ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 2, February 2017

Secure Circuit Ciphertext-Policy Attribute-Based Encryption with Time-Specified Attribute Scheme in Cloud Computing

Pratiksha Patil, Prof. Ramesh Patole

Student, Department of Information Technology, G.H.Raisoni College of Engineering and Management, Domkhel Road Wagholi, Pune, India

Professor, Department of Information Technology, G.H.Raisoni College of Engineering and Management, Domkhel Road, Wagholi, Pune, India

ABSTRACT: In the cloudenvironment, the data owners could uses attribute-based encryption to encrypt the stored data which accomplishing access control and data security. To reduce the cost, the users which have a limited computing power are nevertheless more likely to delegate the mask of the decryption task to the cloud servers. The result shows, attribute-based encryption with delegation come out. Still, there are some problems and questions regarding to previous related works. For example, during the delegation or release, the cloud servers could misrepresent or replace the delegated cipher text and respond a fake result with malevolent intent. As well as for the purpose of cost saving the cloud server may also fraud the eligible users by responding them that they are unworthy. Even, the access policies may not be flexible during the encryption. Since policy for general circuits are used to achieve the strongest form of access control, a construction to design circuit cipher text-policy attribute-based encryption with time-specified attributes scheme has been developed.. In this scheme, every cipher text is labeled with some attribute and a time interval while private key is associated with a time instant. The cipher text can only be decrypted if both the time instant is in the allowed time interval and the attributes associated with the cipher text satisfy the key's access structure.This system is mixed with verifiable computation the dataconfidentiality, the fine-grained access control as well as the correctness of the delegated computing results are well guaranteed at the same time. Moreover, this scheme achieves feasibility as well as efficiency.

KEYWORDS: Cloud computing, Cipher text-policy attribute-based encryption, circuits, verifiable delegation.

I. INTRODUCTION

Presently cloud computing technology is mostly used to store the large amount of data. Within these computing environments, the cloud servers can offer various data services, such as remote data storage and outsourced delegation computation for data storage, the servers store a large amount of shared data, which could be accessed by authorized users. For delegation computation, the servers could be used to handle and calculate numerous data according to the user's demands. To reduce the cost, the users which have a limited computing power are nevertheless more likely to delegate the mask of the decryption task to the cloud servers. The result shows, attribute-based encryption with delegation come out. Still, there are some problems and questions regarding to previous related works. For example, during the delegation or release, the cloud servers could misrepresent or replace the delegated cipher text and respond a fake result with malevolent intent. As well as for the purpose of cost saving the cloud server may also fraud the eligible users by responding them that they are unworthy. Even, the access policies may not be flexible during the encryption. Since policy for general circuits are used to achieve the strongest form of access control, a construction to design circuit cipher text-policy attribute-based encryption with time-specified attributes scheme has been developed. . In this scheme, every cipher text is labeled with some attribute and a time interval while private key is associated with a time instant. The cipher text can only be decrypted if both the time instant is in the allowed time interval and the attributes

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 2, February 2017

associated with the cipher text satisfy the key's access structure. This system is mixed with verifiable computation the data confidentiality, the fine-grained access control as well as the correctness of the delegated computing results are well guaranteed at the same time. Moreover, this scheme achieves feasibility as well as efficiency.

II. REVIEW OF LITERATURE

[1] Attribute-based encryption with verifiable outsourced decryption [1]. The author first formalizes a security model of ABE with verifiable outsourced decryption by introducing a verification key in the output of the encryption algorithm. Then, he presents an approach to convert any ABE scheme with outsourced decryption into an ABE scheme with verifiable outsourced decryption. The new approach is simple, general, and almost optimal. Compared with the original outsourced ABE, our verifiable outsourced ABE neither increases the user's and the cloud server's computation costs except some non dominant operations (e.g., hash computations), nor expands the cipher text size except adding a hash value (which is <;20 byte for 80-bit security level).

[2] Cipher text-policy attribute-based encryption: An expressive, efficient, and provably secure realization [2]. The author presents a new methodology for realizing Ciphertext-Policy Attribute Encryption (CPABE) under concrete and non interactive cryptographic assumptions in the standard model. Our solutions allow any encrypt or to specify access control in terms of any access formula over the attributes in the system. The author presents three constructions within this framework. The first system is proven selectively secure under a assumption that we call the decisional Parallel Bilinear Diffie-Hellman Exponent (PBDHE) assumption which can be viewed as a generalization of the BDHE assumption. The next two constructions provide performance tradeoffs to achieve provable security respectively under the (weaker) decisional Bilinear-Diffie-Hellman Exponent and decisional Bilinear DiffieHellman assumptions.

[3] Cipher text-policy attribute-based encryption: An expressive, efficient, and provably secure realization [3]. The author presents a new methodology for realizing Ciphertext-Policy Attribute Encryption (CPABE) under concrete and non interactive cryptographic assumptions in the standard model. Our solutions allow any encryptor to specify access control in terms of any access formula over the attributes in the system. The author presents three constructions within this framework. The first system is proven selectively secure under a assumption that we call the decisional Parallel Bilinear Diffie-Hellman Exponent (PBDHE) assumption which can be viewed as a generalization of the BDHE assumption. The next two constructions provide performance tradeoffs to achieve provable security respectively under the (weaker) decisional Bilinear-Diffie-Hellman Exponent and decisional Bilinear DiffieHellman assumptions.

[4] How to Delegate and Verify in Public: Verifiable Computation from Attribute-based Encryption [4].In this work the author extends the definition of verifiable computation in two important directions: public delegation and public verifiability, which have important applications in many practical delegation scenarios. Yet, existing VC constructions based on standard cryptographic assumptions fail to achieve these properties.

[5] Verifiable predicate encryption and applications to CCA security and anonymous predicate authentication [5]. In this work, the author focuses on verifiability of predicate encryption. A verifiable predicate encryption scheme guarantees that all legitimate receivers of a cipher text will obtain the same message upon decryption. While verifiability of predicate encryption might be a desirable property by itself, he furthermore shows that this property enables interesting applications.

[6] Privacy-preserving decentralized key-policy attribute-based Encryption [6]. The author propose a privacy-preserving decentralized key-policy ABE scheme where each authority can issue secret keys to a user independently without knowing anything about his GID. Therefore, even if multiple authorities are corrupted,

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 2, February 2017

they cannot collect the user's attributes by tracing his GID. Notably, our scheme only requires standard complexity assumptions (e.g., decisional bilinear Diffie-Hellman) and does not require any cooperation between the multiple authorities, in contrast to the previous comparable scheme that requires nonstandard complexity assumptions (e.g., q-decisional Diffie-Hellman inversion) and interactions among multiple authorities

[7] Attribute based encryption for circuits from multilinear maps [7].The author propose an access control mechanism using cipher text-policy attribute-based encryption to enforce access control policies with efficient attribute and user revocation capability. The fine-grained access control can be achieved by dual encryption mechanism which takes advantage of the attribute-based encryption and selective group key distribution in each attribute group. We demonstrate how to apply the proposed mechanism to securely manage the outsourced data.

[8] Attribute-Based Access Control with Efficient Revocation in Data Outsourcing Systems [8].The author proposes an access control mechanism using ciphertext-policy attribute-based encryption to enforce access control policies with efficient attribute and user revocation capability. The fine-grained access control can be achieved by dual encryption mechanism which takes advantage of the attribute-based encryption and selective group key distribution in each attribute group.

[9] Securely outsourcing attribute-based encryption with checkability [9].The author propose a new Secure Outsourced ABE system, which supports both secure outsourced key-issuing and decryption. Our new method offloads all access policy and attribute related operations in the key-issuing process or decryption to a Key Generation Service Provider (KGSP) and a Decryption Service Provider (DSP), respectively, leaving only a constant number of simple operations for the attribute authority and eligible users to perform locally. In addition, for the first time, he propose an outsourced ABE construction which provides checkability of the outsourced computation results in an efficient way.

[10] Tag-KEM/DEM:A new framework for hybrid encryption [10].The author presents a novel framework for generic construction of hybrid encryption schemes secure against chosen cipher text attack. This new framework yields new and more efficient CCA-secure schemes, and provides insightful explanations about existing schemes that do not fit into the previous frameworks. This could result in finding future improvements. Moreover, it allows immediate conversion from a class of threshold public-key encryption to a hybrid one without considerable overhead, which is not possible in the previous approaches. Finally he present an improved security proof of the KurosawaDesmedt scheme, which removes the original need for informationtheoretic key derivation and message authentication functions.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 2, February 2017

III. SYSTEM ARCHITECTURE

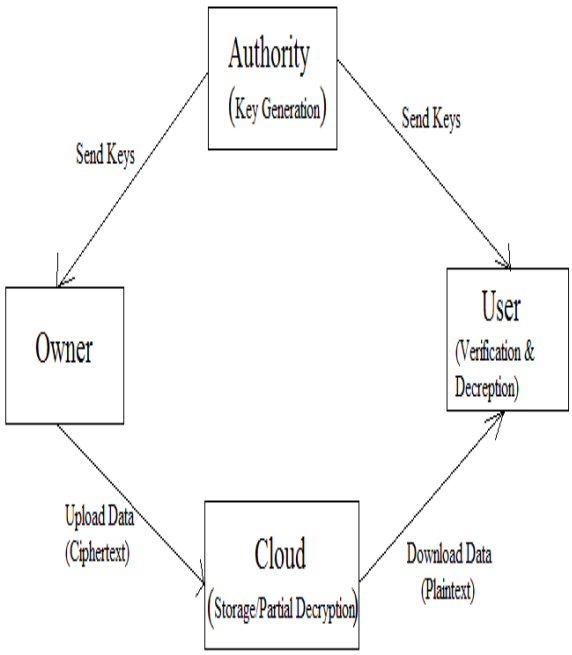

Fig. 1 System Architecture

The system contains four modules,

1) Owner
2) User
3) Authority
4) Cloud Server

- **Owner:** Owner is responsible to upload the data and assign the attribute to data and create the access structure.
- **Authority:** Authority is responsible to generate keys, which are public key, private key, Master key and Transformation key. Public key is used by owner to encrypt the data. Master key is kept secret. Transformation key is used by Cloud server to partially decrypt the cipher text. Private Key is used by user to verify and decrypt the data.
- **User:** User is responsible to access the data.
- **Cloud Server:** Cloud server is responsible to provide storage space and partially decrypt the data when user wants to access.

ADVANTAGES:

- Achieve access control and keep data confidential.
- Reduce the computing cost.
- Achieves security.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 2, February 2017

IV. MATHEMATICAL MODELING

S = {s, e, X, Y, F,φ }

S = Set of system

s = Start of the program

- Register to system.
- Login to system.

X = Input of the program

X = { F, A1,A2,…..An ,k,tm}
Where,
F= File uploaded by Owner.

A1,A2,…..An= Attributes set to file by Owner.

k = encryption key
tm= time spam for which the data is present

Y = Output of the program

Y = {RD}
RD= Retrieved file after decryption from storage system using key (k)

- User can download the file if both the time instant is in the allowed time interval and the attributes associated with the ciphertext satisfy the key's access structure.

Function Fun = {Enck(D), Decrk(E)}
Where, Enck (D) = Encryption of data using key (k)
for storing data in encrypted format
Deck (E) = Decryption of data for retrieving original data

e = End of the program
Which comprise of two states :
If t < tm: Data will be retrieved from storage system.
If t > tm: Data will be not accessible.

φ = Success or failure condition of system
Above mathematical model is NP-Complete.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 2, February 2017

IV. RESULT

1) Result Graph:

Average execution time for data owner.

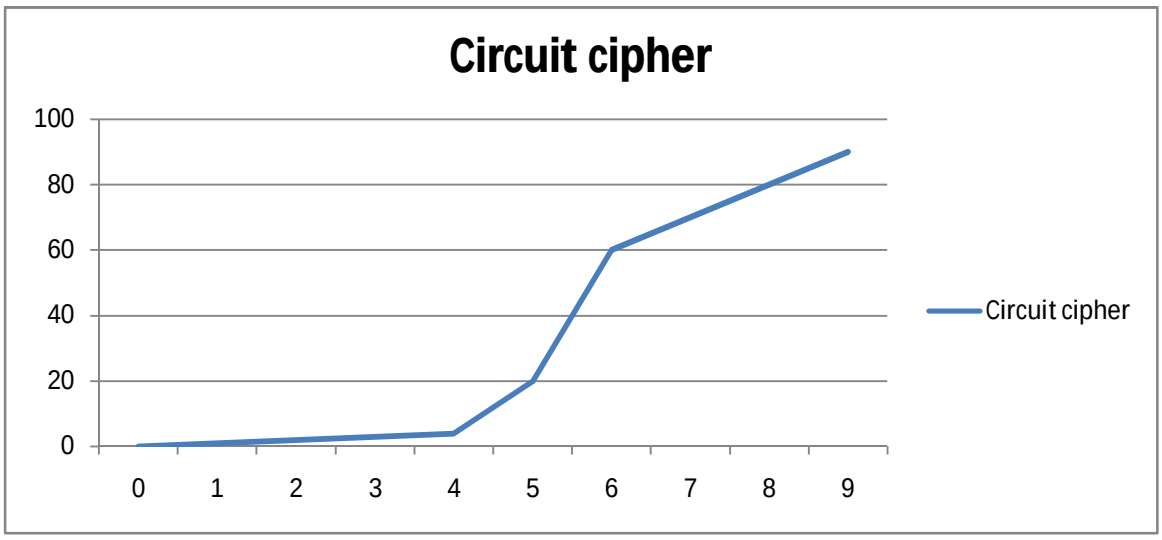

Fig 02X-axis: Depth of circuit y-axis-time

2) Average execution time for cloud server

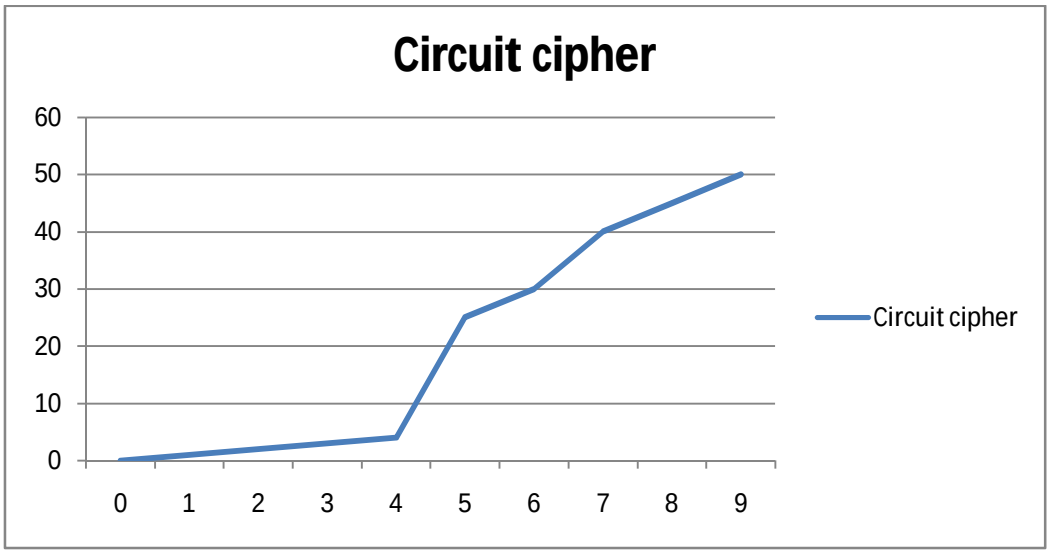

Fig. 03 On x-axis:Depth of circuit,Y-axis:Time

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 2, February 2017

3) Average execution time for Users

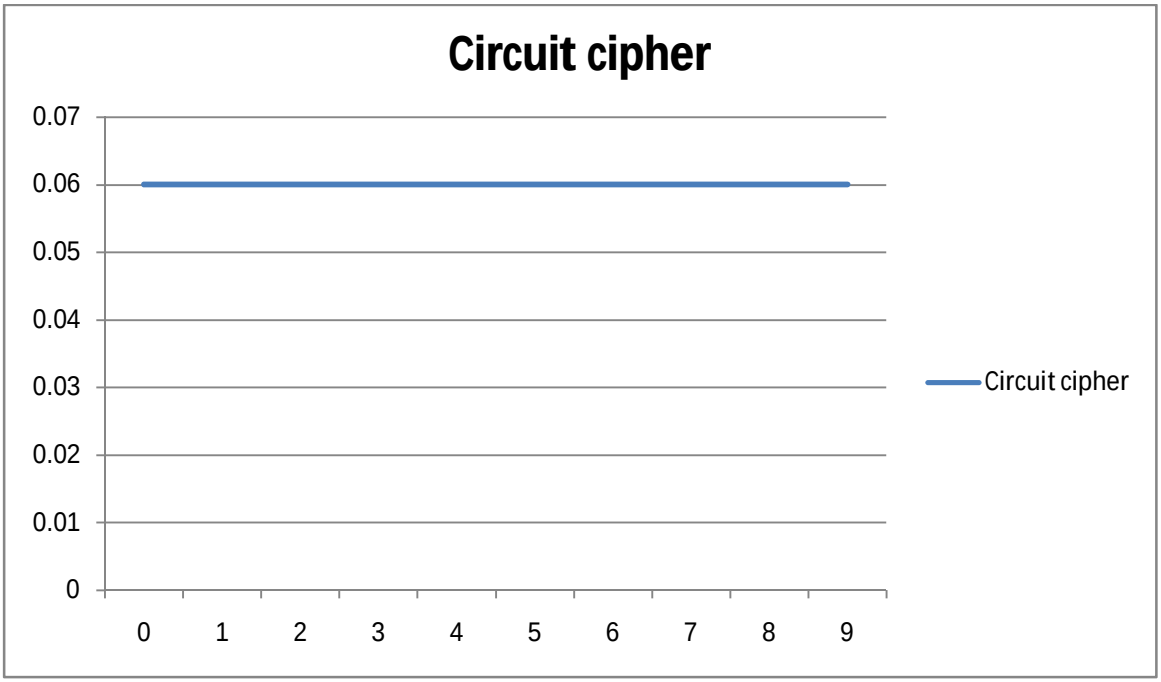

Fig. 04 On x-axis:Depth of circuit,Y-axis:Time

4. Performance Analysis

By considering security it provide better performance than other systems. Means owner uploads the file by accepting the key for encryption. And user can download the file by sending requesting key to authority. When user get the key that time only he can decrypt the file. Circuit cipher text is perform better than identity based encryption that it reduces time for uploading multiple file to multiple user.

V. CONCLUSION

With the fast advancement of adaptable cloud services, a lot of new difficulties have developed. One of the most critical issues is the way to securely delete the outsourced data put away in the cloud severs. We design circuit cipher text-policy attribute-based encryption with time-specified attributes scheme has been developed.In this scheme, every cipher text is labeled with some attribute and a time interval while private key is associated with a time instant. The cipher text can only be decrypted if both the time instant is in the allowed time interval and the attributes associated with the cipher text satisfy the key's access structure. The conclusion show that the method is sensible in the cloud computing. Thus, can be able to achieve data privacy, the fine-grained entrée manages and the demonstrable allocation in cloud.

REFERENCES

[1] J. Lai, R. H. Deng, C. Guan, and J. Weng, "Attribute-based encryptionwith verifiable outsourced decryption," IEEE Trans. Inf. ForensicsSecur., vol. 8, no. 8, pp. 1343–1354, Aug. 2013.
[2] Lewko and B. Waters, "Decentralizing attribute-based encryption," in Proc. 30th Annu. Int. Conf. Theory Appl. Cryptograph. Techn., 2011, pp. 568–588.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 2, February 2017

[3] B. Waters, "Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization," in Proc.14th Int. Conf. Practice Theory Public Key Cryptograph. Conf. Public Key Cryptograph., 2011, pp. 53–70.
[4] B. Parno, M. Raykova, and V. Vaikuntanathan, "How to delegate and verify in public: Verifiable computation from attribute-basedencryption," in Proc. 9th Int. Conf. Theory Cryptograph., 2012, pp. 422–439.
[5] S. Yamada, N. Attrapadung, and B. Santoso, "Verifiable predicate encryption and applications to CCA security and anonymous predicate authentication," in Proc. Int. Conf. Practice Theory Public Key Cryptograph. Conf. Public Key Cryptograph., 2012, pp. 243–261.
[6] J. Han, W. Susilo, Y. Mu, and J. Yan, "Privacy-preserving decentralized key-policy attribute-based Encryption," IEEE Trans. ParallelDistrib. Syst., vol. 23, no. 11, pp. 2150–2162, Nov. 2012.
[7] S. Garg, C. Gentry, S. Halevi, A. Sahai, and B. Waters, "Attribute based encryption for circuits from multilinear maps," in Proc. 33rdInt. Cryptol. Conf., 2013, pp. 479–499.
[8] J. Hur and D. K. Noh, "Attribute-based access control with efficient revocation in data outsourcing systems," IEEE Trans. ParallelDistrib. Syst., vol. 22, no. 7, pp. 1214–1221, Jul. 2011.
[9] J. Li, X. Huang, J. Li, X. Chen, and Y. Xiang, "Securely outsourcing attribute-based encryption with checkability," IEEE Trans. ParallelDistrib. Syst., vol. 25, no. 8, pp. 2201–2210, Aug. 2013.
[10] M. Abe, R. Gennaro, and K. Kurosawa, "Tag-KEM/DEM:A new framework for hybrid encryption," in Proc. 28th Int. Cryptol. Conf., 2008, pp. 97–130.