ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 4, April 2018

A Time-Specified Ciphertext-Policy Attribute-Based Encryption with Circuit's Technique in Cloud Computing

Suraj Lolage,Hema Mangtani, Komal Dongare, Akash Labade, Prof.Shikha Pachouly

Dept. of Computer Engineering, AISSMSCOE, Pune, India

ABSTRACT: In cloud environment, lots of issues regarding security. To achieve security different techniques are used like encryption, decryption, and attribute-based encryption with delegation. Still, in this technique there are some issues and questions like how to trust on cloud server. The cloud servers could misrepresent or replace the delegated ciphertext 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. To overcome all this issues we design new technique Time-specified ciphertext-policy attribute-based encryption with circuits. In this technique, each and every ciphertext is labeled with different attributes and a time interval like start time and end time also provide circuits while private key is associated with a time instant. The ciphertext can only be decrypted if both the time instant is in the allowed time interval and the attributes associated with the ciphertext satisfy the key's access structure. To achieves the more security, the data is divided into multiple fragments and store on multiple nodes instead of storing on single node. This technique achieves data confidentiality, the fine-grained access control as well as the correctness of the delegated computing results.

KEYWORDS*:* Cloud computing, Security, Ciphertext-policy attribute-based encryption, Verifiable delegation, data confidentiality, fragments.

I. INTRODUCTIONS

A. Background:

Cloud computing is innovation that uses advanced computational power and improved storage capabilities. Cloud computing is a long dreamed vision of computing utility, which enable the sharing of services over the internet. 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 ciphertext 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 ciphertext-policy attribute-based encryption with time-specified attributes scheme has been developed. . In this scheme, every ciphertext is labeled with some attribute and a time interval while private key is associated with a time instant. The ciphertext can only be decrypted if both the time instant is in the allowed time interval and the attributes associated with the ciphertext satisfy the key's access structure. This system is mixed with verifiable computation the data

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 4, April 2018

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.

B. Motivation:

In existing system during the delegation, the cloud servers could tamper or replace the delegated ciphertext and respond a forged computing result with malicious intent. They may also cheat the eligible users by responding them that they are ineligible for the purpose of cost saving.So main motivation of this work is to overcome this entire problem. Also achieve Security, provide fine grained access control as well as achieves feasibility as well as efficiency.

C. Objectives:

- To achieve Security.
- To provide fine grained access control.
- To reduce cost.
- To achieves feasibility as well as efficiency

II. RELATED WORK OR LITERATURE SURVEY

[1]. J. Lai, R. H. Deng, C. Guan, and J. Weng (2013) has represents 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 present 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 ciphertext size except adding a hash value (which is <;20 byte for 80-bit security level).

[2]. B. Waters (2011) has represents Ciphertext-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 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.

[3]. B. Parno, M. Raykova, and V. Vaikuntanathan (2012) have demonstrated How to Delegate and Verify in Public: Verifiable Computation from Attribute-based Encryption [3].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.

[4] S. Yamada, N. Attrapadung, and B. Santoso (2012) has design Verifiable predicate encryption and applications to CCA security and anonymous predicate authentication [4]. In this work, the author focus on *verifiability* of predicate encryption. A verifiable predicate encryption scheme guarantees that all legitimate receivers of a ciphertext 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.

[5]. J. Han, W. Susilo, Y. Mu, and J. Yan (2012) Privacy-preserving decentralized key-policy attribute-based Encryption [5]. 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, 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

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 4, April 2018

[6].S. Garg, C. Gentry, S. Halevi, A. Sahai, and B. Waters (2013) has developed Attribute based encryption for circuits from multilinear maps [6].The author propose 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. We demonstrate how to apply the proposed mechanism to securely manage the outsourced data.

[7].J. Hur and D. K. Noh (2011) has represents Attribute-Based Access Control with Efficient Revocation in Data Outsourcing Systems [7].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.

[8]. J. Li, X. Huang, J. Li, X. Chen, and Y. Xiang (2013) has represents Securely outsourcing attribute-based encryption with checkability [8].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.

[9]. M. Abe, R. Gennaro, and K. Kurosawa (2008) Tag-KEM/DEM:A new framework for hybrid encryption [9]. The author presents a novel framework for generic construction of hybrid encryption schemes secure against chosen ciphertext 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 Kurosawa Desmedt scheme, which removes the original need for information theoretic key derivation and message authentication functions.

III. EXISTING SYSTEM AND DISADVANTAGES

In Existing System, The cloud servers could tamper or replace the delegated ciphertext and respond a forged computing result with malicious intent. They may also cheat the eligible users by responding them that they are ineligible for the purpose of cost saving. Furthermore, during the encryption, the access policies may not be flexible enough as well.

Disadvantages of Existing System:

1. There is no guarantee that the calculated result returned by the cloud is always correct.
2. The cloud server may forge ciphertext or cheat the eligible user that he even does not have permissions to decryption.

IV. PROPOSED SYSTEM AND ADVANTAGES

The proposed system design Time-specified ciphertext-policy attribute-based encryption with circuits. In this technique, each and every ciphertext is labeled with different attributes and a time interval like start time and end time also provide circuits while private key is associated with a time instant. The ciphertext can only be decrypted if both the time instant is in the allowed time interval and the attributes associated with the ciphertext satisfy the key's access structure. To achieves the more security, the data is divided into multiple fragments and store on multiple nodes instead of storing on single node.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 4, April 2018

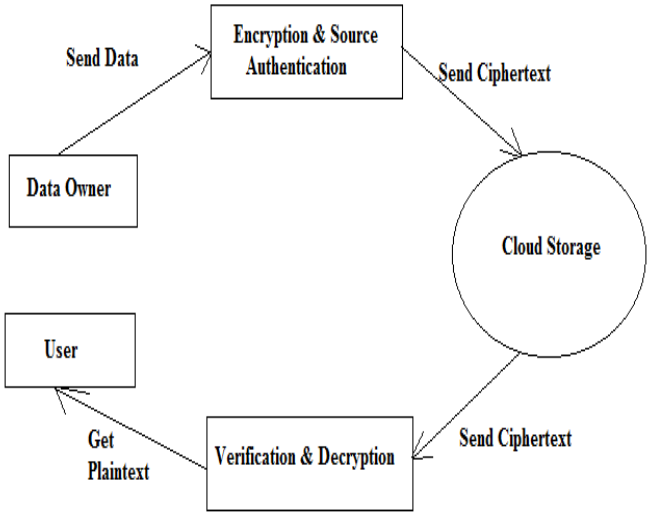


Figure: System Architecture

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 perform authentication of owner and user as well as to generate keys, for encryption and decryption.
- **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 of Proposed System:

- Achieve access control and keep data confidential.
- Reduce the computing cost.
- Achieves security by dividing the data into multiple fragments and stores on multiple nodes.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

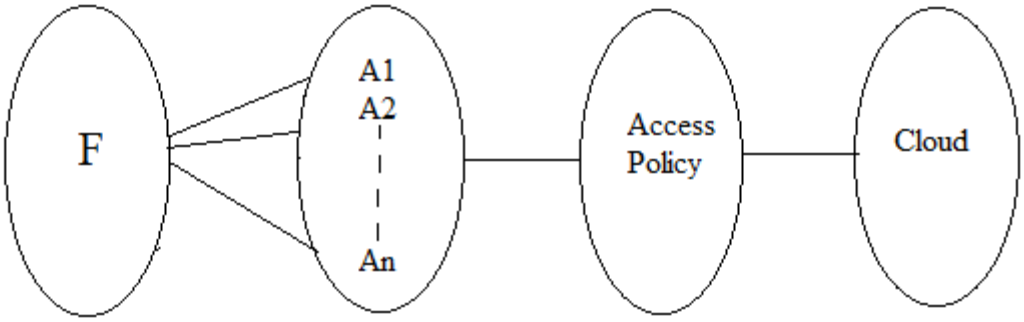
(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 4, April 2018

V. MATHEMATICLE MODEL

A] Mapping Diagram



F= File uploaded by Owner.
A1,A2,…..An= No. of Attributes set to file.
Access policy= Access policy generated by Owner
Cloud= Store file.

B] Set Theory

S = {s, e, X, Y, φ}{s, e, X, Y, t, 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.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 4, April 2018

φ = Success or failure condition of system

Failures:
1. Huge database can lead to more time consumption to get the information.
2. Hardware failure.
3. Software failure.

Success:
1. Search the required information from available in Datasets.
2. User gets result very fast according to their needs.

Above mathematical model is NP-Complete.

VI. SYSTEM PERFORMANCE

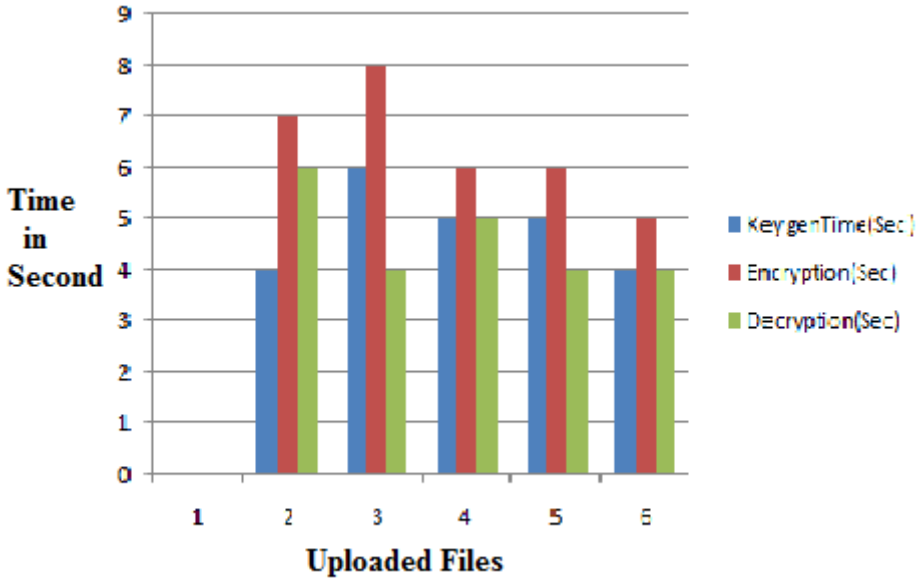


Fig. System Performance

The above result shows the Performance of our system on Uploaded Data. The X-axis contains number of file to be uploaded. Y-axis contains Time in Seconds duplicate. The above graph shows that's our system works efficiently and take minimum time to generate keys, to encrypt the file as well as to decrypt the file

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 4, April 2018

Table:

File	Key genTime(Sec)	Encryption(Sec)	Decryption(Sec)
1	4	7	6
2	6	8	4
3	5	6	5
4	5	6	4
5	4	5	4

The above table shows, the no. of files to be uploaded and how many time require to generate keys,to encrypt ,to decrypt each uploaded file.

VII. 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 delegate the outsourced data put away in the cloud severs.Time-specified ciphertext-policy attribute-based encryption with circuits. In this technique, each and every ciphertext is labeled with different attributes and a time interval like start time and end time also provide circuits while private key is associated with a time instant. The ciphertext can only be decrypted if both the time instant is in the allowed time interval and the attributes associated with the ciphertext satisfy the key's access structure. To achieve the more security, the data is divided into multiple fragments and store on multiple nodes instead of storing on single node. 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 encryption with verifiable outsourced decryption," IEEE Trans. Inf. Forensics Secur., vol. 8, no. 8, pp. 1343–1354, Aug. 2013.
[2] 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.
[3] B. Parno, M. Raykova, and V. Vaikuntanathan, "How to delegate and verify in public: Verifiable computation from attribute-based encryption," in Proc. 9th Int. Conf. Theory Cryptograph., 2012, pp. 422–439.
[4] 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.
[5] J. Han, W. Susilo, Y. Mu, and J. Yan, "Privacy-preserving decentralized key-policy attribute-based Encryption," IEEE Trans. Parallel Distrib. Syst., vol. 23, no. 11, pp. 2150–2162, Nov. 2012.
[6] 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.
[7] J. Hur and D. K. Noh, "Attribute-based access control with efficient revocation in data outsourcing systems," IEEE Trans. Parallel Distrib. Syst., vol. 22, no. 7, pp. 1214–1221, Jul. 2011.
[8] J. Li, X. Huang, J. Li, X. Chen, and Y. Xiang, "Securely outsourcing attribute-based encryption with checkability," IEEE Trans. Parallel Distrib. Syst., vol. 25, no. 8, pp. 2201–2210, Aug. 2013.
[9] 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.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 4, April 2018