A Secure Circuit CP-ABE with Time-Specified Attribute Scheme in Cloud Computing

Sapna A.Gondkar[1]

[1]*Research Scholar, Department of Computer Engineering, Vishwabharati Academy's College of Engineering, Ahmednagar, Savitribai Phule University of Pune, Maharashtra,India*

ABSTRACT

In the cloud environment, data owners could use attribute-based encryption to encrypt the stored data for accomplishing access control and data security. For the purpose of cost saving, cloud server may fraud the eligible users by responding them that they are unworthy. Since policy for general circuits are used to achieve the strongest form of access control, construction to design circuit cipher text-policy attribute-based encryption with time-specified attribute scheme has been developed. In this scheme, each cipher text is labeled with some attribute and a time interval while private key is associated with time instant. The cipher text can only be decrypted if both time instant is in allowed time interval and the attributes related with the cipher text satisfy the key's access structure. This system is varied with verifiable computation, data confidentiality, correctness of the delegated computing results are well assured at the same time with feasibility as well as efficiency.

Keyword: *Cloud computing, Ciphertext-policy attribute-based encryption, Attribute-based encryption, cloud storage, circuits.*

1. INTRODUCTION

Cloud computing is innovation which uses advanced computational power as well as improved storage capabilities. Cloud computing is a long dreamed vision of computing utility, which enable the sharing of services over the internet. Cloud is a large group of interconnected computers, which is a major change in how we store information and run application. Cloud computing is a shared pool of configurable computing resources, on-demand network access and provisioned by the service provider. The advantage of cloud is cost savings. The prime disadvantage is security. The appearance of cloud computing transports a radical novelty to the organization of the data possessions within this calculating surroundings, the cloud servers can present different data services, such as isolated data storage and outsourced allocation calculation etc. For information cargo space, the servers amass a huge quantity of communal information, which might be accessed by certified users. For allocation calculation, the servers could be accustomed to hold and determine frequent data dealing to the user's burden. As applications shift to cloud computing proposals, verifying delegation process using cipher text-policy attribute-based encryption (CP-ABE) is used to guarantee the data privacy and the verifiability of allocation on untruthful cloud servers. Captivating health check data distribution as an example among the rising volumes of health check images and health check records, the medical care associations set a big amount of data in the cloud for dropping. To make such data sharing be achievable, attribute based encryption is used.

There are two forms of attribute-based encryption. One is key-policy attribute-based encryption (KP-ABE) and the second is ciphertext-policy attribute-based encryption. In CP-ABE system, each ciphertext is contains an access structure, and each private key is labeled with a set of descriptive attributes. A user is able to decrypt a ciphertext if and only if the key's attribute set satisfies the access structure associated with a ciphertext. The cloud server provides another service which is delegation computing. The VD-CPABE scheme shows that the untrusted cloud will not be able to learn anything about the encrypted message and build the original ciphertext.

2. LITERATURE SURVEY

2.1 B. Waters (2011) have developed Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization [1]

In this work, the author presents a new methodology for realizing Ciphertext-Policy Attribute Based Encryption (CPABE) under concrete and non interactive cryptographic assumptions in the standard model.The solution of our scheme allows any encryptor to specify access control in terms of any access formula to be defined over 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 is regarded as a overview 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.

2.2 B. Parno, M. Raykova, and V. Vaikuntanathan (2012) proposed - How to Delegate and Verify in Public: Verifiable Computation from Attribute-based Encryption[2]

The author extends the definition of verifiable computation in two significant directions: public delegation and public verifiability, having essential applications in several applied delegation environments. However, existing Verifiable Computation constructions based on standard cryptographic expectations fail to accomplish these properties.

2.3 J. Lai, R. H. Deng, C. Guan, and J. Weng (2013) have proposed Attribute-based encryption with verifiable outsourced decryption [3]

The author first formalizes a security model of ABE with verifiable outsourced decryption by presenting 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 methodology is simple, general, and almost optimal. Contrasted 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 (example hash computations), nor expands the ciphertext size except adding a hash value (which is <;20 byte for 80-bit security level).

2.4 J. Hur and D. K. Noh (2011) have presented Attribute-Based Access Control with Efficient Revocation in Data Outsourcing Systems [5]

The author offers an access control mechanism using ciphertext-policy attribute-based encryption to implement access control strategies with effective attribute and user revocation ability.The fine-grained access control can be accomplished by dual encryption mechanism which takes benefit of the attribute-based encryption and selective group key delivery in every attribute set.

3. PROPOSED SYSTEM

The proposed system 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 confidentiality, the fine-grained access control as well as the correctness of the delegated computing results are well guaranteed at the same time.

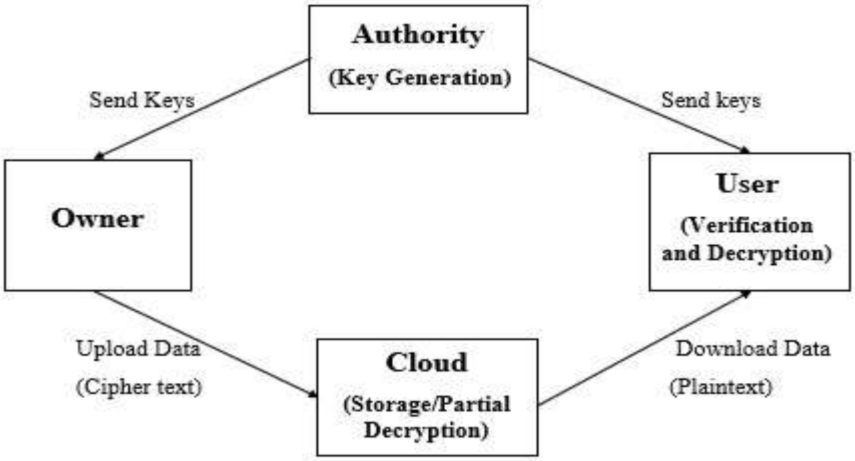

Fig -1 Proposed System Architecture

3.1 Advantages

The proposed scheme introduces low overhead on computation and communication.

- The proposed scheme is more secure and efficient, because circuit ciphertext-policy attribute-based encryption with time-specified attributes scheme is used to encrypt and decrypt the data by setting some attributes and time allocation.
- They seek to guarantee the correctness of the original ciphertext by using a commitment.
- Achieve access control and keep data confidential.
- Reduce the computing cost.
- Achieves securit**y.**

3.2 Implementation Details

- **Data Owner :**

  Information owner will need to register at first in order to access the profile. Then, information proprietor will handover the document to the cloud server in the scrambled arrangement. Arbitrary encryption key is being generated while transferring the file to the cloud. To upload the file owner should be login.

- **Authority :**

  Authorities will need to give the key, according to the client's key solicitation. Each client's solicitation must be elevated to authority to get access key via mail. There are two correlative forms of attribute based encryption. One is key policy-attribute based encryption (KP-ABE) and the other is Cipher-text-Policy Schema based Attribute Encryption (CPSBAE).If the decryption is incorrect then that account will be blocked. The blocked account will get the access only if the authority decides to give the access to the particular account.

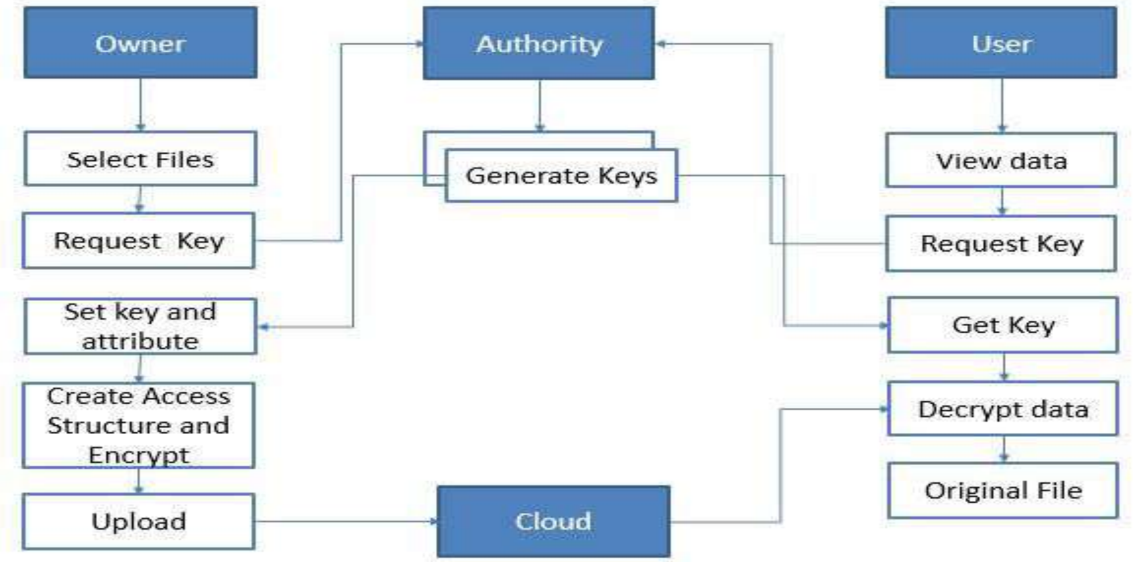

Fig -2 Flowchart

- **Data Consumer :**
  Information Consumer will at first demand the key to the authority to check and decipher the file in the cloud. Now, consumer can get access to the file with respect to key obtained from mail id. According to the key received, the consumer can check and decode the information from the cloud. To do this process the consumer should register in the cloud. To access the particular file consumer must be login.

- **Cloud Storage :**

Cloud server will have access to the file which is transferred by the data proprietor. Cloud server needs to scramble the documents available under their agreement. Furthermore, information user will need to give the particular key in order to decode the cipher text to get the original file. File will be decoded effectively and accommodated for consumer. This process is accomplished only after the cloud is login.

4. SYSTEM ANALYSIS

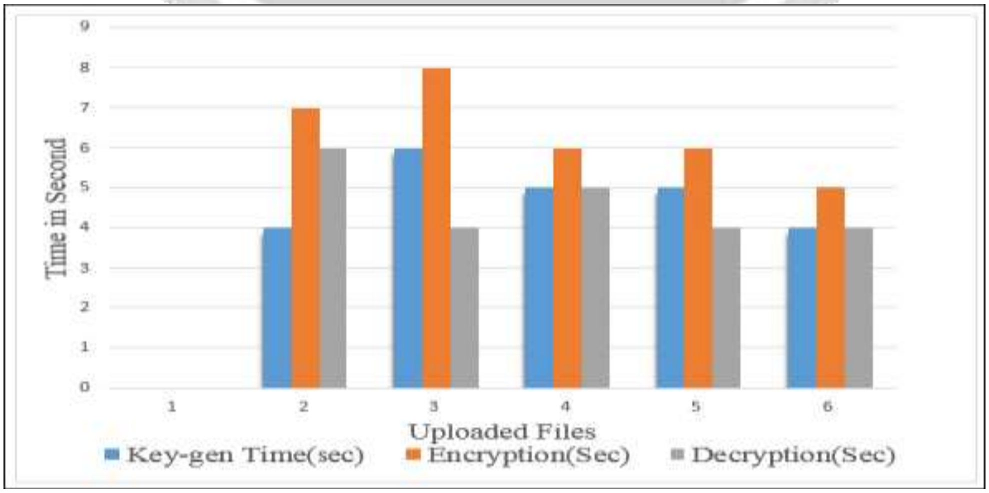

Fig -3 Performance of Proposed Scheme

The result shown in Fig.3 shows the Performance of our system on Uploaded Data. The X-axis contains number of file to be uploaded.The Y-axis contains Time in Seconds. The above graph shows thats our system works efficiently and take minimum time to generate keys, to encrypt the file as well as to decrypt the file.

4.2 Expected Results

The Table-1 given below shows, the number of files to be uploaded and the time spam required to generate keys, to encrypt and decrypt each uploaded file.

Table -1: Expected Results

Files	Key-Gen Time(sec)	Encryption(Sec)	Decryption(Sec)
1	4	7	6
2	6	8	4
3	5	6	5
4	5	6	5
5	4	5	4

5. 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. In proposed scheme, every ciphertext is labeled with some attribute and a time interval while private key is associated with a time instant. A unique property of our proposed scheme is that 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. In addition, we also presented the applicability of our method to the KP-ABE scheme. The experimental strategy demonstrates the effectiveness and efficiency of our proposed work.

6. ACKNOWLEDGEMENT

I hereby take this opportunity to thank the researchers and publishers for making their resources available and teachers for their valuable guidance. Inspiration and Guidance are invaluable in all aspects of life especially on the fields of gratitude and obligation and sympathetic attitude which I received from my respected dissertation guide, Prof. Prabhudev.S whose guidance and encouragement contributed greatly to the completion of this work.Finally,we would like to extend a heartfelt gratitude to my friends and family members.

7. REFERENCES

[1]. 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.

[2]. 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.

[3]. 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.

[4]. 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.

[5] 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. 22012210, Aug. 2013.

[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. 479499.