increase of global information, 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, and 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) [6] in the United States and Canada Health Infoway [7]. 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 the 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 equipments 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 on how to verify that the server responses correctly each time Benabbas et al.. proposed the verifiable database (VDB) as a secure and efficient pdatable 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, the server returns the stored message at this position along with a 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 exist to check the data storage integrity. A simple idea to realize the server response correctness and the data storage integrity of 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 smart watch can upload information about a user's heartbeat and breathing, and an insert able cardiac monitor called Reveal LINQ [21] provides long-term heart monitoring. Similarly, mobile terminals with limited performance used in such applications. The main computation and communication of these low-performing terminals occurs when the user first uploads the database and updates the data each time.

II LITERATURE SURVEY

Verifier-Local Revocation Group Signature Schemes with Backward Unlinkability from Bilinear Maps

An approach of membership revocation in group signatures is verifier-local revocation (VLR for short). In this approach, only verifiers are involved in the revocation mechanism, while signers have no involvement. Thus, since signers have no load, this approach is suitable for mobile environments. Although Boneh and Shacham recently proposed a VLR group signature scheme from bilinear maps,this scheme does not satisfy the backward unlikability. The backward unlikability means that even after a member is revoked, signatures produced by the member before the revocation remain anonymous. In this paper, we propose VLR group signature schemes with the backward unlink ability from bilinear maps.

Group signatures with verifier-local revocation. Acm Conference on Computer & Communications Security

Group signatures have recently become important for enabling privacy-preserving attestation in projects such as Microsoft's ngscb effort (formerly Palladium). Revocation is critical to the security of such systems. We construct a short group signature scheme that supports Verifier-Local Revocation (VLR). In this model, revocation messages are only sent to signature verifiers (as opposed to both signers and verifiers). Consequently there is no need to contact individual signers when some user is revoked. This model is appealing for systems providing attestation capabilities. Our signatures are as short as standard RSA signatures with comparable security. Security of our group signature (in the random oracle model) is based on the Strong Diffie-Hellman assumption and the Decision Linear assumption in bilinear groups. We give a precise model for VLR group signatures and discuss its implications.

Wallet Databases with Observers

Previously there have been essentially only two models for computers that people can use to handle ordinary consumer transactions: (1) the tamper-proof module, such as a smart card, that the person cannot modify or probe; and (2) the personal workstation whose inner working is totally under control of the individual. The first part of this article argues that a particular combination of these two kinds of mechanism can overcome the limitations of each alone, providing both security and correctness for organizations as well as privacy and even anonymity for individuals.Then it is shown how this combined device, called a wallet, can carry a database containing personal information. The construction presented ensures that no single part of the device (i.e. neither the tamper-proof part nor the workstation) can learn the contents of the database — this information can only be recovered by the two parts together

Hierarchical Identity Based Encryption with Constant Size Cipher text

We present a Hierarchical Identity Based Encryption (HIBE) system where the cipher text consists of just three group elements and decryption requires only two bilinear map computations, regardless of the hierarchy depth. Encryption is as efficient as in other HIBE systems. We prove that the scheme is selective-ID secure in the standard model and fully secure in the random oracle model. Our system has a number of applications: it gives very efficient forward secure public key and identity based cryptosystems (with short cipher texts), it converts the NNL broadcast encryption system into an efficient public key broadcast system, and it provides an efficient mechanism for encrypting to the future. The system also supports limited delegation where users can be given restricted private keys that only allow delegation to bounded depth. The HIBE system can be modified to support sub linear size private keys at the cost of some cipher text expansion.

Verifiable Delegation of Computation over Large Datasets

We study the problem of computing on large datasets that are stored on an un trusted server. We follow the approach of amortized verifiable computation introduced by Gennaro, Gentry, and Parno in CRYPTO 2010. We present the first practical verifiable computation scheme for high degree polynomial functions. Such functions can be used, for example, to make predictions based on polynomials fitted to a large number of sample points in an experiment. In addition to the many no cryptographic applications of delegating high degree polynomials, we use our verifiable computation scheme to obtain new solutions for verifiable keyword search, and proofs of irretrievability. Our constructions are based on the DDH assumption and its variants, and achieve adaptive security, which was left as an open problem by Gennaro et al (albeit for general functionalities). Our second result is a primitive which we call a verifiable database (VDB). Here, a weak client outsources a large table to an un trusted server, and makes retrieval and update queries. For each query, the server provides a response and a proof that the response was computed correctly. The goal is to minimize the resources required by the client. This is made particularly challenging if the number of update queries is unbounded. We present a VDB scheme based on the hardness of the subgroup membership problem in composite order bilinear groups.

III EXISTING SYSTEM

We modify the existing functional commitment scheme in order to use the function binding of functional commitment to design an auditable VDB scheme. Two algorithms for updating are added based on the original scheme in . And a modified concrete FC with updates under the computational assumption is constructed. Our construction has fewer parameters and is more efficient than the original scheme in . We point out security problems with scheme and propose a publicly verifiable updatable VDB scheme based on the functional commitment and group signature without incurring too much computational overhead and storage cost. Moreover, our scheme is applicable for large-scale data storage with minimum user communication cost.

Disadvantages

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.

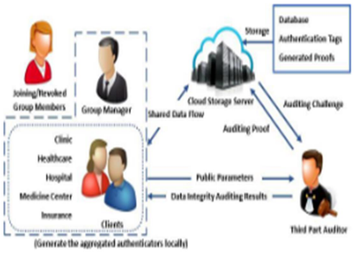
IV PROPOSED SYSTEM

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 un-trusted server. Later, the client can query the server for an item (a message) at position i, the server returns the stored message at this position along with a 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.

Advantages

1. Improving the efficiency.
2. Proof reuse and proof updating technique to prove correctness of the query results

V ARCHITECTURE



VI IMPLEMENTATION

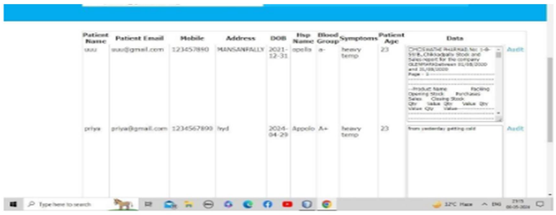
Client: In this module client(clinic, health care, hospital, medicine center, insurance) should register with our Application after their successful register they must joined by the manage. If they joined by the manager into the application he can perform some operations such as upload patient data and view patient data and also can search for other patient data, view patient data and share to other group member.

TPA: here TPA should login with the application after successful login he can perform some operations such as view patients records and audit records if any records has already modified by any user or not and also send the audit request to cloud.

Manager :Here manager can login with the application after successful login he can perform some operations such as view client and join client or revoke clients.

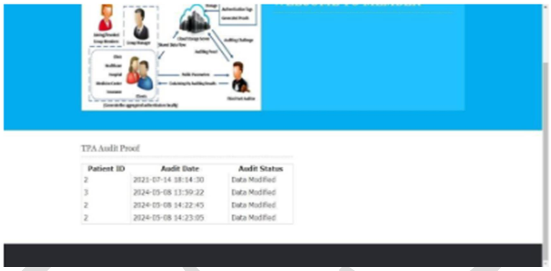
Cloud: Here cloud can login with the application after successful login he can perform some operations such as view clients details and patient details and check audit proof.

VII RESULTS



Patient Name	Patient Email	Mobile	Address	DOB	Hsp Name	Blood Group	Symptoms	Patient Age	Data	
uuu	uuu@gmail.com	123457890	MANSANPALLY	2021-12-31	opello	a-	heavy temp	23	CHOSMATHE PHARMAB No: 1-8-597B, Chikkadpally Stock and Sales report for the company GLENMARK between 01/08/2020 and 31/08/2020 Page - 1 --Product Name Packing Opening Stock Purchases Sales Closing Stock Qty Value Qty Value Qty Value Qty Value	Audit
priya	priya@gmail.com	1234567890	hyd	2024-04-29	Appolo	A+	heavy temp	23	from yesterday getting cold	Audit

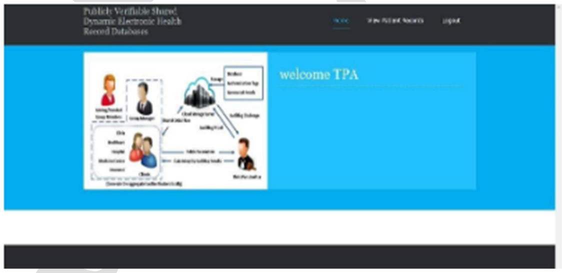
Displays Patient details



TPA Audit Proof

Patient ID	Audit Date	Audit Status
2	2021-07-14 18:14:30	Data Modified
3	2024-05-08 13:39:22	Data Modified
2	2024-05-08 14:22:45	Data Modified
2	2024-05-08 14:23:05	Data Modified

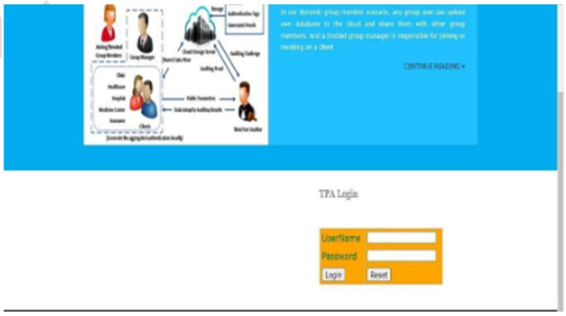
Displays data auditing



Publicly Verifiable Shared Dynamic Electronic Health Record Databases
HOME
View Patient Records
Logout

welcome TPA

TPA homepage

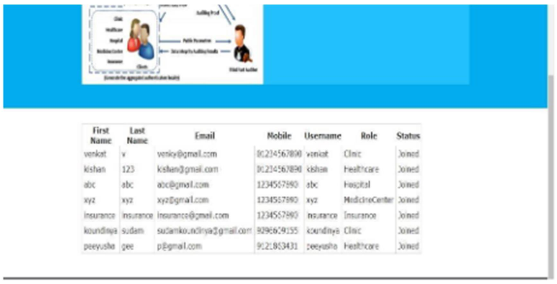


In our dynamic group member scenario, any group user can upload own database to the cloud and share them with other group members. And a trusted group manager is responsible for joining or revoking on a client

TPA Login

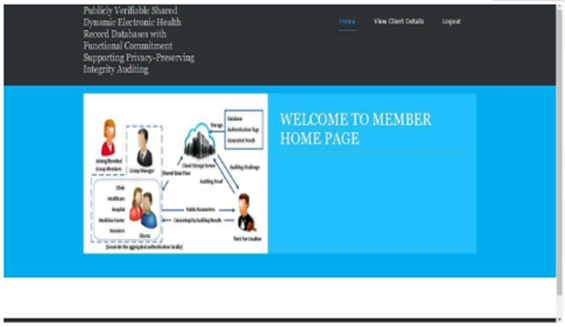
UserName
Password

TPA login



First Name	Last Name	Email	Mobile	Username	Role	Status
venkat	v	venky@gmail.com	01234567890	venkat	Clinic	Joined
kishan	123	kishan@gmail.com	01234567890	kishan	Healthcare	Joined
abc	abc	abc@gmail.com	1234567890	abc	Hospital	Joined
xyz	xyz	xyz@gmail.com	1234567890	xyz	MedicineCenter	Joined
insurance	insurance	insurance@gmail.com	1234567890	insurance	Insurance	Joined
koundinya	sudam	sudamkoundinya@gmail.com	9296629155	koundinya	Clinic	Joined
peeyusha	gee	p@gmail.com	9121853431	peeyusha	Healthcare	Joined

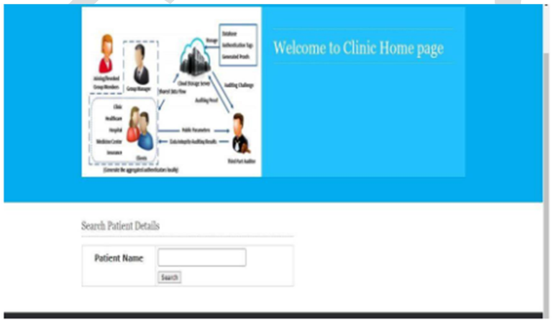
Manager joining/invoking the client



Publicly Verifiable Shared Dynamic Electronic Health Record Databases with Functional Commitment Supporting Privacy-Preserving Integrity Auditing

WELCOME TO MEMBER HOME PAGE

manager homepage

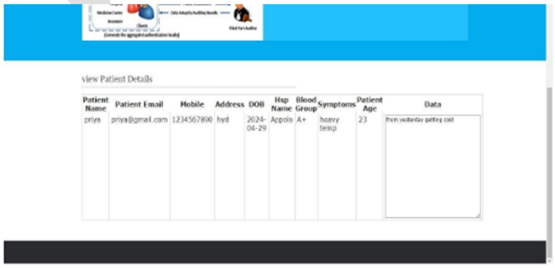


Welcome to Clinic Home page

Search Patient Details

Patient Name

Displays search patient details



view Patient Details

Patient Name	Patient Email	Mobile	Address	DOB	Hsp Name	Blood Group	Symptoms	Patient Age	Data
priya	priya@gmail.com	1234567890	hyd	2024-04-29	Appolo	A+	heavy temp	23	from yestarday getting cold

Client details

VIII CONCLUSION

The concept of verifiable database is a great tool for verifiable EHR storage. However, proof reuse and the technique of proof updating by the server to improve system efficiency fails to achieve data integrity checking. In this work, we propose a novel updatable VDB scheme based on the functional commitment that supports privacy-preserving integrity auditing and group member operations, including join and revocation. Two security requirements of EHR are implemented: the server response correctness and the data storage integrity. Our VDB scheme achieves the desired security goals without incurring too much Computational increase. And our VDB scheme provides the minimum communication cost for the terminal with limited performance. To design 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 our VDB scheme can achieve the desired 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.

[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] Official Website of The Office of the National Coordinator for Health Information Technology (ONC). (2004). Available: https://www.healthit.gov/

[7] Canada Health Infoway. (2001). Available: https://www.infoway-inforoute.ca/en/ [8] 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.

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

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