International Journal of Advance Research in Science and Engineering
Volume No.07, Special Issue No. (01), January 2018
www.ijarse.com
IJARSE
ISSN: 2319-8354

Profile based Anonymization as Heterogeneous Access Isolation Mechanism for Outsourced Personal Health Record in Cloud

Mrs. Dhina Suresh[1], Dr.M.Lilly Florence[2]

[1]*Research Scholar, Department of CS*
St.Joseph's College of Arts and Science for Women Hosur, Tamilnadu, (India)
[2]*Professor, Department of CA*
Adhiyamaan College of Engineering Hosur, Tamilnadu, (India)

ABSTRACT

With the advent of cloud computing, data owners are motivated to outsource their data to public cloud servers while allowing data users to retrieve this data. In this paper, we propose a novel heterogeneous access isolation mechanism named as profiling based Anonymization for outsourced electronic health record in the cloud. Profile based Anonymization contains fine grained access rules for different level of constraints to represent its interaction on the data. It is defence mechanism against the smart attackers. Profile considered as signature for every data user or to the group of user and also corresponding constraints has been placed to that particular profile with encrypted index to anonymize the specified data. In data user scenario, user request the data access to the cloud, user the system retrieves the data by anonymize and non anonymize set of data for the particular profile of the user with utilization of the proxy reencryption. The Proposed model is enable automatic revocation of delegator by change of signature. The Signature will be revised during addition and deletion new user to the group. The system has to be trained initially with different user profile to access the data of the data owner. The experimental analysis proves that the proposed method outperforms against the state of art approaches in terms computation time and precision in the data retrieved.

Keywords: Profile Based Anonymization, Heterogeneous Access Isolation Mechanism, Electronic Health Record, Outsourced Data

I.INTRODUCTION

The Electronic Health Record System is a major proposal of integrating the healthcare records which has been led by healthcare professionals and industry to facilitate the sharing of healthcare information to allow the exchange of patient health information across several enterprise [22], providing clinicians with more information about patients health, aiding the delivery of well-informed diagnosis, and ultimately improving the healthcare service itself [1], [2]. The pertinence is greater as health data is a part of treatment flow. Due to some

reason with health care enterprises [23], [24], [25] patients tend to move between several healthcare institutions to undergo all the required examinations.

Especially, each patient is promised the full control of her medical records and can share her health data with a wide range of users, including healthcare providers, family members or friends. Mostly cloud storage servers are often the targets of various malicious behaviours which may lead to exposure of the private data. In order to prevent the access control towards the patient record a achievable and favourable perspective would be to encrypt the data before outsourcing using public key cryptosystem [3] or through access control constrainst and rules [4].

EHR should only be available to the granted user with the decryption key, but grant user may expose this key with many other users by conducting malicious activity. In order to prevent non authentic data and key sharing privileges in the multi owner scenario and in addition users may overwhelmed with key management overhead, several secure mechanisms have been employed in the cloud such as Proxy Re - encryption scheme[5], [6] and Key aggregate Signature [7].

In this paper, we endeavour to propose a profile based Anonymization technique which contains fine grained access rules for different level of constraints to represent its interaction on the data. It is defence mechanism against the smart attackers. However the data in the cloud in kept encrypted with profile information. Profile considered as signature for every data user and also corresponding constraints is kept in terms of encrypted index to the data access has been placed to that particular profile by encrypting the specified information in the data which has been kept confidential from that particular profile (data user). In data user scenario, user request to the data access is carried out using multi keyword query, the system searches the data by using searchable mechanism and retrieves the result with anonymize and non anonymize content for the particular profile of the user.

The paper is ordered as follows: Section 2 discusses the related works in Secure Sharing of Health Record and its impacts against the performing security under multi owner environment, Section 3 briefly discusses the proposed technique in terms of profile based aggregate Key generation [8] and novel Signature generation for Delegation of Access Rights during addition and deletion of the user to the group. Section 4 presents the experimental results on a huge number of medical records of patients. Section 5 discusses conclusions and future work.

II.RELATED WORK

There exist many techniques to secure the health records are designed and implemented efficiently. Each of these techniques follows some sort of security principles, among few performs nearly equivalent to the proposed framework is described as follows

2.1Encryption Algorithm Schemes

An encryption algorithm endures a reliable connection over the network. It fortifies the data. There is a diverse of enciphering algorithms. Encryption necessitates taking plaintext and converting it to ciphertext using the same key, or secret, to encrypt and decrypt the text. This is symmetric encryption [16] and it is relatively fast

compared to other types of encryption such as asymmetric encryption. The most widely-used algorithm used in symmetric key cryptography is DES and AES (Advanced Encryption Standard). Asymmetric algorithms use two mutual dependent keys, one to encrypt the other to decrypt the data.The most common asymmetric encryption algorithms are the Diffie-Hellman key exchange, and The RSA (Rivest, Shamir and Adleman) asymmetric algorithm.

2.2Timing Enabled Proxy Re-encryption

In this mechanism, system involuntarily revokes the delegation right of the user after a certain time period assigned by the data owner. The duration of the time is enveloped in the ciphertext during the encryption of the file. It has provisioned with diverse effective access time period for each user of data. The System is also enabling with proxy re-encryption in order to provide flexibility in data access without decryption at every instance [26].

2.3User Usage based Encryption

User usage based encryption (UUBE) [17] relies on the searchable encryption scheme to fortify the robust and tough privacy preservation. Usage is portrayed as credential with time frame to each event, event considered as privacy attribute. Data user can decipher an event only if there is a match between the credentials associated with the event. Data user is allowed to maintain credentials according to their usage category. Private keys assigned to the data user as labels with the credentials [9]. A data owner couples each encrypted event with a set of credentials. The Singular Value Decomposition [18] is applied to unused or less used attribute in order to dimensionally reduced feature set or attribute set before the encryption. A weaker notion of data user confidentiality is defined and a secure overlay maintenance protocol is designed to preserve the weak data user confidentiality.

2.4Multi Authority Attribute based Encryption

Chase [19] initiated a MA-ABE technique to overwhelm the drawbacks of a single authority ABE. It uses a Central Authority (CA) and multiple attribute authorities (AA).The trouble with Chase MA-ABE is that the CA can decrypt the encrypted messages which harm the privacy and confidentiality of the data. Chase and Chow [20] proposed a multi authority ABE scheme without the central authority CA. This scheme had no trusted authority which strengthens the user privacy. Distributed pseudo random functions were used in the scheme and it provided collusion resistance to any number of users.

Patient-centric access control method is a set of mechanisms for data access to PHR stored in semi-trusted servers. To achieve fine-grained and scalable data access control attribute based encryption (ABE) techniques is powered to encrypt each patient's PHR file based on the sensitive attributes [10], [11]. A high degree of patient privacy is guaranteed simultaneously by exploiting multi-authority ABE. The scheme also enables dynamic

modification of access policies or file attributes, supports efficient on-demand user/attribute revocation and break-glass access under emergency scenarios.

III.PROPOSED SYSTEM

In this section, we describe Novel Profile based Anonymization a Signature generation Encryption Model which acts as access control mechanism, is given by

3.1System Model

The Electronic Health Record System is constructed with server space to data storage and different entities for registration and access control provision to actors of the cloud server. The Actor are data owner, data user and cloud Admin. Data owner outsource the file to cloud server whereas data user request the access to the file placed by data owner. Cloud Admin provides multiple utilities like secure mechanism for data uploading through encryption and access control algorithm. Search server is also employed by cloud administrator. The search server fulfils search/add/delete mechanisms according to users' invocations whereas the storage provider is accountable for storing data [12].

3.2. Attack model

Spiteful frontage attacker [13] could eavesdrop or intrude and analyze the information such as the enciphered indexes and trapdoors. Guessing attack can also be launched to the cloud server for data access. The revoked users may try to access data beyond the designated access rules using their private keys. The Attacker intends to infer privacy information according to these data. Furthermore, the revoked or repealed delegates may seek to access data beyond the nominated time period using their private keys.

3.3. Notations and preliminaries

- W - Keyword Index namely set of keyword as $W = \{w_1, w_2, w_3, \ldots w_n\}$
- P_i - Profile or Signature
- C_i - Cipher Text
- T_w - Trapdoor of the user or delegator
- K_p, K_d - Public key and Private key of the Data owner to the outsourced Data
- K_A - Aggregate Key for Proxy re encryption

3.4. User Access modelling using Searchable Encryption

The Searchable encryption should allow data owner an enforced authority delegation without revealing his private key. The delegation assignment has to be automatically terminated when the preset effective condition is employed in terms of puzzle. It should prevent the authorized user from accessing the record after some constrainst violations. It has to model in terms of diverse profile to access the data for different categories of delegates.

International Journal of Advance Research in Science and Engineering
Volume No.07, Special Issue No. (01), January 2018
www.ijarse.com
IJARSE
ISSN: 2319-8354

3.5. Access Constraints modelling for User Access

Access Constraints are modelled in terms of profile. Profile has been modelled with set of rules to execute a predefined set of computations which in form of data related information to extract the data [14], [15]. In the access control model to health care data, users and groups are represented by profile (P_i), and they are assigned rights and permissions that inform the cloud server what each user and group can do. Each resource has an owner who grants permissions to data user as depicted in the figure 1.

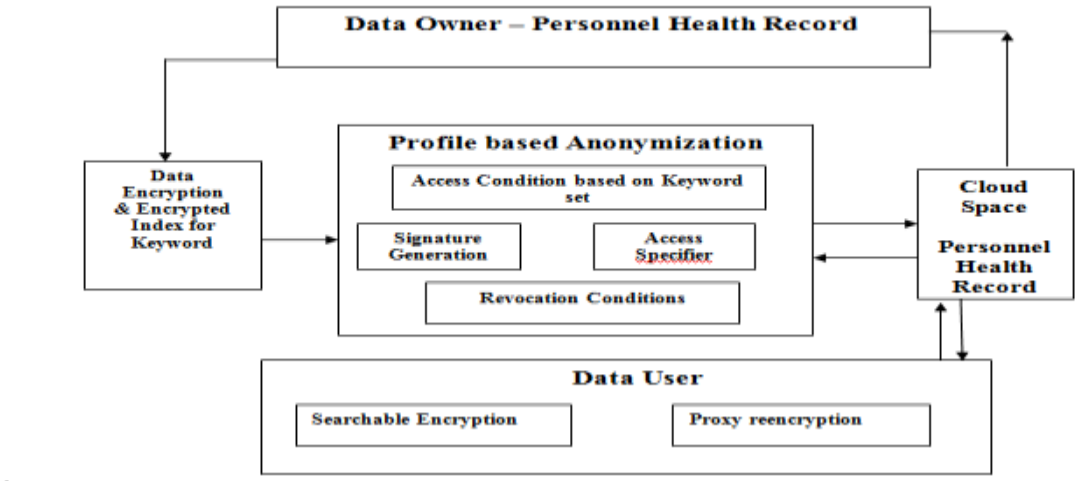

Figure 1 Architecture diagram of the proposed Architecture

During the access control check, these permissions are examined to determine which user can access the resource and how they can access it.

3.6. Data Encryption

It is a symmetric encryption algorithm. The encryption process uses a set of specially derived keys called round keys. These are applied, along with other operations, on an array of data that holds exactly the data to be encrypted [21], [27]. The block to be encrypted is just a sequence of 128 bits. AES works with byte quantities so we first convert the 128 bits into 16 bytes. Array is called state array.

3.6.1 Algorithm 1: AES for Data Encryption

- data block of 4 columns of 4 bytes is state
- key is expanded to array of words
- has 9/11/13 rounds in which state undergoes:
- byte substitution (1 S-box used on every byte)

- shift rows (permute bytes between groups/columns)
- mix columns (subs using matrix multiply of groups)
- add round key (XOR state with key material)
- view as alternating XOR key & scramble data bytes
- initial XOR key material & incomplete last round
- with fast XOR & table lookup implementation

3.6.2 Algorithm 2: AES Decryption

- AES decryption is not identical to encryption since steps done in reverse
- but can define an equivalent inverse cipher with steps as for encryption
- but using inverses of each step
- with a different key schedule
- works since result is unchanged when
- swap byte substitution & shift rows
- swap mix columns & add (tweaked) round key

3.7. Signature generation for Automatic user Revocation using Proxy Re encryption scheme

Ring signature is a group signature for data sharing in the cloud architecture for profile based Anonymization. Ring Signature is to construct an anonymous and authentic data sharing system for end user. Ring signatures differ in two ways, initially there is a way to revoke the anonymity of an individual signature, and second, any group of users can be used as a group without additional setup. Ring signature scheme consists of three algorithms: $KeyGen$, $Sign$, and $Verify$. Proxy server is used for proxy reencryption for data delegation with decryption key, it will valid until the profile signature is modified and updated. Profile signature will be updated once new user joins or leave the group.

3.7.1 Ring Signature Generation

- A group consists of n members $G1, G2, G3, G4, G5, ..., Gn$
- Users which are outside the group G is $U1, U2, U3, U4, U5, ...Un$
- Each group member have their own (private, public) key pairs
- Any group member can upload encrypted file in cloud which is signed by ring signature
- Ring signature of a member = his/her private key and all group members public key
- Each file encrypts with symmetric keys $E1, E2, E3$.

The Process is explained below

3.7.2 Ring Signature for Profile ()

1. Group member $G1$ uploads an encrypted file F in cloud signed with his ring signature
2. Group member $G2$ sends request to edit or update file $F1$ to $G1$ (data owner)
3. $G1$ gives permission to edit.
   - $G2$ can edit only 10% of file content at a time.
   - If the same person asks permission to edit more than 7 times, from the 8^{th} request he has to submit reason with each request.
4. After editing or updating $G2$ signed by his ring signature.
5. All group members get notification about the file editing
6. If the user $U1$ (outside group member) wants to share files $F1, F2, F5, F19, F10$ he sends request to data owner.
7. Data owner share the symmetric keys of requested files in the form of AGGREGATE KEY (completed in phase 1).
8. If $U1$ wants to check the authentication of files, he will send request to key server verifies whether the editor is from group G or not.
9. If $U1$ wants to check the integrity of files, he will send request keys server. Key server verifies data integrity.
10. If Integrity or authentication is incorrect, key server sends notification to user and data will be disclosed.

.

IV.EXPERIMENTAL SURVEY

In this section, we analyse the security of the proposed model against the various attacks. It is an effective scheme against the eavesdropping attack and Guessing attack.

4.1. Dataset Illustration

The database size is taken nearly to different classification which consist of 50GB , 100Gb and 150GB of the record size of the personal health record of the cross enterprise in data center. Most of the experimental outcomes are obtained with an Intel Core I3 processor with 2620 Processors (2.0 GHz) and 4 GB RAM and 500 GB Hard disk using Java programming. Performance Survey of access control mechanism for database size of 150 GB and 100 GB are compared and represented in Table 1 and 2 respectively.

4.2. Performance Assessment for Security

The performance of our suggested scheme is evaluated in terms time taken and privacy are important indicators to evaluate whether a scheme is suitable for the privacy–preserving in the PHR cloud storage.

3.7.1. Computation Time: Analysis of Encryption Time and Decryption Time

In Access Control System the Condition controlled function will enable the EHR data owner to flexibly disseminate his access right to another user in a specified condition. The delegation revocation can be achieved

even when the EHR data owner is offline. The Figure 3.describes the Computation time for encryption and decryption time utilized for securing of the data using public key encryption. The Table 1 describes the performance values of the Access control procedure for database size of 100GB.

4.2.2. Efficiency Analysis: Memory Utilization and Communication Cost

The profile based Anonymization provides the users more convenience to return the accurate results that fulfils users' multiple requirements. The users do not have to request an individual record and rely on an intersection calculation to obtain what they needs. To the best of our knowledge, there is no existing proxy re-encryption searchable encryption scheme could provide the search capability without requiring a random oracle. Our scheme has solved this open problem.

4.3.3. Security Analysis

Proposed System is an effective approach to prevent the eavesdropping attacks over a public communication channel. An outside attacker could easily implement an off-line KG attack by monitoring the information channel between the patient and the data centre; it is controlled by powerful countermeasure applied. Most of the existing schemes have not taken KG attacks into consideration.

Technique	Encryption Time in Milliseconds	Decryption Time in milliseconds	Communication Cost in Size(mb)	Memory utilization in size(mb)	Computation Cost in milliseconds
Profile based Anonymization	105	39	9	25	160
User Usage based Encryption	170	140	17	14	326
Time Enabled Proxy re encryption	200	195	19	12	456
Multi Authority – Attribute Based Encryption	295	270	24	4	719

Table 1 –Database Size of 100 GB

The bilinear pairing computation is the most time consuming operation among all computations. It can be found that the proposed system can achieve a higher efficiency than other existing systems.

International Journal of Advance Research in Science and Engineering
Volume No.07, Special Issue No. (01), January 2018
www.ijarse.com
IJARSE
ISSN: 2319-8354

The proposed model guarantees the security against the attackers including the server attackers and outside attackers could not find the relationship between the given trapdoor and the challenge keywords even though other trapdoors for both delegator and delegate can be obtained.

Thus, the proposed scheme has various useful functions and has stronger security functionality than those of most of the existing searchable encryption schemes.

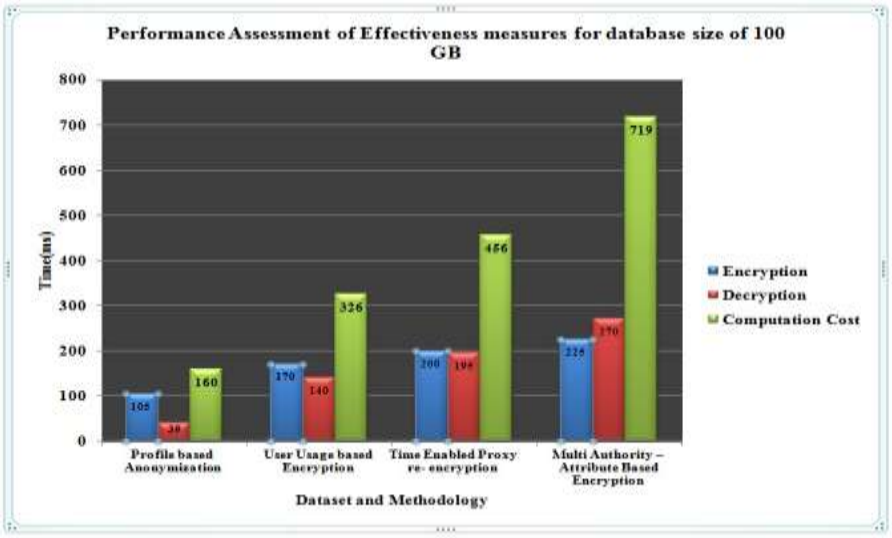

Figure 2 - Performance Assessment of Effectiveness measures for database size of 100 GB

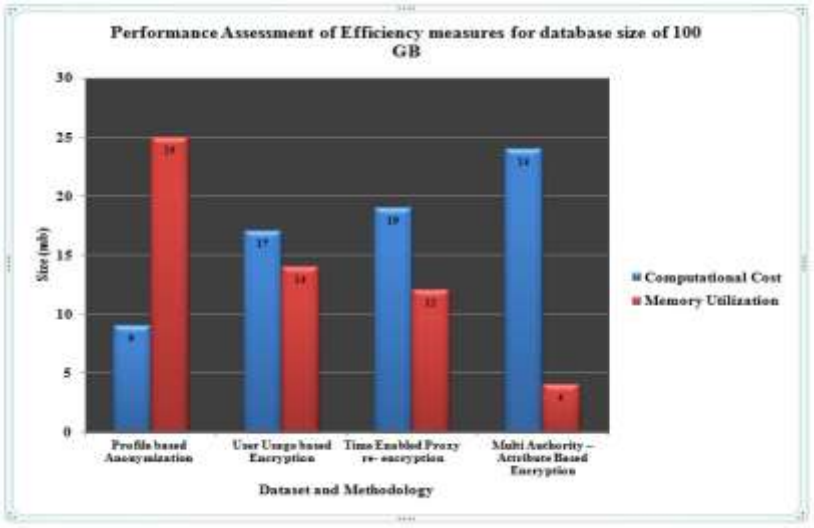

Figure 3 - Performance Assessment of Efficiency measures for database size of 100 GB

The delegation request could be rejected if the signature is Forged and If the time information hidden in the re-encrypted ciphertext is inconsistent with that in the delegation trapdoor, access is denied , hence proposedprofile based signature generation outperforms in terms of secured access in automatic manner.

V.CONCLUSION

We have designed and implemented Profile based Anonymization scheme in the multi tenant environment. The model ensures the high security level towards data sharing against the various attacks by revocation of user if system identifies the misconduct in the data access. . Profile considered as signature for every data user or to the group of user and also corresponding constraints has been placed to that particular profile with encrypted index to anonymize the specified data. It enables dynamic modification of access and revocation of the users to the data of the data owner. In data user scenario, user request the data access to the cloud, user the system retrieves the data by anonymize and non anonymize set of data for the particular profile of the user with utilization of the proxy reencryption. The Proposed model is enable automatic revocation of delegator by change of signature. The Signature will be revised during addition and deletion new user to the group. The system has to be trained initially with different user profile to access the data of the data owner. The Experimental analysis proves that proposed model holds much better efficiency in terms of time, Scalability and Security compared with state of art approaches

VI.ACKNOWLEDGEMENTS

I would like to thank THE LORD MY SAVIOR for guiding and showering HIS blessings throughout my life. I take immense pleasure in thanking my guide Dr. M. Lilly Florence for rendering her valuable knowledge and guidance. I would like to thank my husband for his love and support. I would like to thank my parents and my son for their patience and care. I would like to thank all my well wishers who always stand by my side and guiding me throughout my research.

REFERENCES

[1] M. Li, S. Yu, K. Ren, and W. Lou, "Securing personal health records in cloud computing: Patient-centric and fine-grained data access control in multi-owner settings," in Secure Comm'10, Sept.2010, pp. 89–106.

[2] Lohr,H., Sadeghi,A.-R.,Winandy,M., "Securing the e-health cloud", In: Proceedings of the 1st ACM International Health Informatics Symposium, ser. IHI ' vol. 10, pp. 220–229 (2010)

[3] W. Yau, R. Phan, S. Heng, B. Goi, "Keyword guessing attacks on secure searchable public key encryption schemes with a designated tester," International Journal of Computer Mathematics, vol. 90, no. 2, pp. 2581-2587, 2013.

[4] Shucheng Yu ; Yao Zheng ; Kui Ren ; Wenjing Lou Ming Li, "Scalable and Secure Sharing of Personal Health Records in Cloud Computing Using Attribute-Based Encryption" In IEEE Transactions on Parallel and Distributed Systems (Volume: 24, Issue: 1, Jan. 2013)

[5] K. Liang, Q. Huang, R. Schlegel, D. S. Wong, C. Tang, "A Conditional Proxy Broadcast Re-Encryption Scheme Supporting Timed-Release," In Proc. Information Security Practice and Experience, pp. 132-146, Springer Berlin Heidelberg, 2013.

[6] Yau, W., Phan, R. Heng, S., Goi, B.: "Proxy re-encryption with keyword search, new definitions and algorithms" In: Proceedings International Conferences on Security Technology, Disaster Recovery and Business Continuity, Jeju Island, Korea, vol. 122, pp. 149–160. 13–15 December 2010.

[7] Liu, Q.,Wang, G.,Wu, J.: "Time-based proxy re-encryption scheme for secure data sharing in a cloud environment" Inf. Sci. 258, 355–370 (2014).

[8] Hong Liu ; Huansheng Ning ; Qingxu Xiong ; Laurence T. Yang "Shared Authority Based Privacy-Preserving Authentication Protocol in Cloud Computing" IEEE Transactions on Parallel and Distributed Systems (Volume: 26, Issue: 1, Jan. 2015)

[9]. Ming Li, Shucheng Yu, Yao Zheng, Kui Ren,Wenjing Lou "Scalable and Secure Sharing of Personal Health Records in Cloud Computing using Attribute-based Encryption"IEEE Transaction on Parallel and Distributed computing,2012.

[10] Ibraimi, L., Asim, M., Petkovic, M.: Secure management of personal health records by applying attribute-based encryption. In Technical Report, University of Twente (2009)

[11]. Smitha Sundareswaran ; Anna Squicciarini ; Dan Lin "Ensuring Distributed Accountability for Data Sharing in the Cloud" IEEE Transactions on Dependable and Secure Computing (Volume: 9, Issue: 4, July-Aug. 2012)

[12] D. Boneh, B. Waters, "Conjunctive subset and range queries on encrypted data," in *Proc. 4th Theory of Cryptography Conference*, Amsterdam, The Netherlands, February 21-24, 2007, vol. 4392, pp.535–54, Springer.

[13] B. Zhang, F. Zhang, "An efficient public key encryption with conjunctive-subset keywords search," *Journal of Network and Computer Applications*, vol. 34, no. 1, 262-267, 2011.

[14] J. Li, Y. Shi, Y. Zhang, "Searchable ciphertext policy attribute based encryption with revocation in cloud storage," *International Journal of Communication Systems*, published online, DOI: 10.1002/ dac.2942, 2015.

[15] Li,M.,Yu, S., Cao, N., Lou,W.:Authorized private keyword search over encrypted personal health records in cloud computing. In:ICDCS '11 (June 2011)

[16] Dr.M. Lilly Florence, Mrs.Dhina Suresh, "Cloud security and DES algorithm a review" In International Journal of Computational Intelligence and Informatics, vol. 5, No. 2 (September 2015)

[17] Dr.M. Lilly Florence, Mrs.Dhina Suresh, "Enhanced secure sharing of PHR's in cloud using user usage based attribute based encryption and signature with keyword search" In Cluster Computing The Journal of Networks, Software Tools and Applications" DOI 10.1007/s10586-017-1276-7, Springer.

[18] Jiang, Y., Hayashi, I., Wang, S."Knowledge acquisition method based on singular value decomposition for human motion analysis" In IEEE Trans. Knowl. Data Eng. 26(12), 3038–3050 (2014).

[19] Chase, M.: Multi-authority attribute-based encryption, In: The Fourth Theory of Cryptography Conference (TCC 2007) (2007)

[20] Chase, M., Chow, S.S.: Improving privacy and security in multiauthority attribute-based encryption. In: CCS '09, 2009 pp. 121– 130

[21] W. Cong, N. Cao, K. Ren, and W. Lou, "Enabling secure and efficient ranked keyword search over outsourced cloud data," *IEEE Trans. Parallel Distrib. Syst.*, vol. 23, no. 8, pp. 1467–1479, Aug. 2012.

[22] Microsoft, Microsoft health vault. http://www.healthvault.com

[23] Google Inc, Google health. https://www.google.com/health

[24] California, Confidentiality of Medical Information Act (CMIA).www.leginfo.ca.gov/cgi-bin/displaycode?section=civ-group=00001-01000

[25] 104th United States Congress, Health Insurance Portability and Accountability Act of 1996 (HIPPA). http://aspe.hhs.gov/admnsimp/pl104191.htm (1996)

[26] R. A. Popa *et al.*, "CryptDB: Protecting confidentiality with encrypted query processing," in *Proc. 23rd ACM Symp. Operating Syst. Principles*, Cascais, Portugal, 2011, pp. 85–100.

[27] J. Baek, R. Safavi-Naini, W. Susilo, "Public key encryption with keyword search revisited," in *Proc. International Conference on Computational Science and Its Applications (ICCSA)*, Perugia, Italy, June 30-July 3, 2008, vol. 5072, pp. 1249–1259, Springer.

Mrs.Dhina Suresh

Dhina Suresh was born in Tirunelveli,Tamil Nadu (TN), India, in 1983. She received the Master in Science (M.Sc) in Software Engineering degree from Periyar University, Salem, TN, India, in 2005 and Master of Philosophy(M.Phil.) of Computer Science Degree from the Periyar University, in 2007. Currently she is pursuing my Ph. D in Computer Science in Periyar University, Salem under the guidance of Dr. M.Lilly Florence. Her research area is security in cloud computing.

Dr. M. Lilly Florence

Dr. M. Lilly Florence, Professor, Department of M.C.A, Adhiyamaan College of Engineering, Hosur. She received her Bachelor degree in Mathematics during 1995 and Master degree in Computer Application during 1998 at Manonmaniam Sundaranar University. She completed her M.Tech at Punjab University at 2003. She completed her Ph. D in computer science at Mother Teresa University during 2006 2011. She has published over 14 research papers in International and National journals.