Design Circuit Ciphertext-Policy Attribute-Based Encryption With Time-Specified Attributes Scheme

Supriya Kute[1], Prof. S. B. Javheri[2]
[1, 2] Dept of Computer Engineering
[1, 2] Rajarshi Shahu College of Engineering, Tathawade, Pune

Abstract- *In the cloud environment, data owners may use attribute-based encryption to encrypt archived data that gain access control and data security. In previous related jobs, encryption based on delegated attributes was used. However, there are some problems and questions regarding what works. For example, during delegation or publishing, servers in the cloud may incorrectly represent or replace the delegate code text and respond to a false result with malicious intent. In addition to cost savings, the cloud server can also fool suitable users by telling them they are not worthy. Access policies may also not be flexible during cryptography. Because the general circuit policy is used to achieve the most robust form of access control, a construction has been developed to design an encryption based on attributes of cryptographic text criteria with a specified time attribute scheme. In this scheme, each owner i.e. encrypted text is labelled with attributes (i.e. Job Profile, Experience, Department) and Three different locations will be given for specific time interval. The encrypted text can only be accessible to the user if the time and any one location is within the allowed location,time interval and the attributes associated with the encrypted text satisfy the attribute set. For added security, data is split into multiple fragments and stored in different nodes instead of being stored in a single node. This system is combined with a verifiable calculation of data confidentiality, detailed access control and correction of delegates. Computer results are guaranteed at the same time.*

Keywords- Attribute set, Circuits, Cloud computing, Data confidentiality,Fragmentation,Security,Verifiable delegation.

I. INTRODUCTION

Cloud computing is the latest technology in IT infrastructure. Cloud computing provide larger storage capabilities. Uses advanced computing capabilities to learn and solve problems. Cloud computing is a long-dreamed vision of the usefulness of the computer, which allows the exchange of services on the Internet. It presently cloud computing technology is mostly used to store the large amount of data. Within this environment, the cloud servers consider different types of services, such as remote information processing and externalization delegation data processing, the Cloud server used to place a wide range of information, which is used by authorized person only. In data processing, the servers are used to manage and determine a data followed by the user's requirement.

The result shows, attribute-based encryption come out. Still, there are some problems and queries regarding the previous related works. For example, during the delivery of data or release, the cloud servers may change the text and gives a fake result. As well as for the cost saving purpose the cloud server may say that the eligible users are not authorised for accessing data. Even, the access policies are not much flexible during the conversion from plaintext to ciphertext. Since circuits are used to accomplish the secure form of access structure, where user will able to encrypt and decrypt the file or data depending on attribute set. In this scheme, every time when owner upload file it is labelled with some attribute (i.e. Job Profile, Experience, Department) and three different location will be given for specific time interval. The User can decrypt ciphertext if the time interval, any one location and the attributes matches with Owner's attribute set .All the attributes are attached to each other by using circuits i.e. AND, OR gate. This system is mixed with verifiable computation the confidentiality where only authorised user/owner can access the data, the fine-grained access control .It also gives us guarantee of the correctness of the delegated computing results. Moreover, this scheme achieves feasibility as well as efficiency. Taking Organisation data sharing as an example where Attributes are Job Profile, Department, Experience, Time, Location .If owner of the organization want to send file or information to their employee. Condition is, that file should be accessible to the user who satisfies given requirements. The requirement i.e. access structure is given as

Android developer ∨ CS ∧ 2 years ∧ 10 AM - 2 PM ∧ Tathawade ∨ Akurdi ∨ Shivaji Nagar

When the file is stored in the cloud, it must be in a secure form, or security must be provided. So, let's divide a file into fragments. Each node will only store a fragment for a single file. It provides the guarantee that even if an attacker pirates a file, no valid information will be provided to the attacker. You will get a single fragment that does not contain the appropriate information. The nodes that store each of the fragments are separated from the concept of T coloring. When using T-color, the attacker will not be able to guess the position of the other fragments.

II. OBJECTIVES

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

Main requirement of the research are given as follow:

1. Confidentiality: Only authorized user can access data and authorized owner will able to upload the data. If User’s any of attribute doesn’t match with access structure of ciphertext, plaintext will not be given to that user. It is consider as unauthorized user for accessing that specific file.
2. Verifiable Delegation: File should be properly delivered to the user. System is giving authority to third party to verify the access structure. Third party will perform his task and give it back to you. Key generation, Authentication, Matching access structure is done by Authority.
3. Circuit: In Access structure attributes are attached to each other with the help of circuits.
   AND, OR gate are used in circuit. If access structure output is true (T) than only plaintext is given to the user.
4. Authentication: Authentication provides sender identification. Confirm to the recipient that the received data was sent only by an identified and verified sender.

III. RELETED WORK

In paper [1] authors focus on cryptography and decryption based on attributes with circuits. Multiple attributes are connected to each other through the use of circuits. The circuits are designed with AND, OR port. When the owner loads a file with some attributes in a cloud, the user can download the file if and only if the attributes set meet the requirements of the owners, i.e. if the condition becomes T (True). Ensures data privacy and verifiable delegation.

In paper [2] authors present a security model of encryption and decryption with attribute set of a user in cryptographic algorithm. He proposed a system in which decryption problem of a user get solved. Thus, it presents a path to change any ABE design with the subcontracted decryption into an ABE design with testable subcontract decryption. This new idea is easier

To implement and it is more secure for storing file and it is access by identical user only. Any outsider will not able to get true information which is stored on cloud. It will not extent ciphertext size.

In paper [3] author presents a new methodology for realizing Ciphertext-Policy Attribute Encryption (CPABE) independent cryptanalysis assumptions in the classic style. The output will permit encryptor to define access information management by using any formula related to access across the attribute. The author presents three constructions. The first system is proven to be secure .Second and third constructions consider performance in order to provide more security under the decisional Bilinear-Diffie-Hellman Exponent and decisional Bilinear Diffie Hellman assumptions.

In paper [4] author extends the definition of identical data processing in two different ways: public transformation and public testing, which have important purpose in much experimental story line. Current development is depending on standard cryptanalysis. It was unsuccessful to achieve given characteristics. The major contribution is to create relation between testable computation and attribute-based encryption (ABE).

In paper [6] authors present a decentralized and conservative key privacy protection policy, in which each authority can release secret keys for a user without having any knowledge of their group ID. For this reason, even if there are several corrupt authorities, they will not be able to collect the user's attributes by tracking their GID. In particular, our mechanism requires only hypotheses of general complexity and will not consider any collaboration within the number of authorities, compared to a previous project that requires hypotheses of unusual complications and communication between the numbers of authorities.

In paper [11] the division of files is proposed, which is used to divide the file into numerous fragments. This can be used to combine the number of fragments in a single file. There is”file splitter" software, which is used to split the file into fragments.

You cannot move a large file from one end to the other using the online network. The software created will solve this problem. The split part of the file can contain variable information. It is provided to split a large file into a small bit to load the file. Eventually, the file will be re-associated and assigned as a source file.

In paper [13] authors have solved the problem of regeneration of failed authenticators in the absence of data owners. They introduce a proxy, which is used to regenerate the authenticators, in the traditional public audit system model. In addition, they design a verifiable public authenticator, which is generated with a pair of keys. Therefore, the plan can completely free data owners from online loading.

In paper [14] author presented, Division and Replicating Data for obtaining Security and improving Performance .Each of the file is divided into number of fragments than for each file replica will be created. Each fragment will be stored on different node by using T-Colouring which will provide you more security. By dividing the file into fragment it is not possible for attacker to hack any of file. In order to add more security replication of fragments is given.

IV. PROPOSED SYSTEM

The proposed system design Time-specified ciphertext-policy attribute-based encryption with circuits. In this technique, each encrypted text is labelled with different attributes and three different locations will be given for specific time interval as start time and end time while the key is associated with a moment of time. The User can decrypt ciphertext if the time interval, any one location and the attributes matches with Owner's attribute set .a time interval such. The encrypted text can only be decoded if the time, any one location is within the allowed time frame, location and the attributes associated with the user satisfy the access structure of owner. For added security, when the file is stored in the cloud, the data is split into multiple fragments and stored in multiple nodes instead of being stored in a single node.

The system contains four modules,

1. Owner: the owner is responsible for uploading the data and assigning the attribute to the data and creating the access structure.
2. Authority: the authority is responsible for the authentication of the owner and user, as well as for key generation, for encryption and decryption of data.
3. User: the user is responsible for accessing data, i.e. downloading the file.
4. Cloud Server: the server in the cloud is responsible for providing storage space and partial data decryption when the user wishes to access it.

Advantages of the proposed system:

- Reach access control and maintain data privacy.
- Reduce the cost of IT.
- Reaches security by dividing data into multiple fragments and storing them in multiple nodes.

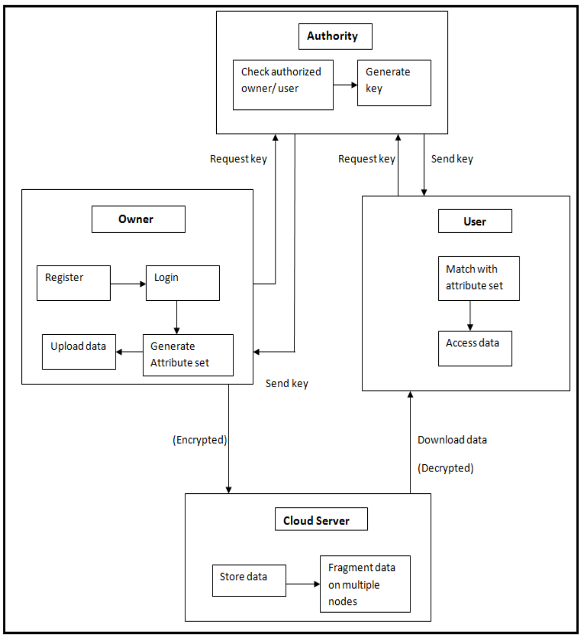

Fig 1. System Architecture

V. PROPOSED ALGORITHM

Initialization:
S^i = i-th node.
O_k = k-th fragment of file.
s_i = Size of S^i
o_k = Size of O_k

1.Fragmentation Algorithm

Input: File
Output: Chunks

```
Step 1. If file is to be split go to Step 2 else go to step 8
Step 2. Input source path, destination path
Step 3. Size = size of source file
Step 4. $F_s$ = Fragment size
Step 5. NoF = Number of Fragments
Step 6. $F_s$ = Size/NoF
Step 7. We get fragments
Step 8. End
```

2.File Fragment placement Algorithm

Input: Fragments
Output: Places on node.

```
Step 1.Calculate number of fragments(NoF).
Step 2.Calculate size of each fragment(Fs).
Step 3.col = open color; close color
Step 4.For (number of fragments)
Step 5.Use shuffle function to generate random node number.
Step 6.if col $S^i$ = open color and $s_i >= o_k$ then
Step 7.$S^i$ < - $O_k$ (Place first fragment on node.)
Step 8.col $S^i$ < - close color
Step 9.end if
Step 10.check open and close color for fragment.
Step 11.Repeat until all fragments are placed on different nodes.
Step 12. End
```

VI. CONCLUSION

Many new challenges have developed with the rapid advancement of adaptive services in the cloud. One of the most critical issues is how to securely delegate the outsourced data stored on cloud servers. In attribute-based cryptography of time-encrypted text-based criteria with circuit technique, each of the encrypted texts is labelled with some attribute (i.e. Job Profile, Experience, Department) and three different location will be given for specific time interval. The encrypted text can only be decoded if the time, any one location is within the allowed time interval, location and the attributes associated with the user satisfy the access structure (Attributes) of the owner. To achieve greater security, data is split into multiple fragments and stored in different nodes rather than being stored in a single node. The conclusion shows that the method is reasonable in cloud computing. Therefore, can be able to achieve data privacy, advanced management and demonstrable cloud assignment.

REFERENCES

[1] Jie Xu, Qiaoyan Wen, Wenmin Li, and Zhengping Jin, “Circuit Ciphertext - Policy Attribute-Based Hybrid Encryption with Verifiable Delegation in Cloud Computing,” IEEE transactions on parallel and distributed systems, vol. 27, no. 1, January 2016

[2] 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.

[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-based encryption,” 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. Parallel Distrib. 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. Parallel Distrib. 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. Parallel Distrib. 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.

[11] Shristi Sharma, ShreyaJaiswal, Priyanka Sharma, Prof. Deepshikha Patel, Prof. Sweta Gupta, “An Approach for File Splitting and Merging” Lecturer, Department of IT Technocrats Institute of Technology, Bhopal.

[12] Quanlu Zhang, Shenglong Li, Zhenhua Li, Yuanjian Xing, Zhi Yang, and Yafei Dai, “CHARM: A Cost-efficient Multi-cloud Data Hosting Scheme with High Availability”. IEEE Transactions on Cloud Computing, Volume: 3March2015.

[13] Jian Liu, Kun Huang, Hong Rong, Huimei Wang, and Ming Xian, “Privacy-Preserving Public Auditing for Regenerating-Code-Based Cloud Storage”. IEEE Transactions on Information Forensics and Security, Volume: 10, Issue: 7, July 2015.

[14] Mazhar Ali, Student Member, IEEE, Kashif Bilal, DROPS: Division and Replication of Data in Cloud for Optimal Performance and Security, IEEE Trans. Inf. ForensicsSecur., vol. 8, no. 8, pp. 13431354, Aug.