A Secure Data Sharing for Hierarchical Sub-Groups using Identity-Based Encryption Scheme for E-Healthcare System

Kumar K[1]Hemanth Kumar[2] G BasamSindu Priya[3] Akshay P[4]Ajay Kumar S M[5]
[1]Assistant Professor
[1,2,3,4,5]Department of Computer Science &Engineering
[1,2,3,4,5]K.S. Institute of Technology,Bengaluru, India

Abstract**—***In the distributed environment it is very much necessary to build a system which share secure data among multiple users. Unavoidable use and far reaching sharing of Electronic Health Records (EHRs) in present day social insurance conditions has brought about high accessibility of patients' medicinal history from any area and whenever, which can possibly influence health to mind administrations both less expensive and of higher quality. In any case, EHRs contain tremendous measures of delicate data which ought to be shielded from unapproved access, generally enabling these records to be gotten by various gatherings may put persistent protection at high hazard. Access control arrangements must guarantee to reflect the control strategies of all medicinal services suppliers who are engaged with creating such basic records and additionally approval approaches of the patient as the essential partner. In this, a fine-grained semantic-based access control demonstrate that backings multi-owner multi-stakeholder arrangement detail and authorization. In the proposed plot, a trusted Policy Server is in charge of assessing access solicitations to patients' health data.*

Keywords—Encryption, E-Healthcare

I. INTRODUCTION

These days, many individuals utilize the web to share their own information including their private information, messages, and so on among different clients.

Electronic-based ones and huge numbers of them have turned out to be associated by means of the Web. The medicinal services space isn't a different case. Human services suppliers utilize Electronic Medical Records (EMRs) for keeping up tolerant health data. Medicinal services, medications frequently require the combination and sharing of restorative information originating from various sources. Such incorporation can prompt more noteworthy efficiency, enhanced patient care, and cost investment funds. However in the meantime, it presents new security and protection challenges. These days, it is extremelyregular for patients to have different social insurance suppliers who might be scattered all through a nation or even the world. These social insurance suppliers may utilize EHRs for coordinating and offering persistent data to each other. EHRs may contain sensitive patient information, for example, lab test results, findings, and pharmaceutical. Mix and sharing of these records must be finished by guaranteeing patients protection through legitimate access control arrangements. Medicinal services suppliers have their own access control strategies and components for shielding patients' medical data from unapproved access.

Moreover, electronic therapeutic gadgets (e.g. wearable trackers) alongside therapeutic applications on cell phones empower patients to produce health data which can be conveyed to the social insurance suppliers for better serving them. Patients may have distinctive protection worries for sharing their delicate health data which can confine access to their data, so medicinal services frameworks ought to give a component to their patients to define their own entrance control approaches.

Distinctive partners in the medicinal services area may not will to share their entrance control arrangements with each other, so a trusted outsider can help in coordinating and authorizing access control approaches of patients and different human services suppliers.

In another approach, a patient's health data can be collected from various sources as a group benefit, the objective of which is to "convey the correct health data to the ideal place at the perfect time" [4]. These People group Health Records are open through Health Data Trade which encourages the flow of clinical data among a few health data frameworks. Considering all previously mentioned situations for sharing medical data among numerous partners in a medicinal services condition, the requirement for having an exhaustive and fine grained access controlling model winds up self-evident. Such a model should regard approval arrangements of every included gathering. In this paper, we propose a fine-grained semantic- based access control model that guarantees to reflect access controlling strategies of all human services suppliers who are associated with producing EHRs and also approval arrangements of the patient as the essential partner. In the proposed plot, approval approaches depend on qualities of various substances in a medicinal services space. A trusted outsider is in charge of joining and assessing approval strategies of various gatherings for a given access asked. The essential commitments of this paper are as per the following:

1) An extensive and fine-grained access control show is proposed for a multi-proprietor multi-partner social insurance condition which regards approval arrangements of all proprietors of an EHR record.
2) The proposed system settles approach conflicts by considering conflict determination procedure of the proprietor of the data.

II. LITERATURE SURVEY

The involvement of the third-party network services, a crucial issue is that the identity attributes in the access control policies often reveal privacy sensitive information about users and leak confidential information about the content. The confidentiality of the content and the privacy of the users are thus not fully protected if the identity attributes are not protected. Further, privacy, both individual as well as organizational, is considered a key requirement in all solutions, including network services, for digital identity management. Further, as insider threats are one of the major sources of data theft and privacy breaches, identity attributes

must be strongly protected even from accesses within organizations. With initiatives such as server the scope of insider threats is no longer limited to the organizational perimeter. Therefore, protecting the identity attributes of the users while enforcing attribute-based access control both within the organization as well as in the server is crucial.

Designing an efficient and secure data sharing scheme for groups in the network is the major issues need to be considered. It is highly recommended that privileged members of a group should be able to fully enjoy the data storing and sharing services provided by the network. More concretely, privileged user in the group is able to not only read data, but also modify his/ her part of data in the entire data file shared by the company. Usually groups are self-possessed of several subgroups organized in a hierarchical manner. Data integrity must be provided for each level of group. Several security schemes for data sharing on un-trusted servers have been proposed. In these approaches, data owners store the encrypted data files in un-trusted storage and distribute the corresponding decryption keys only to authorized users.

III. EXISTING SYSTEM

Some of the existing secure data sharing schemes such as scalable and fine-grained data access control scheme in network based on the key policy attribute-based encryption (KP-ABE) technique , cryptographic storage system, Proxy re-encryption scheme are discussed below.

A. Cryptographic Storage System

CSS [2] enables secure file sharing on untrusted servers, named Plutus proposed by, Kallahalla et al. By dividing files into file groups and encrypting each file group with a unique file-block key, the data owner can share the file groups with others through delivering the corresponding lockbox key, where the lockbox key is used to encrypt the file-block keys. However, it brings about a heavy key distribution overhead for large-scale file sharing. Additionally, the file-block key needs to be updated and distributed again for a user revocation. Files stored on the untrusted server include two parts: file metadata and file data [1]. The file metadata implies the access control information including a series of encrypted key blocks, each of which is encrypted under the public key of authorized users. Thus, the size of the file metadata is proportional to the number of authorized users.

The user revocation in the scheme is an intractable issue especially for large-scale sharing, since the file metadata needs to be updated. However, when a new user joins the group, the private key of each user needs to be recomputed, which may limit the application for dynamic groups.

B. Proxy Re-Encryptions (PRE)

Proxy re-encryption schemes are cryptosystems which allow third-parties (proxies) to alter a cipher text which has been encrypted for one party, so that it may be decrypted by another. PRE to secure distributed storage enables the data owner encrypts blocks of content with unique and symmetric content keys, which are further encrypted under a master public key. For access control, the server uses proxy cryptography to directly re-encrypt the appropriate content key(s) from the master public key to a granted user's public key [1]. Unfortunately, a collusion attack between the untrusted server and any revoked malicious user can be launched, which enables them to learn the decryption keys of all the encrypted blocks.

C. A Scalable and Fine-Grained Data Access Control Scheme

Server is operated by a network service providers cannot be trusted to protect the confidentiality and sensitivity of the data. For instance, an untrustworthy CSP may sell the confidential information about an enterprise to its closest business competitors for making a profit. Therefore, a natural way to keep sensitive data confidential against an untrusted CSP is to store only the encrypted data in the network. Encryption alone however is not sufficient as organizations often have to enforce fine-grained access control on the data. Such control is often based on the attributes of users, referred to as identity attributes, such as the roles of users in the organization, projects on which users are working and so forth. These systems, in general, are called attribute based systems. Therefore, an important requirement is to support fine-grained access control, based on policies specified using identity attributes, over encrypted data. To achieve fine-grained access control on files stored by network Servers, we want to enable the data owner to enforce a unique access structure on each user, which precisely designates the set of files that the user is allowed to access. We also want to prevent network Servers from being able to learn both the data file contents and user access privilege information.

KP-ABE is a public key cryptography primitive for one-to-many communications. In KP-ABE, data are associated with attributes for each of which a public key component is defined. The encrypt or associates the set of attributes to the message by encrypting it with the corresponding public key components. Each user is assigned an access structure which is usually defined as an access tree over data attributes, i.e., interior nodes of the access tree are threshold gates and leaf nodes are associated with attributes. User secret key is defined to reflect the access structure so that the user is able to decrypt a cipher-text if and only if the data attributes satisfy his access structure.

A scalable and fine-grained data access control scheme in network based on the Key Policy Attribute Based Encryption technique(KP-ABE) presented by Ateniese et al. The data owner uses a random key to encrypt a file, where the random key is further encrypted with a set of attributes using KP-ABE. Then, the group manager assigns an access structure and the corresponding secret key to authorized users, such that a user can only decrypt a cipher text if and only if the data file attributes satisfy the access structure. To achieve user revocation, the manager delegates tasks of data file re-encryption and user secret key update to network servers. However, the single owner manner may hinder the implementation of applications with the scenario, where any member in a group should be allowed to store and share data files with others. Secure provenance scheme, which is built upon group signatures and CP-ABE proposed in [5]. Particularly, the system in their scheme is set with a single attribute. Each user obtains two keys after the registration: a group signature key and an attribute key. Thus, any user is able to encrypt a data file using attribute-based encryption

and others in the group can decrypt the encrypted data using their attribute keys. Meanwhile, the user signs encrypted data with her group signature key for privacy preserving and traceability.

Major drawback of this scheme is efficient user revocation. More concretely, the user decryption keys need to be modified after a new user addition or current user revocation. System overhead increases as every time the user decryption keys need to be updated.

IV. CONCLUSION

In this, MoMsAC, a multi-owner multi-stakeholder access control model demonstrate for a social insurance condition which engages diverse medicinal services suppliers and in addition patients to express their fine-grained get to control approaches on their EHR records. For such reason a Policy Server based access control system has been recommended through which proprietors of the data outsource their approval arrangements to the Policy Server and Policy Server is the principle dependable point for assessing access demands in view of those strategies and returning appropriate reactions. The proposed get to control demonstrate is based on the composite EHR metaphysics and the human services philosophy, which enables the proprietors of the medicinal data in defining their entrance to control arrangements. Diverse Semantic Web based models are utilized for indicating, assessing, and upholding approval strategies. We have likewise actualized a model of the proposed model to show the appropriateness of our framework.

ACKNOWLEDGEMENT

The authors would like to thank to the reviewers for their best suggestions.

REFERENCES

[1] E. Goh, H. Shacham, N. Modadugu, and D. Boneh, “Sirius: Securing Remote Untrusted Storage,” Proc. Network and Distributed Systems Security Symp. (NDSS), pp. 131-145, 2003.
[2] M. Kallahalla, E. Riedel, R. Swaminathan, Q. Wang, and K. Fu, “Plutus: Scalable Secure File Sharing on Untrusted Storage,” Proc. USENIX Conf. File and Storage Technologies, pp. 29-42, 2003.
[3] Lei Wang ; Zhonglei Li; Mingkai Chen; Aiqing Zhang; JingWu Cui; BaoyuZheng, secure content sharing protocol for D2D users based on profile matching in social networks, 2017 9th International conference on Wireless Communications and signal processing(WCSP) .
[4] Chesapeake Regional Information System for our Patients. https://www.crisphealth.org/.
[5] Leila Karimi; James Joshi, Multi-Owner Multi-Stakeholder Access control model for a healthcare environment, 2017 IEEE 3rd International Conference on Collaboration and Internet Computing (CIC).
[6] SuphaLakshmi; M. Revathi, Secure data sharing using 3-party decentralized communication, 2016 10th International Conference on Intelligent Systems and Control (ISCO)