International Journal of Applied Engineering Research ISSN 0973-4562 Volume 13, Number 7 (2018) pp. 5190-5196

Enhancing Medical Data Security in the Cloud Using RBAC-CPABE and ASS

Gandikota Ramu[1], Appawala Jayanthi[2]

[1,2] *Department of Computer Science & Engineering,*
Institute of Aeronautical Engineering, Mahipalpur, New Delhi, India.

Abstract

Nowadays, paper-based health data is converted into electronic form, which is called Electronic Health Records(EHRs). The medical information is growing rapidly. So, in-house storage is not an efficient way to handle medical data. The cloud servers are the best option, but security is the main drawback in this servers. To enhance security by encrypting the medical data by assigning roles before outsourcing the data into the cloud. For providing security over the network, it is essential for the data to have a protection mechanism which is provided by encryption of data using Attribute-Based Encryption and by assigning roles for the users in the network. This mechanism is known as Role-Based Access Control (RBAC) and Ciphertext-Policy Attribute-Based Encryption(CP-ABE) which is represented as RBAC-CPABE. In this system involves data-centric role-based access control (DCRBAC) which is dependent on the data objects rather than on the whole of data and thus provides a fine-grained access control capabilities. RBAC-CPABE is based on the cipher-text policy attribute-based encryption scheme and provides the similar efficiency and security, which is demonstrated by the security analysis. This project is used for the purpose of providing security to the data over an alien environment, where the servers have the access to the data. Thus, a robust mechanism is developed for providing security to the data before entering into the cloud by using RBAC-CPABE and Attributing Self Sustaining (ASS) capabilities to the data.

Keywords. EHRs, Security, Cloud Computing, Attribute based Encryption, Ciphertext Policies.

INTRODUCTION

For any organisation in the network, it is imperative for it to provide security to the data that it is holding. The data which is stored in any organisation requires huge chunks of storage space. With augmenting data the space for its storage has to be provided. For addressing this issue, cloud storage concept has been introduced which stores information in a different location away from the users cognizance. Hence, it is essential for the user to provide security to such data which is stored in some distant location. The data which is stored and while in transit is prone to attack from external intruders. It is thus required to provide protection to the data from infringing upon and hence vitiate the risk of attack. The orthodox method of providing security to the data is through encryption and in an encrypted format the data is protected from intruders is as propounded by cloud security alliance. The protection mechanisms which provide security are through public key generation and by the use of identity based encryption (IBE) [1]. The encryption mechanism provides security from external as well as internal infringements. In order to identify the user and to provide an internalised access control for the data either to provide access to the user or to deny the user from getting access to it, it is required to assign a predetermined access policy. For providing such security to the data, a robust mechanism has been introduced. This mechanism is called role base access control (RBAC) [2]. In any organisation hierarchies are established in order to perform task pertaining to the designation of the user. Hence, observing this concept, roles are assigned to the users in the network and certain specifications are stipulated for users to meet the required criteria. By assigning roles to the users, the organisation is providing a control policy for the data, where the data can allow the users to access it or refrain from providing access depending upon the user's credentials. This kind of mechanism where the data is provided with the rights to provide access is known as self-contained data protection. It is the policy that is assigned by the user which is providing security to the data. The issue involved here is that RBAC or a public key or a combination of both cannot provide security to the data over the network. Hence, both are to be integrated in order to provide enhanced security.

There are various problems that are to be addressed by assigning roles to the users. The issues involved with role based access control mechanism are:

- The roles that are assigned in RBAC are directly indicated to the users who are operating it. If the permission is granted to the role then the users who are having such roles can get access to the data. But the problem that is involved with the role is, when permission is assigned to role, the users can infringe upon the data who were not supposed to have access to it. But when permission is assigned to such role, all such users who are having similar roles gets access to the data, thus raising a concern of security. It is hence not viable for the user to be assigned permission to the roles.
- Other viable option that was considered was to assign different roles to individual users and then provide the permission depending upon the requirements. But the requirements are huge and thus the role assignments to the users also accrue over a period of time. This prompts for maintaining of myriad number of roles and also for the user to be associated with many roles assigned to him. This also causes turmoil within the organisation during the maintenance of records whether to let the user have role assigned or to annihilate them. The time is a imperative factor, the assigning of roles to the user and deletion of such roles time in and time out causes the lapse of time. Hence, assigning of roles individually to the users is also not considered a viable answer for access of the data.

- The main focus of RBAC is to provide internal control for the data. The data which is over the network is very much prone to attacks. The service providers cannot be relied upon for the provision of security to the data in the network and hence RBAC provides with such an internal access control mechanism. The data in the network is protected from external elements as the users should prove their authenticity before trying to get access to the data.

From the above propounded factors it can be subsumed that, the self-contained data protection mechanism can't be provided by RBAC alone over the network.

Hence, a mechanism which can be integrated with RBAC for providing self-contained data protection has to be identified. Attribute based encryption (ABE) [3] provides with such a mechanism where data can be provided with a self-protection mechanism. ABE consists of the cipher-text where the text which is in the normal form is encrypted and converted into an unidentifiable form to the user. The cipher-text requires key for deciphering it. Thus ABE consists of a private key and a cipher-text. This attribute based encryption has two variants of it's amongst which one is useful for integrating with RBAC in order to provide security to the data. They are:

- Key policy attribute based encryption (KP-ABE)
- Cipher text policy attribute based encryption (CP-ABE)

Key policy attribute based encryption (KP-ABE):

In KP-ABE, cipher-text is related to the attributes and private key is related with the access policy. But the case is an inverse for the latter ABE scheme.

Cipher-text policy attribute based encryption (CP-ABE)

In CP-ABE, the cipher-text is related to that of access policy where the user's credentials are verified before granting access to the data and private key is related to the set of attributes where the attributes on matching with the user's credentials provide him with the access to the encrypted data to be decrypted into its original form.

For the project, we consider using CPABE as it provides with the access control to the user by verifying his credentials as specified earlier and provides with the private key on verifying the attributes associated with the user.

In this paper, we propound a self-protection mechanism for the data where the data is protected and the access policy regulates the user whether to access the data. This mechanism not only provides with the self contained data protection but also provides security for each data object in the network or for the data that is stored in the cloud. For enhancing security a robust RBAC mechanism with an encryption mechanism has been introduced with is termed RBAC-CPABE. Data has to be provided security over the network and holistic data protection for the entire data is conventionally provided. Our project provides with the provision of security for each data object. For providing security to the individual data object, a data centric role based access control model has been considered.

Protection is provided traditionally to the complete data rather than on the individual data object. In order to provide such security to the individual data object DC-RBAC model has been introduced. DC-RBAC model provides with the restrictions set upon the user from accessing the data. These are role constraints that are assigned to the user's role. For example, a user is assigned with roles, where for a certain role constraints are assigned such that only those users who meet the stipulated criteria and adhere to the constraints are allowed access to the data. Suppose in an organisation a role is assigned to the user where a constraint such as a user not having experience less than years are not allowed to access the data. In addition DC-RBAC also has user constraints and also has environmental constraints.

User attribute constraints are pertinent to the name, experience, salary etc of an individual. The properties of the user related objects are the attributes of the users where as environmental constraints are pertinent to Internet Protocol address, access time etc. These are specified for permitting the access to the individuals who meets the criteria stipulated. Thus, it is a fine-grained access control mechanism pertinent to each data object.

We integrate RBAC with CP-ABE. But CP-ABE alone wouldn't meet the specified mapping policy for DC-RBAC to be mapped with CP-ABE. Hence, an extended version of CP-ABE is considered, which is called extended cipher-text policy attribute based encryption (ECP-ABE). Through ECP-ABE an extended access tree is introduced where the DC-RBAC is mapped with ECP-ABE in order to enhance the security for the data in the cloud. Encryption of the data is made after the mapping to the ECP-ABE is achieved. Here, in ECP-ABE extended leaf nodes plays a prominent part in identifying the attributes of the user and hence enhancing the efficacy of the model which is integrated with it. Through this paradigm shift towards the mapping of the data and encryption RBAC-CPABE provides with a fine grained policy for achieving efficient access control and self-contained protection of data.

LITERATURE SURVEY

When considered the post facto scenario, the pioneers of the RBAC model were Farraiolo and Kuhn [4], they emanated the work in 1992 and this later became popular in mid 1990's. For the given model, it is important to have a secure framework established for transmitting data over the network. The information in the raw form can't be in transit due to the infringement from external agents; hence it is required for it to be in the encrypted format. Cryptography provides with the safer management of the data over the network as the plain text is converted into the cipher-text, which needs a key for its conversion into the original form. The encryption holds a private key, which is present with the authorised user who wants to access the information. Cryptography provides security to the data in the cloud where the RBAC model assigns the role and the user specified with certain role is the only person eligible for accessing the data on proving his authentication through private key provided on request.

RBAC model has turned out to be the most famous model in recent years by making the process of providing simpler access control model. It has the capability of meeting the requirements of both regulation based access control and compulsory access controls. Crampton[5] proposed a partial order relation for

explaining the policies which is a new way of presenting RBAC policies. This concept converts RBAC policies to a way in which information is transmitted termed as information flow policy. In the latter part, this information is converted into encrypted format through cipher-text encryptions in order to form the cryptographic RBAC mechanism. In order to provide the role key hierarchy (RKH) [6] for supporting role hierarchies' zhu et al [7]-[8] proposed this model which consists of cryptographic RBAC model. In this model, it is essential that for each role the user should be assigned a key but assigning such keys for every given role augments a number of keys and which in turn accrues the burden of key management for the one who accesses in case if a user is provided with a myriad number of roles.

Public key encryption which was earlier used for the purpose of encryption and decryption was not efficient and thus, an enhanced version was developed as attribute based encryption (ABE). This attribute based encryption has its own advantage when compared with public key encryption, as for a given data which is in encrypted format can have multiple decryption keys. The underpinning concept was propounded by sahai and waters [10] through fuzzy identity based encryption. This concept was further enhanced by Goyal eta al [11] and introduced key policy identity based encryption (KP-ABE) [12] where the cipher-text is related to attributes and a private key is related to access policy. The first scheme under CP-ABE was put forward by bethencourt et al [13] which is called BSW scheme. The idea of CP-ABE is the reciprocity of the KP-ABE where the private key is related to the attributes and the cipher text is related to the access policy.

In the earlier concept of ABE, the operators that it supported were AND, OR and threshold operators, where the threshold (m, n)states that at least a m number of constraints are to be satisfied amongst total n constraints. For convenience we call it simply threshold operator. We have certain other operators other than AND, OR and threshold operators as NOT and comparative operators(>,<,<= and >=), these operators can't be directly expressed though, are very useful in practice. For providing a solution to this problem, various studies have been made where cheung and Newport [14] propounded the first of the CP-ABE scheme in supporting the NOT operator and was referred as CN, the major disadvantage with this CN is it supports only 'AND' and 'NOT' operators. Further, to enhance the accessibility Junod and Karlov [15] has put forward the concept of attribute based broadcast encryption (ABBE) which espouses 'AND', 'NOT' and 'OR' operators depending on CP-ABE. Ostrovsky et al.[16] propounded a KP-ABE scheme which espouses 'NOT', 'AND', 'OR' and threshold operators. The following table depicts the different schemes of ABE:

Table 1. Comparing various CP-ABE schemes

Scheme	AND	OR	THRESHOLD	NOT	COMPARISON
BSW	YES	YES	YES	NO	YES
W11	YES	YES	YES	NO	YES
HLC	YES	NO	YES	NO	NO
GZC+	YES	NO	YES	NO	NO
LMX+	YES	NO	YES	NO	NO
CN	YES	NO	NO	YES	NO
NYO	YES	NO	NO	YES	NO
EMO	YES	NO	NO	YES	NO
GMS+	YES	NO	NO	YES	NO
JK	YES	YES	NO	YES	NO
OSW	YES	YES	YES	YES	NO
ZHA+	YES	YES	YES	NO	YES
ECP-ABE	YES	YES	YES	YES	YES

There are various policies that use the comparative operators very often. Hence it is essential that such operators are introduced apart from 'AND', 'OR', 'NOT' and threshold operators. These operators are used in the access tree where the attributes are matched in order to provide authenticity to the user, but the numbers are presented in the form of binary digits in BSW which makes it difficult to use. Though zhu et al proposed a comparison based encryption scheme, it was not compatible with the model as it doesn't support the NOT operator. For overcoming this problem an extended version of the CP-ABE scheme which is ECP-ABE was proposed by Lang et al [17] which is highly expressive. Through this scheme, the access tree could support all various kinds of logical and arithmetic as well as comparative operators, which includes AND, OR, NOT,(>,<,<=,>=)and threshold operators.

SECURE CLOUD FRAMEWORK USING RBAC-CPABE

The servers in the cloud are not completely reliable and hence, a protection mechanism has been postulated by us. The data in the cloud is alien to the environment and hence is very vulnerable to the infringements upon it. For reducing the risk of impingement and providing security to the data a self-contained data protection mechanism has been introduced where data is secured in the network. The access control capabilities are provided where the data in the network is having control upon the unauthorised users. This self-protection mechanism is provided not only by role based access control or by identity based encryption but by both of them. Ensuing, a self contained mechanism has been developed where the data is protected is RBAC-CPABE has been introduced.

As shown in figure 1, There are three layers which are involved in the architecture of the system postulated. The layers consist of the owner side where the data is uploaded onto the cloud. Second layer consists of service providers where the cloud

service providers facilitate the provision of service and the third layer is the abstraction layer where information is transmitted in a concealed format.

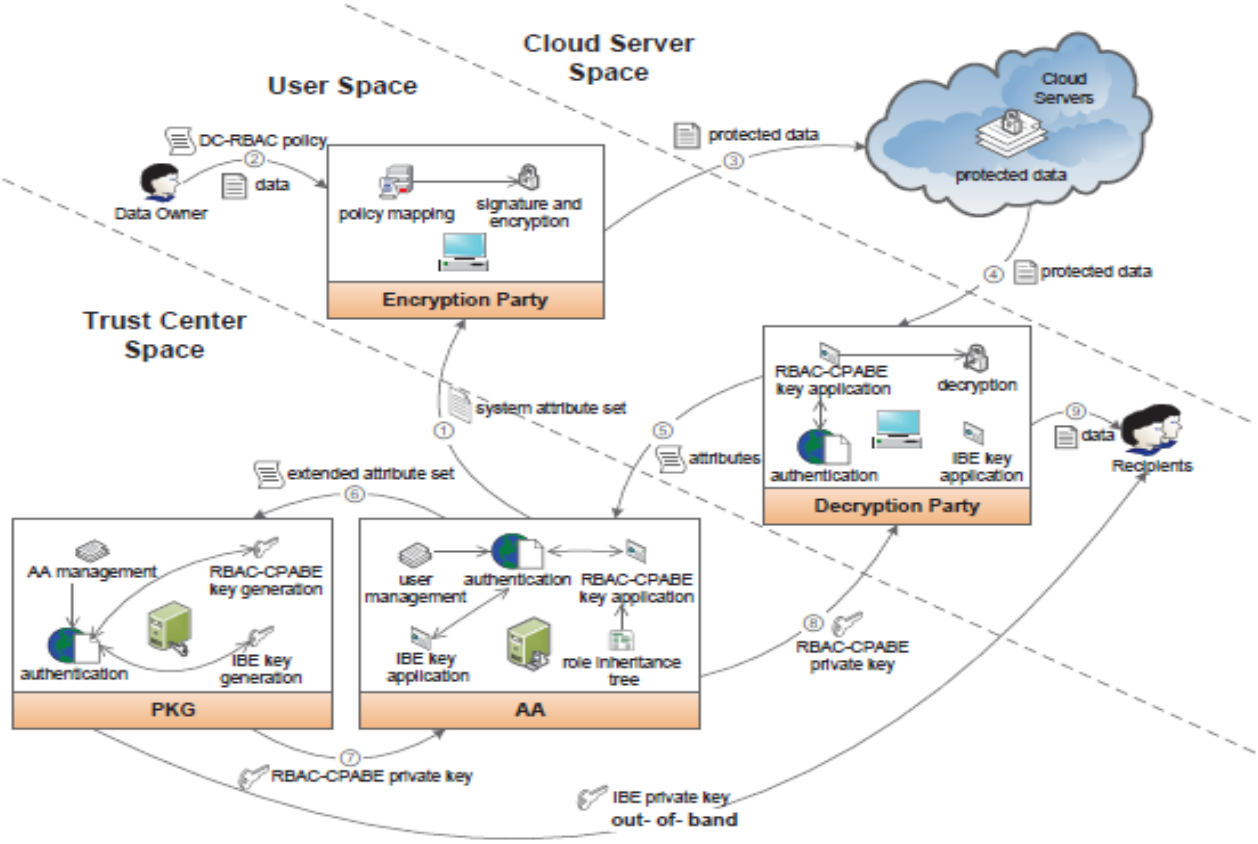

Figure.1. Secure Cloud Framework Using RBAC-CPABE

RESULTS AND ANALYSIS

In this section we discussed about Secure Cloud Framework Using RBAC-CPABE implementation and we compared our system with existing system.

Implementation

In below, we have dipicated implementation results in a brief and clearly expressed manner for better understanding.

Figure 2. Login Page

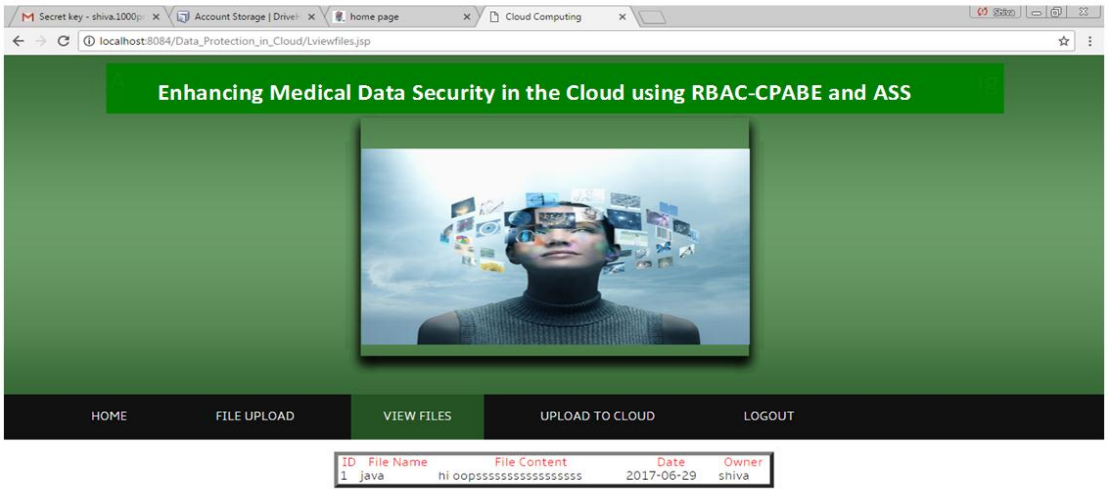

Figure 3. Uploading medical data into cloud servers

Figure 4. User Request

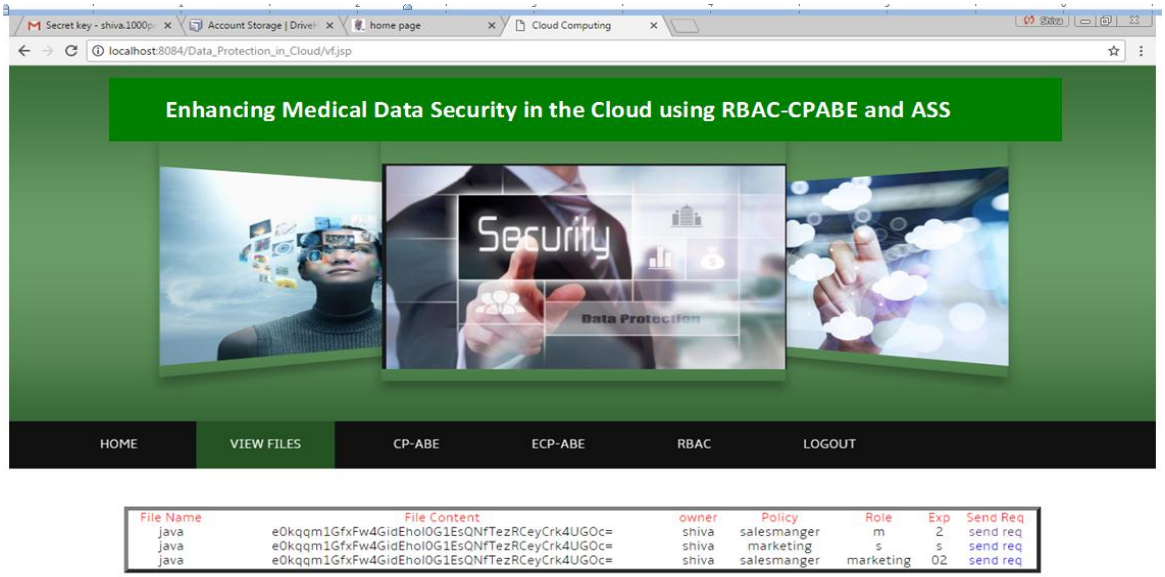

Figure 5. Showing list files in cloud

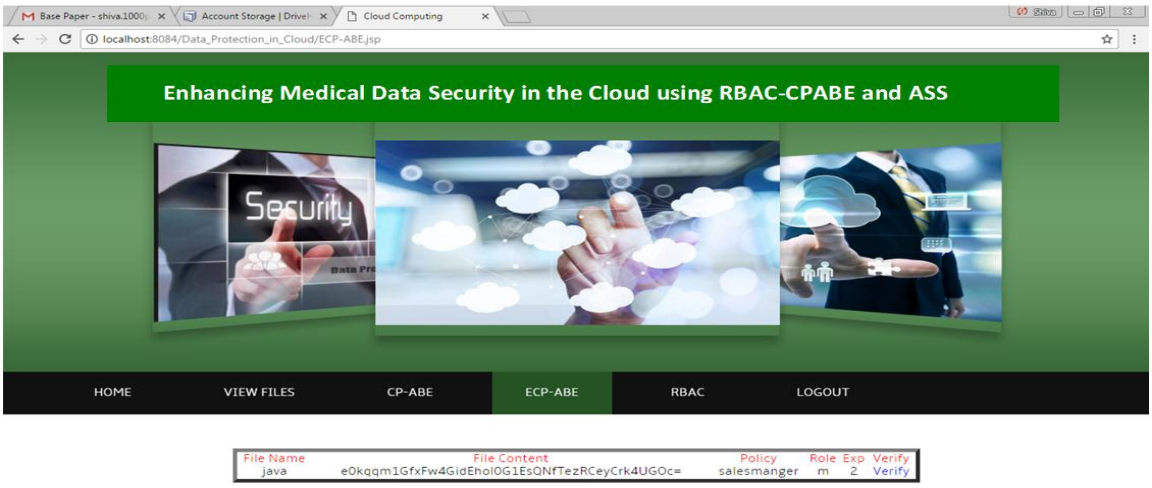

Figure 6. Extended Cipher-text Policy Attribute Based Encryption

Performance Analysis

We compared the performance evaluation of proposed scheme with BSW[18] scheme. Here, we consider the performance time of encryption and decryption functions. The decryption time includes two phases as discussed above. This experiment uses pairing based library (PBC)[19] and a 160-bit elliptic curve group based on the super singular curve '$y^2=x^3+x$' over a 512 bit finite field. All benchmarks test case were performed on a Ubuntu 14.04 desktop platform with Intel Core(TM) Core i7-5500U CPU 3GHz and 8.00GB. All the experiment as results are the average of 20 trials.

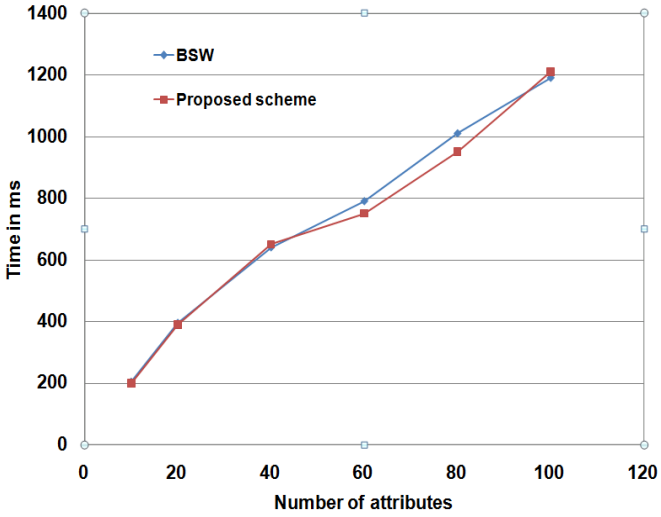

Figure 7. Performance comparison of encryption time from the implementation between the BSW and proposed scheme

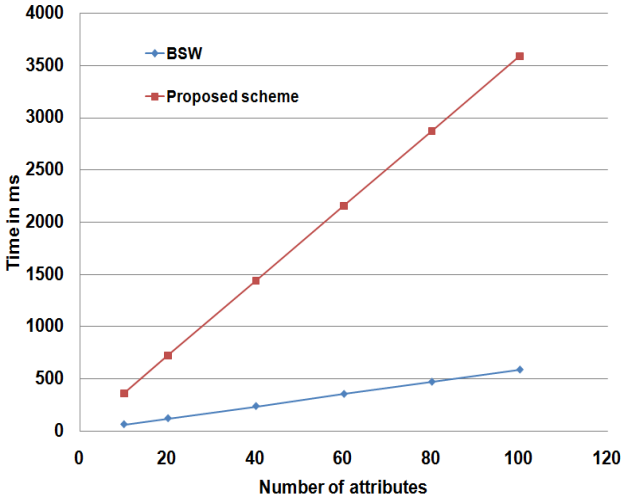

Figure 8. Performance comparison of decryption time from the implementation between the BSW and proposed scheme

Figure. 7 depicts that the total computation time of encryption of EHR's in proposed system is same as in the BSW scheme. Figure. 8 shows that the decryption time of ciphertext is more in proposed scheme because it requires at most '$N_u k$' exponentiations operations are needed in G_0 at worst case. These '$N_u k$' exponentiation operations to achieve user revocation at attribute level. So, the proposed scheme is more efficient in all aspects.

CONCLUSION

Role based access control provides with the access control capabilities. In order to enhance the efficiency of RBAC in providing security to the data over the cloud a secure mechanism which is an encryption method called attribute based encryption has been used. The variant of CP-ABE by using its extended version called ECP-ABE is integrated with DC-RBAC which is oriented towards each data object rather than on the complete data as a cluster. This enhances the

efficiency as the mapping is made between DC-RBAC and ECP-ABE through the usage of extended leaf node and thus provides for its utilisation. The RBAC-CPABE are integrated with each other to enhance the security of the data and the efficient functioning of the system. RBAC-CPABE provides a fine grained self-containing capability to the data and also enhances security..

ACKNOWLEDGEMENTS

The authors are especially indebted to the Science and Engineering Research Board (SERB), Department of Science and Technology (DST), and the government of India for providing an environment for them to do the best work they can.

REFERENCES

[1] A.Sahai and B.Waters, "Fuzzy identity-based encryption," in Advances in Cryptology–EUROCRYPT 2005, vol. 3494. Aarhus, Denmark: Springer Berlin Heidelberg, 22-26 May 2005, pp. 457–473.

[2] Kaiping Xue, Yingjie Xue, Jianan Hong, Wei Li, Hao Yue, David S.L. Wei, Peilin Hong "Robust and audible access control with multiple attribute authorities for public cloud storage", IEEE Transactions on information Forensics and Security, Vol. 12, no.4, pp.953-967, 2017.

[3] R. Ostrovsky, A. Sahai, B. Waters, "Attribute-based encryption with non-monotonic access structures", Proc. 14th ACM Conf. Comput. Commun. Security, pp. 195-203, 2014.

[4] D. Ferraiolo and R. Kuhn, "Role-dependent access control," in 15th National Computer Security Conference. Baltimore, Maryland: National Institute of Standards and Technology, 13-16 October 1992, p. 554lC563.

[5] j. Crampton, "Cryptographic enforcement of role-based access control," in Formal Aspects of Security and Trust. Pisa, Italy: Springer Berlin Heidelberg, September 16-17 2011, pp. 191–205.

[6] Y. Zhu, G.-J. Ahn, H. Hu, and H. Wang, "Cryptographic role-based security mechanisms dependent on role-key hierarchy," in Proceedings of the 5th ACM Symposium on Information, Computer and Commu-nications Security. Beijing, China: ACM, 13-16 April 2010, pp. 314–319.

[7] Y. Zhu, H.-X. Hu, G.-J. Ahn, H.-X. Wang, and S.-B. Wang, "Prov-ably secure role-based encryption with revocation mechanism," Journal of Computer Science and Technology, vol. 26, no. 4, pp. 697– 710, 2011.

[8] Y. Zhu, G. J. Ahn, H. Hu, D. Ma, and S. Wang, "Role-based cryptosystem: A new cryptographic RDAC system dependent on role-key hierarchy," IEEE Transactions on Information Forensics and Security, vol. 8, no. 12, pp. 2138–2153, 2013.

[9] Zhou, V. Varadharajan, and M. Hitchens, "Enforcing role-based access control for secure data storage in the cloud," The Computer Journal, vol. 54, no. 10, pp. 1675–1687, 2011.

[10] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in Advances in Cryptology–EUROCRYPT 2005, vol. 3494. Aarhus, Denmark: Springer Berlin Heidelberg, 22-26 May 2005, pp. 457– 473.

[11] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in Proceedings of the 13th ACM conference on Computer and communi-cations security. Alexandria, Virginia, USA: ACM, 30 October-3 November 2006, pp. 89–98.

[12] N. Attrapadung, B. Libert, and E. Panafieu, "Expressive keypolicy attribute-based encryption with constant-size ciphertexts," in Proceedings of the 14th International Conference on Practice and Theory in Public Key Cryptography. Springer, 2011, pp. 90–108.

[13] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in Proceedings of IEEE Symposium on Security and Privacy. IEEE, 2007, pp. 321–334

[14] L. Cheung and C. Newport, "Provably secure ciphertext policy ABE," in Proceedings of the 14th ACM conference on Computer and communications security. Alexandria, Virginia, USA: ACM, 29 October-2 November 2007, pp. 456–465.

[15] P. Junod and A. Karlov, "An efficient public-key attribute-based broadcast encryption scheme allowing arbitrary access policies," in Proceedings of the 10th annual ACM workshop on Digital rights management. Chicago, Illinois, USA: ACM, 04-08 October 2010, pp. 13–24.

[16] R. Ostrovsky, A. Sahai, and B. Waters, "Attribute-based encryption with non-monotonic access structures," in Proceedings of the 14th ACM conference on Computer and communications security. Alexan-dria, Virginia, USA: ACM, 29 October-2 November 2007, pp. 195– 203.

[17] B. Lang, R. Xu, and Y. Duan, "Extending the ciphertext-policy attribute based encryption scheme for supporting flexible access control," in Proceedings of the 10th International Conference on Secu-rity and Cryptography. Reykjavik, Iceland: IEEE, 29-31 July 2013, pp. 1–11.

[18] J. Bethencourt et al. "Ciphertext-Policy Attribute-Based Encryption," Proceedings IEEE Symposium Security and Privacy, pp. 321-334, 2007

[19] The Pairing-Based Cryptography Library, http://crypto.stanford.edu/pbc/