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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

Encryption Technique as Two Layer Encryption for Preserving Privacy on Public Cloud

Mayur Parma

M.E Student, Dept. of Computer Science, DYPCOE, Ambi, Maharashtra, India

ABSTRACT: To preserve privacy and secure access control in Public cloud use of two layer encryption algorithms provides better result but use of 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 old approach has all the responsibilities on data owner to encrypt data and re-encrypt updated or modified data it incur 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 result

KEYWORDS: Privacy, identity, SSL, cloud computing, policy decomposition, encryption, and access control.

I. INTRODUCTION

On-demand computing is another name of Cloud computing, is 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, cheap cost of services, 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 several limitations. As the data owner does not have a copy of the data, whenever the user dynamics or Access Control Policies (ACPs) change, the data owner needs to download and decrypt the data, again re-encrypt it with the new keys, and upload the encrypted data. Notice also that this process must be applied to all the data encrypted with the same key. But this is not possible when the data set to be re-encrypted is large. In order to give the new keys to the users, the data owner needs 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. Therefore the cloud can learn sensitive information about the 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].

DOI: 10.15680/IJIRCCE.2016. 0406374

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 TLE approach has many advantages. When the policy or user dynamics changes, there is only the outer layer of the encryption needs to be updated. As the outer layer encryption is performed at the cloud, no data transmission is required between the data owner and the cloud. Further, 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. Instead, 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 one to reduce the load on the Owner and delegates as much access control enforcement duties as possible to the Cloud. Specifically, it provides a better way to handle data updates, user dynamics, and policychanges. The system goes through one additional phase compared to existing approach [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.

II. RELATED WORK

The existing 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) Whenever the user dynamics change the owner download and decrypt the data and re-encrypt the new keys and upload the encrypted data. As the data owner does notKeep 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 identity attributes of the users is not taken into account. So that cloud can learn information about the users and organizations.

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 incur high communication and computation cost [8][9].

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 issuance
- Identity token registration
- Data encryption and uploading
- Data downloading and decryption
- Encryption evolution management

Identity token issuance
Identity Provider (IdPs) provide 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 registration
Users register their token to obtain secrets in order to later decrypt the data they are allowed to access. Users register their tokens related to the attribute conditions in ACC with the Owner, and the rest of the identity tokens related to the

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

attribute conditions in ACB/ACC with the Cloud. When Users register with the Owner, the Owner issues them two set of secrets for the attribute conditions in ACC that are also present in the sub ACPs in ACPB Cloud. 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 Data Owner, User, Cloud and the Identity Provider (IdP):

- Owner defines the access control policies (ACP) and uploads encrypted documents to the cloud.
- Cloud holds the encrypted data of the owner, public information indexed to the policy configurations.
- IdP is a trusted third party in cloud that 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

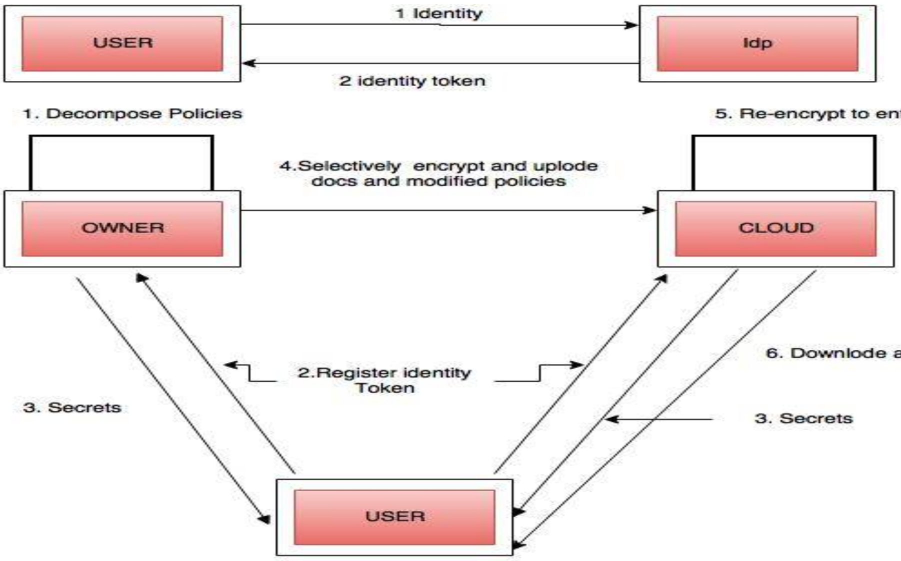
The Owner encrypts the data based on the Owner's sub ACPs in order to hide the content from the Cloud and then uploads them along with the public information generated by the AB-GKM for key generation algorithm and the remaining sub ACPs to the Cloud. After that the Cloud encrypts the data based on the keys generated using its own AB-GKM key [4] generation algorithm. In which AB-GKM Key generation at the Cloud takes the secrets issued to Users and the sub ACPs given by the Owner into consideration to generate keys[9].

Data downloading and Decryption

To access the data Users download encrypted data from the Cloud and decrypt twice. OLE key will be generated first by using public information tuple then the Owner generated public information tuple is used to derive the ILE key using 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[10][11].

Encryption Evolution 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 re-encrypted with a new key. As the Cloud performs the access control enforcing encryption, it simply re-encrypts the affected data without the intervention of the Owner.


USER
1 Identity
Idp
2 identity token
1. Decompose Policies
5. Re-encrypt to enforce policies
4.Selectively encrypt and uplode
docs and modified policies
OWNER
CLOUD
6. Downlode and decrypt twice
2.Register identity
Token
3. Secrets
3. Secrets
USER

DOI: 10.15680/IJIRCCE.2016. 0406374

III. PROPOSED ALGORITHM

1. 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[11].

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

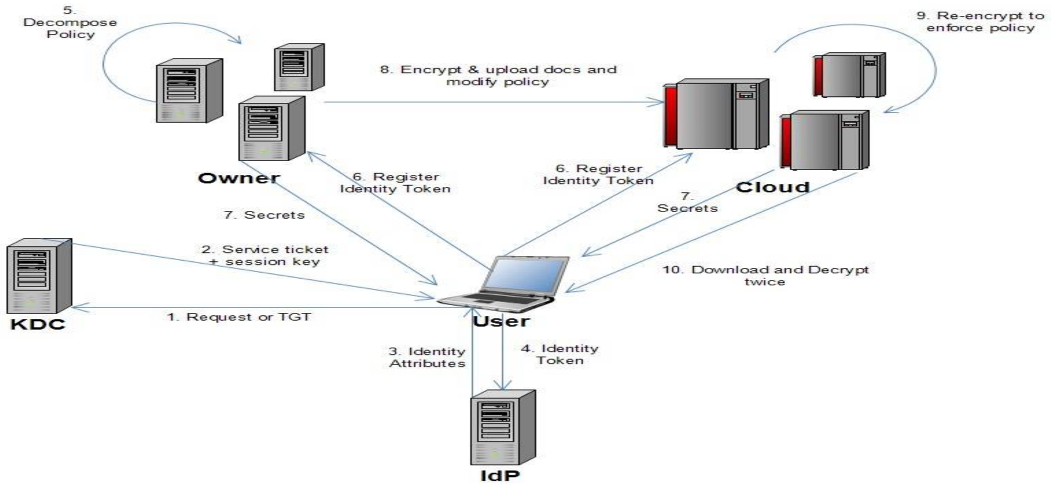

5. Decompose Policy
8. Encrypt & upload docs and modify policy
9. Re-encrypt to enforce policy
Owner
6. Register Identity Token
6. Register Identity Token
Cloud
7. Secrets
7. Secrets
2. Service ticket + session key
KDC
1. Request or TGT
User
10. Download and Decrypt twice
3. Identity Attributes
4. Identity Token
IdP

Fig 2 : Two Layer Encryption with Single Sign on approach

1. EXPREIMENTAL RESULT

The results of blowfish have a better performance than AB-GKM algorithms. AB-GKM showed poor performance results compared to blowfish algorithm since it requires more processing power and for blowfish no attack is known to be successful against it.

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 1 : Encryption Time of two algorithms in seconds

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

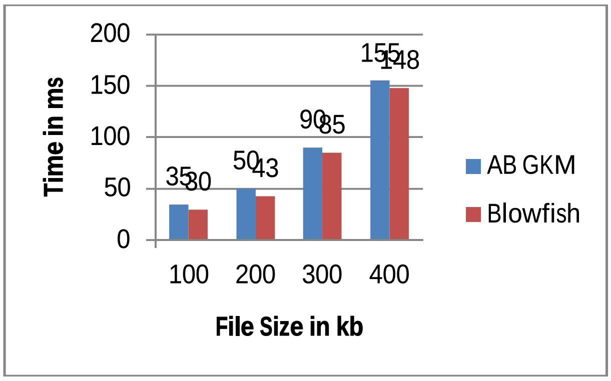
International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

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

Table 2 :Decryption Time of two algorithms in seconds



Graph 1 : Comparison between AB GKM and Blowfish

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

Table 3 : Comparison between AB GKM and Blowfish

IV. 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 responsibilities as possible to the Cloud while minimizing the information exposure risks due to colluding Users and Cloud it will guide towards performing two layer encryption algorithm and help to plan for applying SSL and single sign on approach.

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 the33rd 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 Computerand 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