International Journal of Engineering & Technology, 7 (2.20) (2018) 90-92

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

A secure attribute-Based encryption scheme in cloud computing

Naresh Vurukonda*, S. Trijan kumar, J.V. Rajasekhar Reddy, A. Adithya, Sekhar Babu Boddu

[1]*Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Guntur, India.*
**Corresponding author E-mail:naresh.vurukonda@kluniversity.in*

Abstract

Singular Health care record ensuring the consolidated server to keep up the patient near and dear and SHR organizations are redistributed to expert centre. The main reason is about health report. The patient mainly wants to control the offering kept up to high assurance and security. The security game plans are used to shield the individual information from group. Calm data can be gotten to by an extensive variety of people. Each master is consigned with get to approval for a particular plan of characteristics. For that we are using four entities which are Data owner, End user, and key distribution centre and cloud service provider. In order to achieve fine-grained and versatile data get the chance to control for SHR`s, we utilize Attribute-Based Encryption (ABE) frameworks to encode each patient SHR report. Distinctive data proprietors approach comparative data regards. The prefer plan could be extended to Hierarchical Attribute-Based Encryption (HABE) for get the chance to control instrument.

1. Introduction

Dispersed process, as a creating handling perspective, engages customers to easily upload the SHR in cloud, so as to acknowledge benefits on-ask. Moving customer side data to cloud offers inconceivable solace to customers, as they get to SHR in the cloud at whatever point and wherever, using any contraption, without pondering the capital dare to send the gear establishments. Specifically for little and medium-sized endeavour's with obliged spending designs, they can acquire cost hold reserves and versatility to scale (or specialist) wanders on ask for, using cloud organizations to managing wanders, attempt wide contacts and also plans, et cetera. In any case, let on a cloud pro centre (CSP), worked for make an advantage, to manage private corporate data, raises shrouded security and insurance issues. For instance, a scheming Cloud service provider (CSP) might pitch the ordered information around an endeavour to its closest business adversaries for making advantage. In this way trademark technique to keep susceptible data mystery against an untrusted CSP to store only the encrypted data in to the cloud. We consider the going with application circumstance (see Fig. 1): Organization pays a CSP for sharing corporate data in cloud servers. Expect the business division (SD), the inventive work office (RDD), and the store office (FD) are collaborating in Task X. The SD administrator needs to store encoded customer for essential examination (URA) in the cloud, so simply the staff must have certain verifications can get to the report. For instance, The SD chief may demonstrate an entrance control approach for this URA, as showed up in Fig.

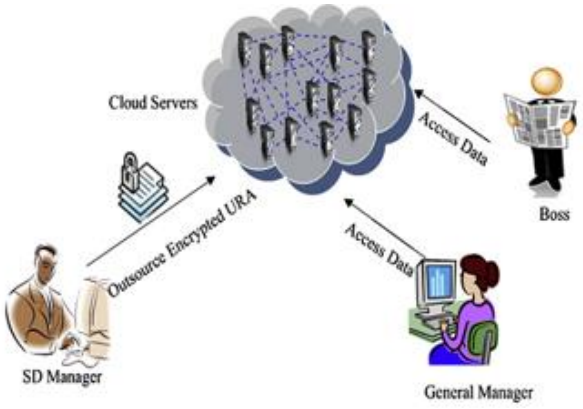


Fig. 1: Sample application scenario

the path control system can be passed on Boolean condition over characteristics. Every trademark includes site determining to which party regulates the property and an identifier portraying a trait itself, both of which can be tended to a strings and connected with solitary colon character as separator. The cut in every site indicates a relationship between normal and a subordinate.[12] The sense behind along these lines control technique is that this URA should simply be gotten to by the chief and the general authority of the undertaking, the general population from Assignment X, and the working environment manager who are secured with Undertaking X. Moreover, the social event that directions characteristics "is Boss", "is General Manager", and "in Project X" better than the party controls properties "is Department Manager", "in SD", "in RDD" and "inFD". In the above application, the encrypter doesn't know the correct characters of typical beneficiaries, rather he has an approach to manage and portray them utilizing certain sensible properties. Thusly, got a handle on encryption framework ought to fortify a quality base access structure. Adaptable encryption outlines, for example, cipher text-framework trademark based encryption (CP-ABE), can be gotten a handle on to give a fine grain get the chance to control for the encoded information. CP-ABE licenses to encode information demonstrating an entry control policy over characteristics, with the target that lone clients with an

Copyright © 2018 Authors. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

arrangement of traits fulfilling this framework can translate the taking a gander at information. For instance, the information blended utilizing the section structure that lone the client with attributesa1anda2, or the client with attributea3, can decrypt the information. Regardless, the information is outsourced to the cloud; they got CP-ABE configuration ought to in addition give the running with properties:

(1) Superior: In the passed on figuring condition, clients may get to information at whatever point and wherever utilizing any gadget.[13] Right when a client needs to get to information utilizing a thin customer with kept data transmission, CPU, memory restricts the CP-ABE plot ought to be of superior. That is the correspondence expenses and checks cost's showed by the CP-ABE configuration ought sufficiently low, with the target that the client can effectively recover information from the cloud, and a while later translate it utilizing the customer.

(2) Full Delegation: In an epic scale meander with different representatives, every worker needs to ask for puzzle key from the property expert (AA), when he joins the undertaking. In the event that every single one of these authorities requires their conundrum keys from authority (AA), there will be an execution bottleneck on the authority access (AA). [14] To diminish the workload on that, some (CP-ABE) plans give key game plan between clients, which leads client to make quality confuse, keys containing his own unique subset property mystery keys for different clients. Regardless, a full course of action instrument, which can exemplify the diverse structure in the undertakings, is more often tries outsourcing information in a cloud. Full game plan deduces key undertaking between AAs, where every AA freely settles on choices on the structure of semantics characteristics.

(3) Scalable revocation: The excellence of gigantic scale attempt with high turnover rate, an versatile evident repudiation plot is needed. It can deny the information to the clients, once they are undertaking no more its workers. A client endorsement is invalidated will notwithstanding hold the keys issued earlier. [15] The consistent disavowal conspire all around requires the authorities access (AAs) to unpredictably re-encode information, and remake new mystery keys to residual embraced clients. This approach will cause over whelming work stack on (AAs). A more adaptable approach abuse the rich assets in cloud by enabling the (AAs) to appoint the CSP to re-encode information and re-convey keys to clients, under the condition that cloud service provider (CSP) knows nothing about the information and key's. In light of heretofore said examination, it required to propose an ensured information sharing course of action, which meanwhile accomplishes top of the line, full undertaking, and adaptable foreswearing. Our obligations are as per the following:

1. We underwrite a dynamic property based encryption (HABE) appear, by interfacing the changed levelled character based encryption (HIBE) framework and the CP-ABE structure. The HABE represent, which hardens the property of various levelled time of keys in the HIBE framework, and the property of adaptable access control in the CP-ABE structure, is more appropriate to the earth of attempt's sharing information in the cloud.
2. We propose a (HABE) contrive in perspective of proposed appear, which requires steady number of bilinear guided operations in the midst of unscrambling, to give tip top.
3. We propose a flexible denial plan, which licenses to appoint a huge bit of count genuine errands in renouncement the cloud service provider(CSPs) without revealing data substance, by apply middle person re-encryption (PRE) and loop re-encryption (LRE) to the (HABE) plot.

2. Problem definition

The issue is connected with a broader domain, where different SHR proprietors and customers are incorporated. The proprietors suggest patients whose therapeutic data is being secured. The clients are the general population who endeavour to get to them. There exists a focal server where proprietors put their flimsy therapeutic information, attempted by clients to get entrance. Customers approach the SHR reports through the server to examine or write to some individual's SHR, and the customer can at the same time have area to different proprietors' data. This prompts the need of Multi-Expert Attribute Based Encryption (ME-ABE).

1. Balancing activity of Unapproved Clients: An indispensable need powerful SHR get the opportunity to can't avoid being to enable "calm driven" sharing. This derives the patient ought to have a total control over their own particular thriving record. It clarifies which customers should approach their therapeutic record. Customer controlled read/form access and cancelation are the two focus security focuses for any electronic prosperity record system. Customers secured make get the opportunity to control in SHR setting appoints neutralizing activity of unapproved customers to get to the record and advancing it.
2. Fine Grained Access Control: It get the opportunity to control should be maintained as in different customers are affirmed to examine particular courses of action of chronicles. The essential objective off framework to execute secure patient-driven SHR get to and gainful key organization meanwhile. At whatever point a customer's quality isn't any more real, the customer should not have the ability to get to future SHR archives using that attribute.
3. Trademark Renouncement: This is for the most part known as quality disavowal. The SHR structure should reinforce customers from both the individual space and furthermore open territory. Since the game plan of customers from individuals by and large space may be broad in evaluate and uncommon, the structure should be exceedingly flexible, to the extent versatile quality in key organization, correspondence, computation and limit. In addition, the proprietors' undertakings in controlling customers and keys constrained to value dealing with.

3. Solution framework

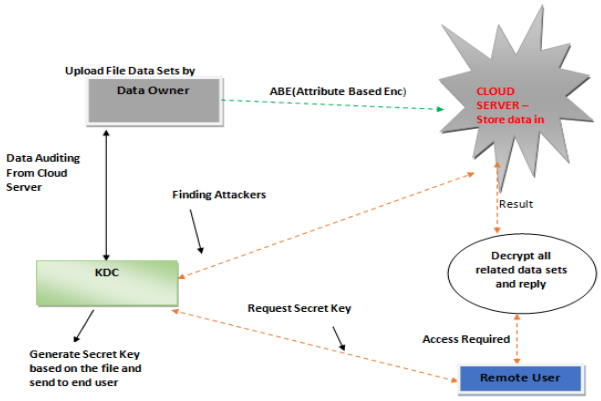
The basic objective of the framework is to give secure access of SHR in a patient driven way and competent key association. To begin with, the structure is extended into various security regions like Individual space (IS) and Open space (OS).The following entities are required for the secured sharing and accessing of SHR.

- **Data Owner:** In this module, the data proprietor moves their data in the cloud server .For the security reason the data proprietor encodes the data record and after that store in the cloud. The Information proprietor can have fit for controlling the encoded data record. Furthermore, the data proprietor can set the passage advantage to the mixed data archive. Proprietor can set the entrance benefit to the scrambled information document.
- **Cloud Server:** The cloud master association manages a cloud to give data amassing organization. Data proprietors scramble their data archives and store them in the cloud for conferring to data customers. To get to the regular data archives, data purchasers download mixed data records of their energy from the cloud and after that interpret them. It is responsible for affirming all end customers.
- **Key Distribution center:** KDC is trusted store confirmation parameters and offer open question administrations for these parameters, for example, producing mystery key in view of the document and

send to the relating end clients. It is in charge of catching the assailants.

- **Data Consumer/End User:** In this module, the client can just access the information record with the scrambled key if the client has the benefit to get to the document. For the client level, every one of the benefits is given by the Information proprietor and the Information clients are controlled by the information proprietor as it were. Clients may attempt to get to information documents either inside their entrance benefits, so malevolent clients may intrigue with each other to get touchy records past their benefits. He is sending solicitation to KDC to create mystery key and KDC will produce the secret key and send to comparing end client.
- **Attacker (Unauthorized User):** Attacker adds the malicious data to block cloud server. The Unauthorized user will considered as an attacker.

The following is the step by step procedure of how the SHR can be stored and accessed in a secure manner



ABE --- Attribute Based Encryption
Data Sets --- Personal Details, Medical Report, Medical Summary

Among the entities Data Owner is the one who uploads the singular health records (SHR) of the patients. If the data owner has to upload the SHR, he/she must register into cloud or if he is already registered he needs to sign in to share the data into cloud. During uploading of the data, when the file is selected, the contents of the file along with the file name will be encrypted using RSA encryption algorithm and the cipher text will be shown which will be uploaded. After uploading the SHR files, they are visible to cloud service provider with encrypted file names and encrypted data. If an End user wants to access the SHR files then he needs the secret key to view the files. Now the end user is asked for the filename and data owner's name and will request the key. The data owner will ask the KDC to generate the key and send it to requested end user. Now the key distribution centre will generate the secret key as per the requirement and will send it to the respective end user. Now the end user can access the required SHR record by entering the secret key generated for that file. The accessed SHR record will be decrypted using RSA algorithm and the plain text will be visible to the end user. If some un-authorized person tries to access a SHR file by entering wrong secret key then a dialog box will be shown stating that the person is an attacker and the user name along with wrong secret key that has been used will be stored in the cloud. All the transaction that are being done in this application will be stored in the cloud and can be seen by Cloud service provider.

4. Conclusion and Future Work:

In this paper, we thought about another necessity of ABE with outsourced unscrambling obviousness. We adjusted the primary model of ABE with unravelling proposed by Green et al.to join irrefutable status. We furthermore proposed a strong ABE plot with certain outsourced deciphering and showed that it is secure and obvious. Our arrangement does not rely upon unpredictable prophets. To review the practicability of our arrangement, we completed it and coordinated trials in an imitated outsourcing condition. As anyone might expect, the arrangement fundamentally lessened the estimation time required for resource limited devices to recover plaintexts. A structure of secure sharing of individual flourishing records has been proposed in this paper. Open and Individual access models are outlined out with security and confirmation empowered part. The structure watches out for the unmistakable difficulties brought by different SHR proprietors and clients, in that the trap of key association is to a great degree decreased. The structure is moved up to help dynamic methodology association.

References

[1] Li M, Yu S, Zheng Y, Ren K & Lou W, "Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption", *IEEE transactions on parallel and distributed systems*, Vol.24, No.1,(2012), pp.131-143.

[2] Foreman J, "At risk of exposure: in the push for electronic medical records, concern is growing about how well privacy can be safeguarded", *LA Times*, (2006).

[3] Boldyreva A, Goyal V &Kumar V, "Identity-based encryption with efficient revocation", *ACM CCS, ser. CCS '08*, (2008), pp. 417–426.

[4] Ibraimi L, Petkovic M, Nikova S, Hartel P & Jonker W, "Ciphertext-policy attribute-based threshold decryption with flexible delegation and revocation of user attributes", *Technical Report*, (2009).

[5] Narayan S, Gagn´e M & Safavi-Naini R, "Privacy preserving SHR system using attribute-based infrastructure", *ser. CCSW*, (2010), pp. 47–52.

[6] Chase M., "Multi-authority Attribute Based Encryption", *TCC, volume 4392 of LNCS*, (2007), pp.515–534.

[7] Liang X, Lu R, Lin X & Shen XS, "Ciphertext policy attribute based encryption with efficient revocation", *Technical Report, University of Waterloo*, (2010).

[8] Yu S, Wang C, Ren K & Lou W, "Achieving secure, scalable, and fine-grained data access control in cloud computing", *IEEE INFOCOM*, (2010).

[9] Attrapadung N & Imai H, "Conjunctive broadcast and attribute-based encryption", *Pairing-Based Cryptography–Pairing*, (2009), pp.248–265.

[10] Ruj S, Nayak A & Stojmenovic I, "Dacc: Distributed access control in clouds", *10th IEEE TrustCom*, (2011).

[11] Zhen Y, "*Privacy-preserving personal health record system using attribute-based encryption*", Doctoral dissertation, Worcester Polytechnic Institute, (2011).

[12] M¨ uller S, Katzenbeisser S & Eckert C, "Distributed attribute based encryption", *Information Security and Cryptology–ICISC*, (2008), pp.20–36.

[13] Korde P, Panwar V & Kalse S, "Securing personal health records in cloud using attribute based encryption", *International Journal of Engineering and Advanced Technology*, Vol.2, No.4,(2013), pp.95-97.

[14] Yu S, Wang C, Ren K & Lou W, "Attribute based data sharing with attribute revocation", *ASIACCS'10*, (2010).

[15] Dong C, Russello G & Dulay N, "Shared and searchable encrypted data for untrusted servers", *Journal of Computer Security*, (2010).