

# Two Layer Encryption for Preserving Privacy on Public Cloud

Mayur Parma  
M.E. 2<sup>nd</sup> Year Student DYPCOE,  
Ambi

Saurabh Deshmukh, PhD  
Dean Academic R&D DYPCOE,  
Ambi

## ABSTRACT

To preserve privacy and secure access control in Public cloud use of two layer encryption algorithms provides better result, but use of the secure hypertext transfer protocol and single sign on approach will increase the efficiency regarding security. It will help owner to improve communication and computation cost as the fine grain access control performed on cloud side and improves security. As an old approach has all the responsibilities of data owner to encrypt data and re-encrypt updated or modified data it incur a high computation cost. As Public cloud is third party so data owner are not able to trust on cloud for security purpose so fine grain access cannot get delegate to cloud side. To overcome this problem and increase security use of two layer encryption algorithms and secure Sockets Layer (SSL) along with Single sign on approach will provide better results.

## Keywords

Identity, Privacy, SSL, policy decomposition, Encryption, Cloud computing, Access control, Blowfish.

## 1. INTRODUCTION

On-demand computing is another name of Cloud computing, it provides on-demand all shared resources, data and information to computers and other devices. It is a model for on-demand, enabling ubiquitous access to a shared pool of configurable computing resources. Users and enterprises get various capabilities to store and process their data in third-party data centers by use of Cloud computing and storage solutions provide in cloud. It will help to achieve coherence and economies of scale, similar to a utility over a network by sharing of resources. Due to the advantages of high computing power, high performance, scalability, accessibility as well as availability the Cloud computing has high demand in service or utility.

Today world are totally depends on internet, to operate internet we required to store data that will get modified or operated so more space required and mostly all data should available in dynamic ways that's need full field by cloud computing. To operate all data dynamically there is need to store and as per modification there should be need to make necessary changes on data all changes on data made mostly by data owner and also to increase security there is a need to encrypt and decrypt data that way we preserve privacy in cloud. Old approach however has many limitations. As the data owner does not have a copy of the data, whenever the user data or Access Control Policies (ACPs) change, the data owner has to download and decrypt the data and again re-encrypt it with the new keys, and upload the encrypted data. This process has to be applied to all the data encrypted with the same key. It will not work when the data to be re-encrypted is large. In order to give the new keys to the users, it is necessary for the data owner to communicate privately by making private communication channels with the users. In

which privacy of the identity attributes of the users is not taken into account. So that cloud can learn sensitive information about the users and their organization [2].

Now to preserve privacy in cloud again one task comes who will handle fine-grain access control that will know as delegation of access control. We have two options who will able to handle fine grain access control that is data owner side or cloud side. Two cases for fine-grain access control again comes to discussion that if cloud handle all the task of delegation of access control then there is a possibility of information exposure risk due to the colluding users and cloud, to discuss second case if data owner handle fine-grain access control then it will incur high computation and communication cost. In previous approach data owner are in charge of encrypting the data. To overcome this task from data owner Mohamed Nabeel and Elisa Bertino proposed two layer encryption algorithms for preserving privacy on public cloud [3].

That will overcome task of data owner and solve the problem that if cloud perform fine-grain access control then there is a possibility of information exposure risk due to the colluding users and cloud. In this approach Mohamed Nabeel and Elisa Bertino develop a technique such that cloud performs fine-grain access on data but there is no information exposure risk due to the colluding users and cloud. The two layer encryption approach has some advantages. During the policy or user dynamics changes, there is only the outer layer of the encryption needs to be updated. When the outer layer encryption done at the cloud, no data transmission is required from the data owner and to the cloud. In which both the cloud service and data owner utilize a broadcast key management scheme so the actual keys do not need to be distributed to the users. Behalf of it, users are given one or more secrets which allow them to derive the actual symmetric keys for decrypting the data. This two layer enforcement allows reducing the load on the Owner and delegates as much access control enforcement duties as possible to the Cloud side. So, it provides a better way to handle data updates, user dynamics, and policy changes. [4].

The rest of the paper is organized as follows. Section II gives an overview of related works. In Section III, complete description of the existing system. Section IV future work that plan to implement. Concluding remarks of our research are made in Section V.

## 2. LITERATURE REVIEW

Here we go through various paper related to work explain above firstly Mohamed Nabeel, Ning Shang and Elisa Bertino introduced a concept of two layer encryption algorithm. They overcome the problem that data owners are in charge of encrypting the data so they will perform fine grain access control on data that will enforces high computation and communication cost to owner. In their approach cloud

performs fine grain access control so it will reduce owner's task of computation. In which fine grain access control performs on cloud side so to perform these task ACP decomposition plays an important role. To communicate with user and cloud there is novel algorithm used as Attribute Based Group Key Management ABGKM algorithm. Which helps to overcome problems occur during symmetric key distribution in encryption and decryption process [1]?

Encryption in group data item performs by using different symmetric key for each group. In such situation users are given the keys for the data items they are allowed to access. To overcome these drawbacks that is to reduce the number of keys distributed users have been proposed exploiting hierarchical and other relationships among data items. Nabeel, Ning Shang and Elisa Bertino proposed new algorithm. This paper explains two layers of encryption on each data uploaded to the cloud. Such as, the data owner performs a coarse grained encryption over the data in order to protect the confidentiality of the data from the cloud. The cloud then performs fine grained encryption over the encrypted data provided by the data owner based on the ABAC policies provided by the data owner. In which if policy or user dynamics changes then only the outer layer of the encryption needs to be updated [2].

For Broadcast Group Key Management (BGKM) and proved the security to BGKM scheme, there is ACV-BGKM scheme. Again it proposed optimizations to significantly improve the performance of the ACV-BGKM scheme. Based on BGKM scheme, it proposed an approach to support attribute-based access control while preserving privacy of user's identity attributes for sharing documents in public cloud storage service. Their approach is supported by a new group key management scheme which is secure and allows qualified users to efficiently extract decryption keys for the portions of documents they are allowed to access, based on the entered information they have received from the data owner[3].

AB-GKM schemes which are develop by improving shortcomings over ABE that is Attribute Based Encryption. AB-GKM supports a large set of conditions over a set of attributes. When any change occurs in the group, the rekeying operations do not affect the information of existing group members and thus there is no need of establishing expensive private communication channels. It also provides the similar advantage when the group membership conditions change. As the group key function is very efficient as it only requires a simple vector inner product and/or polynomial interpolation. This scheme also avoid resistant to collusion attacks. There is no possibility for multiple group members to combine their private information in a useful way to derive a group key which they cannot derive individually. It will develop good algorithm for broad cast group key management that will improve communication security over cloud [6].

Lastly OACerts, an attribute certificate scheme that enables oblivious access control. It develop the notion of OCBE and provably secure and efficient OCBE protocols for the Pedersen commitment scheme and predicates such as  $=, \neq, \leq, \geq, <, >$ , as well as conjunctions and disjunctions of multiple predicates. It explain how user obtains a service only if the attribute values satisfy the policy of the service provider, without knowing the service provider learns anything about these attribute values [5].

### 3. EXISTING SYSTEM

The system represents several encryption based access control policies over the data with encrypted group of different symmetric key controls. Single layer encryption algorithm preserve user privacy but it has some drawbacks such as

- 1) Data owner download and decrypt the data and re-encrypt with the new keys and upload the encrypted data whenever the user data changes. As the data owner does not keep copy of data. If data item have large set then it is not possible.
- 2) There is need of new keys to the users then data owner needs to establish private communication channels with the users.
- 3) The user's privacy does not taken into account.
- 4) As the data owner are in charge of fine grain access control, data owner have to enforce all the ACPs initially and subsequently after users are modify or revoked or change. So the owner incurs high communication and computation cost [3].

Two layer encryption overcome drawbacks of SLE as Idp Fine grained attribute based access control of data with double encryption can be achieved simply by encrypting each of the subset of the data that confirms to the same set of policies with the symmetric key [3].

- Identity token selection
- Identity token uploading
- Data encryption and uploading
- Data downloading and decryption
- Encryption process management

#### Identity token selection

Identity Provider (IdPs) use to identity tokens to Users based on their identity attributes. IdP are trusted third parties. After issuing identity token IdPs need not to be online.

#### Identity token uploading

Users upload their token to obtain information (secrets) in order to later decrypt the data they are allowed to access. As per the attribute conditions users register their information (Tokens) related to the condition with the Owner, and the rest of the identity information (tokens) related to the attribute conditions as per the Cloud. When Users register with the Owner, the Owner get them two set of secrets for the attribute conditions in owner's way that are also present in the sub ACPs in Cloud information on cloud side ACPs. The Owner keeps one set and gives the other set to the Cloud. Two different sets are used in order to prevent the Cloud from decrypting the Owner encrypted data.

This scheme consists of mainly four entities that are Data Owner, User, Cloud and the Identity Provider.

- Defining ACP by Owner and uploads encrypted documents to the cloud.
- Cloud holds the encrypted data that are encrypted by owner and public information indexed to the policy configurations.
- IdP is third party in cloud which issues identity tokens to the users based on the identity Attributes confirmed by the user. This has been done based on a commitment scheme such as Pedersen commitment.

**Data encryption and uploading**

Based on the Owner’s sub ACPs that are the Owner encrypted data in order to keep it secret content from the Cloud and uploads them along with the public

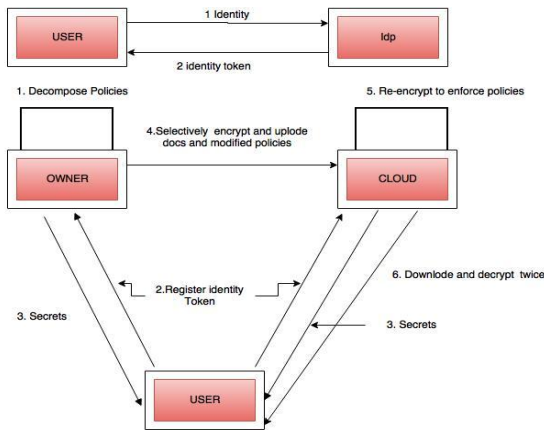
information generated by the algorithm such as AB-GKM for key generation algorithm and the other sub ACPs to the Cloud. After that the Cloud encrypts the data by considering the keys generated using its own AB-GKM key [4] generation algorithm. In which AB-GKM Key generation at Cloud generate keys by taking secrets issued to Users and the sub ACPs given by the Owner into consideration

**Data downloading and Decryption**

To access the data users download encrypted data from the Cloud and decrypt twice. Outer layer key will be generated first by using public information tuple then the owner generated public information tuple is used to derive the inner layer key by the use of the AB-GKM KeyDer algorithm. If the User satisfies the original ACP applied to the data item by using these two keys user allow to decrypt a data item.

**Encryption process Management**

Over time, either encrypted data may go through frequent updates or ACPs changes or user credentials may change. In such conditions, data already encrypted must be encrypted again with a new key. As the cloud performs the access control enforcing encryption, it only re-encrypts the affected data without the intervention of the Owner.



**Fig 1 : Two Layer Encryption**

**4. PROPOSED SYSTEM**

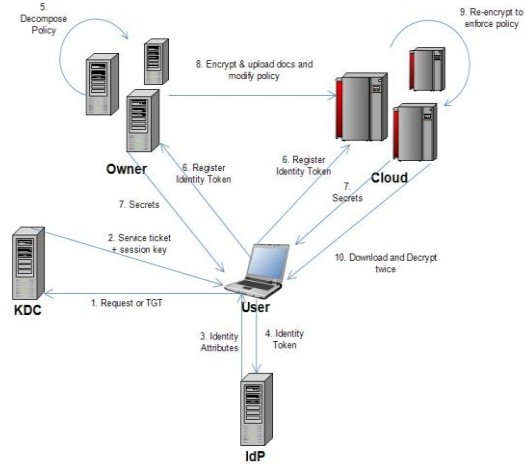
We plan to execute two layer encryption algorithms by applying two approaches that is Secure Socket Layer (SSL) and single sign on approach. It will increase security and assurance to data integrity. It will also helpful to user regarding convenience re-login and improve security parameter by applying secure socket layer. In this we are using Kerberos protocol for authenticating users by their login credentials

Kerberos is one of the types of Single Sign-On (SSO) protocol to provide Ticket passing and validation of user login. Kerberos will validate the user login, if user is authenticated it will generate the login ticket available for some instance of time and send tickets to application and user browser, then user login will be done by forwarding user authentication ticket to application and signature checking of that ticket.

To develop Kerberos Protocol we can use SHA-1 to generate and verify user login ticket.

OpenSSL security layer will be provided by https protocol, so we are configuring our application on https protocol by using https dummy java certificate and tomcat server.

In which we add blowfish algorithm for better result of encryption and decryption



**Fig 2 : Two Layer Encryption with Single Sign on approach**

**5. EXPERIMENTAL RESULT**

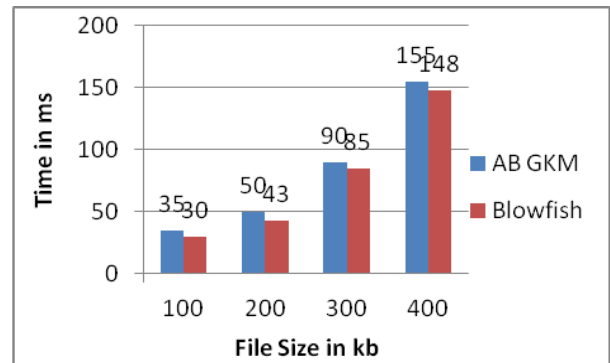
The result of Blowfish have a better performance over AB GKM shows poor performance result compared to blowfish algorithm since it required more processing power and for blowfish no attack is known to be successful against it.

**Table 1 : Encryption Time of two algorithms in seconds**

| File Size | AB GKM | Blowfish |
|-----------|--------|----------|
| 1 MB      | 5.234  | 0.283    |
| 5 MB      | 7.52   | 0.954    |
| 10 MB     | 11.167 | 1.683    |
| 50 MB     | 21.964 | 10.233   |
| 100 MB    | 23.319 | 14.823   |

**Table 2: Decryption Time of two algorithms in seconds**

| File Size | AB GKM | Blowfish |
|-----------|--------|----------|
| 1 MB      | 2.629  | 0.634    |
| 5 MB      | 6.157  | 1.71     |
| 10 MB     | 9.043  | 4.581    |
| 50 MB     | 31.00  | 22.076   |
| 100 MB    | 37.561 | 25.965   |



**Graph 1 : Comparison between AB GKM and Blowfish**

**Table 3 : Comparison between AB GKM and Blowfish**

| File Size Kb | AB GKM | Blowfish |
|--------------|--------|----------|
| 100          | 35     | 30       |
| 200          | 50     | 43       |
| 300          | 90     | 85       |
| 400          | 155    | 148      |

## 6. CONCLUSION

In this system a two layer encryption based approach to solve data owner side encryption problem by delegating as much of the access control enforcement task as possible to the Cloud while minimizing the information exposure risks due to colluding Users and Cloud. This system will reduce the time of performance by using blowfish algorithm. Applying SSL and single sign on approach improve security.

## 7. REFERENCES

- [1] M. Nabeel and E. Bertino, "Privacy Preserving Delegated Access Control in the Storage as a Service Model," Proc. IEEE Int'l Conf. Information Reuse and Integration (IRI), 2012.
- [2] N. Shang, M. Nabeel, F. Paci, and E. Bertino, "A Privacy-Preserving Approach to Policy-Based Content Dissemination," Proc. IEEE 26th Int'l Conf. Data Eng. (ICDE '10), 2010.
- [3] M. Nabeel, N. Shang, and E. Bertino, "Privacy Preserving Policy Based Content Sharing in Public Clouds," IEEE Trans. Knowledge and Data Eng., vol. 25, no. 11, pp. 2602-2614, Nov. 2013
- [4] M. Nabeel and E. Bertino, "Towards Attribute Based Group Key Management," Proc. 18th ACM Conf. Computer and Comm. Security, 2011.
- [5] J. Li and N. Li, "OACerts: Oblivious Attribute Certificates," IEEE Trans. Dependable and Secure Computing, vol. 3, no. 4, pp. 340-352, Oct.-Dec. 2006
- [6] M. Nabeel and E. Bertino, "Attribute Based Group Key Management," to appear in Trans. Data Privacy, 2014.
- [7] A. Shamir, "How to Share a Secret," Comm. ACM, vol. 22, pp. 612-613, Nov. 1979.
- [8] Mohamed Nabeel and Elisa Bertino, Fellow, IEEE "Privacy Preserving Delegated Access Control in Public Clouds", IEEE Transactions on Knowledge and Data Engineering, Vol. 26, No. 9, September 2014.
- [9] S. D. C. di Vimercati, S. Foresti, S. Jajodia, S. Paraboschi, and P. Samarati, "Over -encryption: Management of access control evolution on outsourced data," in Proceedings of the 33rd International Conference on Very Large Data Bases , VLDB Endowment, pp. 123–134, 2007
- [10] Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute -based encryption for fine-grained access control of encrypted data," Proceedings of the 13th ACM conference on Computer and communications security. New York, NY, USA: ACM, pp. 89–98, 2006.
- [11] A .Reddy, GudivadaLokesh and N. Vikram "Privacy Preserving Delegated Access Control in Public.