Privacy-Preserving With Authentication For Multi-Owner Data Sharing In Cloud Environment

G. V. Kapse¹, Dr. V. M. Thakare², Prof. S. S. Sherekar³, A. V. Kapse⁴

¹Student, Department of computer science, S. G. B. Amravati University, Amravati, India, kapsegayatri8@gmail.com
²H. O. D, Department of computer science, S. G. B. Amravati University, Amravati, India, vithakare@yahoo.com
³Professor, Department of computer science, S. G. B. Amravati University, Amravati, India, ss_sherekar@rediffmail.com
⁴Student, Shankarlal Khandelwal senior college of Art, Commerce & Science, Akola, India, abhishekkapse4@gmail.com

ABSTRACT
Cloud services provide great conveniences for the users to enjoy the on-demand cloud applications without considering the local infrastructure limitations. The main requirement of the service is guarantee the confidentiality of the data. However, the anonymity of the service clients, one of the most essential aspects of privacy, should be considered simultaneously. Paper proposed new approach which provides secure storage and control sharing of patient’s health data. Explore key policy attribute based encryption as well as multi-authority attribute based encryption to enforce patient access control policy such that public user can download the data but only authorize user should view the medical records. This supports multiple owner scenarios and divides the users in the system into multiple security domains that greatly reduce the key management complexity for owners and users.

Keywords — Cloud computing, data sharing, authentication, data storage, multi-owner, privacy preservation, etc.

1. INTRODUCTION
Research in cloud computing is done by the both academic and industrial worlds. In cloud computing, users can outsource their computation and storage to clouds with the help of Internet. This reduces the burden of users of maintaining resources on site. Clouds can provide different services like applications e.g., Google Apps, Microsoft online, infrastructures e.g., Amazon’s EC2, Nimbus, Eucalyptus, and platforms to help developers write applications e.g., Amazon’s S3, Windows Azure. As services are outsourced to cloud, privacy and security are of immense concern in cloud computing. On one hand, before initiating any transaction, the user should authenticate itself, and on the other hand, it must be ensured that the cloud does not tamper with the data that is outsourced. User privacy is also required so that the cloud or other users do not know the identity of the user. The cloud can hold the user accountable for the data it outsources, and likewise, the cloud is itself accountable for the services it provides. The validity of the user who stores the data is also verified. Apart from the technical solutions to ensure privacy and security, there is requirement of law enforcement.

Personal Health Record (PHR) is emerged as a patient-centric model of health information exchange. It enables the patient to create and control their medical data which may be placed in a single place such as data centre. Due to the high cost of building and maintaining specialized data centres, PHR services are outsourced to cloud service providers, e.g., Microsoft Health Vault, Google Health. It is very nice to have convenient PHR data services for everyone, there are many security and privacy risks which could impede its wide adoption. The main concern is about whether the patients could actually control the sharing of their sensitive personal health information (PHI), when it is stored on a semi-trusted cloud server. Due to the high value of the sensitive Personal Health Information, the third-party storage servers are often the targets of various malicious behaviours which may lead to exposure of the PHI. The main concern is about the privacy of patients’ personal health data and who could gain access to the medical records when they are stored in a cloud server. In cloud computing storage, the data owner and cloud servers are from two different domains. On one hand, cloud servers are not entitled to access the outsourced data content for data confidentiality; on the other hand, the data resources are not physically under the full control of data owner. Storing personal medical records on the cloud server leads to need of Encryption mechanism to protect the medical health record, before outsourcing to the cloud. To deal with the potential risks of privacy exposure, instead of letting the service providers encrypt patients’ private

IJRISE www.ijrise.orgeditor@ijrise.org [604-610]
data, medical records sharing services should give patients full control over the selective sharing of their own medical data. The medical records should be encrypted along with traditional access control scheme provided by the cloud server.

For solution, propose the patient-centric, secure sharing of PHRs stored on semi trusted servers, and focus on dealing with the challenging and complicated key management issues. In order to protect the personal health data stored on a semi trusted server, adopt attribute based encryption (ABE) as the main encryption technique. Using ABE, access policies are defined based on the attributes of data or users, which enable a patient to selectively share PHR encrypting the file under a set of attributes among a group of users, without the need to know a complete list of users.

2. BACKGROUND

Author proposed a privacy-preserving ciphertext multi-sharing mechanism. It combines the merits of proxy re-encryption with anonymous technique in which a ciphertext can be securely and conditionally shared multiple times without leaking both the knowledge of underlying message and the identity information of ciphertext senders or recipients [1].

A novel authorized accessible privacy model (AAPM) is established. Patients can authorize physicians by setting an access tree supporting flexible threshold predicates. Then, based on it, by devising a new technique of attribute-based designated verifier signature, a patient self-controllable multi-level privacy-preserving cooperative authentication scheme (PSMPA) realizing three levels of security and privacy requirement in distributed m-healthcare cloud computing system is proposed [2].

To enable cloud servers to perform secure search without knowing the actual data of both keywords and trapdoors, author systematically construct a novel secure search protocol. To rank the search results and preserve the privacy of relevance scores between keywords and files, also proposes a novel Additive Order and Privacy Preserving Function family. To prevent the attackers from eavesdropping secret keys and pretending to be legal data users submitting searches, author propose a novel dynamic secret key generation protocol and a new data user authentication protocol [3].

Author proposes a shared authority based privacy-preserving authentication protocol (SAPA) to address privacy issue for cloud storage. In the SAPA, 1 shared access authority is achieved; 2 attribute based access control is adopted 3) proxy re-encryption is applied to provide data sharing among the multiple users [4].

Author proposes privacy preserving authenticated access control scheme, in which, the cloud verifies the authenticity of the user without knowing the user’s identity before storing information. Scheme provides access control in which only valid users are allowed to decrypt the stored information. The scheme prevents replay attacks and supports creation, modification, and reading data stored in the cloud. Also, scheme is decentralized and robust [5].

Paper introduces Privacy-Preserving with authentication for Multi-owner data sharing in cloud environment and these are organizes as follows. Section I Introduction. Section II discusses Background. Section III discusses previous work. Section IV discusses existing methodologies. Section V discusses attributes and parameters and how these are affected. Section VI proposed method and outcome result possible. Finally section VII Conclude this paper.

3. PREVIOUS WORK DONE

Liang, et al. [1] proposed a ciphertext sharing mechanism with the following properties: Anonymity: given a ciphertext, no one knows the identity information of sender and receiver. Multiple receiver update: given a ciphertext, the receiver of the ciphertext can be updated in multiple times. Author refers to this property as “multi-hop”. Conditional sharing: a ciphertext can be fine-grained shared with others if the pre-specified conditions are satisfied. Achievements: Author investigates a new notion, AMH-IBC-PRE and formalizes the definition and security model by incorporating the definitions.

Zhou, et al. [2] proposed a novel authorized accessible privacy model (AAPM), for the multi-level privacy-preserving cooperative authentication which is established to allow the patients to authorize corresponding privileges to different kinds of physicians located in distributed healthcare providers by setting an access tree supporting flexible threshold predicates. Based on AAPM, a patient self-controllable multilevel privacy-preserving cooperative authentication scheme (PSMPA) in the distributed m-healthcare cloud computing system is proposed, realizing three different levels of security and privacy requirement for the patients.

Zhang, et al. [3] defined multi-owner model for privacy preserving keyword search over encrypted cloud data, in which proposed an efficient data user authentication protocol, which not only prevents attackers from eavesdropping secret keys and pretending to be illegal data users performing searches, but also enables data user authentication and revocation. Author systematically construct a novel secure search protocol, which enables the cloud server to perform secure ranked keyword search without knowing the actual data of both keywords and trapdoors, and allows data owners to encrypt keywords with self-chosen keys and allows authenticated data
users to query without knowing these keys. Also, proposed an Additive Order and Privacy Preserving Function family (AOPPF) which allows data owners to protect the privacy of relevance scores using different functions according to their preference, while still permitting the cloud server to rank the data files accurately.

Liu, et al. [4] aims to address a user’s sensitive access desire related privacy during data sharing in the cloud environments, and it is significant to design a humanistic security scheme to simultaneously achieve data access control, access authority sharing, and privacy preservation. Author address the aforementioned privacy issue to propose a shared authority based privacy-preserving authentication protocol (SAPA) for the cloud data storage, which realizes authentication and authorization without compromising a user’s private information. The main contributions are as follows. 1) Identify a new privacy challenge in cloud storage, and address a subtle privacy issue during a user challenging the cloud server for data sharing, in which the challenged request itself cannot reveal the user’s privacy no matter whether or not it can obtain the access authority. 2) Propose an authentication protocol to enhance a user’s access request related privacy, and the shared access authority is achieved by anonymous access request matching mechanism. 3) Apply ciphertext policy attribute based access control to realize that a user can reliably access its own data fields, and adopt the proxy re-encryption to provide temporary authorized data sharing among multiple users.

Ruj, et al. [5] proposed the privacy preserving access control with authentication for security of cloud data, the following points covered in scheme:
1) Distributed access control of data stored in cloud so that only authorized users with valid attributes can access them. 2) Authentication of users who store and modify their information of the cloud. 3) The identity of the user is protected from the cloud during authentication. 4) The architecture is decentralized, meaning that there can be several KDCs for key management. 5) The access control and authentication are both collision resistant. 6) The proposed scheme is resilient to replay attacks. 7) The protocol supports multiple read and writes on the data stored in the cloud. 8) The costs are comparable to the existing centralized approaches, and the expensive operations are mostly done by the cloud.

4. EXISTING METHODOLOGIES
Author proposed construction for unidirectional AMH-IBCPRE; it achieves multiple ciphertext receiver update, conditional data sharing, anonymity and collusion-safe. Author defines four security models for different practical purposes.
• The security model of MH-IBCPRE is the basic one, in which a challenger plays the game with the adversary to launch Chosen Ciphertext Attacks (CCA) to the original ciphertext and re-encrypted ciphertext in order to solve a hard problem.
• Author considers where a proxy colludes with delegatee to compromise the underlying message and the secret key of delegator. Here, the protection of the message is very difficult to achieve as the delegate can always decrypt the corresponding ciphertext for the proxy. The secret key of the delegator, however, is possible to be secured.
• For the definition of collusion attacks model, author allows an adversary to acquire all re-encryption keys, and the adversary wins the game if it outputs a valid secret key of an uncorrupted user. Author’s definition is in the selective model in which the adversary has to output a target identity at the outset of the game.
• As to the security model of anonymity, it is complicated in the sense that we categorize the game into two sub-games: one is the anonymity for delegator; the other is the anonymity of re-encryption key [1].

The basic e-healthcare system illustrated in Fig. 1 mainly consists of three components: body area networks (BANs), wireless transmission networks and the healthcare providers equipped with their own cloud servers. The patient’s personal health information is securely transmitted to the healthcare provider for the authorized physicians to access and perform medical treatment.
In multi-owner and multi-user cloud computing model, four entities are involved, as illustrated in Fig. 2; they are data owners, the cloud server, administration server, and data users.

Data owners had collection of files $F$. To enable efficient search operations on these files which will be encrypted, data owners first build a secure searchable index $I$ on the keyword set $W$ extracted from $F$, and then they submit $I$ to the administration server. Finally, data owners encrypt their files $F$ and outsource the corresponding encrypted files $C$ to the cloud server. Upon receiving $I$, the administration server re-encrypts $I$ for the authenticated data owners and outsources the re-encrypted index to the cloud server. Once a data user wants to search $r$ keywords over these encrypted files stored on the cloud server, he first computes the corresponding trapdoors and submits them to the administration server. Once the data user is authenticated by the administration server, the administration server will further re-encrypt the trapdoors and submit them to the cloud server. Upon receiving the trapdoor $T$, the cloud server searches the encrypted index $I$ of each data owner and returns the corresponding set of encrypted files. To improve the file retrieval accuracy and save communication cost, a data user would tell the cloud server a parameter $k$ and cloud server would return the top-$k$ relevant files to the data user. Once the data user receives the top-$k$ encrypted files from the cloud server, he will decrypt these returned files.

Fig. 3 shows the interactions among $\{U_a, U_b, S\}$, in which both $U_a$ and $U_b$ have interests on each other’s authorized data fields for data sharing. The presented interactions may not be synchronously launched, and a certain time interval is allowable.
According to proposed privacy preserving authenticated access control scheme user can create a file and store it securely in the cloud. Scheme consists of use of the two protocols ABE and ABS, refer to the Fig. 5. There are three users, a creator, a reader and writer. Creator Alice receives a token \(\gamma\) from the trustee. On presenting id like health insurance number, the trustee gives her a token \(\gamma\). There is multiple KDC which can be scattered. A creator on presenting the token to one or more KDCs receives keys for encryption/decryption and signing. In the Fig. 4, SKs are secret keys given for decryption, Kx are keys for signing. The message MSG is encrypted under the access policy X. The policy decides who can access the data. The creator decides on a claim policy Y, to prove her authenticity and signs the message under this claim. The ciphertext C with signature is \(c\), and is sent to the cloud. The cloud verifies the signature and stores the ciphertext C. When a reader wants to read, the cloud sends C. If the user has attributes matching with policy, it can decrypt and get back original message. Write proceeds in same way as file creation.

Fig-4: Secure cloud storage model [5].

5. ANALYSIS AND DISCUSSION

Author proposes a concrete construction for unidirectional AMH-IBCPRE, in which it achieves multiple ciphertext receiver update, data sharing, and collusion-safe, for dynamic group, scheme is applicable to many real-world applications, like secure email forwarding, electronic encrypted data sharing, where secure encrypted data sharing needed [1].

Author proposes, a novel authorized accessible privacy model and a patient self-controllable multi-level privacy preserving cooperative authentication scheme gave three levels of security and privacy requirement in the distributed m-healthcare cloud computing system. PSMPA can resist different kinds of attacks and gave better performance than previous schemes in terms of storage, computational and communication overhead [2].

Author schemes enable authenticated data users to achieve secure, convenient, and efficient search for multiple data owners’ data. To authenticate users and detect attackers, author proposed protocol; so that cloud perform secure search among multiple owners data encrypted with different secret keys, author also construct protocol to rank search results and show that approach is computationally efficient, for large data and keyword sets [3].

Author identified privacy challenge during data accessing in the cloud computing, to this authentication established to guarantee data confidentiality and data integrity. By wrapping values are exchanged during transmission and data anonymity achieved. User privacy enhanced by accessing requests to privately inform the cloud server about the user access request. Forward security realized by the session identifiers [4].

Author presents a privacy preserving access control scheme for clouds. Author’s scheme provides fine-grained access control as well as authenticates users who store data over the cloud. The cloud is unable to know the identities of the users who stores data, but verify the user’s credentials and decentralized key distribution [5].

<table>
<thead>
<tr>
<th>Privacy-preserving techniques</th>
<th>Advantages</th>
<th>Disadvantages</th>
</tr>
</thead>
<tbody>
<tr>
<td>Multi-Hop Identity Base Proxy Re-Encryption</td>
<td>A ciphertext can be securely and conditionally shared multiple times</td>
<td>confidentiality of the data</td>
</tr>
<tr>
<td>PSMPA</td>
<td>1) Resist various attacks 2) No issue of computational, communication and storage overhead.</td>
<td>Authorized physicians institutions can recover the patient’s information.</td>
</tr>
<tr>
<td>Privacy preserving keyword search in a multi-owner cloud model</td>
<td>1) Data owner scalability 2) Data user revocation 3) Security</td>
<td>1) decryption capability 2) secure fuzzy keyword search in a multi-owner paradigm</td>
</tr>
<tr>
<td>Shared authority based privacy preserving authentication protocol</td>
<td>1) Ubiquitous network access 2) Location independent 3) Authentication 4) Data anonymity</td>
<td>1) User privacy 2) Security</td>
</tr>
<tr>
<td>Privacy preserving authenticated access control scheme</td>
<td>1) Collusion secure 2) Resistant to replay attacks 3) Protects privacy of the user</td>
<td>Cloud knows the access policy for each record stored in the cloud.</td>
</tr>
</tbody>
</table>

Table-1: Comparison between various privacy preserving with authentication techniques

6. PROPOSED METHODOLOGY
To provide secure access of PHR for patient-centric manner and efficient key management, the system is divided into various security domains such as Personal domain (PSD) and Public domain (PUD). Each domain controls only a subset of its users. For every domain, one or multiple authorities are assigned to give the access of data. For personal domain the owner of the PHR manages the record and performs key management. The number of users in the personal domain is less and is personally connected to the owner so it is easy. Public domain consists of number of users so difficult to manage easily by the owner. Hence propose public Attribute Authorities (AA) to control disjoint subset of attributes.

In propose system, there are numbers of SDs, owners, AAs, and users, and two ABE systems are involved; for PSD KP-ABE scheme and for PUD MA-ABE scheme is adopted. Data owner uses KP-ABE system to manage the secret keys and access rights of users in their PSD. And to achieve security of health records, Attribute based encryption (ABE) is adopted. Data is classified according to attributes. PHR owner encrypts record according to attributes and user satisfying those attributes may obtain decryption key to the data access. In multi-authority ABE (MA-ABE) scheme, many attribute authorities operate simultaneously, each handle secret keys for different set of attributes. MA-ABE system is comprised of k attributes authorities and one central authority.

Following algorithms are used in system:
1) **Set up:** the central authority or other trusted authority run a random algorithm. It takes security parameter as input and outputs a public key, secret key pair for every attribute authorities, also outputs a system public key and master secret key which will be used by the central authority. 2) **Attribute Key Generation:** An attribute authority run a random algorithm. It takes authority’s secret key, a user’s GID, the authority’s value dk, and attributes in the authority’s domain as input and output secret key for the user. 3) **Central Key Generation:** It is run by the central authority. It takes the master secret key and input is a user’s GID and outputs are secret key for the user. 4) **Encryption:** It is runs by sender. It takes a set of attributes for each authority, a message, and the system public key as input and output is the cipher text. 5) **Decryption:** A deterministic algorithm runs by a user. It takes a cipher-text, that is encrypted under attribute set and decryption keys for that attribute set as input. And output is a message m.

As ABE and MA-ABE have some limitations. So the AB broadcast encryption technique is used. The system is designed to manage PHR. The system is divided into six modules.

**Fig-5: Architecture of patient record sharing**

1) **Data Owner:** The data owner module is designed to maintain the patient details. The attribute selection model is used to select sensitive attributes. PHR is maintained with different attribute collections. Data owner assigns access permissions to many different authorities. 2) **Cloud Provider:** The cloud provider module is used to store the PHR values and these PHR values are stored in databases. Data owner uploads the encrypted PHR to the cloud providers. User access information's are maintained under the cloud provider. 3) **Key Management:** The key management module is designed to manage key values for various authorities. Key values are uploaded by the data owners. In key management process key insert and key revocation tasks takes place. Dynamic policy based key management scheme is used in the system. 4) **Security Process:** The security process handles the ABE operations. Different encryption tasks are carried out for each authority. Attribute groups are used that allow role based access. Data decryption is performed under the user environment. 5) **Authority Analysis:** Authority analysis module is designed to verify the users with their roles. Authority permissions are initiated by the data owners. Authority based key values are issued by the key management server. The key and associated attributes are provided by the central authority. 6) **Client:** The client module is used to access patients. In the system personal and professional access models are used. Access category is used to provide different attributes. The client access log maintains the user request information for auditing process.
OUTCOME AND POSSIBLE RESULT
The proposed framework of secure sharing of personal medical records in cloud computing, considering partially trustworthy cloud servers, assume that to fully realize the patient-centric concept, patients shall have complete control of their own privacy by encrypting their medical record files so to allow fine grained access. Public and Personal access models are design with security and privacy enabled mechanism.

7. CONCLUSION
Paper proposed the detail design framework of secure sharing of personal medical records in cloud computing. Considering partially trustworthy cloud servers, patients shall have complete control of their own privacy through encrypting their medical record files to allow fine-grained access. The attribute-based encryption model is enhanced to support operations with MAABE. The system is improved to support dynamic policy management model. Thus, Personal Health Records are maintained with security and privacy.

FUTURE SCOPE
In future, would like to protect the privacy of user attributes and identified a new privacy challenge during data accessing in the cloud computing authority sharing. However, to integrate ABE into a large-scale PHR system, important issues such as key management scalability, dynamic policy updates, and efficient on-demand revocation will be solved.

REFERENCES