Dynamic Federation in Identity Management for Securing and Sharing Personal Health Records in a Patient-centric Model in Cloud

Ramkinker Singh[1], Vipra Gupta[1], Mohan K.[2]
Final year, Computer Science and Engineering[1] and Professor, Computer Science and Engineering[2]
Vellore Institute of Technology (University),
Vellore-632014, India.
ramkinker1@gmail.com[1]
guptavipra@gmail.com[1]
mohan.k@vit.ac.in[2]

***Abstract*—Cloud computing today is widening its wings in all fields, where a Personal Health Record is coming up as an important area of interest. But due to sensitivity of the records stored, security and efficient sharing methodology is the need of the hour. Patient information stored in a third party i.e. Cloud service Provider (CSP) needs to be accessed by different domains of user, needing different level of information. We are proposing Attribute Based Encryption (ABE) to provide the user only the necessary information and distributing the key of those attributes. Also, Hacking of user profiles is a common scenario, so to further strengthen the security of PHR we introduce A Trust based Dynamic Reputation Architecture. Trust based system restricts the access of crucial data using dynamically calculated reputation. CSP first authorizes the user using its identity and trust before providing it the encrypted PHR.**

***Index Terms*— Dynamic trust management, Attribute based encryption, Cloud Computing, Fine-grained access control, Identity management, Personal Health Records, Privacy, Data Privacy.**

I. INTRODUCTION

Development in the fields of shared computing, service oriented architecture and web services have led to the birth of cloud computing. It provides a combination information, software and computing power which are available in different locations over a network, providing services by offering resources which are scalable, robust, keeping in mind the affordability [4]. With this advancement along with the one in health sector, digitalization of Personal Health Record (PHR) is gaining a lot of importance in recent years. Cloud provides both software-as-a-service as well as storage-as-a-service; these features further extend the development of health sector on cloud. Clients (patients) no more want to carry their big file of medical history, they want an easy access their data from anywhere they are. To satisfy this demand, new technology has emerged

To store data on network specifically on cloud database so that a client can create his profile or account, edit it and even change the user access permissions. The users of PHR are widely divided into two categories, personal and professional. Personal users may be friends, family, relatives on the other hand professional users are research scholars, doctors, insurance company etc. The users from latter category are more diverse and hence to get access to a patient's PHR patient's permission is mandatory. Thus it provides a patient-centric architecture.

In this complicated environment, security and identity management issues need to be addressed, given the given the dynamic nature, heterogeneity and distribution of data present. For this scheme, federated Identity Management (IdM) has come up as an imperative technique to implement the global scalability which is needed for the working of cloud technology. Also, protected allotment of decryption key to trusted parties is also crucial. When patients' data is stored on a cloud, patients control over his medical information is lost. Thus, Patient-centric model is constantly emerging as an intimate part of sharing information with user domains. It not only provides the client with full control over his data but also over its access permissions. Secondly, with the increase in the number of malicious attacks, the data is never secure. The only viable solution to this problem is encrypting the data on the client side, and then storing it in the cloud. To give full control to the client over his data, the encryption policy should be fine grained, as well as the user should be able to give permission as well as revoke it whenever he feels necessary [5]. We will be considering our server as a semi-trusted party thus to deliver a fine-grained approach encryption technique used is Attribute Based Encryption (ABE)[6].In ABE, the data is encrypted based on its attributes, and the decryption key is generated for each attribute. Thus client has full control over his PHR and its sharing among potential users providing only that information which is sufficient for each user domain, keeping the rest transparent. Hence, the client does not have to create a key for

each and every user, but just have to specify a key for each domain of user dividing them into different categories for various user domains. Also break-glass access for emergency personals during a critical situation and revocation of key from user is also supported. Also, number of attributes is directly proportional to the management, distribution and revocation of key.

In recent time, SSO has been widely recognized and used, because user only needs to login once instead of logging in for every service, but when these services are mutual between different service providers i.e. in a federated environment, just SSO is not sufficient. This calls for identity management, where service providers integrate and share their identities over a secure network.

A client in a private cloud can use community cloud's applications if there is a trust relationship between them, even if they use different types of client's identities. Multi-provider and multi-service environments are provided by the cloud, applications fuse the data and services provided by different clouds, which follow different policies of service, privacy terms and locations. Therefore, we need to change the trust of a client according to the algorithm, so as to achieve dynamic trust as a static trust will put client's information at risk due to the dispersed and overt nature of cloud ecosystem. Trust layer is included to focus on reputation manager, to allow secure communication between unknown parties. Trust acts as a second level key for access between unknown parties. Trust is dynamically calculated based on historical data, accesses, trust statements from other parties etc. Hence the complete PHR data is secured.

The ECP has been used to provide a user-centric approach for cloud computing applications in consumer electronics devices. It reduces the interaction between SP's and IdP's by providing full control over its identities thereby improving privacy. Now using the concept of consumer cloud environment along with Personal Health Record we can build a trusted and secure model with minimum or no attacks. This new model would incorporate the features of encrypted PHR along with the versatility of federated identity, to provide a framework for trusted and secure distribution of sensitive data over multiple clouds.

II. RELATED WORK

This section will be discussing about the technologies and methodologies being used in health related clouds and other fields, for providing a user friendly, multi-user secure access. We will be talking about the types of access controls, the encryption methods, identity provision protocols, security control.

A. Traditional access control for EHRs-

In the traditional systems the EHR was stored on the CSP, which gave full authority to CSP over its access control and data.

There are various proposed models, including attribute-based access control (ABAC) and role-based (RBAC) [7]. In RBAC [8], the role of user and the associated privileges are used to determine the user's access right. The role concept in RBAC is broadened to attribute by ABAC like resource, entities and environment's properties. ABAC is more favourable than RBAC because of its flexibility in policy descriptions [7]. However the CSPs cannot be trusted with the sensitive PHR. Therefore fully patient-centric system cannot be realized because the patient loses the physical control over its data. Hence the PHR needs to be encrypted.

B. Enforcing access control of outsourced data through cryptography

In these techniques the servers are taken as partially trusted. Fine grained encryption is used to restrict who has the read permission for which attributes.

Solution based on Symmetric key cryptography (SKC). Vimercati et.al gave a symmetric key derivation method based solution for semi-trusted servers to secure the outsourced data [9], it achieves fine grained access control. In [10], For efficient key distribution, hierarchical model for arrangement of PHR files is used. In [11], the data of the client is encrypted block by block, and a tree is constructed to minimize the no of keys. In this scenario if the number of users are more than then managing becomes difficult, as well as the key distribution is a big problem.

Other solutions included public key cryptography because they separated the user's read and write privileges. Benaloh et.al. [10] Proposed HIBE (hierarchical identity based encryption) which had high key management overload.

SKC and PKC(Public key cryptography) all suffer from low scalability because it's based on one-to-one encryption technique, whereas each PHR might have a large number of users. So to get rid of these types of problem, improving efficiency is very important. Hence attribute-based encryption [12] is used, it is one too many based encryption type. In ABE [6], a set of users characterized by attributes is given a set of data using encryption. This was used by several works then to outsource data [13][14][15][16].But still in a multi-owner PHR, patient-centric access control is still missing. In [17] all user's and patients are controlled by a single authority, but in this scenario also authority has keys for all owner's thus, still no privacy is guaranteed.

C. Identity management in cloud computing

Even though there have been many advancements in fields of authentication and authorization using user-centric approach in the areas of media sharing, cloud services, and personal content none of them deals with dynamic federated identity management. paper [18] provides a methodology of authentication in consumer electronic devices, by giving the permissions to the user to share their content rights and services in secure and trusted environments, temporarily. The zero-knowledge proof methodology preserves user's privacy while providing him his identity. But, dynamism in trust relationship management is not addressed in this process. For virtual machine user authentication, Zero-knowledge proof techniques can be used as given in [19]. It proposes an active bundle scheme called IdM wallet, for securing personal user information from untrusted parties, using entity-centric model. This paper addresses issues like trust and privacy using trust evaluation model and audit services model.

D. Dynamic federation between cloud providers

Though being realised as a crucial link in usability and scalability, my important aspects are still to be addressed in dynamic trust establishment. Though In [20] a SAML based three-phase cross-cloud federation agent technologies and model is proposed, but establishment of trust between unknown parties is not given. Also, the developing next generation computer application is the base for distributed environment trust management peer-to-peer systems [21]. In the technique [22] trust values are found based on personal dependencies in a community using reputation based on local and global scope.

E. Confidentiality

Confidentiality management is an important for aspects, client's trust and legislation when he tries to access consumer cloud computing. While legislation in different geography may have different rules, but broad privacy principles specified in [23] are applicable in most parts. The author has given many suggestions and techniques to make a privacy aware IdM architecture like specifying and limiting the usage of user data and reducing the amount of information sent to and stored in the cloud, allowing user choice, maximizing user control, providing the customer with privacy feedback and protecting sensitive customer information. In [19] many principles are used for managing the disclosure of identities. Also, for mitigating issues like frauds, identity misuse, unauthorized access to personal data etc and consumer cloud scenarios, Fair Information Principles [24] can be applied. Second issue to be addressed is the cross-site sharing and tracking of data collection mainly used by advertising or personalization. Using this track data stored at a trusted cloud provider can invoke doubt in user. Federal Trade Commission [25] has pointed out the user's right to opt out of Web tracking. Hence, we can say that still many issues on privacy in consumer cloud that are needed to be addressed. In cloud scenario, critical privacy issues demands the need for faithful digital identity infrastructure which is nicely pointed out by the author in [26]. Also, in [27] we can find a fine example on preserving user's privacy in consumer electronics and how cloud computing technologies can help in it. It gives a technique to maintain user's privacy while exchanging EHR in a cloud platform, but access issues to this data and not fully addressed.

III. PROBLEM DEFINITION

Personal Health Record (PHR) is basically to digitalise the health related data, where in the client i.e. the patient stores his information into a database provided by the cloud service provider. He creates his PHR account which he can update and delete freely without any restrictions. There will be many variety of users for this data like acquaintance, doctor, researcher etc. our client might want to disclose only a part of his data, which may also be different for different set of users. To make this transaction smooth, safe and secure we will are proposing identity management along with encryption. Users will also be having access right for many patients, and thus there must be some trust and reputation of each user to indicate about his trustworthiness. Also client may have his account on different SPs, thus giving rise to cloud federation.

Here we are considering our SP partially-trusted entity, i.e. it follows all the protocols and procedure but at the same time want to read the data stored in its database [28] [29]. This is not the only problem, sometimes some user, even after having an above threshold trust, might get compromised and tries to gain access of data which is out of his range. to combat these problems and many more, we have many technologies, techniques coming up like SAML v2, OAuth [1], X.509 [1] which we will be using to safeguard our sensitive PHR. these are some of the standards for identity management. Cryptographic technique required in this case has to be fine-grained like Attribute Based Encryption [6].

SAML deals with a XML-based schema developed by OASIS which permits the entities to transfer secure tokens online. In an SAML message exchange procedure, one entity is dependent entity and the other is asserting entity. The dependent entity sends a request to the asserting entity and relies on its response to take his decisions on security, whereas an asserting entity analyses the data to check its authentication, if he is authorised to access data etc. ID-FF is the base for these specs given by Liberty Alliance [20]. The main motto is to provide profess standard to safeguard the data about identity during online proceedings.

OAuth i.e. Authorization Protocol uses any common authentication method e.g. username and password to verify the user. It allows an end-user to access any resource of server, on part of a resource owner. Thus, user's profile credentials are protected while accessing protected data.

X.509 is an authentication framework used to authentication and generates a digital certificate. Trust relationships are necessary between identity provider and service provider so that a user can have only one federated identity through which he can perform transactions within a circle-of-trust (CoT) [3]. Different service providers, identity providers come together and form a circle-of-trust based on some agreement which defines the trust relationship between them.

Limited anonymity is provided by a method by SAML privacy assistance [21] through pseudonymous persistent and volatile identities. Volatile identities are mainly used when the user is trying to access any resource during SSO process, thus any relation between the identities can't be deduced. While, permanent identities exist, until otherwise deleted. Thus permanent identity is used in federated environment where user accesses services of more than one CSP through his accounts in them.

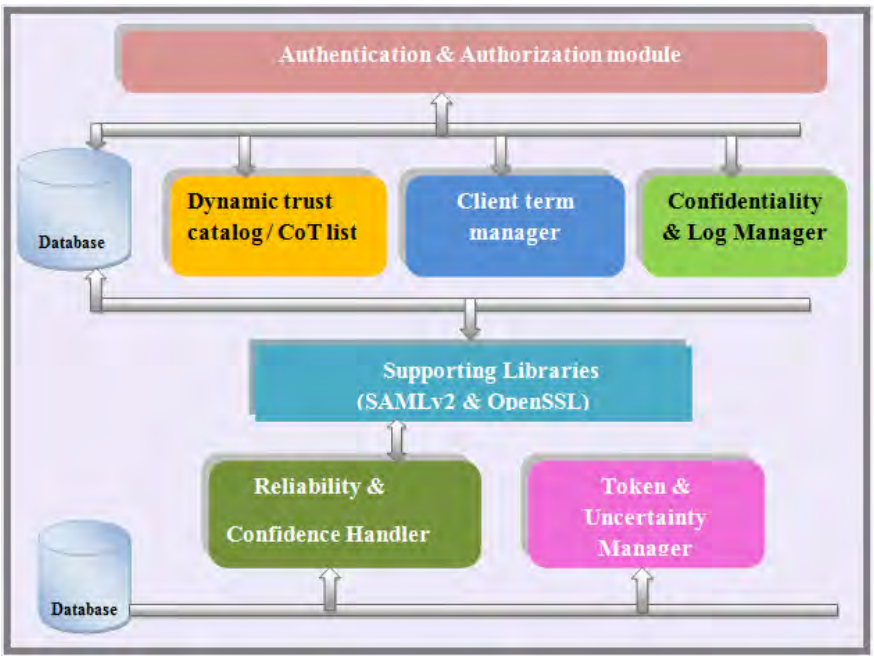

Fig 1. Identity Provider architecture and its modules in cloud computing

IV. PROPOSED ARCHITECTURE

The concept of identity management basically aims at providing a common knowledge to service provider's (SP's), identity providers (IdP's) and the enhanced client. The ECP provides the basic patient centric approach in cloud computing environment.ECP has the required knowledge so as to minimize the direct interaction between SP's and IdP's, thus providing full patient-centric approach to privacy.

A. Authentication & Authorization module

<AuthnRequest> is received and processed by this module,it could be sent from SP or ECP. In the domain of CSP, this module issues such requests. The prime purpose of this module is to verify that the user requesting the particular service, as in for example in our scenario the health record, is basically who he claims to be it enables different authentication techniques including PKI, password and username.

In Authorization scenario the tokens and attributes exchanged pass the information whether the particular user is authorized to view the data or use the resources.

It manages the SAML authentication assertions and attributes statements. Minimizing the complexity and costs is the prime aim of this module.

B. Client's term Manager

This module manages the identifiers for users and session data after the user is registered. Session data is created by the CSP once the user is authenticated. This data is stored till the user is logged in or using the service, once the user logs out the tokens are destroyed. This helps the IdP to track user's movements and activities.

This module further requests profile of the devices to support multi-device SSO.

This module is also responsible for managing and storing user's credentials, as well as managing profiles and enforcing policies. Credentials can be either username/passwords, digital certificates etc. These features provide

a centralized perspective to the user over all the different applications having client's health record on different clouds. This module also interacts with the ECP for determining which IdP is appropriate for verifying it for the requested service.

C. Dynamic trust list/CoT Management

This module is responsible for the administration of the circle of trust, it contains information like previous interaction scores, keys, trust level, reputation scores etc. This information is dynamically updated by other modules. Circle of trust is between many identity providers and service providers who have come together under an agreement and federation technology to form a trust relationship between them [3].

D. Supporting Libraries (openSSL, SAMLv2)

Basic supporting libraries like IdM and cryptographic implementing SAMLv2/ID-ff functionalities and cryptographic protocols and algorithm are also included. A "lite" version of these libraries is also included in the user's side.

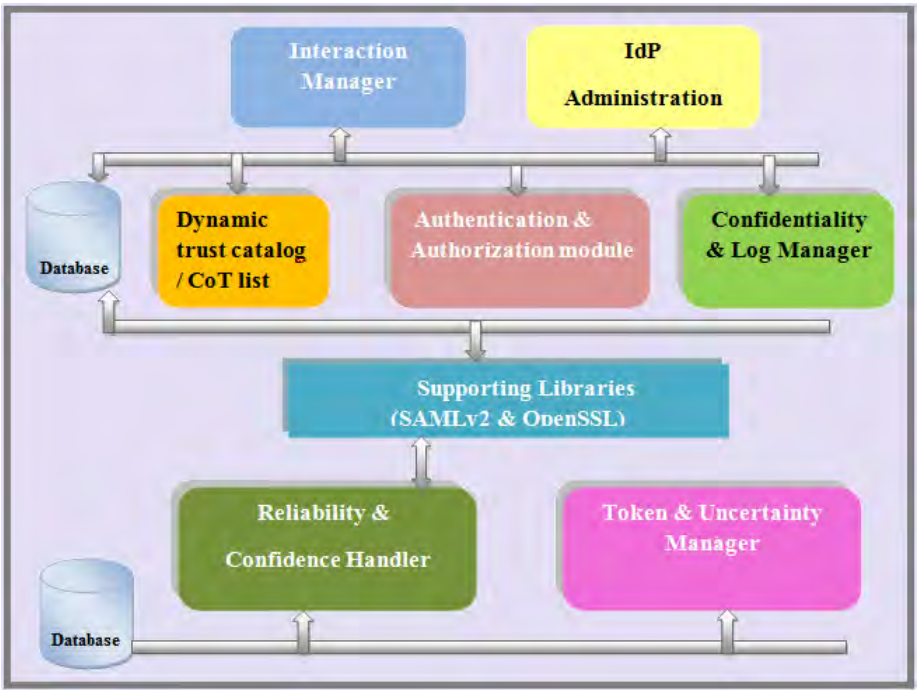

Fig 2. Identity Provider architecture and its modules for Enhanced Client Profile in cloud computing scenario

E. Reliability & Confidentiality Manager

This module is responsible for managing requests and responses. It collects, distributes and manages. This module is also responsible for managing the trust database. It manages the trust dynamically, establishes trust relationship and also provides trust data for other modules. The trust data is a combination of information received from the behaviour of the entities and trust information send by trusted third parties. Thus it creates a general data in the federation. Also it is responsible for making richer context related decisions.

F. Token & Uncertainty Manager

For the analysis of the risk generating factors and to maintain a log of past transaction, Reliability and confidentiality manager is connected to this module. This module creates a dynamic trust value related to each identity, as this will keep changing with time.

G. Confidentiality & Log Manager

This module is in charge for user identifier management, along with the analysis of how user data is being used. The prime purpose of this module is to hide user's identity and data.

The monitoring tools and the audit tools log the fields that are accessed, they just show which fields are accessed without showing the actual data. The user is able to access services without divulging his identity. The use of different pseudonyms enables different range of identification and authentication.

V. DETAILED DESCRIPTION

Providing a secure environment for our user's PHR is the main motto of our schema. When the client creates his account on a CSP, his data is encrypted using ABE and is then stored in our partially-trusted cloud database. He can also update his data sharing policy, which can be done with assistance from server. Multiple clients can

have data on multiple CSP's. But one client has his entire data on a single CSP. The potential users (viewers) of a PHR can be broadly divided into personal and professional. The personal user will be in close relation with the client e.g. friend, family, acquaintance. While, the professional users can be insurance person, doctor, research scholar etc, who may or may not be known to PHR owner.

In professional domain for strong privacy assurance of client, multi-authority attributes based encryption CC MA-ABE [30] is used. It has multiple attribute authorities (AA), each having a separate attribute set for a particular category of professional user. In the access policy, role attributes are defined (refer implementation example), which represent the professional role of a person. This role attribute provides access in other words sort of binding takes place between attributes and roles. These access policies are set by the owner of the data. AA is responsible to authenticate and distribute the keys to its set of users. As professional set of user are the bulk part of users, hence a lot of key management load is freed from client. While encrypting, clients can specify their own access control protocols for their PHR data, without having to know the authorized users in that category. For emergency purpose, a separate attribute is specified for direct access. The users who can contribute i.e. update or write on patients data are given write access keys by AA's.

CC MA-ABE is nothing but a KP-ABE scheme in which user's secret key is used to enforce access policies, but these key policies do not transpose to document access policies. The CC MA-ABE can support user-specified text access policy with certain amount of flexibility [2], if certain rules of specifying which attributes are required in the cipher text are followed.

In the personal domain of users, the client has a relation with these users, and hence can allot them their access liberty one-by-one. As this domain has very less users, there is not much burden on client either. KP-ABE will be best method for this access policy and key distribution [31]. In this the client has to identify the data attributes which will be visible to all the personal users. The PHR application creates two keys, public and private. The public can be directly distributes through the online medical social network. While for the secret key, either when the client is initially using his profile, he can define a personal user's access liberties and the application can generate the key for the same and distribute it e.g. Skype, or when a personal domain wants to access some data, he can send a request to the client through the same online medical social network. The owner can respond to this request and grant the requested subset of data. The application's module can then get access network, generate the key using keygen of KP-ABE that encloses in his access structure.

When a user want to access any patient's record, then the concept of trust and federated identity comes in picture. Different clients PHR can be on different clouds, hence accessing those services would require trust data to be transferred among the IdP and CSP.

The appraisal got from users in a group or association can be used to calculate reputation as a sum whole of this evaluated trustworthiness as stated by Josang [33]. This information in combination with other data like history of past interactions can be used to take just decisions. But this dimension of trust has not been fully implemented yet. Both assertion and protocol is changed if we add reputation to SAML. [32] provides a new assertion, compliant with the extension technique. The custom statement <ReputationStatement>, transmit through response message.

In its structure the beginning part is the header, whose content is same as standard. The common segment consists of the assertion identifier (ID), the subject, the time of issue and sender's name. The <subject> tag is the identifier of the user for whom the reputation information has been asked. The statement also has a body part which contains data associated with reputation metric. These include reputaionInstant (data freshness), ReputationScore (reputation value), DistributionFunction (aggregate the reputation), Context (situation for making reputation). SAML "assertion query and request protocol" is used for exchanging the <ReputationStatement>.

Key Revocation

The client may also sometimes want to revoke some access privileges or user domain. There are 4 main cases- (a) the client may want to withdraw a professional user domain as a whole, i.e. lift a role attribute privilege. (b) Revocation of a professional user access privilege in a particular professional user domain. This is done by AA, which belongs to that client. (c) The client may want to withdraw a personal user domain as a whole, i.e. lift a role attribute privilege. (d) Revocation of a personal user access privilege in a particular personal user domain. This can be done by client himself.

User revocation is not possible in primary CC MA-ABE in an efficient manner. By combining the ideas of YWRL' revocable KP-ABE [31] and [29], this can be achieved to design an improved MA-ABE scheme as said in [2]. The client can re-encrypt his PHR cipher text data and update the keys of all other users. This computing can also be done on server to improve efficiency.

Data write access

Client cannot always update his medical records i.e. PHR, also not anyone can be granted write access privilege e.g. doctors should be allowed to update his records with new information but insurance person or research scholar can't. There needs to be a write access control granted by the PHR owner as well as the organisation in which the user works, which can further be authorized by the server. This can be achieved by using signature as given in [2].

Break-glass access for emergency

In an emergency, the proposed access policy is not practically applicable. There needs to be an emergency access method to access the patient's PHR. For this, each client creates an emergency attribute, which may be under his personal user domain and grant its access key to the emergency department before hand. The emergency department saves it in his database under the patient's identity. To access it, the emergency staff's identity and the emergency situation has to be verified by the ED, only then he gets the access. For this situation, when the emergency department sends a data grant request to a CSP under whom it is not already registered, the trust and reputation value can be increased to its maximum level to skip the reputation exchange procedure for cloud federation and thus fast delivery of the data. Also, the patient can revoke the access key after the emergency is over, re-encrypt it and sent it over to the ED department again [2].

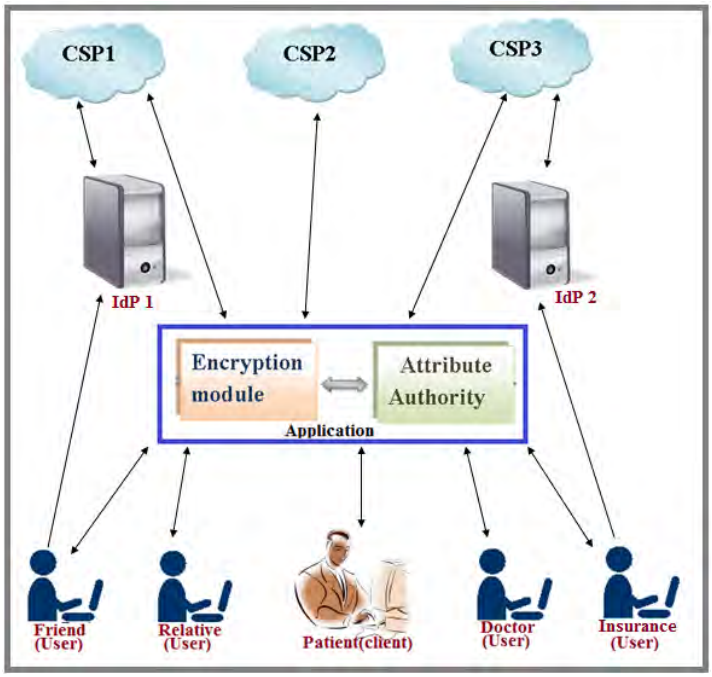

Fig 3. The proposed framework for sharing the client's PHR in a secure way with Identity Provider, CSP and the healthcare application.

VI. IMPLEMENTATION

We have implementing the above proposed architecture using cloud foundry [34] and have achieved success. Cloud Foundry software is developed by VMware and is released on the terms of Apache License 2.0. It's an open source cloud computing Platform-as-a-Service (PaaS). Ruby is used as the primary language. The source and development community for this software is available at cloudfoundry.org

Example

1. Suppose John wants to store his PHR into the database on cloud. Here we take it as CSP2. Let the name of the file is G1 (named as "PHR; history, emergency, allergy). First encryption is done both under G1's data labels (using KP-ABE) and role-based file access policy P1 (under MA-ABE). The policy is decided based on either recommended settings or john's own personal preferences. The break glass key is also sent to the ED. John also decides the access rights of users in his PSD.
2. Now if a user let bob wants to access these records in CSP2. CSP2 performs a check in order to determine who should be asked to authenticate bob. The authenticator here will be the IdP. It checks metadata stored to see if the recognized IdP is known.
3. In case suppose IdP1 is not acknowledged, reliability and confidentiality manager runs the algorithm to accumulate reputation about it, by sending a <ReputationRequest>, acting as a requester.
4. IdP2 and CSP1 together respond by sending a <ReputationResponse> containing <ReputationStatement>, if it's a success, in case of failure a error message is generated. They act as reputation responder. In case the IdP1 is trusted on the basis of the information sent by the responders, the entire metadata of IdP1 is

downloaded into CSP2, and SSO is initiated. Then the CSP2 asks for authentication of bob from IdP1. Bob is authenticated by IdP1 by sending a successful authentication response. Finally the service is granted to bob.

5. These services can be like, for example bob requests information about PERSONAL INFO or MEDICAL HISTORY. The client application distributes key with the access structure (personal_info^medical_history). Using this key the friend is able to decrypt data.

If another user say Billy, who is a doctor in a clinic wants to access the data, he can obtain his key from multiple AA (e.g. American medical association (AMA) etc). But he cannot decrypt G1 because the role attributes do not comply with P1.

In the end, if the medical emergency staff person temporarily obtains the break-glass key from ED, will be able to access the file G1, due to emergency attribute in it.

VII. CONCLUSION

This paper proposes a new architecture for storing and sharing of personal health records in federated cloud environment. We have considered partially trusted servers. To fully apply the patient-centric concept, patient should have full control over their privacy by encrypting the PHR's and providing fine grained access. We also here addressed the problem of key management, and were able to reduce its complexity. Using ABE we were able to make sure that patients are able to give access not only to personal users but also to users of public domain. Break glass entry and user revocation further increases the usability and give our system the required flexibility. We have extended this approach to dynamic federation of clouds. As cloud computing has come up as an important part of one's life, the number of CSP's increasing day by day, it's very important to create a common methodology of authentication and authorization. We provide this by using privacy enhanced and trust-aware IDM architecture which is in consent with SAMLv2/Id-ff standards. This gives us an efficient way to manage identities and access control over multiple CSP's. With the embodiment of reputation information and Trust-aware ECP, mobile users can also take part in the cloud-federation in a more active way. Reputation extensions even allow the CSP's to make richer trust decisions. Dynamic trust and risk management helps to monitor user's behaviour and helps to make decisions of allowing the access, declining or revoking. On the cloud scenario it helps our user to access these records or services without revealing their true identity, thus privacy is realised. This framework takes the concept of storing health records to whole new level. Now PHR's can be stored anywhere on any CSP, and can be accessed by anyone of any domain, with proper access permissions.

We further wish to fully implement the above framework on an open source cloud.

REFERENCES

[1] Rosa Sánchez, Florina Almenares, Patricia Arias, Daniel Díaz-Sánchez, and Andrés Marín "Enhancing Privacy and Dynamic Federation in IdM for Consumer Cloud Computing" IEEE Transactions on Consumer Electronics, Vol. 58, No. 1, February 2012

[2] Ming Li, Shucheng Yu, Yao Zheng and Kui Ren, and Wenjing Lou1 "Securing Personal Health Records in Cloud Computing: Patient-centric and Fine-grained Data Access Control in Multi-owner Settings"IEEE Transactions on parallel and distributed systems vol. XX, NO. XX, XX 2012

[3] http://docs.oracle.com/cd/B28196_01/idmanage.1014/b25355/intro.htm

[4] A. Beloglazov, R. Buyya, Y. C. Lee, and A. Zomaya, "A taxonomy and survey of energy-efficient data centers and cloud computing systems," Univ. of Melbourne, Technical Report CLOUDS-TR-2010-3, 2010.

[5] K. D. Mandl, P. Szolovits, and I. S. Kohane, "Public standards and patients' control: how to keep electronic medical records accessible but private," *BMJ*, vol. 322, no. 7281, p. 283, Feb. 2001.

[6] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in *CCS '06*, 2006, pp. 89–98.

[7] M. Scholl, K. Stine, K. Lin, and D. Steinberg, "Draft security architecture design process for health information exchanges (HIEs)," *Report, NIST*, 2009.

[8] D. F. Ferraiolo, R. Sandhu, S. Gavrila, D. R. Kuhn, and R. Chandramouli, "Proposed NIST standard for role-based access control," *ACM TISSEC.*, vol. 4, no. 3, pp. 224–274, 2001.

[9] S. D. C. di Vimercati, S. Foresti, S. Jajodia, S. Paraboschi, and P. Samarati, "Overencryption: management of access control evolution on outsourced data," in *VLDB '07*, 2007, pp. 123–134.

[10] J. Benaloh, M. Chase, E. Horvitz, and K. Lauter, "Patient controlled encryption: ensuring privacy of electronic medical records," in *CCSW '09: Proceedings of the 2009 ACM workshop on Cloud computing security*, 2009, pp. 103–114.

[11] W. Wang, Z. Li, R. Owens, and B. Bhargava, "Secure and efficient access to outsourced data," in *CCSW '09*, 2009, pp. 55–66.

[12] M. Li, W. Lou, and K. Ren, "Data security and privacy in wireless body area networks," *IEEE Wireless Communications Magazine*, Feb. 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. [Online]. Available: http://purl.org/utwente/65471

[14] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving secure, scalable, and fine-grained data access control in cloud computing," in *IEEE INFOCOM'10*, 2010.

[15] ——, "Attribute based data sharing with attribute revocation," in *ASIACCS'10*, 2010.

[16] X. Liang, R. Lu, X. Lin, and X. S. Shen, "Patient self-controllable access policy on phi in ehealthcare systems," in *AHIC 2010*, 2010.

[17] S.Grzonkowski and P.Corcoran, "Sharing Cloud Services: User Authentication for Social Enhancement of Home Networking", *IEEE Transactions on Consumer Electronics*, vol.57, no.3, May 2011.

[18] P. Angin, B. Bhargava, R. Ranchal, N. Singh, L. Lilien and L. Ben Othmane, "An Entity-centric Approach for Privacy and Identity Management in Cloud Computing", in Proc. of the 29th IEEE International Symposium on Reliable Distributed Systems (SRDS), pp. 177-183, 2010.
[19] A. Celesti, F. Tusa, M. Villari, and A. Puliafito, "Three-Phase Cross-Cloud Federation Model: The Cloud SSO Authentication", 2nd International Conference on Advances in Future Internet (AFIN), 2010.
[20] L. Xiong and L. Liu, "PeerTrust: Supporting Reputation-Based Trust for Peer-to-Peer Electronic Communities", *IEEE Transactions on Knowledge and Data Eng*., vol. 16, no. 7, pp. 843-857, 2004.
[21] H. Hexmoor, "Trust-based protocols for regulating online, friend-of-a-friend communities", *Journal of Experimental & Theoretical Artificial Intelligence*, pp. 1-21, 2009
[22] S. Pearson, "Taking Account of Privacy when Designing Cloud Computing Services", in Proc. of the Software Engineering Challenges of Cloud Computing (CLOUD'09), ICSE Workshop, 2009.
[23] Federal Trade Commission, "Privacy Online: Fair Information Practices in the Electronic Marketplace", A Federal Trade Commission Report to Congress. Washington DC, May 2000.
[24] Federal Trade Commission (FTC), "Protecting Consumer Privacy in an Era of Rapid Change", Preliminary FTC Staff Report, Dec. 2011.
[25] A. Cavoukian, "Privacy in the clouds", Identity in the Information Society, Dec. 2008
[26] Z. Li, E. Chang, K Huang, and F. Lai, "A Secure Electronic Medical Record Sharing Mechanism in the Cloud Computing Platform", in Proc. of the 15th IEEE International Symposium on Consumer Electronics, 2011.
[27] S. D. C. di Vimercati, S. Foresti, S. Jajodia, S. Paraboschi, and P. Samarati, "Over-encryption: management of access control evolution on outsourced data," in *VLDB '07*, 2007, pp. 123–134. [b28]
[28] S. Yu, C. Wang, K. Ren, and W. Lou, "Attribute based data sharing with attribute revocation," in *ASIACCS'10*, 2010.
[29] M. Chase and S. S. Chow, "Improving privacy and security in multi-authority attribute-based encryption," in *CCS '09*, 2009, pp. 121–130.
[30] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving secure, scalable, and fine-grained data access control in cloud computing," in *IEEE INFOCOM'10*, 2010.
[31] "The health insurance portability and accountability act." [Online]. Available: http://www.cms.hhs.gov/HIPAAGenInfo/01 Overview.asp
[32] A. Jøsang, R. Ismail, and C. Boyd, "A survey of trust and reputation systems for online service provision", *Decision Support System*, vol. 43, no. 2, pp. 681-644, Elsevier (ed.), 2007.
[33] www.cloudfoundry.com