Journal of University of Babylon, Engineering Sciences, Vol.(26), No.(3): 2018.

A Hybrid Verifiable and Delegated Cryptographic Model in Cloud Computing

Jaber Ibrahim Naser
Ministry of Education , Directorate of Education Qadisiya
jaberalidami@gmail.com

Abstract

Access control is very important in cloud data sharing. Especially in the domains like healthcare, it is essential to have access control mechanisms in place for confidentiality and secure data access. Attribute based encryption has been around for many years to secure data and provide controlled access. In this paper, we proposed a framework that supports circuit and attributes based encryption mechanism that involves multiple parties. They are data owner, data user, cloud server and attribute authority. An important feature of the proposed system is the verifiable delegation of the decryption process to cloud server. Data owner encrypts data and delegates decryption process to cloud. Cloud server performs partial decryption and then the final decrypted data are shared for users as per the privileges. Data owner thus reduces computational complexity by delegating decryption process cloud server. We built a prototype application using the Microsoft.NET platform for proof of the concept. The empirical results revealed that there is controlled access with multiple user roles and access control rights for secure and confidential data access in cloud computing.

Keywords :– Cloud computing, Encryption, Decryption, Verifiable delegation of decryption, Partial decryption

الخلاصة

التحكم بالوصول مهم جدا في تبادل البيانات السحابية. و خاصة في مجالات مثل الرعاية الصحية، فمن الضروري ان تكون هناك ألية لمراقبة قائمة الدخول من اجل السرية و الوصول الامن للبيانات. و قد تم التشفير القائم على السمة لسنوات عديدة لتأمين البيانات و توفير الوصول المراقب. في هذا البحث اقترحنا اطاراً يدعم آلية التشفير الدارة و السمة التي تتضمن اطرافا متعددة. هم مالك البيانات ، مستخدم البيانات ، خادم السحابة و سلطة السمة. ومن السمات الهامة للنظام المقترح هو التفويض الذي يمكن التحقق منه لعملية فك التشفير الى خادم السحابة. مالك البيانات يقوم بتشفير البيانات و مندوبين عملية فك التشفير الى السحابة. خادم السحابة يؤدي فك التشفير الجزئي و من ثم يتم مشاركة بيانات فك التشفير النهائي للمستخدمين وفقاً للامتيازات. مالك البيانات يقلل من التعقيد الحسابي من خلال تفويض خادم السحابة علمية فك التشفير. قمنا ببناء تطبيق النموذج الاولي باستخدام منصة مايكروسوفت دوت نت لأثبات هذا المفهوم. و أظهرت النتائج التجريبية أن هناك وصولا خاضعا للرقابة مع تعدد أدوار المستعملين و حقوق التحكم في النفاذ من أجل النفاذ الآمن و السري إلى البيانات في الحوسبة السحابية.

الكلمات المفتاحية:– الحوسبة السحابية ، التشفير ، فك التشفير ، امكانية التحقق من تفكيك فك التشفير، فك التشفير الجزئي.

1. Introduction

Cloud computing is a new model of computing in which Internet based computing resources are provided to public in pay as you go fashion. The cloud computing technology enables users and organizations to gain access to different services related to infrastructure, platform and software. The cloud computing allows access to computing resources without capital investment. The data outsourced to cloud is stored in data centres. The usage of cloud computing can be done with any Internet-aware device. Users can avail cloud computing services through the Internet without time and geographical restrictions.

It is evident that cloud computing provides a huge amount of computing resources that can be accessed from any device through the Internet. There are different kinds of cloud deployments. The deployment models include private cloud, public cloud, community cloud and hybrid cloud. Whatever be the deployment model, it is essential to have data access control mechanisms in place. The private cloud allows users of an organization to gain access to cloud. Public cloud allows general public to gain access to cloud. Amazon, Google, and IBM are providing public cloud for instance. Community cloud is the cloud built by two or more similar

organizations. Only users of those organizations can gain access to community cloud. Hybrid cloud is the cloud which is made up of two or more clouds. For example, private cloud and public cloud combination are the most common hybrid approach.

It is evident that the public cloud can be accessed by anyone in the world. In this context, it is important to have access control mechanisms. Many researchers contributed towards providing access control mechanisms. Many of the mechanisms are based on ABE(Sahai and waters , 2005 ; Han *et.al.,* 2012;Goyal *et.al.,* 2006; Garg *et.al.,* 2013) which provides controlled access to health care or any such data. In this paper, we proposed a framework that helps in controlling data sharing. The proposed model demonstrates different roles such as data owner, user, cloud server and authority. Authority is nothing but attribute authority which determines how access is given to different attributes.

The remainder of the paper is structured as follows. Section II reviews literature related to ABE and other such schemes. Section III presents proposed framework its implementation demonstrating controlled access to data. Section IV presents experiments and results while section V concludes the paper and provides recommendations for future work.

2. Related Works

This section provides reviews of related works of encryption models in cloud computing. Sahai and Waters (Sahai and waters , 2005) presented Attribute Based Encryption (ABE) for more efficient accessibility of data in the cloud. They further focused in (Han *et.al.,* 2012; Goyal *et.al.,* 2006) on authorities and policies that are authored by them. Later on they (Garg *et.al.,* 2013) constructed KP-ABE while earlier systems used Boolean formulae. The concept of hybrid encryption was proposed in (Cramer and Shoup , 1998; Cramer and Shoup , 2004) where a key encapsulation mechanism was proposed. They employed symmetric encryption model along with one time MAC. Similar kind of work was carried out in (Hofheinz and Kiltz , 2007; Abe *et.al.,* 2008; Kurosawa *et.al.,* 2004). They were able to ensure high security needs. Right from the inception of ABE, multiple advances came into existence. The notion of outsourcing computation as explored in (Li *et.al.,* 2013; Hur and Noh, 2011) was assumed importance in the research. In this fashion, first outsourced decryption with ABE was proposed by (Green *et.al.,* 2011).

Subsequently (Lai *et.al.,* 2013) proposed outsourced decryption which was verifiable. Such schemes provide a guarantee of correctness in the form of commitments. Data owner produces commitment without considering the privacy of his identity, forgery attacks are possible. To overcome this problem circuit key-policy ABE (CP-ABE) was proposed in (Garg *et.al.,* 2013). This work had anti-collusion concept which is closer to conventional access control mechanisms. The anti-collusion concept is evaluated with sufficient computations in cloud computing. From his kind of encryption model VD-CPABE came into existence. The latter assumes that untrusted cloud has no learning capability (Granlund and the GMP development team. 2013). The cipher text of this approach has two things known as CPABE encapsulation mechanism as explored in (Nagao *et.al.,* 2005) and then encrypt MAC mechanism as explored in (Bellare and Namprempre, 2000). In (Coron *et.al.,* 2013) multi-linear maps are used over integers in order to simulate the schemes. It is very important as the scheme is verifiable. However, delegation of decryption is made verifiable in this paper.

3. Proposed System

I proposed architecture for the proposed system. It has four parties involved. They are data owner, user, cloud server and authority. The data owner is responsible to encrypt data and send it to cloud server. However, the encrypted data are subjected to MAC cipher text and decryption process delegated to cloud server. The cloud server is responsible to have a partial decryption process as it was delegated to it by the data owner. The delegation is for reducing computational cost incurred by the data owner. Once partial decryption is made by the server, then the MAC cipher text obtained through partial encryption is subject to verification and further decryption to obtain the original data sent by the data owner. This was medical data is shared. However, the sharing is subjected to privileges possessed by users. These privileges are granted by the authority which is implicit and not shown in the architectural diagram shown in Figure 1.

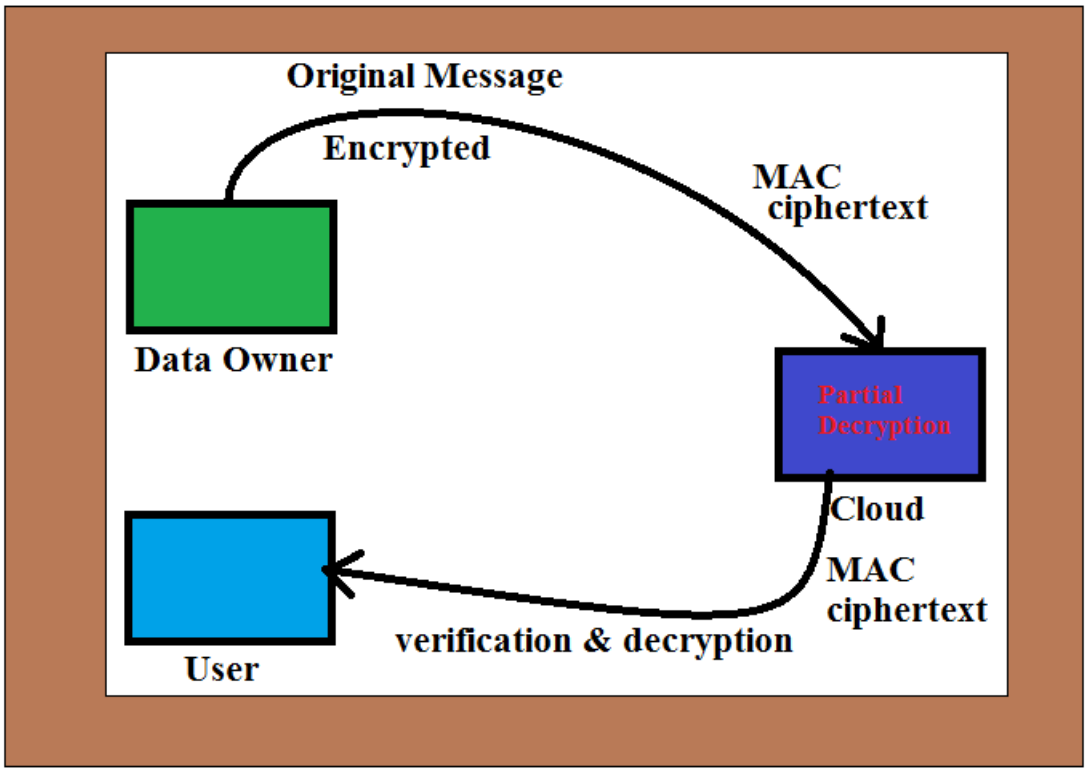

Figure 1: Architectural overview of the proposed system

As shown in Figure 1, it is evident that the proposed system makes use of encryption and decryption mechanisms as power the roles specified. The roles include data owner, user, cloud server and authority. The data owner is able to upload content to the cloud server, view files and sign out. The symmetric key is used to have encryption process. Another key used for the same is the encryption key. MAC code is generated and the data is encrypted as follows.

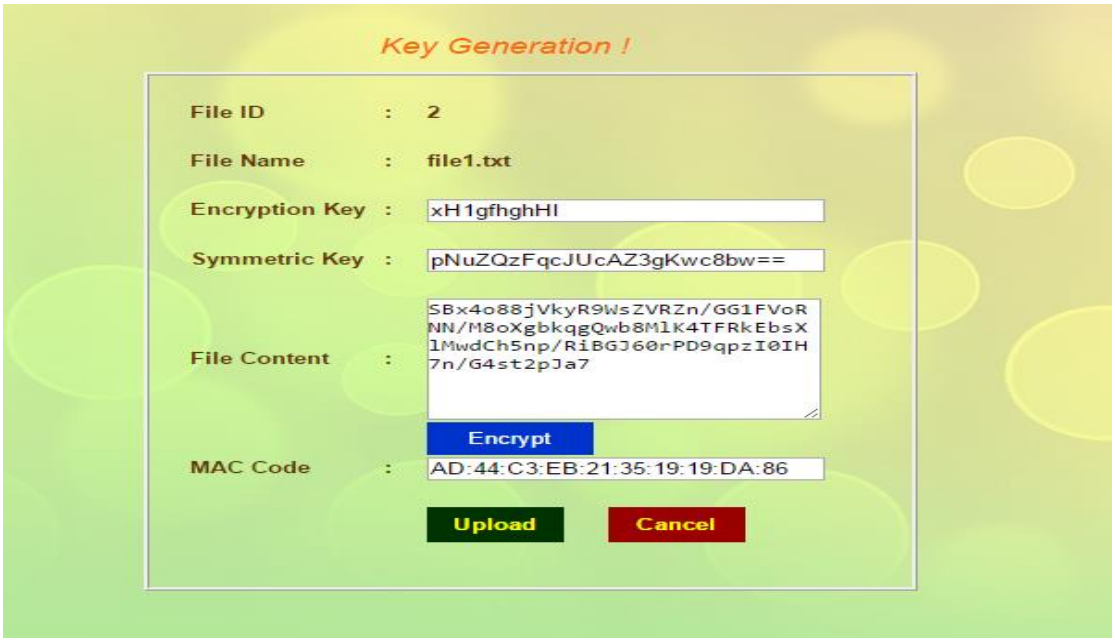

Figure 4: shows selected file and encryption done by the data owner

As shown in Figure 4, the file content is subjected to encryption which converted it into cipher text. Then the MAC code is also generated that before data is uploaded to cloud server. After this, the user can send request for files and view files as per the permissions. The user request goes to cloud server. Then the cloud server can view owner files, and user requests. Then the cloud performs partial decryption process. The authority can view files and provide access key that can be used by data owner and data user according to the privileges granted by the data owner.

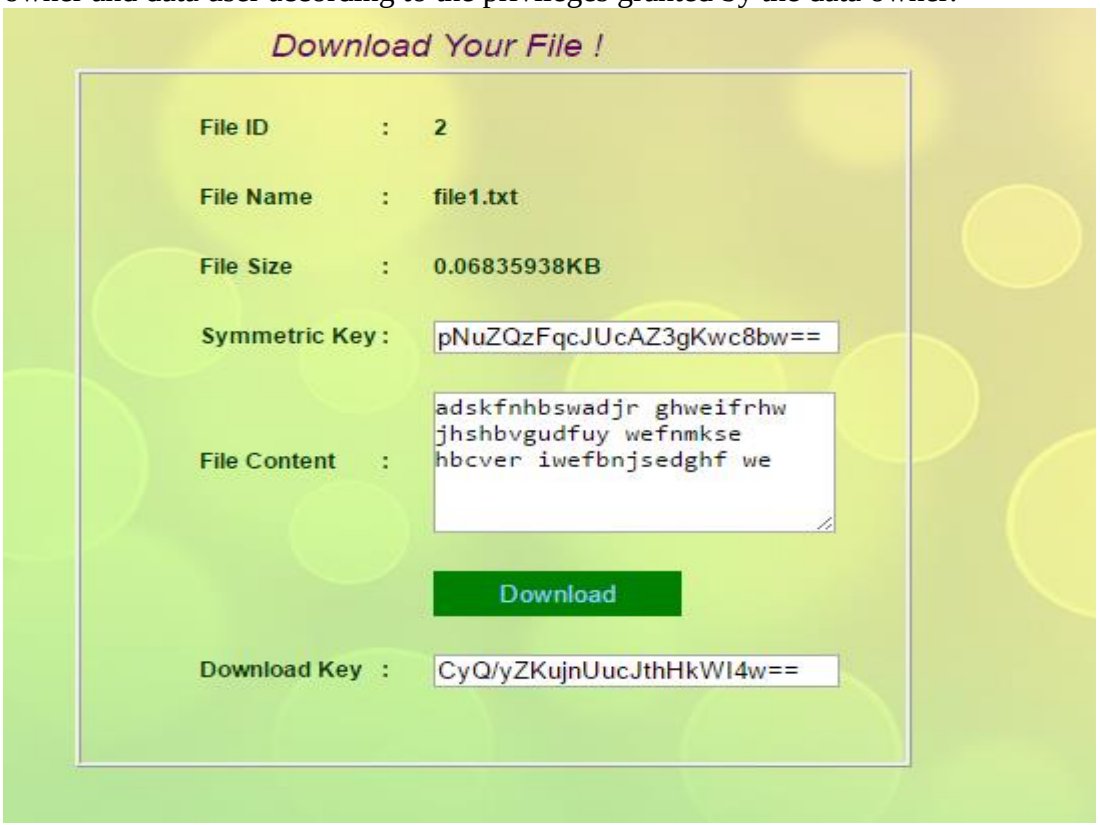

Figure 5: Decryption and download of file

As shown in Figure 5, it is possible to have download key and symmetric key to decrypt and download file. This operation can be performed by data owner and data users. Data user's should have privileges to do this.

4. Experimental Results

The proposed system is implemented using the Microsoft.NET platform. Visual Studio is the development environment used. C# programming is used to provide functionality while ASP.NET is used for designing web based application. ADO.NET is used to perform database operations programmatically. The notion of circuits is used to perform encryption and decryption effectively. The results are observed in terms of average execution time in seconds taken for data owner, cloud server and user against the depth of the circuit.

Table 1: Average execution time against depth of the circuit for data owner

Depth of the Circuit	Avg Execution Time (s)
1	0
2	0
3	0
4	1
5	3
6	5
7	10
8	20
9	40
10	80

As shown in Table 1, the results revealed that the depth o circuit has its impact on the execution time. The execution time is increased when depth of the circuit is increased in the cryptographic primitives.

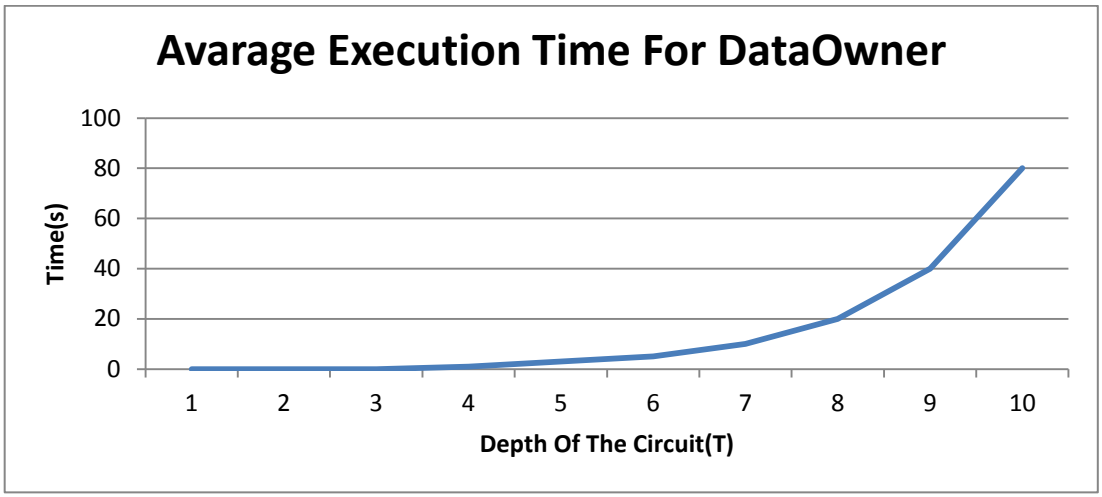

Figure 6: Average execution time for data owner

As shown in Figure 6, it is evident that there are two trends in the results. The first trend is that the average execution time is same for the depth of the circuit 1, 2 and 3. Afterwards, the average execution time is increased gradually as the depth of the circuit is increased for data owner.

Table 2: Average execution time vs. depth of circuit for cloud server

Depth of the Circuit	Avg Execution Time (s)
1	0
2	0
3	0
4	1
5	2
6	3
7	5
8	10
9	20
10	40

As shown in Table 2, the results revealed that the depth of the circuit has its impact on the execution time. The execution time is increased when the depth of the circuit is increased in the cryptographic primitives for cloud server.

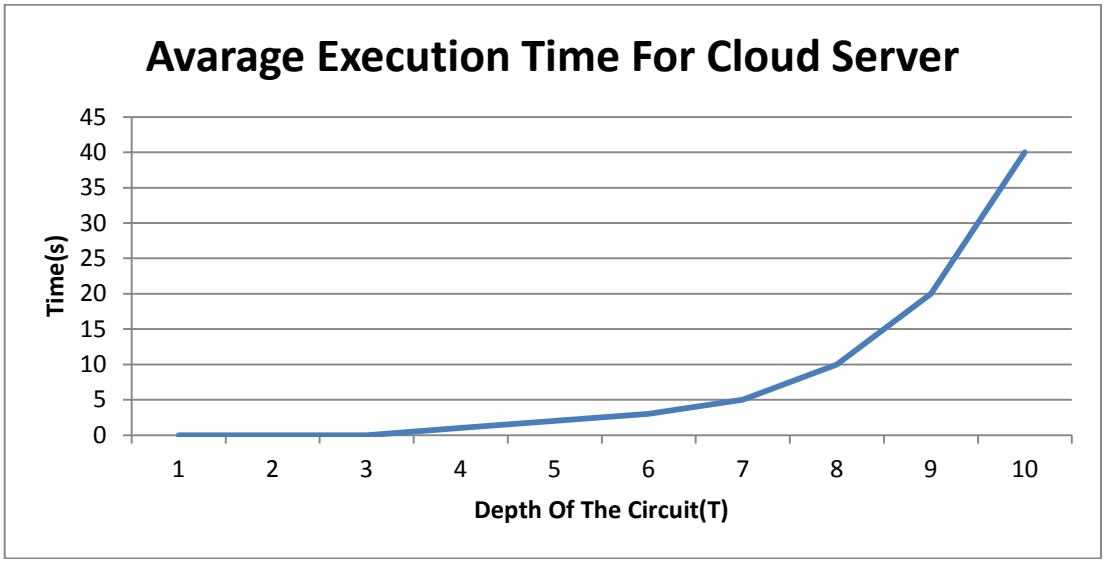

Figure 7: Average execution time for cloud server

As shown in Figure 7, it is evident that there are two trends in the results. The first trend is that the average execution time is same for the depth of the circuit 1, 2 and 3. Afterwards, the average execution time is increased gradually as the depth of the circuit is increased for cloud server.

Table 3: Average execution time against depth of the circuit for user

Depth of the Circuit	Average Execution Time (s)
1	0.063
2	0.063
3	0.063
4	0.063
5	0.063
6	0.063
7	0.063
8	0.063
9	0.063
10	0.063

As shown in Table 3, the results revealed that the depth of the circuit has no impact on the execution time. The execution time is same when the depth of the circuit is increased in the cryptographic primitives for user roles.

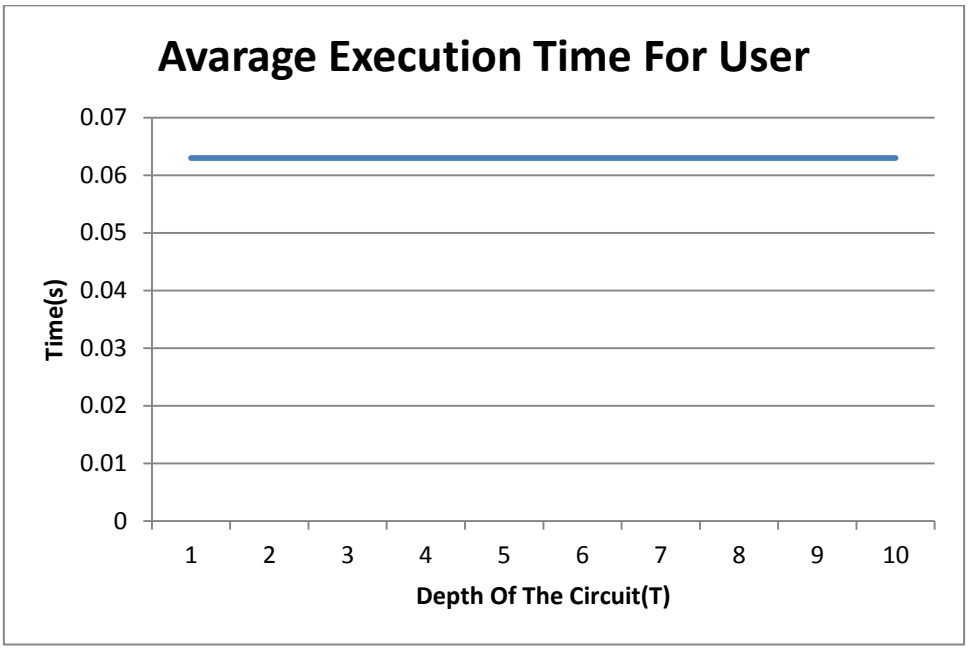

Figure 8: Average execution time for user

As shown in Figure 8, it is evident the average execution time taken for user against different depth of the circuit remains same. Interestingly from 1 through 10 of the depth of the circuit, the execution time is same that is 0.063 seconds.

5. Conclusions and Future Work

In this paper, we proposed and implemented a framework that takes care of efficient medical data sharing in cloud computing. The proposed framework implements a hybrid verifiable and delegated encryption model where the decryption process is delegated to the cloud server for scalability and reduction of computational complexity at the data owner side. According to the proposed model, data owner encrypts data to be outsourced to cloud server. After encryption, MAC cipher text is generated which is associated with the data stored in the cloud. The cloud server is responsible to perform partial decryption based on the privileges granted by attribute authority. The attribute authority also provides access control to users. Users can perform verification and decryption once the data is given by the cloud server after granting access rights. Data owner is capable of viewing decrypted files. We built a prototype application using the Microsoft.NET platform for proof of the concept. The empirical results revealed that there is controlled access with multiple user roles and access control rights for secure and confidential data access in cloud computing. This research can be extended further by introducing different attacks and evaluating the proposed model for its ability to withstand attacks.

References

Abe M., Gennaro R., and Kurosawa K. ., 2008, "Tag-KEM/DEM:A new framework for hybrid encryption," in Proc. 28th Int. Cryptol. Conf, pp. 97–130.

Bellare M. and Namprempre C., 2000, "Authenticated encryption: Relations among notions and analysis of the generic composition paradigm," in Proc. 11th Int. Conf. Adv. Cryptol., pp. 531–545.

Coron J., Lepoint T., and Tibouchi M., 2013, "Practical multilinear maps over the integer," in Proc. 33rd Int. Cryptol. Conf., pp. 476– 493.

Cramer R. and Shoup V. , 2004, "Design and analysis of practical publickey encryption schemes secure against adaptive chosen ciphertext attack," SIAM J. Comput., vol. 33, no. 1, pp. 167–226.

Cramer R. and Shoup V., 1998, "A practical public key cryptosystem provably secure against adaptive chosen ciphertext attack," in Proc. 18th Int. Cryptol. Conf., pp. 13–25.

Garg S., Gentry C., Halevi S., Sahai A., and Waters B. ,2013, "Attributebased encryption for circuits from multilinear maps," in Proc. 33rd Int. Cryptol. Conf., pp. 479–499.

Goyal V., Pandey O., Sahai A., and Waters B. , 2006, "Attribute-based Encryption for Fine-grained access control of encrypted data," in Proc. 13th ACM Conf. Comput. Commun. Security, pp. 89–98.

Granlund T. and the GMP development team. 2013 . GNU MP: The GNU multiple precision arithmetic library, 5.1.1 [Online]. Available: http://gmplib.org/

Green M., Hohenberger S., and Waters B. , 2011, "Outsourcing the decryption of ABE Ciphertexts," in Proc. USENIX Security Symp., San Francisco, CA, USA, p. 34.

Han J., Susilo W., Mu Y., and Yan J. , Nov. 2012, "Privacy-preserving decentralized key-policy attribute-based Encryption," IEEE Trans. Parallel Distrib. Syst., vol. 23, no. 11, pp. 2150–2162.

Hofheinz D. and Kiltz R. E. ,2007, "Secure hybrid encryption from weakened key encapsulation," in Proc. 27th Int. Cryptol. Conf., pp. 553–571.

Hur J. and Noh D. K. , Jul. 2011, "Attribute-based access control with effi- cient revocation in data outsourcing systems," IEEE Trans. Parallel Distrib. Syst., vol. 22, no. 7, pp. 1214–1221.

Kurosawa K. and Desmedt Y., 2004, "A new paradigm of hybrid encryption scheme," in Proc. 24th Int. Cryptol. Conf., pp. 426– 442.

Lai J., Deng R. H., Guan C., and Weng J., "Attribute-based encryption with verifiable outsourced decryption," IEEE Trans. Inf. Forensics Secur., vol. 8, no. 8, pp. 1343–1354, Aug. 2013.

Li J., Huang X., Li J., Chen X., and Xiang Y. , Aug. 2013, "Securely outsourcing attribute-based encryption with checkability," IEEE Trans. Parallel Distrib. Syst., vol. 25, no. 8, pp. 2201–2210.

Nagao W., Manabe Y., and Okamoto T. , 2005, "A universally composable secure channel based on the kem-dem framework," in Proc. 25th Int. Cryptol. Conf., pp. 426–444.

Sahai A. and Waters B. , 2005, "Fuzzy identity based encryption," in Proc. 30th Annul. Int. Conf. Theory Appl. Cryptograph. Techn., pp. 457–473.