A SECURE STORAGE OF PERSONAL HEALTH RECORDS IN CLOUD COMPUTING USING MA-ABE

P.SIVAKUMAR
PG scholar,
Department of Computer Science and Engineering, Valliammai Engineering College, Chennai, Tamilnadu, India.
vvsiva.p@gmail.com

K.DEVI
Assistant Professor,
Department of Computer Science and Engineering, Valliammai Engineering College, Chennai, Tamilnadu, India.
devii.jeya@gmail.com

V.Deepalakshmi
PG scholar,
Department of Computer Science and Engineering, Valliammai Engineering College, Chennai, Tamilnadu, India.
deepavijay.kpm@gmail.com

Abstract- Individual wellbeing record (PHR) is a developing patient-driven model of wellbeing information trade, which is frequently sent to be put away at an outsider, for example, cloud suppliers. To guarantee the patients' control over access to their own PHRs, Multi-Authority Attribute Based Encryption is an effective technique to encode the PHRs. PHR in cloud is hard to keep up, in view of security issues in performing the read and compose operation of patient records. A Multi-Authority Attribute Based Encryption (MA-ABE) procedure is proposed to scramble each PHR document. An abnormal state of patient protection is ensured by abusing Multiple-Authority Attribute Based Encryption. It additionally gives security and versatility. To accomplish the accessibility, reliability and classification of the information put away in the cloud, the proposed framework scrambles client's information and makes utilization of the RAID (Redundant Array of Independent Disks) innovation guideline to oversee information dispersion crosswise over distributed storage suppliers. The circle disappointments are abstained from utilizing XOR (Exclusive OR)- equality check in RAID level 5. Attack level equality (RAID 5) utilizes a deletion code to produce equality data at the square level or bit level. On the off chance that any information is lost because of circle disappointment, the equality data is utilized to recreate the lost information in the fizzled plate. The proposed framework actualizes the RAID idea for PHR stockpiling model in distributed computing to give key administration and information rebuilding.

Keywords: *Cloud Computing, ABE, MA-ABE, Personal Health Records, RAID.*

I. INTRODUCTION

Distributed computing transform into predominant, more defenseless data are being concentrated keen on the cloud, for example, messages, individual wellbeing records, government reports, and so on. As of late, individual wellbeing record (PHR) has showed up as a patient-driven model of wellbeing data swap over [7]. It lets a patient to make, handle, and arrange his/her own wellbeing information in one spot amid the web, which has completed the storage room, recovery, and dispersion of the wellbeing data more proficient. Every patient has guaranteed the full control of his/her medicinal records and can impart their wellbeing information to expansive scope of clients, and also social insurance suppliers, relatives or companions. PHR proprietors need to choose seeing encryption of documents and also get to security to clients. Clients like relatives and companions can get to PHR record with proportional decoding key. The approved clients like restorative specialists, drug specialists and analysts could either need to get to the PHR for individual use and for some particular reasons as well. To keep individual heath information put away on semi trusted servers, this paper get on Multi Authority quality based encryption (MA-ABE) as the significant encryption primitive. Utilizing MA-ABE, patient have the capacity to specifically circulate his/her PHR among set of clients by encoding records under an arrangement of qualities without knowing complete rundown of clients.

1.1 Redundant Array of Inexpensive Disks(RAID)

Attack permits data to get to a few plates. Strike utilizes taking after systems plate striping (RAID Level 0), circle reflecting (RAID Level 1), redesign the equality (RAID Level 4), and plate striping with equality (RAID Level 5), striping with twofold circulated equality (RAID Level 6) and consolidate reflecting and stripping (RAID Level 10) [17].We are utilizing RAID level 5 strategy as a part of distributed computing to accomplish excess, lower inertness, expanded transmission capacity, and amplified capacity to recuperate from hard circle crashes. The RAID 5 model is utilized to parcel the capacity and copy the first information in various circles. Strike reliably circulates information over every drive in the exhibit. Strike then separates the information into reliably measured lumps (normally 32K or 64k, albeit different qualities are satisfactory). At the point when the information is perused, the procedure is turned around, giving the hallucination that the different drives in the exhibit are really one huge drive. Level 5 is the most well-known sort of RAID. By circulating equality over a few or the majority of an exhibit's part circle drives, RAID level 5 wipes out the compose bottleneck characteristic in level 4. The main execution bottleneck is the equality computation process. With present day CPUs and Software RAID, that for the most part is not a major issue. Likewise with level 4, the outcome is topsy-turvy execution, with peruses generously outflanking composes. Level 5 is frequently utilized with compose back reserving to decrease the asymmetry. The capacity limit of Hardware RAID level 5 is equivalent to the limit of part plates, less the limit of one part circle. The piece interleaved circulated equality circle exhibit takes out the equality plate bottleneck present in the square interleaved equality plate cluster by appropriating the equality consistently over the greater part of the circles [1]. An extra, much of the time disregarded point of interest to dispersing the equality is that it additionally conveys information over the greater part of the circles instead of over everything except one. This permits all plates to take an interest in overhauling read operations rather than excess plans with devoted equality circles in which the equality plate can't partake in adjusting read demands. Piece interleaved appropriated equality circle exhibit have the best little perused, vast compose execution of any excess plate cluster. Little compose solicitations are fairly wasteful contrasted and excess plans, for example, reflecting nonetheless, because of the need to perform read-adjust compose operations to redesign equality. This is the real execution shortcoming of RAID level 5 plate clusters.

1.2 Personal Health Record

The Public wellbeing operational gathering clarifies PHR as: an electronic capacity through which people can get to, handle and disperse their wellbeing data, and that of others for whom they are guaranteed, in a private, secure, and classified environment .The Personal Health Record (PHR) is an Internet-based arrangement of devices that let individuals to contact and synchronize their lifetime wellbeing data and manufacture suitable parts of it accessible to the individuals who need it. PHRs present an incorporated and finish perspective of wellbeing data, including data individuals make themselves, for example, cautioning signs and prescription use, data from specialists, for example, investigation and test outcomes, and data from their drug stores notwithstanding insurance agencies. People get to their PHRs by method for the Internet, by means of cutting edge security and protection controls, sooner or later and also from each area. Relatives, specialists or school attendants can watch parts of a PHR when crucial and crisis room staff can recover indispensable data from it in a crisis [7]. Individuals can utilize their PHR as a correspondences center point: to send email to specialists, move data to specialists, get test result and get to online self improvement instruments. PHR interfaces each of us to the unimaginable conceivable of current social insurance and gives us control over our own data.

II. RELATED WORKS

Utilizing ABE, access arrangements are communicated in light of the characteristics of clients, which allows a patient to specifically split her PHR among an arrangement of clients by scrambling the document under an arrangement of traits, without the need to know an entire rundown of clients. Growing the limit of a RAID-5 exhibit with including of plates, information must be migrated between circles to influence additional space and execution pick up.

Drawbacks

- The saved data's are in encrypted format by means of public key encryption.
- It provides a smaller amount security for data's.
- RAID-5 scaling is restricted by preserving a round-robin data distribution after adding disks.

2.1 Attribute Based Encryption (ABE)

By method for ABE, access strategies are communicated taking into account the client's properties that empowers a patient to specifically disperse their PHR amongst an arrangement of clients by scrambling the record under an arrangement of characteristics. The troubles of encryption and decoding strategies are enormously decreased utilizing Attribute Based Encryption strategy. Be that as it may, to incorporate ABE into an expansive scale PHR framework is difficult because of the on-interest denial, key administration versatility and element approach upgrades. [13]Cipher content Policy Attribute-Based Encryption (CP-ABE) permits scrambling information under an entrance arrangement, determined as a coherent mix of qualities. Such figure writings can be decoded by anybody with an arrangement of qualities that fits the approach.

a. Attribute Based Access Control

In PHR file, access methods are decided by the PHR Owner for particular actor usages. This model follows the PHR Owner have all access rights, Doctors had read and write access controls, but the patient, insurance clients and patient family members have only read access. File should be uploaded and maintained by PHR owner. The modifications of patient's records are done by doctors.

b. Secure Attribute Based Structures

Attributes describe, categorize, or interpret the datum to which they are assigned, but the traditional attribute architectures and cryptosystems are unprepared to provide security in the face of various access requirements and environments. [11]M.Pirretti introduces a novel secure information management architecture based on emerging attribute-based encryption (ABE) primitives and demonstrated a policy system that meets the requirements of complex policies. Cryptographic optimizations that greatly improve enforcement effectiveness were offered based on the needs of those policies.

2.4 Key Policy Access Control

Contrasted and the edge strategy a fine-grained access control can be accomplished in key approach techniques. The ciphertexts marked with an arrangement of traits and private keys are connected with a more summed up access control structure in key approach techniques. One of the impediments of key approach is that since access arrangements are incorporated with clients' private keys, the information proprietor has restricted control over who can decode the information. Likewise, the information proprietor must trust the key backer and utilize a trusted server to store the majority of the expressive access structure in plaintext. Goyal et al, proposed the primary key-arrangement plan (KP-ABE)[16] in 2006..

2.5 Ciphertext Policy Access Control

Ciphertext-approach is another finegrained access control. Be that as it may, characteristics in ciphertext-strategy are connected with keys while access structures are inserted into the ciphertext. With this way, the information proprietor can figure out who can decode. In addition, if the arrangement should be redesigned as often as possible, the ciphertext-strategy can be more adaptable since the information proprietor just needs to overhaul the entrance structure in the ciphertext. This makes ciphertext-strategy closer to Role Based Access Control (RBAC). In edge arrangement and key-strategy, agreement resistances are guaranteed by utilizing a mystery sharing plan (SSS) with an arbitrary polynomial for every private key. However in ciphertext-approach, SSS no more holds subsequent to the entrance structure is moved far from the key and the ciphertext is just left with properties. The Ciphertext-strategy must use a two-level arbitrary concealing system, which makes utilization of gatherings, with proficiently processable bilinear maps, to randomize the private key[15].

2.6 RAID Based Parity Method

In a bit-interleaved, equality plate cluster, information is reasonably interleaved bit-wise over the information circles, and a solitary equality plate is added to endure any single plate disappointment. Every read demand gets to all information plates and each compose demand gets to all information circles and the equality plate [1]. Therefore, stand out solicitation can be adjusted at once. Since the equality circle contains just equality and no information, the equality plate can't take an interest on peruses, bringing about marginally bring down read execution than for excess plans that disperse the equality and information over all plates. Bit-interleaved, equality circle clusters are much of the time utilized as a part of uses that require high data transmission however not high I/O rates.

III. PROPSED SYSTEM

3.1 Problem Definitions

This paper depicts a PHR framework where there are a few PHR proprietor, PHR buyers, and RAID stockpiling models in distributed computing. This paper additionally prescribes a story ABE-based skeleton for patient-driven secure dispersion of PHRs in distributed computing surroundings, under the multi-proprietor foundations. To manage the key administration challenges, we uniquely isolate the clients in the framework into three sorts of spaces to be specific Public, PHR Owner and Emergency areas. In people in general space, we make utilization of multi-power ABE (MA-ABE) to improve the security and avoid key escrow inconvenience. The circle striping and pivoted equality, RAID-5 accomplishes elite, vast limit, and information unwavering quality. To pick up a uniform information conveyance, the insignificant portions of information pieces and equality squares to be moved for RAID-5 scaling are indistinguishable to the rate of new circles.

Advantages:

- The complexities in encryption, key generation and decryption are reduced by using MA-ABE.
- XOR-parity check used to avoid of data disk failures and make the restore of the data using parity disk.

The PHR owners know how to identify personalized role-based access guidelines at some stage in file encryption. The Architecture Diagram for Proposed system is given in Fig 1.

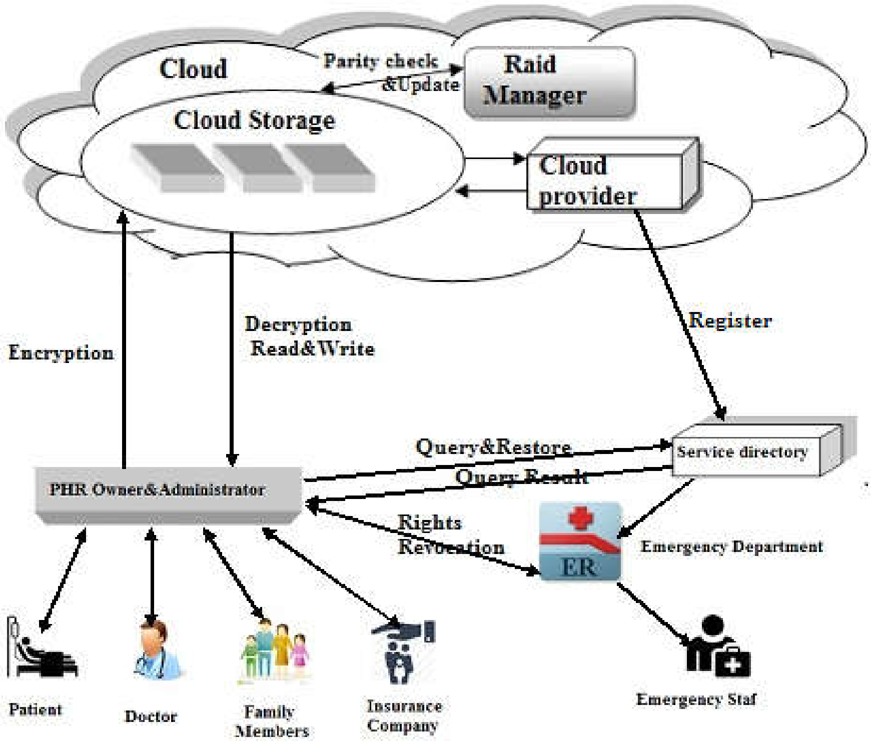

Fig 1: Architecture Diagram

Engineering outline demonstrates the relationship between various segments of framework. This chart is vital to comprehend the general idea of framework. The proposed framework engineering outline demonstrates the cloud enrollment utilizing administration index, and gets access from cloud supplier pool.

The PHR Owner gives open and private keys to getting to the PHR records by clients, specialists and patients. The crisis division needs to see the PHR records implies the authorization get from any one approved client with the distinguishing proof of crisis customers. The crisis division can read the PHR records; they can't adjust any report of the PHR points of interest. The administration index used to enlist the cloud for new clients and redesign the information's in cloud memory utilizing RAID-5 strategies.

3.2 MA-ABE Security implementation for PHR:

This framework makes utilization of MA-ABE calculation to give security to the PHR in cloud. The power traits in this framework incorporates clinic administrator, patients, specialists, relatives, healing facility staffs and crisis customers. The encryption and decoding is done in light of the entrance rights (read and compose) of the powers. Fig 2 clarifies the strides included in the MA-ABE calculation.

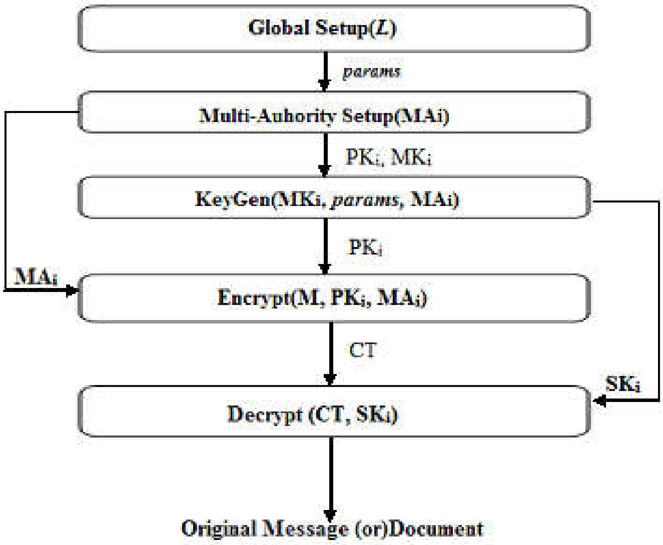

Fig 2 MA-ABE implementation flow

The MA-ABE algorithm used in this system involves four main steps viz. initializing the setup, generating secret key, Encryption and decryption. The detailed explanations of these steps are given below.

Setup:

The setup algorithm takes data and security parameters as inputs and gives Public key (PK_i) and Master key(MK_i) as outputs.

1. Global setup algorithm takes as input, Public parameter ***L*** and outputs the system parameters *params*.

Global Setup(1^L) ->params.

2. In authority setup algorithm, Multi Authority (MA_i) generates their own Public-Master key pair (PK_i,MK_i)

Multi-Authority Setup(MA_i)->(PK_i, MK_i).

Where **i** ranges from 1, 2, . . . , N.

Generating Secret Key:

The key generation algorithm takes the input public parameter value *params,*master key of attribute and multi authority structure and outputs the Secret Key(SK_i), Public Key(PK_i) for each attributes.

KeyGen(MK_i, *params*, MA_i) -> (PK_i,SK_i)

Encryption:

This method take the input message(M), Multi Authority attribute (MA_i) and each authority's Public key (PK_i) to be encrypted with and outputs the cipher text(CT).

Encrypt(M, PK_i, MA_i) -> CT

Decryption:

This decryption algorithm takes cipher text (CT) and the secret key (SKi) as input and gives out the original message (M) as output.

Decrypt (CT, SK$_i$) -> M

3.3 Ex-OR parity algorithm for RAID-5:

Parity is a form of error detection that uses a single bit to represent the odd or even quantities of `1's and `0's in the data. Parity usually consists of one parity bit for each eight bits of data, which can be verified by the receiving end to detect transmission errors.

```
If ((a=0)&&(b=0))&&((a=1)&&(b=1))
        Parity doesn't check the data
Otherwise
        Parity checks and reloads the data.
```

After checking the parity if it results in disk failure, the parity updating model retrieves the losing data.

This framework makes utilization of MA-ABE calculation to give security to the PHR in cloud. The power characteristics in this framework incorporates doctor's facility administrator, patients, specialists, relatives, healing facility staffs and crisis customers. The encryption and unscrambling is done taking into account the entrance rights (read and compose) of the powers. Fig 2 clarifies the strides included in the MA-ABE calculation.

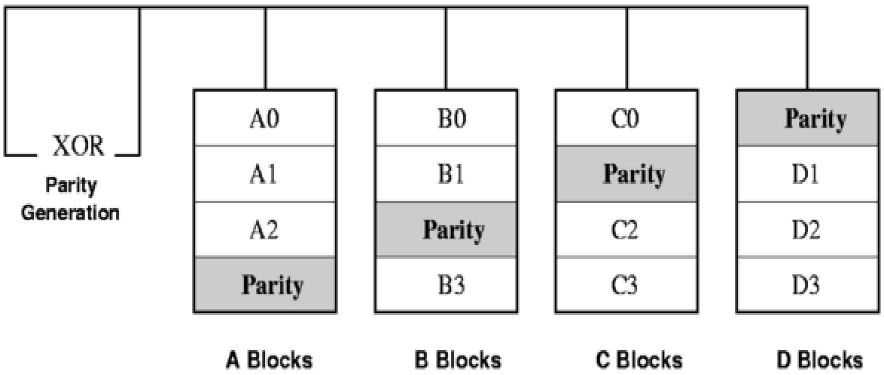

Fig 2: RAID-5: Independent data disks with distributed parity

The equality data in RAID can either be put away on a different, devoted drive, or be blended with the information over every one of the drives in the exhibit. Most RAID plans are intended to work on fall flat stop plates. Any plate disappointment in RAID (counting the equality circle) can be recouped from the remaining circles by simply performing a XOR on their information.

3.4 Parity-based Updating algorithm for RAID

Step 1: Identify a block by its zone number, strip number, and disk number.

Step 2: RAID parity block identifies the disk which is lost in the associated block Sets and then adding as many numbers of new disks as necessary.

Step 3: The amount of updating blocks is calculated using

Updating Ratio = (total num of blocks should be updated) / (total num o f original blocks).
= m/(n+m).

Where, **m** is the number of new blocks.

n is the number of existing blocks.

The failed disk is identified and it is replaced by the new disk. The data of the failed disk is retrieved using the parity algorithm and placed into the new disk.

IV. Conclusion and Future work:

In this paper, an arrangement of secure sharing of individual wellbeing records in distributed computing utilizing MA-ABE is talked about. This framework addresses the one of a kind difficulties brought by different PHR proprietors, clients and enormously lessens the unpredictability of key administration. Information maintaining so as to unwavering quality is guaranteed by RAID-5 the equality data as the XOR total of all the information obstructs in a stripe and a few squares are replicated in a stripe, without need of deleting old pieces. Later on, we will concentrate on the RAID-6 model for enhancing productivity, dependability of capacity and twofold equality in distributed computing.

REFERENCES

[1] Guangyan Zhang, Weimin Zheng, and Keqin Li, “Rethinking RAID-5 Data Layout for Better Scalability”, IEEE Transactions on computers, vol. 63, Aug 2014.

[2] Jiguang Wan, Jibin Wang, Changsheng Xie, and Qing Yang, Fellow, “S2-RAID: Parallel RAID Architecture for Fast Data Recovery” IEEE Transactions,Vol. 26, No.6, June 2014.

[3] Vijay Varadharajan, Udaya Tupakula, “Security as a Service Model for Cloud Environment”, IEEE Transactions on network and Service Management, vol. 11, no. 1, March 2014.

[4] Marian K. Iskander, Tucker Trainor, Dave W. Wilkinson,Adam J. Lee, “Balancing Performance, Accuracy, and Precision for Secure Cloud Transactions”, IEEE Transactions, vol. 25, No. 2, Feb 2014.

[5] Aijun Ge, Jiang Zhang, Rui Zhang, Chuangui Ma,and Zhenfeng Zhang, “Security Analysis of a Privacy Preserving Decentralized Key-Policy Attribute-Based Encryption Scheme” IEEE Transactions on Parallel and Distributed Systems, Vol. 24, No.11, November 2013.

[6] Daniel Fitch, Haiping Xu ,“A raid-based secure and fault-tolerant model for cloud information storage”, University of Massachusetts Dartmouth North Dartmouth, MA 02747,USA, April 2013.

[7] Ming Li, Shucheng Yu, Yao Zheng, “Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption”, IEEE Transactions on Parallel and Distributed System, pp. 131-143, 2013.

[8] Alexandru Iosup, Simon Ostermann, M. Nezih Yigitbasi, Thomas Fahringer, “Performance Analysis of Cloud Computing Services for Many-Tasks Scientific Computing”, IEEE Transactions on Parallel and Distributed Systems, vol. 22, no. 6, June 2011.

[9] Qian Wang, Cong Wang, Kui Ren, “Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing”, IEEE Transactions on Parallel and Distributed Systems, vol. 22, no. 5, May 2011.

[10] Guangyan Zhang, Weimin Zheng, and Jiwu Shu, “ALV: A New Data Redistribution Approach to RAID-5 Scaling” IEEE Transactions on Computers, vol. 59, No. 3, March 2010.

[11] M. Pirretti, P. Traynor, P. McDaniel, and B. Waters, “Secure attribute-based systems,"Journal of Computer Security, vol. 18, no. 5, pp. 799-837, 2010.

[12] J. Hur and D. K. Noh, "Attribute-based access control with efficient revocation in data outsourcing systems,"IEEE Transactions on Parallel and Distributed Systems, vol. 99, 2010.

[13] L. Ibraimi, M. Petkovic, S. Nikova, P. Hartel, and W. Jonker, “Ciphertext-policy attribute based threshold decryption with flexible delegation and revocation of user attributes,” 2009.

[14] L. Ibraimi, M. Asim, and M. Petkovic, "Secure management of personal health records by applying attribute based encryption," Technical Report, University of Twente, 2009.

[15] J. Bethencourt, A. Sahai, and B. Waters, “Ciphertext-policy attribute based encryption,” in Security and Privacy, 2007. SP’07. IEEE Symposium on. IEEE, 2007, pp.321–334.

[16] V. Goyal, O. Pandey, A. Sahai, and B. Waters, “Attribute-based encryption for fine-grained access control of encrypted data,” in Proceedings of the 13th ACM conference on Computer and communications security. ACM, 2006.

[17] http://www.webopedia.com/TERM/R/RAID.html.