Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 04, April-2020

Identity based Data Sharing and Profile Matching using Probabilistic Key in Cloud

Reshmi Paul
Department of Computer Science and Engineering,
SRM Institute of Science and Technology,
Chennai, India.

Dr. A. Jeyasekar
Department of Computer Science and Engineering, SRM Institute of Science and Technology,
Chennai, India.

***Abstract*:- Cloud technology is popular since the utilizations and their information are expanding hugely step by step. It gives usefulness to overseeing data information in a conveyed and pervasive way supporting many platform. Data sharing and security problem are the principle issue to the increasing use of health care, since health information is delicate. However issues, for example, risks of privacy exposure ,versatility in key administration, adaptable access and effective uses denial always been the most significant difficulties for accomplishing good-grained cryptographically upheld information access control. Right now structure a protected information move and profile coordinating plan with probabilistic open key encryption in correspondence test to diminish the size of open key which helps in decreasing the capacity and furthermore time productive. Our probabilistic open key encryption plot when executed in a bilinear gathering, it can check whether two figure writings are scrambled of a similar message. Strangely, in encryption or decoding system bilinear mapping isn't required in Public Key Encryption conspire except if when individuals need to do in fairness test between two figure messages that might be produced utilizing diverse open keys. Additionally the profile coordinating component dependent on Probabilistic Public Key Encryption with fairness test(PPKEET) causes patient to discover companions in a security saving way with age of trapdoors and structure social connections as indicated by the desire. The security examination and trial results demonstrated that our plan is ensuring the information and giving right medicine in cloud**.

Index Terms:- Data security, health information secure, profile matching, re-encryption

I. INTRODUCTION

The essentials for capacity and nonstop accessibility of e-Health information require the usage of the cloud computing administrations. cloud computing is creating as a promising point of view for registering and is drawing the thought from both academia and industry. The cloud computing model moves the figuring foundation to outsider specialist organizations that manage the equipment and programming assets with vital cost diminishes.

cloud computing has exhibited unfathomable potential to improve joint exertion among various health associations and to fulfill the ordinary necessities, for instance, scale, deftness, cost sufficiency, and accessibility. Moreover, development of patient wellbeing records to the cloud storage reduces the social insurance suppliers from the infrastructure tasks.

Inspite of the reality there is no standard meaning of the e-Health cloud, it might be considered as a stage that, other than taking care of enormous volumes of the wellbeing information, in like manner fills in as an organized administration of the wellbeing information over different health services suppliers. The wellbeing information can also be extricated from different databases for medications and other diagnostic purposes. Normally, the cloud involves layered components, for instance, physical capacity, correspondence foundation, application, and correspondence framework. Moreover, the e-Health cloud foundation may be:

(a) actualized inside by the human services supplier (private),
(b) kept up by some outside gathering (public),
(c) or is kept up by the human services supplier and outside gathering together (cross breed).

Without mindful idea, patients may encounter the genuine medical data spillage from the cloud.

For example, a considerable number of Electronic Health Records have been undermined lately. Consequently, it is noteworthy that the EHRs ought to be put away in an encrypted form. Regardless
of whether the CSP is untrusted or traded off, the data keeps up security and privacy All the while, the encrypted records ought to be shared in a sensible way. In light of likely divulgence of medical data records put away and traded in the cloud, the patients concerns ought to basically viewed as when structuring the privacy mechanisms.

Different methodologies have been utilized to prevent the privacy of the health data in the cloud surrounding. Now, there are many techniques utilized to save data security in MHSN, such as public-key encryption (PKE), identity-based encryption (IBE), identity-based broadcast encryption (IBBE) and attribute-based encryption (ABE).

In an IBBE framework, user progressively choose particular gathering of clients, and encrypt the data accordingly just authorized users can decode is a significant crude of ID-based cryptography. All things considered it is a type of public key encryption where the public key of a identifier is some different data about the identity of the user (for example a user's email address). This implies a sender who approaches the public parameters of the framework can encrypt a data for example the text of the receivers name or email address as a key. The receiver finds its decryption key from a central authority, which should be believe as it produces secret keys for each user. In PKE system, Public-key cryptography, or asymmetric cryptography, is a system that uses number of keys: public keys which may be spread

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 04, April-2020

widely, and private keys which are known only to the authority.

The creation of such keys verifies on cryptographic algorithms based on mathematical demands to form one-way functions. security only requires keeping the private key private; the public key can be openly used without compromising security.

In PE method, probabilistic encryption is the use of various in an encryption algorithm, so it will usually yield differen t ciphertexts when encrypting a similar message many time s.it in general, yield various ciphertexts. The term "probabilistic encryption" is normally utilized in similar to public key encryption algorithms, anyway different symmetric key encryption algorithms accomplish a same thing(e.g., block ciphers when utilized in a chaining mode, for example, CBC). To be assure, that is, to hide away even partial data about the plaintext, an encryption algorithm must be probabilistic .

The patient can fill up their encrypted health record to server with IBBE method and offer their disease report with authorized doctor in a protected and efficient way. We present data re encryption construction with attribute based condition which allows the doctor to contact with specialist to recommend him as indicated by the disease. Thus, the re-encrypt the ciphertext with a secret key. During the technique of data sharing, the patients might need to make clients who have same disease with in server. Assume that Bob experiences headache and stomach pain, yet he needs to find a friend who has a headache. At that point he will produce a trapdoor on headache and send it to the server. The server will provide the profile match algorithm not known with the exact information. The server sends the similar results to Alice and Bob, so both can built relationship.

In this phenomena, a secure and safe information sharing and profile matching scheme for cloud computing is verified. Compared with the other version of this paper there are some contributions: (1) Reducing the storage size and the size of the trapdoor key. (2) data is encrypted and re encrypted for strong security, The remaining of the paper is as :

1.Introduction **2**. Related work **3**.we introduce scheme overview **4**.detailed construction **5**.experimentalresults **6**.conclusion

II.RELATED WORK

The work is for the most identified authorized access for outcoming information and probabilistic based encryption with identity based encryption for securing data transmission.. To improve upon one to many encryption methods, for example, IBE can be used. In International journal of pure and mathematic paper on IBE[1] , a user can send a trapdoor to the server where the server searches for encrypted data deployed by the identifier to find whether encryptions are of same plaintexts. In IEEE transaction paper on personal health data in cloud using ABE[2],depicts on the several data owners and leverage. Addition we perform test with probabilistic public key to achieve flexible authorization.

A .Health record preservation

A central security of EHRs ought to be encrypted to ensure data privacy. Numerous plans were proposed to gurantee data security in cloud. Assad et al.[3] introduced to include the condition of workmanship security saving methodologies in e-wellbeing mists. Additionally, the privacy preserving methodologies are gathered into cryptographic and non-cryptographic. Barua.[4] proposed ESPAC which similarly utilizes ABE to receive tolerant driven control. Liu et al.[5] introduced EHR which licenses data authority to complete most encryption algorithm make the ciphertext with extremely less cost. correspondingly with arrangement ,ABE based ideas [6][7] likewise redistributed expensive calculation to CSP to less overhead of client side.In request to make sure about EHR many schemes were proposed on cloud and IBE schemes were one of them as this mechanism utilizes unique id as the public key and less the computation cost of patient. ceceile *et al*[8] propose first public key broadcast encryption scheme which implies that the size of ciphertext and that of private key are small constants. However, these schemes may said same encryption when there are a various of accessors.

B .Identity based encryption with ciphertext and public keys

The algorithm IBE was proposed by Ming Li .[2] which performs IBE with equality testing by using the concept bilinear pairing. The computational cost and performance has been proved and it is better than the past achievements. Zing *et al*.[5] proposed an IBEET scheme with bilinear pairing, which less the need for time-less Hash To Point function. Each IBE function has been performed for computational cost. where Ming Li et *al*.[2] characterize single direction picked ciphertext against from a picked personality assault. .Moreover X.An *et al*.[8] proposes the public key is of size small in the maximum size m of arrangement of receivers, which is smaller than the quantity of possible clients in the framework and the system does not have to be fixed in the setup. However little attention has been diverted on all searchable encryption methods proving IBEET to be more practical solution in coming years for efficient searching and security in cloud. The work includes reducing the size of trapdoor and public key which helps in reducing the storage size.

C.Profile similarity in cloud

Profile matching is a proficient method for comparing at changed clients, individual profiles in cloud and social communities. Two standards ways were verified. The main way considers the client data as a lot characteristics and the subsequent route dependent on secret sharing and homomorphic algorithm. It proposed a private coordinating data in social community, which subtle among clients and says a range of matching schemes . and also a new privacy preserving profile matching based on symmetric encryption without trusted third party.

Inspite of an spy can do the test on any ciphertext without authorization ,it may release more data. which permits the client to control the difference of its ciphertext with others. Hence provider need to execute the test algorithm according to policy.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 04, April-2020

III. SCHEME OVERVIEW

D. System model

Our proposed scheme based on data sharing and profile matching model in cloud is appeared in fig 1 include five substances : central authority, cloud service provider , patient, Doctor, Specialist

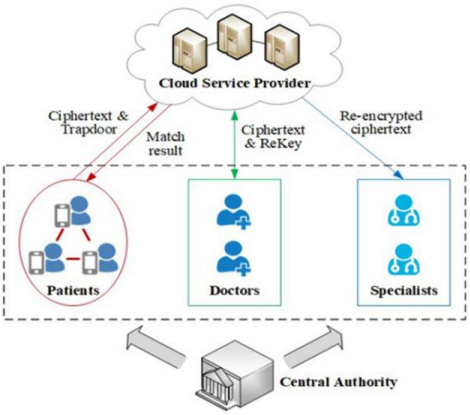

Fig 1

Central authority

The central authority is based for initializing the attribute keys and secret keys for clients.

Csp

The csp is applied for data store and keeping the details of all keys of users in protected manner

Patient

The patients update their details and get secret keys with their personalities. They encode record utilizing IBBE technique to server and approved doctors could decrypt them. Similarly, patients with similar symptoms can create trapdoors and create connections as indicated by their wish.

Doctor

Approved doctors can decrypt the patients ciphertext that is in server. while experiencing with an issue that required to counsel with a specialist, the doctor can create a re-encryption request and in this way the server changes over the ciphertext into an IBE-encrypted structure for the specialist.

Specialist

The specialist decode the re-encrypted ciphertext with secret key gave by the doctor and afterward he can assist his recommendation. During the procedure, the patients might need to make friends to other people who have similar disease through server and they would prefer not to release their private data.

E .Overview of framework

The aim of project is to safe data transfer between the patient and doctor and in the scheme of profile matching the trapdoor key size should be smaller in size .So the whole overview has been implemented in this way:
user/ patient have to register their personal information like name, mail ID, mobile number and their disease. Doctor's in the same way will register their details. Those details of doctor and patient will be stored on database and server. After registration user/Patient/Doctor will get user ID and password to access the application. So, when the patient will register herself/himself, he/she can see the doctor's profile and can send a request according to their choice. To access the hospital records we are creating user Id and password for authentication

The patient and doctors register in the framework to acquire their secret keys. The patient encrypt the EHRs utilizing IBBE algorithm and outsourced ciphertext to server, subsequently just approved doctors could decode them. The IBBE scheme comprises of public key of less size in the maximum size m of the arrangement of users, which is smaller then the quantity of possible clients in the framework encoded under a short symmetric key. In addition in our plan the Private Key Generator(PKG) can progressively provide new individuals without adjusting recently appropriated data. we will implement Diffie-Hellman key exchange process where the key that will be generated in server and the key that will generate after the request sent by the patient to doctor will be same. Doctor and Server are both publicly available numbers. Suppose, server and doctor generate their own private key and changed it publicly, the next person received the key and from that produce a secret key after which they have the similar secret key. The doctor will use that secret key to decrypt the file.we are implementing the accessing process for users as well as Doctors. Both patient and doctor have user id and password to access the file .System will check their id and password. If it matches then they can view the details otherwise server will provide decoy file which will contain false data and it will display to confuse the unknown person and alert will be send to both doctor and patient. we are using steganography which is the practice of ,matching a file, message, or video within different file ,image or video. These will be hiding patient's personal information and their report about disease. So, only the access doctor could see all the report ,image and videos. After receiving the patient report in ciphertext the authorized doctor decrypt it and want to negotiate with a specialist while encountering a problem .

Now, the doctor can produce a request to server and thus the server will convert ciphertext into an IBE-encrypted information for specialist. Meanwhile the doctor will generate a secret key for the specialist with whom he want to consult. The specialist could decode the re-encrypted request with the secret key send by the doctor and assist his advice and directly he will send it to the patient. If the doctor

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 04, April-2020

wants to discuss with the specialist to generate the secret key he need to run re key algorithm .During the procedure, the patient need to make friends up to other people who have similar symptoms through server and they would prefer not to release their private data. In this process both the patient encrypt their EHR respectively and meanwhile they generate the trapdoor on the ciphertext respectively. The server could run the profile match mechanism not knowing the particular data .Suppose one patient is suffering from two types of problem but only when he wants to find a similar client has the same type of problem from the two types. Then he will create a trapdoor for that disease and will send it to the server. The patient can apply a trapdoor on one side of their ciphertext according to their wish. Now to generate trapdoors we have to perform equality test with cryptographic algorithm. Let user A wants to check about his condition and he search for people with similar symptoms. This is done by generating trapdoor where the user sends his IDA and intermediate private key. Trapdoors are those which act as one way function and its output is used to perform equality test on two cipher texts. The server uses the Identity, Trapdoor function and encrypted message of this user and check for equality. If match found they return true and if not it returns false.

IV CONSTRUCTION

F. Key generation

Right now, our development for PPKEET by 2-level HIBE plans and sign plans. In the future, [ID1.ID2] means an identity of a 2-level HIBE scheme HIBE = (Setup, KeyExt, Encryption, Decryption)where ID_1 is the first level character and ID_2 is the next level chracter. $[M_0 \| M_1]$ denotes the concatenation of messages M_0 and M_1.

Our strategy: In our development, to help an equality test, on utilizing a 2-level HIBE scheme rather than an IBE scheme. For given a mark plot Sig = (G, S, V) and a 2-level HIBE conspire HIBE = (Setup, KeyExt, Encryption, Decryption), the given encryption process for a message M is as per the following: 1) G(λ) → (vks, sks), 2)E nc(mpk, [0.vks], M) → C0, 3) E nc(mpk, [1.vks], H(M)) → C1 for a hash func-tion H, 4) S(sks, [C0‖C1]) → σ, and 5) yield ct = (vks, C0, C1, σ).A ciphertext includes two ciphertexts C_0, C_1. of the basic HIBE conspire. The previous is an encryption of the message, so it empowers to acquire the specific message by decrypting it utilizing a decryption key for the personality [0.vks]. Then again, the latter is an encryption of a hash value of the message, so it empowers to play out a equality test by decrypting it. utilizing an decryption key for the character [1.vks] and contrasting of different ciphertexts.

Description

We give a idea of our PPKEET construction below.

Setup(λ) : A protected parameter λ, generate

1. a 2-level HIBE conspire = (Setup, KeyExt, Encryption, Decryption),

2. a hash work H : {0; 1}* □ M for the message space,

what's more,

3. a computerized plot Sig = (G, S,V).

framework parameter params = {H, HIBE, Sig}. We verifiably set

the message space of our PKEET plan to the message space M of HIBE.

- KeyGen (params) : On input params, it runs Setup(λ) □ (mpk, msk) and yields an public key pk = mpk and a secret key sk = msk Encryption(pk, M) : Inspite to prevent the security of data M the patient runs encryption algorithm.
It takes pk and a message M ε M as inputs and runs
1. G(λ) → (vk_s, sk_s),
2. Enc(pk, [0.vk_s], M) → C_0,
3. Enc(pk, [1.vk_s], H(M)) → C_1, and
4. S(sk_s, [C_0 || C_1]) → σ.
It outputs a ciphertext ct = (vk_s, C_0, C_1, σ).
Decryption(sk,ct) :The doctor receives the decryption key. On input ct, parse ct to (vk_s, C_0, C_1, σ). Then, it performs as follows:
1. Run KeyExt(sk, [i.vk_s]) → $sk_{[i.vks]}$ for i = 0, 1.
2. Decrypt C_0 and C_1 by running Dec($sk_{[0.vks]}$, C_0) → M' and Dec($sk_{[1.vks]}$,C_1) → h'.
3. If h' = H(M') and V(vk_s; [C_0||C_1], σ) → 1, t M'.
Otherwise,
output ⊥.
Td(sk_i) : It takes a identifier U_i's secret key sk_i as an input, provide KeyExt(sk_i,1) → $sk_{i,1}$, and outputs td_i = $sk_{i,1}$.

-**Tes**t(td_i, ct_i, td_j , ct_j): It takes trapdoors td_i , td_j and ciphertexts ct_i , ct_j for
users U_i , U_j , respectively, as parameter. For k = i, j,

1. parse ct_k to ($vk_{s,k}$, $C_{k,0}$, $C_{k,1}$, σ_k),
2. run KeyExt(td_k, [1.$vk_{s,k}$]) → $sk_{k,[1.vks,k]}$, and
3. run Dec($sk_{k,[1.vks,k]}$, $C_{k,1}$) → h'_k.

If $h'_i = h'_j$; then comes 1. Otherwise, 0

G. Profile matching

The server determines whether the cipher texts contain similar information as indicated by the approval.

STRATEGY

- a_i an attribute used to indicate a profile,
- P 1.$a_i$andP 2.a_i are estimation of an attribute a_i in Profile P1 and Profile P2,
- w (a_i) the computed/assigned character of an attribute [0, 1], ∈

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 04, April-2020

sim (P 1.a_i, P 2.a_i) the same score computed be-tween the character of an attribute in P1 and P2 ∈ [0,1],
sim^l (P 1.a_i, P 2.a_i) the new same score computed the values of an attribute in P1 and P2 ∈ [0,1],

The new same scores of all attributes are sent to a decision making algorithm. The task of this algorithm is to return a identity, v. This is shown in Algorithm 1.

Algorithm1: Deciding whether two profiles contain the same cipher text
Input: p1,p2: profile of user 1 and user 2
P1.ai and p2.ai are two character of an attribute ai in

```
1 begin
  2 for each ai in (P1,P2)
  3 do k[ai] = sim^l (P1.ai, P2.ai)
  4   end
    5  D= f (k)
    6 if D>th so
       R=4
   7 end
```

V.PERFORMANCE EVALUATIONS

H.Functional comparison

We differentiate our scheme with IBEET ideas in terms of data preservation, profile matching and flexible authorization.

Functionality	B.abinya[1]	Ming Li[2]	L.Wu [3]	Y.Liu[5]	X.An [8]	Our scheme
Data security	IBBE	IBE	IBE	IBE	ABE	IBE
encryption	No	No	No	Yes	Yes	IBE
Re encrypted data security	IBE	_	_	PKE	ABE	Access policy
Profile match	_	_	Yes	Yes	_	Yes
Flexible authorization	_	_	Yes	Yes	_	Yes

Table I flexible authorization

Despite the fact that X.An et al[8]achieves approval ,the approval token is created by two clients, which may not be applicable in cloud. Ming et al[2] the client need to pick the information must match to the wishes by various trapdoors.

I. Experimental Results

The experimental results of trapdoor key size depicted in the following table

schemes	Trap gen 1	Trap gen 2	Test 1	Test 2	Test 3
Ming Li[2]	0.0136	32.0129	75.7607	45.2521	12.6613
L.Wu[3]	0.0103	-	63.3425	-	-
Y.yang[7]	0.0213	-	75.7607	-	12.6613
Our scheme	0.0167	5.4256	62.0126	58.1099	51.4712

VI.CONCLUSION

First provide data preservation in cloud with IBBE scheme, which allow patient to put EHRs to server protectively and share them with doctor efficiently. Then we provide data re - encryption technique which allows doctor to change the stored ciphertext into a new ciphertext under IBE, for the specialist, not changing any data. Furthermore, we add a profile matching system based PPKEET which can achieve authorization and help users to find same users in a protected and efficient way.

REFERENCES

[1] B.Abinaya ,C.Mahalakshmy, A.Srilakshmi "Identity Based Encryption With Equality Test For Efficient Search On Cloud Data",in int. journal of pure and mathematics,2018,224-233"
[2] Ming Li Shucheng Yu,"Scalable and Secure Sharing of personal Health Records in cloud computing using Attribute-based Encryption" IEEE
[3] transact on parallel and distributed system.,vol.1,.2013".
[4] A.Abbas and S.U.Khan,"A review on the state-of-the-art privacy preserving approaches in the e-health clouds," IEEE J. Biomed. Health Informat.,vol.18,no.4,pp. 1431-1441, Apr.2014."
[5] M.Barua, X.Liang, R.Lu, and X.Shen, "ESPAC:Enabling security and patient-centric access control for eHealth in cloud computing," Int,J.Secur.Netw.,vol.6, nos.2-3,pp.67-76,2011."
[6] Y.Liu,Y."zang,J.ling, and Z.Liu,"Secure and fine-grained access control on e-healthcare records in mobile cloud computing," in proc. IEEE INFOCOM,San Diego,CA,USA,March.2010,pp.1-9"
[7] Y.yang,X.Liu, R.H.Deng and Y.Li,"Lightweight sharable and traceable secure mobile health system,"IEEE Trans.Dependable Secure Comput.,to be published, doi: 1109/TDSC.2017.2729556."
[8] Y.Yang, X.Liu, and R.H.Deng,"Lightweight break-glass access control system for healthcareInternet-of-Things,"IEEEtrans.Ind.Inform.,to be published, doi:10.1109/TII.2017.2751640"

AUTHORS PROFILE

Reshmi Paul, is currently pursuing Master's Degree in Computer Science and Engineering at SRM Institute of Science and Technology, Kattankulathur, Chennai, India. She pursued her Bachelor's from Satyabama, TN. Her areas of interests is Cloud Computing.

Dr. A. Jeyasekar is an associate professor of Computer Science and Engineering at SRM Institute of Science and Technology, Kattankulathur, Chennai, India. He earned his PhD in Heterogeneous Network from SRM, Chennai, India. He has over 13 years of experience in Teaching and Research. His areas of interests are Internet of Things and Software Engineering.