Applied Mathematics & Information Sciences
An International Journal

http://dx.doi.org/10.18576/amis/130210

A Partial Grained Attribute-Based Encryption for Secure Data Access in the Cloud Environment

M. P. Revathi and P. D. Sheba Kezia Malarchelvi*

Department of Computer Science and Engineering, J.J. College of Engineering and Technology, Tiruchirappalli-09, TamilNadu, India

Received: 2 Aug. 2018, Revised: 12 Dec. 2018, Accepted: 22 Dec. 2018
Published online: 1 Mar. 2019

Abstract: A recent fast-developing method for easy access and sharing of medical data is to maintain the patients' information in the form of Electronic Health Record (EHRs). Nowadays, these EHRs are most frequently outsourced and stockpiled at third parties namely cloud servers. This reduces the burden on health care providers but introduces more safety problems like revealing of health data to unapproved parties due to access, by not only illegitimate users but also unauthorized access by legitimate users. Though illegitimate users can be identified by authentication mechanisms, unauthorized access by authentic users cannot be restricted by such authentication mechanisms. To guarantee the control of the users' access, efficient access-control mechanisms and access-policies are required. This research paper introduces an innovative data access mechanism based on Partial grained Attribute-Based Encryption (PABE) and policies to access, depending on users' roles in cloud servers. The proposed secure data access aims at providing attribute-based keys selectively only to sensitive data thereby restricting access to sensitive data alone to reduce accessing validation time rights.

Keywords: Role based users, data access key, access-control matrix or policy, key management.

1 Introduction

Recently, both industrial and academic worlds are concentrating more in the area of cloud computing. Various Cloud applications are available: for instance Google Apps and Microsoft online, the infrastructures namely Nimbus, Eucalyptus and Amazon Elastic compute cloud. Some of the platforms for writing applications are Amazon simple storage service and Windows Azure. The huge amounts of information accumulated at clouds are due to enormous amount of medical health records and social media networks. Information security and privacy are major concerns with cloud computing and hence mechanisms for authentication, confidentiality and access-control are highly essential.

Large quantity of data is kept in remote cloud, so more attention is given to the access-control. There are a lot of access-control methods existing namely User-Based access-control (UBAC), Attribute-Based access-control (ABAC), Role-Based access-control (RBAC) etc. At UBAC, the access-control list comprises the authorized data user to avail the data.

Kuhn et al. [1] permitted data to reach users if they have roles in similarity. Only authorized senior-level secretaries and faculties possess the rights for accessing the data while the junior-level secretaries are not authenticated. Here, an ABAC allows users to access a group of attributes conforming to the access-control policy.

access-control in health care system has been already discussed [2, 3]. Data are accessed by policy makers, researchers, doctors and staff members in the hospital. The data are encrypted by attribute-based encryption with access policies. The keys are provided to users and the users with the keys are able to decrypt data in the cloud.

Goyal et al. showed that the data owners have policy to access the encrypted data [4]. Secret keys and attributes are issued through the attribute authority to the receiver. The keys are employed to decrypt information, if it matched with the attribute.

Fine-grained access-control mechanisms are complex and time consuming whereas coarse granularity offers less security. Hence, this paper attempts to devise a partial grained access-control mechanism wherein access to sensitive attributes are stringent according to the users' roles than access to insensitive attributes. The remaining part of this paper is organized as below: Section 2 elaborates the related works on data access-control schemes. In Section 3, the proposed partial grained

[*] Corresponding author e-mail: reva.lokven@gmail.com

access-control mechanism for safeguarding access of EHRs (Electronic Health Records) is presented. The experimental results are presented in Section 4 and Section 5 provides the conclusion.

2 Related Works

Requirement for scalability, flexibility and accessibility of outsourced data has been studied by Zhiguo et al. [5]. The authors introduced Hierarchical Attribute Set-Based Encryption (HASBE) by extending cipher text policy and Attribute Set-Based Encryption (ASBE) with a hierarchical arrangement of users. However, the technique is more complex and time consuming.

Only if data security is effectively assured during interactions between the cloud and users in cloud computing. So, the mutual trustworthy relationship among cloud platform can be established. Lin et al. implemented a new method of access-policy model which is the combination of Trust Management (TM) and Mutual Trust-Based access-control (MTBAC) [6]. Reliable relationships among cloud services and users are provided by mutual reliable mechanism.

Visualization framework for inter-domain access-control policy integration was proposed by Pan et al. [7], which combines Role-Based access-control (RBAC) policies based on role map and integrated result has been visualized by the authors. The algorithm for role map describes a hybrid role hierarchy but constraints for security are not satisfied and also compose visualization easier.

Cipher text Policy Attribute-Based Encryption (CP-ABE) is one of the widely used technologies for data access-control at cloud storage. The owner of the data gives direct control on access policies to the users; here attribute revocation is the main problem. So, Kan et al. designed revocable data access-control method for multi-authority cloud storage systems [8].

New decentralized access-control suggested by Sushmita et al. [9] for secure storage of data at cloud employs an access authority. In this technique the secure cloud validates the user identity of authentication prior to storing the information. It helps modifying, creating and reading of information stored securely and prevents replayed attacks in cloud.

A new key management has been proposed by Mohamed et al. which is known as Broadcast Group Key Management (BGKM) [10]. The benefits of the system are adding a new user or revoking the existing users and the access policies for updating public information.

Hur proposed a new scheme which is CP-ABE for an information-shared system [11]. The main characteristic of the model is the secure transmission between data storage and the centre of key generation, user revocation has been done by the proxy encryption.

Yong et al. presented a novel approach based on multi message cipher text policy attribute-based encryption [12]. This approach is used for sharing scalable media based on data consumer fields like name, age and gender rather than the precise list of the consumers' names. This approach is more effective since it permits.

As the content provider uses an access-control policy to encrypt the messages. Users decrypt the cipher text based on the access-policy.

ABE schemes are based on encrypting the attributes individually and providing the decryption keys to the users. ABE provides access only to those attributes which the user is permitted to access. However, encrypting every attribute with a different key is complex and time consuming. So, this work attempts to reduce the complexity by separating sensitive and insensitive attributes and restricting the access to sensitive attributes alone based on the user role.

In this technique, every sensitive attribute is encrypted individually with different keys and the insensitive attributes are encrypted as a whole using a single key. Therefore, all the users are provided access to general insensitive information while access to sensitive attributes is provided by checking the users' role and providing decryption keys only for those attributes for which the role is eligible. Thus, the access to sensitive attributes alone is restricted which improves the time for access.

3 Proposed System Architecture

This architecture consists of four components: Data Owner (D), Role Based Users, access-control Matrix (ACM) and Access Provider (AP). The first component of this system is the data owner who collects the information about the various roles of users like doctor, nurse, patient, lab technician, pharmacy and insurance.

The data owner also collects EHRs of patients and identifies the sensitive attributes $(SA_1, SA_2, SA_3, \ldots, SA_n)$ and insensitive attributes (ISA). The data owner generates the sub-keys. The data owner then strongly encrypts the sensitive attributes the encrypted EHRs are stockpiled in the cloud storage. Secondly, the data users who want to make use of the data get key from the AP according to their role.

The third part illustrates access-control matrix which gives the rights to access each attribute according to the role of the users. AP is accountable for verifying the role of the user and providing dynamic key to the users to make use of the available data in cloud storage.

Fig. 1 depicts the conception about the proposed architecture of data access-control in secure cloud storage.

3.1 Data Owner

The data owner or healthcare provider collects patient details. Secrecy is kept with data using AES and DES

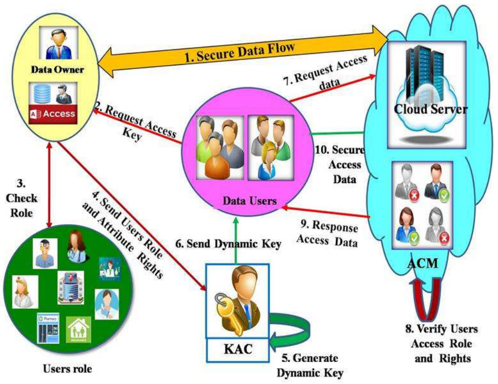
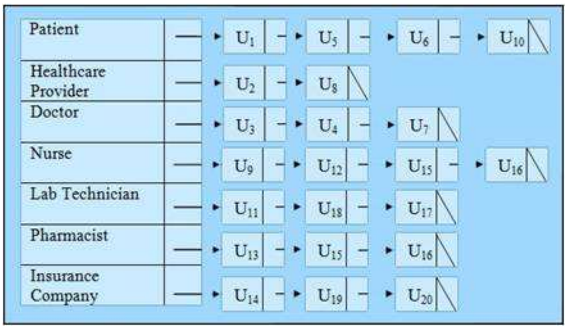


Fig. 1: Proposed architecture diagram of data access-control



Patient	U_1	U_5	U_6	U_{10}
Healthcare Provider	U_2	U_8		
Doctor	U_3	U_4	U_7	
Nurse	U_9	U_{12}	U_{15}	U_{16}
Lab Technician	U_{11}	U_{18}	U_{17}	
Pharmacist	U_{13}	U_{15}	U_{16}	
Insurance Company	U_{14}	U_{19}	U_{20}	

Fig. 2: Users role list–an example

algorithm. The data owner identifies the sensitive attributes (SA_is) and encrypts them individually with 128 bit keys using AES algorithm and encrypts the insensitive attributes as a whole with DES with a 64 bit key. The data owner then stores the encrypted EHRs in the cloud storage. The EHR and encrypted EHR are can be represented as follows:

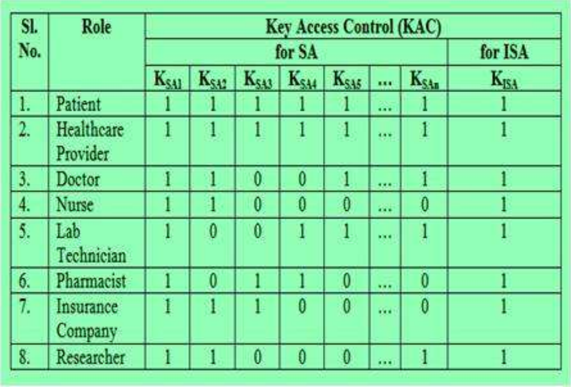
$$EHR = \{SA_1, SA_2, SA_3, SA_4, SA_5 \dots SA_n\} \cup \{ISA\}$$

$$E[EHR] = E_{KSA1}[SA_1] \cup E_{KSA2}[SA_2] \cup E_{KSA3}[SA_3] \cup \cdots \cup E_{KSAn}[SA_n] \cup E_{ISA}[ISA]$$

3.2 Access Provider (AP)

An Access Provider is responsible for sanctioning all related permissions to access in an automatic system and safe guarding the secrecy by recognizing and preventing unsanctioned access appropriately. The Access Provider (AP) associates a role for every user during user registration and maintains a list namely Users Role List as shown in Fig. 2.

The Access Provider also maintains a Key access-control Matrix (KACM) which specifies the attribute keys that are allowed for different roles. A sample KACM is depicted in Fig. 3. The values ‘1’ and ‘0’ in the KACM indicate that the corresponding attribute key can be provided to the user or not respectively, a sample KACM is depicted in Fig. 3.



Sl. No.	Role	Key Access Control (KAC)							
		for SA							for ISA
		K_{SA1}	K_{SA2}	K_{SA3}	K_{SA4}	K_{SA5}	...	K_{SAn}	K_{ISA}
1.	Patient	1	1	1	1	1	...	1	1
2.	Healthcare Provider	1	1	1	1	1	...	1	1
3.	Doctor	1	1	0	0	1	...	1	1
4.	Nurse	1	1	0	0	0	...	0	1
5.	Lab Technician	1	0	0	1	1	...	1	1
6.	Pharmacist	1	0	1	1	0	...	0	1
7.	Insurance Company	1	1	1	0	0	...	0	1
8.	Researcher	1	1	0	0	0	...	1	1

Fig. 3: Key access-control matrix (KACM)-example

Suppose a user with doctor role requests access to the EHR, he sends a request to the Access Provider (AP) who first authenticates the user and identifies his roles from the users’ role list. After identifying his role as Doctor for example, the AP checks the key access-control matrix and provides the decryption keys K_{SA_1}, K_{SA_2}, K_{SA_5}, $\dots$, K_{SA_n} and K_{ISA} because there is a value 1 in the KACM only for these keys and hence the user can decrypt only the attributes SA_1, SA_2, SA_5, $\dots$, SA_n and ISA which are the attributes that a user in doctor role is eligible to access. The user in doctor role is allowed to perform permitted operations described in Table 2 on these attributes. Whenever a user is revoked the node representing that user is deleted from the role list and whenever a new user registers, a node representing that user is added to the role list corresponding to his role. The operations involved in the proposed system are illustrated in Fig. 4.

3.3 Users’ Roles

Users’ roles are data owner, patients, doctors, nurses, lab technicians, pharmacist and insurance company.

Data owner: or healthcare provider has special rights to select any of the six alternative operations of append, view and creation of role for users, modify to construct access-control matrix and delete. A unique patient id is automatically assigned, if the option append is chosen particularly, the data owner requires registering the record of a patient and by selecting ok, it will be uploaded to the cloud storage. Similarly when view option is chosen, the data owner requires inputting the decryption key and the patient id to be viewed. The data owner can edit data, while view modify option is opted. In case, delete option is decided, the data owner the PHR will be deleted.

Patients: his health data is stored in the secured cloud storage. If the patients wish, they may login into their personal details at any time. The Fig. 5 represents the

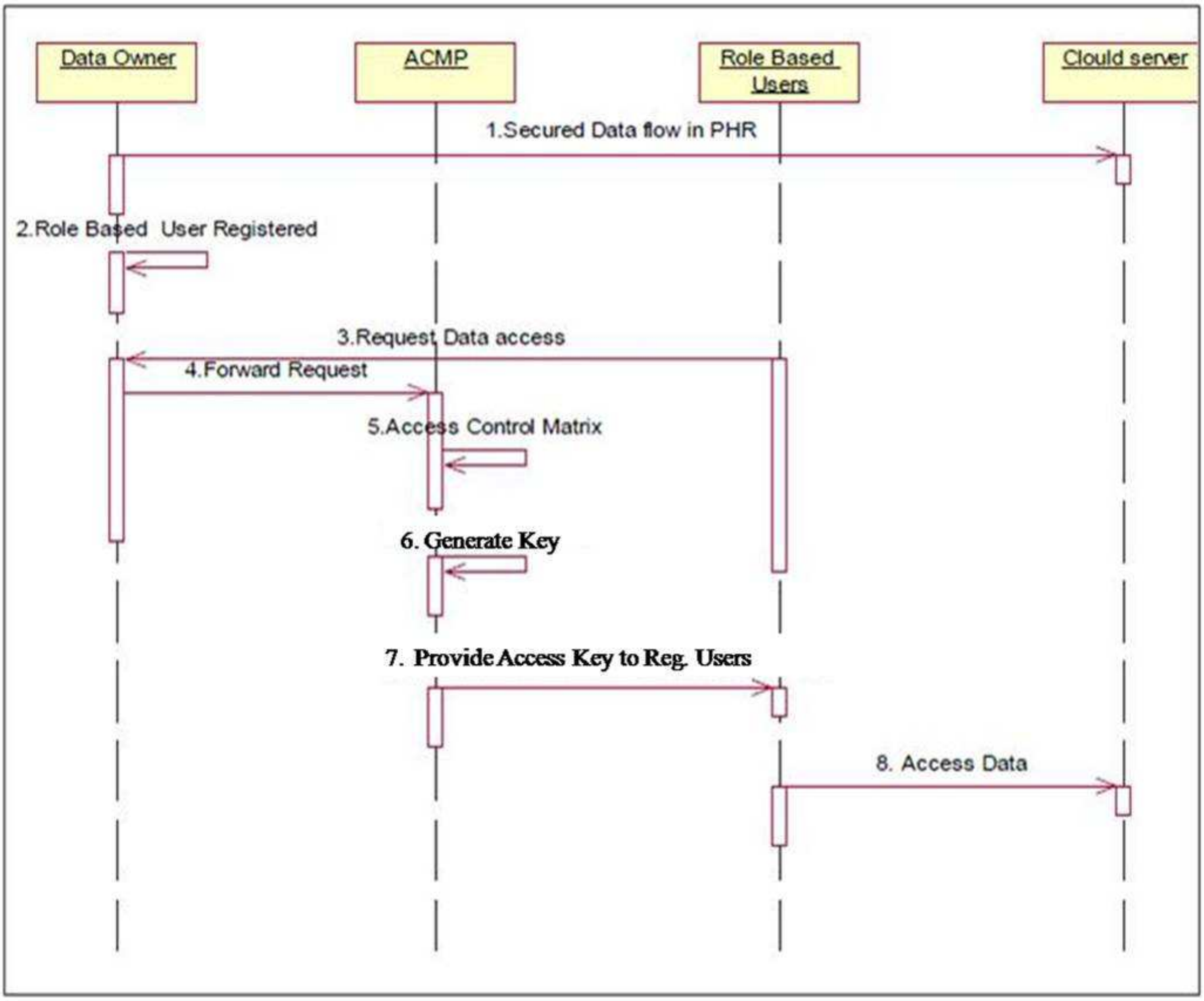


Fig. 4: Sequence diagram of the proposed system

Table 1: Patient access-control matrix

Patient Attributes \ Rights	View	Modify	Append	Delete
Pat-id	Yes	No	No	No
Pat-name	Yes	No	No	No
Pat-address	Yes	Yes	No	No
Pat-mobile no	Yes	Yes	No	No
ECP-name	Yes	Yes	No	No
ECP-mobile	Yes	Yes	No	No
Pat-DOB	Yes	No	No	No
Pat-age	Yes	No	No	No
Pat-gender	Yes	No	No	No
Pat-occupation	Yes	No	No	No

patient role use case diagram and Table 1 mentioned the corresponding patient access-control matrix.

Doctor: they access the patient information, check the reports and provides right prescription. Table 2 describes doctor access-control matrix, Fig. 6 deals with the use case diagram of doctor.

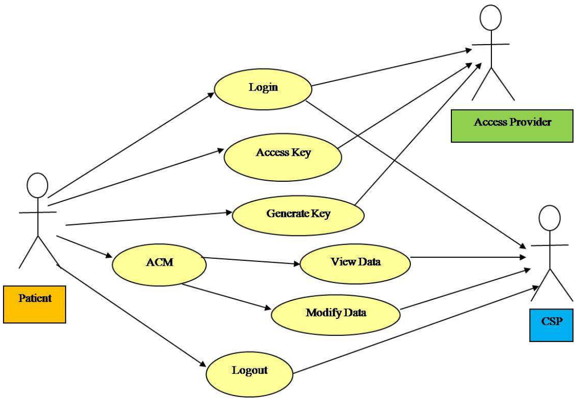


Fig. 5: A use-case diagram of role patient

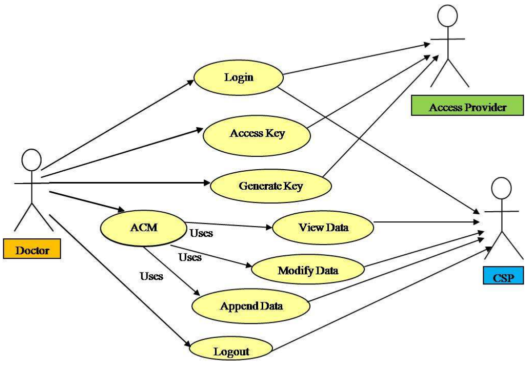


Fig. 6: A use-case diagram of role doctor

Table 2: Doctor access-control matrix

Doctor Attributes \ Rights	View	Modify	Append	Delete
Pat-id	Yes	No	No	No
Pat-name	Yes	No	No	No
Reason for visit	Yes	Yes	No	No
All history	Yes	Yes	No	No
TP-investigation	Yes	Yes	Yes	No
TP-medication	Yes	Yes	Yes	No
TP-procedure	Yes	No	Yes	No

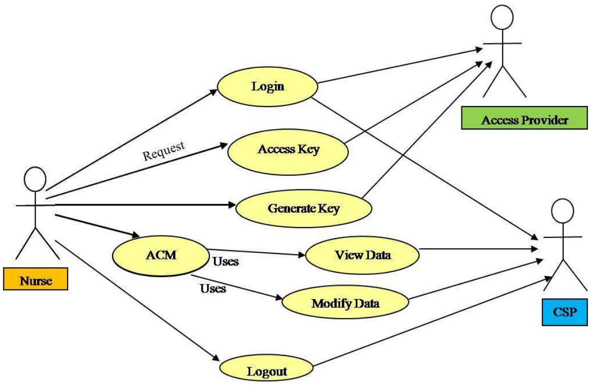


Fig. 7: Role nurse-use case diagram

Nurse: The duty of nurse is that the she records all patient-related information, she verifies regularly the details of the report of the patient and keeps it ready for storing it to the cloud. The Figs. 7, 8, 9 and 10 show the use case diagram of nurse, lab technician, pharmacist and insurance.

Tables 3, 4, 5 and 6 represent access-control matrix of nurse, lab technician, pharmacist and insurance.

Lab Technician: his duty is to get the test reports of the patient like blood test and include the details in the appropriate EHR.

Pharmacist: his duty is to access the prescriptions and issue the suitable medicines to the patients as per the prescription of the doctor

Table 3: Nurse access-control matrix

Nurse Attributes \ Rights	View	Modify	Append	Delete
Pat-id	No	No	No	No
Pat-name	No	No	No	No
CEV-Systolic BP	No	No	Yes	No
CEV-Diastolic BP	No	No	Yes	No
Temp	No	No	Yes	No
Respiration rate	No	No	Yes	No
Height	Yes	No	Yes	No
Weight	No	No	Yes	No

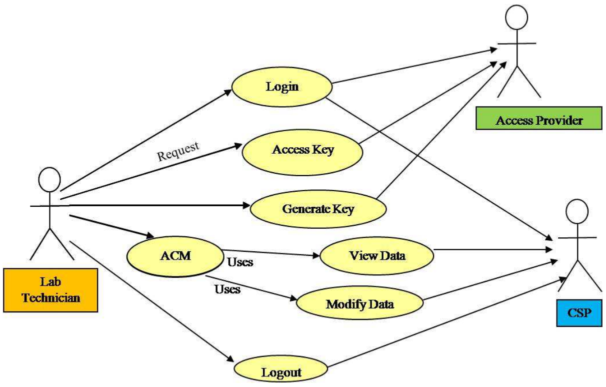


Fig. 8: Role lab technician-use case diagram

Table 4: Lab technician access-control matrix

Lab Technician Attributes\Rights	View	Modify	Append	Delete
Pat-id	Yes	No	No	No
Pat-name	Yes	No	No	No
Blood Group	Yes	No	Yes	No
EGC-report	Yes	No	Yes	No
Blood report	Yes	No	Yes	No
Description	Yes	No	Yes	No

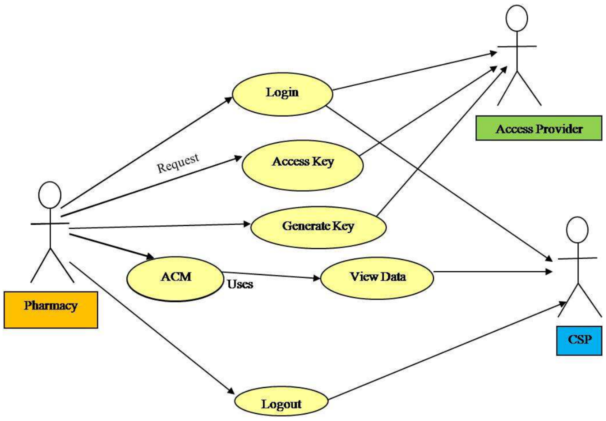


Fig. 9: A use-case diagram of role pharmacist

Insurance: is claimed depending on the real condition after registering patient's information.

Table 5: Pharmacist access-control matrix

Pharmacist Attributes \ Rights	View	Modify	Append	Delete
Pat-id	Yes	No	No	No
Pat-name	Yes	No	No	No
Prescription	Yes	No	No	No

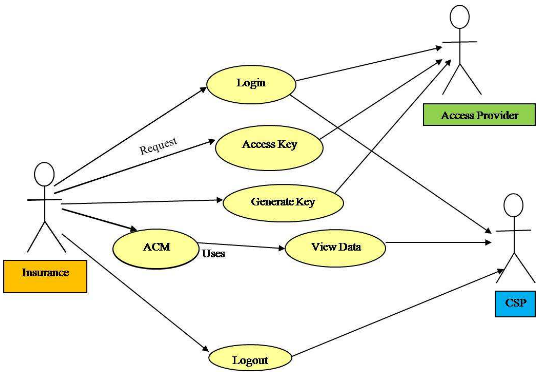


Fig. 10: A use-case diagram of role insurance

Table 6: Insurance company access-control matrix

Insurance Attributes \ Rights	View	Modify	Append	Delete
Pat-id	Yes	No	No	No
Pat-name	Yes	No	No	No
Pat-address	Yes	No	No	No
Clinic Summary	Yes	No	No	No
Bill Amount	Yes	No	No	No

4 Experimental results and Discussion

The proposed secure data access is implemented in medical data. It contains totally 45 attributes, 25 sensitive attributes and other 20 attributes are insensitive. This system applies AES and DES algorithms for encryption and decryption. The DES algorithm is used to encrypt the Insensitive Sensitive Attributes (ISAs) and AES algorithm to encrypt the Sensitive Attributes (SA_1, SA_2, ...,SA_n). Table 7 presents the execution time taken to encrypt and decrypt a sample set of 7 sensitive attributes SA_1, SA_2, SA_3, SA_4, SA_5, SA_6, SA_7 and that of the insensitive attributes are ($ISA_{1,...,20}$). For example, the time taken in ms to encrypt sensitive attributes SA_1, SA_2 are 0.0028 ms and 0.0059 respectively. The time taken in ms for insensitive attributes is 0.0718.

Similarly, the decryption time taken is ms for individual sensitive attributes and insensitive attributes are presented in Table 7. The decryption time for Insensitive attributes in ms is 0.0329. Fig. 11 depicts the execution time with different algorithms on sensitive and insensitive attributes.

The data access is based on the users' role list and key access-control matrix. First, the users register their details such as name, id, date of birth, roles, designation etc. The admin generates a new user-id and password which is being sent to the user's email. The user can then use this id and password when they wish to access their data from the cloud. But only the encrypted PHR is then retrieved and to decrypt it the user has to send request to the access provider who generates the corresponding keys after checking user role and sends the keys back to the user. The secure data access mechanism described in Section 3 provides the key for accessing insensitive attributes to all the users irrespective of their roles and only restricts access to sensitive data based on their roles. This reduces the key distribution time significantly.

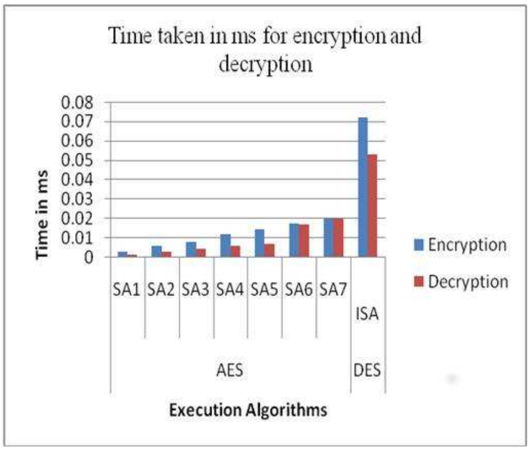


Fig. 11: Execution time with different algorithms in sensitive and insensitive attributes

5 Conclusion

In cloud computing, the control mechanism for accessing data is essential for guaranteeing security of data. Because of outsourcing data and unreliable cloud servers, the access-control has grown to be a critical concern in cloud secure storage systems. Available control schemes for accessing data are not suitable now, as they create either several encrypted copies of the similar information or they want an absolutely reliable secure cloud server. Hence, in this paper, an access-control mechanism to restrict access to data in the cloud based on users' roles, key policy, key access control matrix and partial grained attribute-based encryption has been proposed to ensure that only the authorized users are provided with access to sensitive data.

References

[1] D.R. Kuhn, E.J. Coyne and T.R. Weil, Adding Attributes to Role Based Access Control, IEEE Computer, vol. 43, no. 6, pp. 79–81 (2010).

[2] 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

Table 7: Time taken in ms for encryption and decryption with sensitive and insensitive attributes

Alo / Technique	AES							DES
	SA_1	SA_2	SA_3	SA_4	SA_5	SA_6	SA_7	ISA
Enc	0.0028	0.0059	0.0079	0.0119	0.0146	0.0174	0.0202	0.0718
Dec	0.0015	0.0031	0.0045	0.0059	0.0069	0.0172	0.0198	0.0329

Settings, Proceedings of 6th International ICST Conference on Security and Privacy in Communication Networks (SecureComm), pp. 89–106 (2010).

[3] S. Yu, C. Wang, K. Ren and W. Lou, Attribute Based Data Sharing with Attribute Revocation, Proceedings of ACM Symposium on Information, Computer and Communication Security (ASIACCS), pp. 261–270, (2010).

[4] V. Goyal, O. Pandey, A. Sahai and B. Waters, Attribute Based Encryption for Fine Grained access-control of Encrypted Data, Proceedings of ACM Conference on Computer and Communication Security, pp. 89–98, (2006).

[5] Zhiguo Wan, Jun'e Liu, and Robert H. Deng, HASBE: A Hierarchical Attribute Based Solution for Flexible and Scalable access-control in Cloud Computing, IEEE Transaction on information Forensics and Security, vol. 7, no. 2, pp. 743–754 (2012).

[6] Lin Guoyuan, Wang Danrul, Bie Yuyul, Lei Min, MTBAC: A Mutual Trust Based Access Control Model in Cloud Computing, IEEE Journal and Magazines China Communication, vol. 11, no. 4, pp. 154–162 (2014).

[7] Pan Li, Liu Ning, Z.I. Xiaochao, Visualization Framework for Inter Domain Access Control Policy Integration, IEEE Journal and Magazines China Communication, vol. 10, no. 3, pp. 67–75 (2013).

[8] Kan Yang, and Xiaohua Jia, Expressive, Efficient and Revocable Data Access Control for Multi Authority Cloud Storage, IEEE Transaction on Parallel and Distributed Systems, vol. 25, no. 7, pp. 1735–1744 (2014).

[9] Sushmita Ruj, Milos Stojmenovic, and Amiya Nayak, Decentralized Access Control with Anonymous Authentication of Data Stored in Clouds, IEEE Transaction on Parallel and Distributed Systems, vol. 25, no. 2, pp. 384-394, (2014).

[10] Mohamed Nabeel, Ning Shang, and Elisa Bertino, Privacy Preserving Policy Based Content Sharing in Public Clouds, IEEE Transactions on knowledge and Data Engineering, vol. 25, no. 11, pp. 2602–2614 (2013).

[11] Junbeom Hur, Improving Security and Efficiency in Attribute Based Data Sharing, IEEE Transactions on knowledge and Data Engineering, vol. 25, no. 10, pp. 2271–2282 (2013).

[12] Yong dong Wu, Zhuo Wei, and Robert H. Deng, Attribute Based Access to Scalable Media in Cloud Assisted Content Sharing Networks, IEEE Transaction on Multimedia, vol. 15, no. 4, pp. 778–788 (2013).

M. P. Revathi is the Assistant Professor, Department of Computer Science and Engineering at J.J. College of Engineering and Technology Tiruchirapalli, TamilNadu, India. She completed B.E. (Computer Science and Engineering) in V.M.K.V Engineering College in the year 1995 and M.E. (Computer Science and Engineering) in J.J. College of Engineering and Technology in the year 2007. Her areas of interest include Network Security, Cloud Security, Theory of Computation, Compiler design and Computer Architecture. She has published more than 3 research papers in journals and conferences.

Sheba Kezia Malarchelvi is the Professor and Head of the Department of Computer Science and Engineering at J.J. College of Engineering and Technology Tiruchirapalli, TamilNadu, India. She completed B.E. (Computer Engineering) in Mepco Schlenk Engineering College in the year 1991 and M. E. (Computer Science) in the Regional Engineering College (Presently NITT) in the year 1995. She completed Ph.D. (Computer Science and Engineering) in the year 2010 from Bharathidasan Institute of Technology, Bharathidasan University, Tiruchirapalli, TamilNadu, India. Her areas of interest include Image Encryption, Digital Watermarking, Steganography, Network Security, Cloud Security and Big Data. She has published more than 65 research papers in journals and conferences.