Secure attribute based electronic health records transaction with de-duplication check on cloud

[1]Kumari Neha, [2]Mr. Madhu BR
[1]M.Tech Student, [2] Associate Professor

[1][2]Department of Computer Science & Engineering, SET, Jain University Bengaluru, Karnataka

ABSTRACT

Electronic Health Records System (EHRs) is the form of system that provides storage of patient health records in digital electronic form. These records can be stored to any storage service provider depending on patient interest, and timely access by patient or doctor from any geographical location. Formerly, much more constraint was there for sharing health records by patient to the medical specialist, this results loss of records and leak of personal information. Proposed system introduce attribute based signature scheme ABS which allow patient to sign records with predicate from the attribute provided by authority. It also use secret hashing algorithm for de-duplication check while uploading the health records to the cloud.

Keywords: Electronic Health Records System, Attribute Base signature, Secure Hash Algorithms, Central Authority.

I. INTRODUCTION

Electronic Health Records System (EHRs) or Electronic Medical Records System (EMRs) is an electronic application through which individual can access, manage and share their health information… in private, secure and confidential environment [1]. It contains retrospective, concurrent, and prospective information of the patient and provides continuous, efficient and quality integrated health care [2]. Its access right managed and controlled by patient or service provider depending on model. With the increasing demands for flexible access to health information and service it is necessary for the service provider to protect patient personal information on top priority.

In EHRs we proposed Attribute Based Signature (ABS) scheme where a Central Authority (CA) generate attribute for the patient, patient use any one of the predicate from attribute to sign records and outsource encrypted records to the cloud. In general signature used in this model doesn’t reveal information about the patient and his attribute. Model also proposes secure hash algorithms to check de-duplication while outsourcing to the cloud.

II. RELETED WORK

One of the major obstacles for any data sharing model is how to protect privacy of individuals whose data have been collected and shared between different entities, these data such as medical records are quite sensitive for Record Owner (RO). There are many proposed model which promised confidentiality of data and records to the record owner.

The Escrow Free Attribute-Based Signature [3] propose multiple attribute authorities (AAs) to generate the attribute-based private key in the attribute-based setting, it make use of a key extraction protocol to replace the key generation algorithm in attributed-based signature (ABS), from which the key generation centre (KGC) cannot forge a signature on behalf of a legal user with attributes satisfying the corresponding predicate, despite the of participation in generating the signing key.[3] The proposed system append a signer revelation protocol to ABS system to enable a user to confirm or deny his/her identity of producing an attribute-based signature.

Multi-authority Attribute-base [4] system propose complex policies using AND, OR, and threshold conditions. It depends on central authority to assure the usability of attribute keys a user getting from different attribute authorities. To prevent collusion attacks it adopts a unique global identity (GID) [4] for a user to bind his attribute keys and identity together. Secret key from the central authority help the verification be independent of the user's identity. Model [5] includes large number of binary and finite-set attribute compress into a single attribute base. The core idea is to encode discrete binary and finite-set values as prime numbers and use divisibility property for efficient proofs of presence or absence. [6] Attribute based Ring signature proposes signer's anonymity when it signs messages on behalf of a 'ring' of possible signers. It uses novel notion of ring signature which is called attribute-based ring signature. It allows the signer to sign message with its attributes from attribute centre. ABS scheme [7] introduce non-monotone predicates which are expressed using AND, OR, NOT and Threshold gates.

Similarly all signature schemes [3-17] provide a valid signature that doesn't reveal any details about the way it was actually generated.

III. PROPOSED SYSTEM

In existing system, records are shared among the entities with different security mechanism [3-17], which increase system dependency on multiple authorities and introduce overall performance delay in the system. Model also not considers duplicate records outsourced to cloud. Our proposed model use Attribute Based Signature Scheme and Secure Hash Algorithm for encryption decryption and de-duplication check respectively. System identifies all its entity and generate secret key with the help of Central Authority and his master key, these secret key use as input to compute predicate to sign the records. Signed records is outsourced and shared with entities. In second phase propose system create hash value of the records and compare with existing hash value stored before outsource to cloud.

Architecture View

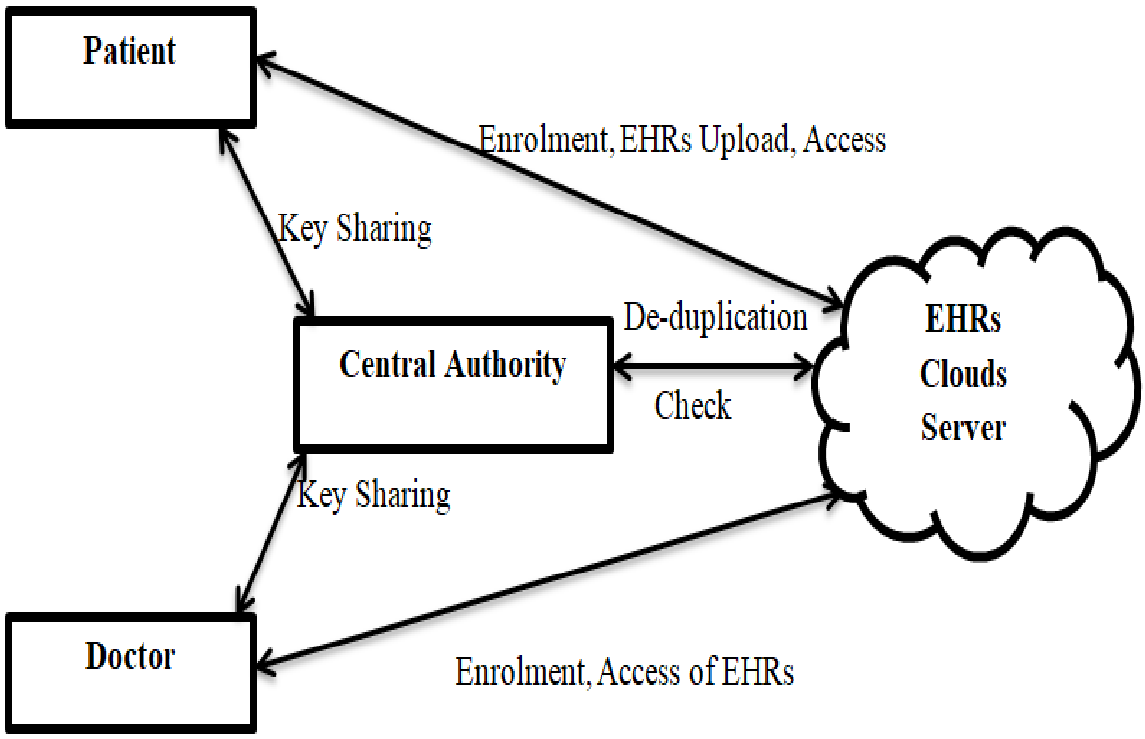

Figure 3.1

IV. IMPLEMENTATION

Propose system contains following four modules:

A. Modules

Authorities:

Authority is the prime entity in the EHRs system. He uses his maser key to generate secret key for the patient and doctor. This secret key is responsible for signing the records with predicate satisfied by it. It use secure hashing algorithms to generate hash value of the records, this hash value is compared with uploaded hash records for de-duplication and uploaded if found unique.

EHRs Cloud:

The EHRs Cloud is a cloud storage service; where patient store their health records and seeks for expert medical opinion from expert health specialist. It acts as storage for hosting service for different entities.

Patient:

Patient is the health record owner, he enrol to the system and request central authority for the attribute private key. Patient sign records with the predicate that satisfied by the provided attribute and outsource records to EHRs Cloud.

Data Verifier (Doctors):

Doctor is the record verifier he is responsible for timely access the uploaded records using his secret key and provide expert health opinion for the patient. His secret computed by the central authority at the time of enrolment.

B. Algorithms

Attribute based signature use following five steps:

- **Central Authority:** It use security parameter to generate (Pk, Sk) where Pk and Sk denotes public key and private key of the authority.
- **KeyGen :** It generate (Pu, Su) using (Sa, Gid, A) by the central authority. Here Pu and Su are public and private key of the patient, Gid is global identifier and A is attribute set of patient.
- **Sign:** To sign the record patient use his private key, authority public key and predicate satisfied by his attribute (Pa, Su, Y).
- **Verify:** Verifying authority (Doctor) verify the signature embedded in message using public key of the user, patient attribute set A and signature with the predicate.

SHA 512

Secure Hashing Algorithms used for records de-duplication check. This hash mechanism creates 512bits hash code for records being outsources to the cloud and check hash value with hash database, if it found unique it is uploaded otherwise it point to existing records.

V. RESULT

The proposed system implements the secure health records sharing with deduplication among different entities. As records are shared between the entities the major concerned among patient are for privacy and confidentiality of the records. This implemented system protect the concerned using public private key model depending upon single central authority, which increase the performance and check the duplicate records for being uploaded. This system is best suited model for the quick, secure sharing of electronic health Records.

VI. CONCLUSION

To protect the privacy of patient electronic health records and loss of person information attribute based signature is introduced, which provide the essential requirement to ensure the performance of the EHRs system. In this system authority generates the secret key and disseminates it to the signing authority. Authority also uses

Secret Hashing Algorithm (SHA) for de-duplication. Finally the EHRs system is protected with encryption and de-duplication.

REFERENCES

[1] Connecting for Health. Connecting Americans to their healthcare. final report of the working group on policies for electronic information sharing between doctors and patients. NewYork: Markle Foundation, 2004.

[2] Kristiina Hayrinen, Kaija Saranto, Pirkko NykanenDefinition, structure, content, use and impacts of electronic health records: A review of the research literature journal homepage: www.intl.elsevierhealth.com/journals/ijmi

[3] Hui Cui, Guilin Wang, Robert H. Deng, Baodong Qin Escrow free attribute-based signature with self-revealability.

[4] M. Chase, Multi-authority attribute based encryption, Springer, 2007

[5] JCamenisch, J., Groß, T.: Efficient attributes for anonymous credentials. In: CCS 2008, pp. 345–356. ACM, New York (2008)

[6]Li, J., Kim, K.: Attribute-based ring signatures, IACR,

[7] T. Okamoto K. Takashima "Efficient attribute-based signatures for non-monotone predicates in the standard model" Proc. 14th Int. Conf. Practice Theory Public Key Cryptography vol. 6571 pp. 35-52 2011. https://link.springer.com/10.1007/978-3-642-19379-8_3

[8]A. Lewko, B. Waters “Decentralizing Attribute-Based Encryption,” in Advances in Cryptology - EUROCRYPT 2011, International Conference on the Theory and Applications of Cryptographic Techniques, Tallinn, Estonia, May 15-19, 2011, pp. 568-588

[9] J. Li, N. Chen, Y. Zhang, “Extended file hierarchy access control scheme with attribute based encryption in cloud computing,” IEEE Transactions on Emerging Topics in Computing , pp.1-1, March, 2019, 10.1109/TETC.2019.2904637.

[10] A. Lewko, T. Okamoto, A. Sahai, K. Takashima and B. Waters, “Fully secure functional encryption: Attribute-based encryption and (hierarchical) inner product encryption,” in Advances in Cryptology - EUROCRYPT 2010, Lecture Notes in Computer Science, vol. 6110. Heidelberg, Germany: Springer-Verlag, May 30 – June 3, 2010, pp.62–91.

[11] J. Han, W. Susilo, Y. Mu, “PPDCP-ABE: privacy-preserving decentralized ciphertext-policy attribute-based encryption,” In Computer Security-ESORICS 2014, Springer International Publishing: Cham, Switzerland, 2014, pp. 73–90.

[12] M. Wang, Z. Zhang, C. Chen, “Security analysis of a privacypreserving decentralized ciphertext - policy attribute - based encryption scheme,” Concurrency & Computation Practice & Experience, vol. 28, no. 4, pp. 1237-1245, August 18, 2016, •

10.1002/cpe.3623.

[13] K. Emura, A. Miyaji, A. Nomura, et al., “A Ciphertext-Policy Attribute-Based Encryption Scheme with Constant Ciphertext Length,” in International Conference on Information Security Practice and Experience, Springer-Verlag, 2009, pp. 13-23, April 13-15.

[14]M. ChaseChase and S. S. Chow, “Improving privacy and security in multiauthority attribute-based encryption,” in Proc. 16th ACM Conf. CCS, November 09 – 13, 2009, pp. 121–130.

[15] J. Han, W. Susilo, Y. Mu and J. Yan, “Privacy-preserving decentralized key-policy attribute-based encryption,” IEEE

Transactions on Parallel and Distributed Systems, vol. 23, no. 11, pp. 2150–2162, Nov. 2012, 10.1109/TPDS.2012.50.

[16] J. Li, S. Hu, and Y. Zhang, “Two-party attribute-based key agreement protocol with constant-size ciphertext and key,” Security and Communication Networks, Article ID 8738960, 10 pages, 2018, 10.1155/2018/8738960.

[17] J. Li, Q. Yu, and Y. Zhang, “Hierarchical attribute based encryption with continuous leakage-resilience,” Information Sciences, to be published. DOI: 10.1016/j.ins. 2019.01.052