Abstract

Contemporary business models deals with gargantuan amount of data which governs the complete business body and such mammoth amount of data need to be shared among distributed entities for better productivity. In this paper we have proposed a secure data sharing model which ensures that the data remains unaltered while sharing it with other entities. Any information which is shared with other system entities gets vanished from the data owner, which makes data sharing more vulnerable in the present scenario. The proposed model incorporates the concept of assigning distributed authority which takes care of the shared information. The model adopts the distributed attribute based encryption technique to secure the data sharing process in a distributed environment and implemented against the traditional attribute based model and proved that the attribute spooling is eliminated. To enable a secure data sharing and access in a multi access ubiquitous environment, the proposed secured data sharing protocol enhances the attribute based encryption for distributed environment (DABE). The security model uses a two-folded approach for enabling secure data sharing among the parties, initially it allows the data owner to define their access policy along with their attributes then it encapsulates the attributes with the cryptographic parameters and keeps it under the control of attribute authority. As a second fold, to enhance the data interaction process within the system entities a secured channel is created using a public key crypto system. In our model, we encrypted every attribute of the user against a unique private key component, hence spooling of known attribute yields no results to the adversaries. The proposed model remains owner centric, by granting permission to the data user to determine who can access what, when and where while other traditional models fail to achieve this. The confidentiality threshold has been increased by validating the data origin and accessing entity by using robust cryptographic methodology. Our model is designed to offer low overhead and high secure platform to share the data between the data owner and accessing entities. The protocol uses a distributed approach by creating independent authorities thus increasing the system efficiency. The proposed security protocol has been tested in a ubiquitous health care environment and the results are proved to be efficient in terms of overhead, security and spooling.

Keywords: Access Policy, Attribute Authority, Health Data, Secure Data Sharing, Tunnelling, Ubiquitous Computing

1. Introduction

The invisible usage of computers by individuals which makes the human computer interaction more efficient is called ubiquitous computing. The computers become invisible to users but they can experience anywhere computing by integrating everyday activities. This can also be termed as pervasive computing. The usage of ubiquitous computing finds greater application in health care, transportation, home care etc., due to its anywhere availability and flexibility. Since ubiquitous computing has certain issues like scalability and resource constraints, integrating the ubiquitous application with the cloud has made it more efficient and demandable thus solving the problem of scalability and resource constraints. In recent years the cloud based pervasive computing has paved its
way for more advanced inventions and advancements in areas like health care, home care etc. Since it is cloud based the concern of security has increased. So the security issue has become a greater concern in this area. In this paper a cloud based pervasive health care scenario is considered. Enormous work has been carried out in the past in the area of security and privacy. The term ubiquitous healthcare means making the healthcare available everywhere, anytime pervasively. This makes healthcare more uninterrupted to our everyday life, independent of wherever we are it is made available anywhere anytime. In recent years healthcare has become one of the main application areas of ubiquitous computing. Some of the advantages of ubiquitous health care are as follows:

- Fast response to critical medical conditions regardless of the geographical location.
- Easy and fast access to other medical experts suggestions
- Use of medical expertise in rural locations of the country
- Intelligent personal health monitoring system
- Efficient medical data management.

Security plays a major role in the health care areas and its concern has increased to greater extent when it becomes cloud based health care since all the health data of the patient are stored and processed over the internet by a third party. The importance of security is to ensure confidentiality and availability, to prevent hacking and for authentication. Some security issues to mention are:

- Patient security in terms of Confidentiality
- Security for the Electronic Health Records which is accomplished by
  - Authentication
  - Data Integrity
  - Access control
- The Systems Security which involves
  - Secured Transmission
  - Secured Processing
  - Secured Storage
- Since it is cloud based the security on the internet is the primary concern which deals with
  - Reliability of the health data over the internet.
  - Secured data storage and retrieval.

Thus security involves privacy, confidentiality where privacy means the extent to which the disclosure of the user data are controlled and confidentiality means how far the exchange of the data between the user and the medical expert is kept undisclosed to others. Hence in general the term security means maintaining the privacy and confidentiality through policies, procedures.

By considering the above security issues in health care in this paper a RSA-DABE based approach has been proposed to enhance the security of health data sharing in a cloud based ubiquitous environment.

Susan Hohenberger and Brent Waters proposed an agile deciphering model with Attribute Based Encryption scheme that hinge on number of distinct attributes correlated with an access policy, in lieu of shortening the length of the cipher information. Trenchant attributes considerably in large numbers makes this system impertinent for the CP-ABE where the access policy is premeditated by the data owner and the deciphering is done by the recipient. Decentralizing Attribute Based Encryption technique provides a multi authority environment to achieve fine-grained access control over the shard data. In this model any number of entities can be the authority that issues the private keys to other system entities. In case of CP-ABE, a single data owner might shred his/her data with multiple members under various authorities by defining their own access policies. Under this scenario, decentralization failed to have better control over the attributes shared among entities. Guojun Wang, Qin Liu, Jie Wu proposed a Hierarchical Attribute Based Encryption for fine-grained access control in cloud storage service. HABE coalesce Hierarchical ID based encryption and CP-ABE, where as an centralized managing authority termed root master controls Domain Managers (DM) which maintains the users and attributes.

Muller, Katzenbeisserand Eckert, proposed a Distributed Attribute-Based Encryption (D-ABE), where an arbitrary number of authorities have global control over attributes which are used to encrypt the data. This model follows the basics of CP-ABE to offer cryptographically limited access control among the parties, performs decryption with a constant number of attribute-policy pairing. A protocol to improve privacy and security in Multi-Authority Attribute Based Encryption has been proposed by Melissa Chase et al. They claimed that it is unrealistic to manage the entire attributes allied to a community with the single attribute authority. Melissa Chase et al follow the principle of and insisted that existence of trusted third party limits the user’s privacy. Hence, authors proposed a unique protocol to enhance privacy and security in multi authority environment by
abolishing the trusted third parties. In 2013, Ming Li et al., proposed a system for scalable and secure sharing of personal health records in cloud computing using attribute based encryption standard. A patient-centric framework secures the PHR in semi trusted systems and in pursuance of reducing the complexity implicated with key management, their model carves the users into a range of domains. Our proposed model enables the data owners to securely share the personal health records among the health professionals by utilizing the strategy of Distributed Attribute Based Encryption (DABE). This distributed environment enables efficient data outsourcing by connecting various health communities to an arbitrary number of attribute authorities. To the best of our knowledge there is no work related for secure key exchange in attribute based encryption using a public crypto system. Hence, the proposed architecture enables secure key exchange mechanism to the distributed environment through RSA public key cryptosystem. The literature study enlightens issues like, providing control over the entire attributes of the system entities, lack of user control over decentralized architecture, responsive data management among inter-health communities, flexible and secure key exchange. Our proposed architecture addresses the aforementioned issues by merging D-ABE and public key infrastructure, RSA.

2. Proposed Architecture for Secured Data Sharing

The privacy and security of the patient health data in an ubiquitous environment can be maintained by applying symmetric key crypto system to it so that the data are securely stored in the storage provided by a third party. In a cloud based pervasive health care sharing of data while using the above crypto system offers high confidentiality but at the same time demands for more number of data re-encryption with respect to the number of recipients for the same data file as shown in Figure 1.

This increases the computational cost on the user side thereby making the system inefficient for resource constrained applications. Since sharing of data is not possible using the symmetric key crypto system and as data sharing is an important feature of healthcare applications where the patient may intend to receive suggestion from other health professionals the Symmetric system becomes inefficient to handle sharing of data among a group of medical experts. In order to achieve a secured data sharing in a cloud based pervasive health care application within a group of health communities a Distributed Attribute Based Encryption (DABE) has been used, which achieves an efficient and secured health data sharing between the user (patient) and the medical experts. Group sharing of data between the user and a group of doctors has been achieved using the DABE method which is very essential for a health care system.

2.1 Overview of DABE and RSA

2.1.1 Background of DABE

Distributed Attribute Based Encryption, is a public key encryption standard which allows the data owner to share their information among group by achieving encryption

| Table 1. | Notations used in Proposed Protocol |
|----------|-----------------------------------|
| **Key Representation** | **Description** |
| MK       | Master secret key |
| PK       | Master public key |
| SK<sub>u</sub> | Secret key of the user |
| SK<sub>A,u</sub> | Secret key of the attribute used by the user |
| Ska      | Secret key of attribute authority |
| PK<sub>A</sub> | Attribute public key |
| PK<sub>u</sub> | User’s public key |
| RSK<sub>u</sub> | RSA secret key of the user |
| RPK<sub>u</sub> | RSA public key of the user |

Figure 1. Secured RSA-DABE architecture.
through user centric access policies. The three major components involved in DABE are as follows,

- Master.
- Attribute Authority.
- Users.

2.1.1.1 Master

Primary task of master is to interact with the attribute authority during key generation and to distribute the users’ secret key.

2.1.1.2 Attribute Authority

Attribute authority is designed in such a way that, it takes control over the entire attributes which prevails in the system. Attribute authority records the complete structure and semantics of all the attributes along with its (attribute’s) public key and secret key. Attribute authority verifies the legitimacy of the user and issues an secret attribute key for decryption mechanism. Public key of the attribute is readily available for all participants of the system.

2.1.1.3 Users

Users can perform major cryptographic actions like encryption and decryption in the distributed environment. During encryption process, data owner generates his/her health data and defines their own access policy (Access policy determines ‘who to access what’). In order to make access policy flexible, DABE supports all the access policies in the form of Disjunctive Normal Forms (DNF). Cipher information can be generated by encryption the file with the public keys of the attributes corresponds to the access policy. Similarly during decryption, secret attribute keys can be retrieved from the attribute authority, which in-turn can be used for decrypting the cipher information.

Steps involved in DABE

The fundamental working of DABE is shown in Figure 2 and can be illustrated as follows,

- **Setup** : The setup algorithm takes input as security parameter and generates system wide Public Key (PK) and Master Key (MK).
- **CreateUser** : The CreateUser method takes input as PK,MK and user identity u. It generates an user Public Key (PK_u), that will be used by attribute authority to return SK_u and SK_A,u.
- **Create Authority** : This algorithm takes attribute identity a and generates an attribute secret key SKa. Attribute authority limits this function to be a non iterative, hence for each new attribute identity a, there exists only one secret key.
- **Request Attribute PK** : This algorithm gets initiated whenever, the attribute authority gets an request for attribute public by the user. Before issuing the public key of the requested attribute, attribute authority performs identity based legitimacy check and then issues the attribute public key. Similarly Request Attribute SK returns secret key of the attribute to the user, on secret key request.
- **Encrypt** : Encryption algorithm is executed by the data owner to generate the Cipher Text (CT), by considering access policy, message and public keys of the attributes associated with access polices as input.
- **Decrypt** : The Decrypt algorithm is execute by the data recipient to recomputed the original message from the received cipher information by applying attribute secret keys as a parameter.

DABE Based Encryption and Decryption

Initialization

- Read security_Param;
- generate PK, MK;
- PK_u = createUser(PK, MK, u);
- SK_a = createAuthority(PK, a);

Encryption

for i=1 to x
- PK_lA = getAttributePK(PK, A, SK_a);
- encrypt(PK,M, PK_lA...x,A);
return CT;

Decryption

- SK_A,u = getAttributeSK(PK, A, SK_a, u, PK_u);
- decrypt(CT, A, SK_A,u, PK, SK_u);
return M;

Figure 2. Key mapping in DABE architecture.
2.1.2 Background of RSA

RSA is one of the practicable public-key cryptosystem used for secure key exchange mechanism. RSA is proposed by Ron Rivest, Adi Shamir and Leonard Adleman in 1977. This algorithm performs encryption using publically available key of the recipient and in contract decryption is done using the secret key of the recipient. The basic principle of RSA is factoring problem (practical difficulty of factoring two large prime numbers). The three major steps involved in RSA as follows,

- Key Generation.
- Encryption.
- Decryption.

2.1.2.1 Key Generation

- Choose two prime numbers p and q randomly and compute n=p*q. Where n, is a key length.
- Calculate φ(n) = φ(p)φ(q) = (p−1)(q−1) = n - (p + q –1), where φ is a Euler’s totient function.
- Choose an integer e, such that 1< e < φ and gcd(e, φ(n)) = 1. Also release e as a public key (which is globally available).
- Compute secret key d as follows, d ≡ e⁻¹ (mod φ(n)).
- RSA key pairs are (e,d).

2.1.2.2 Encryption

As stated earlier encryption can be done using receiver’s public key, whereas the data can only be decrypted by the private key of the desired receiver.

\[ c \equiv m^e \pmod{n} \]

2.1.2.3 Decryption

On the receiving the cipher data c, the receiver can perform decryption by applying his secret key d over the received cipher information.

\[ M \equiv c^d \pmod{n} \]

2.1.3 Need for RSA

The chance of key tampering increases with the increase in number of keys used by the algorithm. Also it has been observed that Distributed Attribute Based Encryption consumes more number of keys than co-existed ABE models. Hence with the objective of offering efficient key exchange mechanism among the system parties, the proposed RSA-DABE model is accompanied by the RSA key exchange process.

2.2 Proposed RSA-DABE Security Protocol

Along with the steps involved in the traditional DABE scheme which is explained in section II-A, the following steps is added for the RSA-DABE to create the secured channel as shown in Figure 3.

2.2.1 RSAkeyGen(u, PK)

RSAkeyGen algorithm generates and distributed RSA key pairs for each components in the traditional D-ABE scheme through an secured channel. This algorithm takes the input as identity of each user and a globally available master public key PK and outputs arbitrary number of key pairs for secure key transmission in the proposed RSA-DABE scheme.

2.2.2 CreateMchannel(RPK_m, RSK_m, RPK_u, RSK_u, SK_u, Ts)

The CreateMchannel algorithm is executed to enable secure transmission of SK_u between master and user by creating an RSA channel. This algorithm takes RSA key set of master and user, personalized secret key of u and a time stamp Ts to encrypt the SK_u with RPK_u and distributed to the u. CreateMchannel is executed by master’s RSA module whenever a call is made to CreateUser algorithm of the traditional DABE scheme.

![Figure 3. Key mapping in RSA-DABE architecture.](image-url)
2.2.3 CreateAAchannel(RPK_{AA}, RSK_{AA}, RPK_{u}, RSK_{u}, SK_{A}, u, T_s)

The CreateAAchannel algorithm is executed to create a secure key channel between AA and user. Parameters such as RSA key set of AA and user, SK_{A,u}, and Time stamp T_s are given as an input to encrypt SK_{A,u}. CreateAAchannel is executed by the RSA manager whenever user calls RequestAttributeSK for decryption process.

**Initialization**

**RSA_Setup:**
Generate RPK_{u}, RSK_{u};

**Initialize:**
generate PK, MK;
PK_{u} = createUser(PK, MK, u);
SK_{A} = createAuthority(PK, A);

**Encryption:**
for i=1 to x
PK_{i,A} = getAttributePK(PK, A, SK_{A});
encrypt(PK_{i,A} M, PK_{i,1, x,A});
return CT;

**Decryption:**
CSK_{A,u} = getAttributeSK(PK, A, SK_{A}, u, PK_{u});
return E((SK_{A,u}, RPK_{u}) CT);
CSK_{u} = E(SK_{u}, RPK_{u});
SK_{u} = D(CSK_{u}, RSK_{u});
SK_{A,u} = D(CSK_{A,u}, RPK_{u});
D(CT, A, PK, SK_{A,u});

Let G be a group of legitimate users with the cardinality of n and U be the universal singleton set which contains the master public key PK.

\[G = \{ u_1, u_2, u_3, \ldots, u_n \}\]
\[|G| = n\]
\[U = \{ PK \}\]

Consider an empty set P, which holds the public keys of all the elements in G.
\[P = \{ \phi \}\]

Secured Channel Creation in RSA-DABE Protocol is given in Figure 4.

Let F be the generator function, which generates the public keys for all values of G and registers with P.
\[P = F(PK_{[u_i]}) \text{ Where } i=1,2, \ldots, n\]
\[\text{(for all values) } G \rightarrow u_i = \{P_{[u_i]}\}\]

Similarly, the generator function F generates a personalised secret key SK, for all the elements of G,
\[S = \{ \phi \}\]
\[S = F(SK_{[u_i]}) \text{ Where } i=1,2, \ldots, n\]
\[\text{(for all values) } G \rightarrow u_i = \{S_{[u_i]}\}\]

In the above step, the secret key of user SK_{u} is distributed by the generator function to the set of all elements in G. This scenario is highly vulnerable to the attackers because an attacker A, can obtain SK of a legitimate element of G and a publically available PK of G, then A impersonate himself as a valid element of G and cause damage to the system.

This challenge is eliminated by creating an M channel in RSA-DABE scheme before transmitting the SK_{u} to the element of G by S.

Let CT be an empty set, which holds the cipher value of each SK which corresponds to set of all elements in G.
\[CT = \{ \phi \}\]
\[CT = F(E(S_{[u_i]})) \text{ Where } i=1,2, \ldots, n\]
\[E = c \equiv m^{RPK_{u}} \text{ (mod n)}\]
\[\text{(for all values) } G \rightarrow u_i = \{D(CT_{[u_i]}))\}\]
\[\text{Where } D = m \equiv c^{RSK_{u}} \text{ (mod n)}\]
\[CT = \{ \phi \}\]

Similarly, the generator function F generates a personalised secret key for the attributes associated with element of G. Hence RSA-DABE scheme enables another secure channel known as A channel while transmitting the SK_{A,u} key.

\[SA = \{ \phi \}\]
\[SA = F(SK_{[A,u]}) \text{ Where } i=1,2, \ldots, n\]
\[CT = F(E(SA_{[u_i]})) \text{ Where } i=1,2, \ldots, n\]
As security and privacy is an important concern in ubiquitous computing environment, preserving security and privacy is a major research concern for a pervasive computing environment. The ubiquitous environment provides high scalability and data access flexibility to the system users. In this paper we proposed an RSA based security protocol called RSA-DABE by altering the traditional Distributed Attribute Based Encryption scheme. This protocol enables secure sharing of health data among the group of health communities. The proposed protocol maintains the data integrity by creating an authenticated key exchange channel among the system parties. In order to test the performance of proposed RSA-DABE protocol, a health care application has been developed using java and hosted in the Amazon cloud instance to support ubiquitous computing environment.

Health care applications demands for easy data access, resource availability, cryptographically restricted access control over the personal data and data confidentiality. Various healthcare applications has been proposed in accordance with above mentioned issues but limits its efficiency in the shared environment where multiple data consumers attempts to access the data. Utilization ratio of health care applications can be increased by allowing the data owners (eg Patient) to securely share their personal health information among the group of health communities.

3.1 Implementation Scenario

The developed ubiquitous healthcare application is well suited for a data owner who readily wants to share his personal information among multiple data consumes for better productivity. The system adopts patient-centric principle by enabling the data owners to have access over their data. We referred full access as data owner can determine who can access what. The remaining part of the paper assumes that data owner as patient, multiple data consumes as healthcare professionals (eg: doctor, nurse, special surgeon, pharmacy etc) and data to be shared as personal health records.

3.2 Secure Sharing using RSA-DABE Protocol

The proposed RSA-DABE system demands the patient P, to register with the system by providing the set of user credentials, \(\{c_1, c_2, c_3, \ldots , c_i\}\) O, where O represents set of credentials belongs to a single patient. The RSA manager operates over the O and produces a key pair comprises of RPK and RSK as RSA_manager O \(\rightarrow\) \(\{\text{RPK}_o, \text{RSK}_o\}\). Master component of the proposed protocol process the \(\text{P}({\text{patient ID}})\) to extent the key ring of P by adding \(\text{PK}_r\) to it. As a critical factor patient P creates his own set of attributes which is crucial to perform encryption and decryption of personal health record. After successful generation of attribute set, the patient register his attributes with attribute authority AA, which in turn produces public and secret key for each attribute generated by the patient. Patient requests AA to send the secret key of the patient P by passing his identity (any one element from credential set O). CreateAchannel algorithm (a part of proposed RSA-DABE protocol) gets executed by the master component and secret key of the patient were distributed securely through authenticated M channel. The final component of the patients’ key ring consists of secret keys for all the attribute in the Patient generated attribute list. As similar to M channel A channel has been created by executing the createAchannel algorithm (a part of proposed RSA-DABE protocol) to deliver the secret key for all the element of attribute list.

Our protocol construction follows the fundamental of CP-ABE key policy, hence it is mandatory for the patient to define their access policy AP, in order to achieve cryptographically limited access control over his/her personal health record. The practical implementation of proposed health care application allows patient to define their access policies in Disjunctive Normal Form (DNF) containing an identifier and an attribute qualifier. Identifier consists of sequential string (for example URL) which can be posted to the server as request and attribute qualifier is a key-value pair which describes the identifier. Patient collects his/her personal health information I, and binds with the AP to generate cipher text CT. And the generated CT can be shared among the members of health community for data access. The proposed RSA-DABE protocol limits the data access only to the members whose attribute key matches with the patients AP. The proposed model ensures that RSA keys were generated according to the standard illustrated in
section III-A and DABE key standards abides with the schema mentioned in\textsuperscript{3}.

Hence in this paper we implemented a secure data sharing application embedded with novel security protocol. The secure data sharing protocol has been designed in such a way that it shares the cryptographic parameters in the authenticated channel among the system entities to enhance confidentiality. Proposed protocol enhanced the traditional schema of DABE to offer a cryptographically restricted access control. The major issues like scalability and anytime resource access in ubiquitous environment were sorted by hosting the application in the cloud.

3.3 Reduced Key Overhead

The traditional Distributed Attribute Based Encryption scheme achieves sharing of patients’ health record among health communities by involving seven numbers of keys, out of which two open keys. DABE model distributes such open keys, which are crucial for cryptographic actions in an unsecured environment. Such unsecured sharing of keys increases the chance of tampering (illustrated in section II (need for RSA) also large number of keys increases the transmission overhead. The aforementioned issue with key transmission overhead is reduced in proposed RSA-DABE model by hiding the open keys from the malicious invaders there by reducing the number of keys involved in the distribution mechanism. Thus reducing the key overhead. Figure 3.

3.4 User Revocation in RSA-DABE

Proposed secure sharing protocol in cloud supports ubiquitous computing model without the involvement of semi-trusted or fully-trusted third part entities. Also patient-centric principle grants full access rights over their personal health record among the professional members of health care community. Since access policy AP defined by patient remains constant for all the members of the health community which restricts patient from limiting data access to a particular doctor. Early versions of healthcare application implements user revocation either by redefining the AP or by altering the attribute set.

Aforementioned scenario adheres high computational cost to the patient because of total re-encryption scheme. In the proposed model (RSA-DABE), system level component known as Attribute Authority (AA) governs the control over all the attributes of the legitimate users in the attribute list. AA issues personalized secret key of the attributes to the user after verifying the identity of the data consumer, hence proposed secure data sharing protocol performs identity based access control mechanism over the set of all elements (members) in the healthcare community. Without deviating from the patient-centric principle, the proposed application embedded with secure data sharing protocol retrieves the identity of desired consumer from the user.

\[
\text{www.hospitalone.com : designation=doctor AND}
\text{www.hospitalone.com : division=cardiology OR}
\text{www.hospitalone.com : division=pulmonary AND}
\text{www.hospitalone.com : designation=nurse AND}
\text{www.hospitalone.com : division=cardiology Sample Access policy (in DNF format)}
\]

3.5 Efficiency of the System

The efficiency of the proposed protocol is found to be high when compared to other earlier security protocols. Since we are using distributed attribute based encryption scheme which has the global control over all the attribute set which prevails in the system. As a result Attribute Authority (AA) governs the attribute set.

\[
\begin{align*}
AA = \{ & \{A_{S_1} = \{a_1, a_2, \ldots a_n\}\} \\
& \{A_{S_2} = \{a_1, a_2, \ldots a_n\}\} \\
& \ldots \\
& \{A_{S_n} = \{a_1, a_2, \ldots a_n\}\} \}
\end{align*}
\]

Let the patient ‘P’ generates an access policy AP by retrieving the attribute set AS from AA. The cryptographic model of data-policy binding can be illustrated as

\[
P:- G(\text{AP}) \sigma^{\text{(AA)}} A_{S_1} \quad P:- E(F || \text{AP}) \rightarrow CT (1)
\]

The generator and requestor function are represented as G and σ Patient P, Encrypts (E) the File (F) with the newly generated Access Policy (AP). The same patient P, re-encrypts the same personal health record (F) by requesting the Attribute Set (AS) from AA with the intent of sharing it among another health community.
\[ P: G(\text{AP}_P) \{ k, \sigma(AA) \}_{A_{S_y}} \] 
\[ P: E(F || \text{AP}_P) \rightarrow CT \quad (2) \]

From (1) and (2), the patient \( P \) obtains the same cipher data even though the data owner performs re-encryption. Since in the proposed model, the global body \( AA \) governs the entire attribute set, patient re-encryption process obtains same attribute set (AS) values by validating the patient identity. This feature prevents attribute pooling (users from two or more healthcare community aggregates their attributes, in order to access the patients’ health record) thereby increases the system efficiency to the next level.

4. Conclusion

Anywhere anytime attribute of ubiquitous computing makes security and privacy a difficult task while storing, sharing, processing the user data. The essence of ubiquitous computing is made more demandable by converting the ubiquitous application into a cloud based, so that the scalability and cost issue of the ubiquitous computing can be overcome. The proposed protocol (RSA-DABE) is implemented and tested in a cloud based health care application and found that it achieves high scalability and fast data access. Health care applications involve sharing of personal health record data among the members of health professional for better utilization of the system and as the traditional cryptographic techniques limits their service in a distributed environment. The protocol RSA-DABE is designed in accordance with the distributed ABE to enable the primary users of the system to share their health data and cryptographically restricted access control is achieved by creating a secured RSA key exchange channels. The proposed protocol modifies the traditional version of DABE with the RSA key exchange standards to maintain the data integrity while sharing of health data. From the results obtained it is inferred that the proposed protocol achieves reduced key overhead and enhances the efficiency of the system by eliminating attribute pooling mechanism since Attribute Authority governs the attributes of all the system entities. The user revocation is performed by allowing Attribute Authority to adopt identity based access control mechanism.

5. References

1. Hohenberger S, Waters B. Attribute-based encryption with fast decryption. 2013; 7778:162–79. Available from: https://eprint.iacr.org/2013/265
2. Lewko A, Waters B. Decentralizing attribute-based encryption. Advances in Cryptology – EUROCRYPT 2011. International Association for Cryptologic Research; Tallinn, Estonia. 2011. p. 568–88.
3. Wang G, Liu Q, Wu J. Hierarchical attribute-based encryption for fine-grained access control in cloud storage services. ACM. 2010:735–7.
4. Muller S, Katzenbeisser S, Eckert C. Distributed attribute-based encryption. Proceedings of ICISC. 2009; 5461:20–36.
5. Chase M, Chow SSM. Improving privacy and security in multi-authority attribute-based encryption. ACM, CCS. 2009 Nov.
6. Chase M. Multi-authority attribute based encryption. TCC. Springer; 2007; p. 515–34.
7. Li M, Yu S, Zheng Y, Ren K, Lou W. Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption. IEEE Transactions on Parallel and Distributed Systems. 2013 Jan; 24(1):131–43.
8. RSA Public key cryptosystem. Available from: http://en.wikipedia.org/wiki/RSA_%28cryptosystem%29
9. Steffenel LA, Pinheiro MK. Leveraging data intensive applications on a pervasive computing platform. Elsevier Procedia Computer Science. 2015; 52:1034–9.
10. Rajkumar K, Swaminathan P. Combining TCP and UDP for secure data transfer. Indian Journal of Science and Technology. 2015 May; 8(S9):285–91.
11. Baek SS, Won YS, Han DG, Ryou JC. The effect of eight-shuffling AES implementations techniques against side channel analysis. Indian Journal of Science and Technology. 2015 Mar; 8(S5):91–7.