ISSN No. 0976-5697

Volume 6, No. 6, June - July 2015

International Journal of Advanced Research in Computer Science

REVIEW ARTICLE

Available Online at www.ijarcs.info

A Survey on Privacy Preserving and Access Control in Public Clouds

Radhika Makadia
Student, Department Of Information Science
R.V. College of Engineering, Bangalore, India.

Abhilash Kumar Patra
Student, Department Of Information Science
R.V. College of Engineering, Bangalore, India.

Rashmi R
Assistant professor, Department Of Information Science
R.V. Collage of Engineering, Bangalore, India.

Abstract: With the advent of cloud computing, sharing data through any cloud service provider has never been more economical and easier than now. It offers improved processing and storage resources as on-demand services with reduce cost, and increase efficiency, performance and reliability. All of these features and more encourage enterprises, governments and others to migrate to the cloud. However, such cloud providers more vulnerable to threats. Hence, data privacy and security issues have been major concerns for many organizations utilizing such services. The target of this survey is to explore various mechanisms like Encryption, Authentication, Key management used on clouds; that provide security, scalability and flexibility access control over public clouds.

Keywords: Privacy; Security; Cloud Computing; Encryption; Access Control;

I .INTRODUCTION

Cloud computing has been considered as one of the promising solutions to our increasing demand for accessing and using resources provisioned over the Internet. The increased use of cloud computing services such as Gmail and Google Docs has pressed the issue of privacy concerns of cloud computing services to the utmost importance. Data often contains sensitive information and should be protected as mandated by various organizational policies and legal regulations. In this era, even sensitive data is stored and shared on the internet using trusted service providers.

Today for many organizations they need to store their enormous amount of data. Network storage providers are giving the resources for these organizations on demand. The National Institute of Standards and Technology (NIST) defines the cloud computing as "*A model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal Management effort or service provider interaction*" [1].Cloud Computing aiming at giving capabilities to use powerful computing systems with reducing the

Cost and increasing the efficiency and performance [1].

However, with all of these promising facilities and benefits, there are still a number of technical barriers that are preventing Cloud Computing services. The latest cyber-attacks on high profile firms (Amazon, Google and Sony's PlayStation) and the predictions of more cyber-attack on cloud infrastructure are threatening to slow the take-off of cloud computing [2, 3, 9].

The numbers of cyber-attacks are now extremely large and their threats are so problematic, that many organizations are having trouble determining threats and vulnerabilities .And confused how to pose the greatest risk and how resources should be allocated to ensure that the most probable and damaging attacks are dealt first. These security concerns and attacks should be taken care, as the growth of the global market of cloud services could reach $270 billion by 2020 [3, 12, 15].

Currently many companies are using Access based or Cipher text based encryptions And Attribute or policy based encryptions etc; yet no mechanism is perfect. Our objective is to look at the cloud computing security challenges with all available schemas, which hinder migration to the requirements for a better, secure utilize the cloud.

II. LITERATURE SURVEY

A. Attribute-based Encryption Scheme

Many times in cloud computing, Users need to share sensitive objects with others based on the recipients' ability to satisfy a policy in distributed systems. One of the encryption schemes is Attribute Based Encryption (ABE) which is a new paradigm where such policies are specified and cryptographically enforced in the encryption algorithm itself [4,13,18].

In this scheme, the authority generates keys according to attributes; and these attributes of public key(*pk*) and master key(*mk*), which are generated by the authority, should predefine (means that it will list attributes which will be used in the future). If any data user who wants to add to this system, and he owns to attributes don't include predefined attributes. The authority will redefine attributes and generate a public key and master key again. And data owner's role in this scheme is to encrypt data with a public key and a set of descriptive attributes. A data user's role is to decrypt encrypted data with his private key sent from the authority, and then he can obtain the needed data. For decrypting data, attributes in data user's private key will check by matching with the attributes in encrypted data. If the number of "matching" is at least a threshold valued, the data user's private key will be permitted to decrypt the encrypted data. The attributes in user's private key and the encrypted data can let this scheme achieve access control. The authorized users can use their private key to decrypt the corresponding data. The whole mechanism can be called as Single Layered Encryption (SLE) [fig 1] [5].

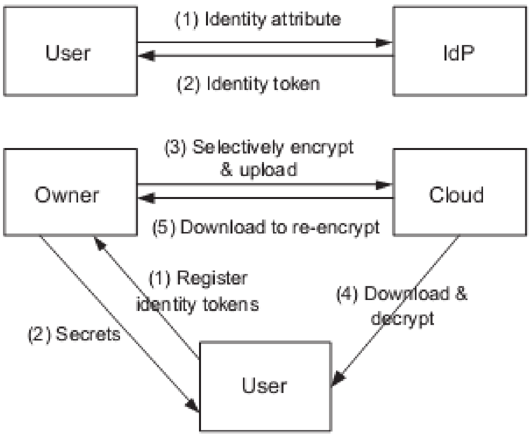

Fig 1: Single Layer Encryption approach

Pseudo code 1: (Generation of key “owner & Cloud side”)

```
i.   Program initialize
        Initialize attribute “l”
ii.  Generation of key “k” using “l”
iii. Generation of pk & mk using “k”
iv.  User assigned with key “k”
v.   Start “Encryption” using pk & mk
```

Pseudo code 2: (User access)

```
i.  User sends key “k” to owner
ii. Matching the key “k” using “pk”
       If yes
            Do “Decryption”
       Else
            “Access denied”
```

Drawback:

The SLE approach supports fine-grained attribute-based access control policies and preserves the privacy of users from the Cloud. But, here the Owner is in charge of encrypting the data before uploading it to the third-party server as well as re-encrypting the data whenever user credentials or authorization policies change and managing the encryption keys. The Owner has to download all affected data before performing the selective encryption. The Owner thus has to bear more communication and computation costs, which then negate the benefits of using a third party service.

A.1. Enhanced Attribute Based Encryption Scheme

A better approach should delegate the enforcement of fine-grained access control to the Cloud. Under such approach, referred to as two-layer encryption (TLE) [5][fig 2], the Owner performs a coarse grained encryption, whereas the Cloud performs a fine grained encryption on top of the data encrypted by the coarse grained encryption. The two-layer encryption should be performed such that the Owner first encrypts the data based on one set of sub policies and the Cloud re-encrypt the encrypted data using the other set of policies. The two encryptions together enforce the original policies as users should perform two decryptions in order to access the data.

For example, consider the policy (P1 ∧ P2) ∨ (P1 ∧ P3). This policy can be decomposed as two sub policies P1 and P2 ∨ P3.Notice that the decomposition is consistent; that is, (P1 ∧ P2) ∨ (P1 ∧ P3) = P1 ∧ (P2 ∨ P3).The Owner enforces the former by encrypting the data for the users satisfying the former and the Cloud enforces the latter by re-encrypting the Owner encrypted data for the users satisfying the latter. Since the Cloud does not handle P1, it cannot decrypt the Owner encrypted data and thus confidentiality is preserved. Checking users, those would satisfy the original policy to access the data by performing two decryptions. An analysis of this approach suggests that the problem of decomposing for coarse and fine grained encryption while assuring the confidentiality of data from the third party and the two encryptions together enforcing the policies is not complete. We have thus investigated optimization algorithms to construct near optimal solutions to this problem.

Pseudo code 3: (Generation of key “owner & Cloud side”)

```
i.   Program initialize
        Initialize attribute “l”
ii.  Generation of key “k” using “l”
iii. Assign key to User
iv.  Encrypting key “k”
v.   Generation of “pk” & “mk” using policy information
        PI
vi.  Encryption of data using “pk” & “mk”
```

Pseudo code 4: (User access)

```
i.  User sends key “k” to owner
ii. Matching the key “k” using “pk”
If yes
      Do “Decryption”
Else
      “Access denied”
```

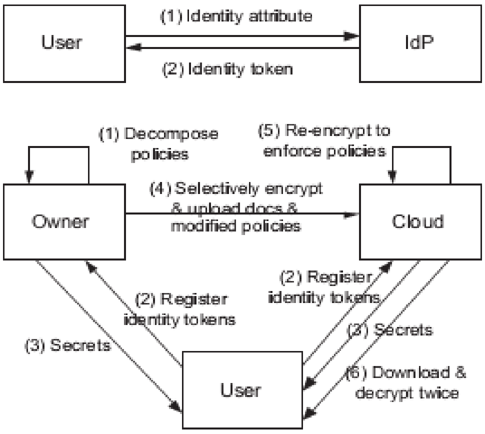
User
IdP
(1) Identity attribute
(2) Identity token
(1) Decompose policies
(5) Re-encrypt to enforce policies
Owner
Cloud
(4) Selectively encrypt & upload docs & modified policies
(2) Register identity tokens
(3) Secrets
(2) Register identity tokens
(3) Secrets
(6) Download & decrypt twice
User

Fig 2: Two Layer Encryption approach

Drawback:

Even providing so much of privacy and access control its computational overhead is high. Maintenance of the whole mechanism is costly.

B. Expressive Key Policy Attribute Based Encryption

Among the encryption methods in clouds Attribute-based encryption (ABE), allows fine grained access control on encrypted data. Here in key-policy Attribute based encryption, the primitive enables senders to encrypt messages with a set of attributes and private keys are associated with access tree structure that specifies which all the cipher texts the key holder is allowed to decrypt. Many of the ABE systems, the cipher text size grows linearly with the number of cipher text attributes and the only known exceptions only support restricted forms of threshold access policies. Introducing the expressive key-policy attribute-based encryption (KP-ABE) schemes allowing for non-monotonic access structures (i.e., that may contain negated attributes) and with constant cipher text size. Towards achieving this goal, show that a certain class of identity-based broadcast encryption schemes generically yields monotonic KP-ABE systems in the selective set model [19,20].

A new efficient identity-based revocation mechanism, when combined with a particular instantiation of mentioned general monotonic construction, gives rise to the first truly expressive KP-ABE stable size cipher texts. Also they reduce the number of pairing evaluations to a constant, which appears to be a unique feature among expressive KP-ABE schemes [6].

Pseudo code 5:

```
  i.    Taking input security
  ii.   Take input message “M”, “pk”, “l”
  iii.  Start encryption using credentials
  iv.   Generate “sk”

  Decryption:
    i.  Take input “sk” and compare
    ii. If yes
          “Do decryption”
        No  “Exit”
```

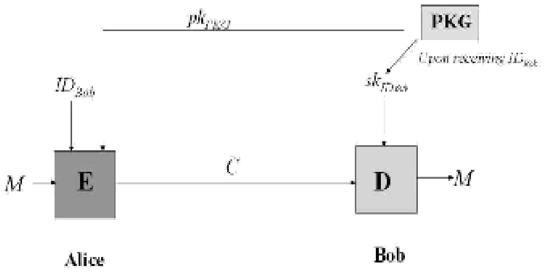

Fig 3: Key-Policy Attribute Based Encryption

C. Cipher text-Policy Attribute-based Encryption Scheme:

Recently Bettencourt et al.[6] proposed a cipher text policy attribute-based scheme, and the access policy in the encrypted data (cipher text). In key policy attribute-based encryption, the access policy is in user's private key, but the access policy is switched to the encrypted data in cipher text policy attribute-based encryption. And a set of descriptive at-tributes are associated with the user's private key, and the access policy is built in the encrypted data. The access structure of the encrypted data is corresponding to the user's private key with a set of descriptive attributes. If a set of attributes in user's private key satisfies the access structure of the encrypted data, the data user can decrypt the encrypted data; if it cannot, the data user cannot obtain the message.

In cipher text-policy attribute-based encryption (CP-ABE), depends how attributes and policy are associated with cipher texts and users’ decryption keys. In this scheme, a cipher text is associated with a monotonic tree access structure and a user’s decryption key is associated with set of attributes. In this scheme, the roles of cipher texts and decryption keys are switched as that in KP-ABE) the cipher text is encrypted with a tree access policy chosen by an encryptor, mean while decryption key is created with respect to a set of attributes. Since users’ decryption keys are associated with a set of attributes. Thus, it is more natural to apply CP-ABE, instead of KP-ABE.

Pseudo code 6:

```
  v.     Taking input security
  vi.    Take input message “M”, “pk”, “l”
  vii.   Start encryption using credentials & policy

  Decryption:
    iii. Take input “M” & “pk”, and compare
    iv.  If yes
           “Do decryption”
         No  “Exit”
```

D .Cipher Text Policy Attribute Set Based Encryption

Cipher text Policy Attribute Set Based Encryption (CP-ASBE)- a new form of CP-ABE that represent user attributes as a monolithic set in keys, organizes user attributes into a recursive set based structure and allows users to impose dynamic constraints on how those attributes may be combined to satisfy a policy. Specifically CP-ASBE allows, 1) user attributes to be organized into a recursive family of sets and 2) policies that can selectively restrict decrypting users to use attributes from within a single set or allow them to combine attributes from multiple sets. Thus, by grouping user attributes into sets such that those belonging to a single set have no restrictions on how they can be combined, CP-ASBE can support compound attributes without effecting the performance [6,7].

E. Hierarchical Identity Based Encryption

Wang et al.[6,7,8] proposed a hierarchical attribute-based encryption scheme composed of a hierarchical identity-based encryption scheme (HIBE) and a cipher text-policy attribute-based encryption scheme. This scheme used the property of hierarchical generation of keys in HIBE scheme to generate keys. Moreover, it used disjunctive normal form (DNF) to express the access control policy, and the same domain authority in this scheme administered all attributes in one conjunctive clause. There are four roles in this scheme.1) The role of cloud storage service is that let a data owner can store data and share data with users.2) The role of data owner is encrypting data and sharing data with users.3) The role of the root authority is generating system parameters and domain keys, to distribute them.4) The role of domain authority is managing the domain authority at next level and all users in its domain, to delegate keys for them. Again it can distribute secret keys for users. And users can use their secret keys to decrypt the encrypted data and obtain the message.

The key generation in this scheme adopts a hierarchical method. The root authority generates a root master key for domain authority at the first level. The system public key and the master key of the domain authority at first level are used to create the master keys for the domain authorities at the next level by the root authority or the domain authority at the first level. In addition, the do-main authority generates the user identity secret key and the user attribute secret key for the authorized user.

F. Hierarchical Attribute Set Based Encryption

Hierarchical attribute-based encryption (HABE) to achieve fine-grained access control in cloud storage services by combining hierarchical identity-based encryption (HIBE) and CP-ABE. This scheme also supports fine-grained access control and fully delegating computation to the cloud providers. But, here the HABE uses disjunctive normal form policy and assumes all attributes in one conjunctive clause are administrated by the same domain master. Resulting the same attribute may be administrated by multiple domain masters according to specific policies, which is difficult to implement in practice. Yet, again compared with ASBE, this scheme cannot support compound attributes efficiently and does not support multiple value assignments.

TABLE 1: COMPARISON OF DIFFERRENT ENCRYPTION & ACCESS CONTOL SCHEMES

Methodology	ABE-SLE	ABE-TLE	KP-ABE	CP-ABE	CP-ASBE	HIBE	HASBE
Parameter							
Access Control	Low	High	Low; High if associated with re-encryption technique	Average Realization of complex Access Control	Comparatively Low	Comparatively low	Very high
Efficiency	Average	High	Average High for broadcast type encryption	Average Not efficient for modern enterprise environments	Average	Better Lower when compared with ABE schemes	High efficiency and flexibility
Computational Overheads	Average	Average	High	Average	Average	Higher	Less Overheads
Confidentiality	Average	High	Average	High	High	Higher	Highest
Scalability	Low	Average	Average	High	High	Higher	Highest

III. CONCLUSION

This paper surveys different encryption schemes used in clouds. Many encryption schemes like ABE-SLE, ABE-TLE, KP-ABE, CP-ASBE, CP-ABE, HIBE and HASBE are discussed in which all the schemes are concentrated in efficient access control and encryption. These schemes can be classified according to their access policy. The access policy in the user's private key is KP-ABE, and the access policy in the encrypted data is CP-ABE. Moreover, the access structure is predefined in these schemes; if a new user wants to access data and his attributes are not in the access structure, these encrypted data will be regenerated. The HASBE & ABE-TLE scheme
Seamlessly incorporates a hierarchical structure of system users by applying a delegation algorithm to ASBE. Finally the HASBE scheme concluded the realization of scalable, flexible, and fine-grained access control in public cloud computing at most reliable level (Table 1).

IV. REFERENCE

[1] P. Mell and T. Grance, “The NIST definition of cloud computing,” Published in: Services (SERVICES), 2011 IEEE World Congress on ISBN: 978-0-7695-4461-8© 2011 [Accessed: 15-Oct-2012].

[2] Younis A.Younis, Madjid Merabti and Kashif Kifayat” Secure Cloud Computing for Critical Infrastructure” ISBN: 978-1-902560-27-4 © 2013 PGNet.

[3] G. Miklau and D. Suciu, “Controlling access to published data using cryptography,” in VLDB ’2003: Proceedings of the 29th international conference on Very large data bases. VLDB Endowment, 2003, pp. 898–909.

[4]J.Bethencourt, A. Sahai and B. Waters, “Ciphertext-policy attribute based encryption,” IEEE Symp. Security and Privacy, Oakland, CA, 2007.

[5] M. Nabeel and E. Bertino, “Privacy reserve-ing delegated access control in the storage as a service model,” in EEE International conference on Information Reuse and Integration (IRI), 20-12.

[6] Zhiguo Wan, Jun'e Liu, and Robert H. Deng, "HASBE: A Hierarchical Attribute-Based Solution for Flexible and Scalable Access Control in Cloud Computing" IEEE Transactions on Information Forensics And Security, Vol. 7, No. 2, April 2012.

[7] Zhiguo Wan, Jun'e Liu, and Robert H. Deng, "HASBE: A Hierarchical Attribute-Based Solution for Flexible and Scalable Access Control in Cloud Computing" IEEE Transactions On Information Forensics And Security, Vol. 7, No. 2, April 2012.

[8] G.Wang, Q. Liu, and J.Wu, "Hierachical attribute-based encryption for fine-grained access control in cloud storage services," ACM Conf. Computer and Communications Security (ACM CCS), Chicago, IL, 2010.

[9] J. Camenisch, M. Dubovitskaya, R. R. Enderlein, and G. Neven. Oblivious transfer with hidden access control from attribute-based encryption. In SCN 2012: Proceedings of the 8th International Conference on Security and Cryptography for Networks, pages 559–579, 2012.

[10] N. Shang, M. Nabeel, F. Paci, and E. Bertino. A privacy-preserving approach to policy-based content dissemination. In ICDE 2010: Proceedings of the 2010 IEEE 26th International Conference on Data Engineering, 2010.

[11]W. a Jansen, "Cloud Hooks: Security and Privacy Issues in Cloud Computing," in 2011 44th Hawaii International Conference on System Sciences, 2011, pp. 1–10.

[12] Ahmed E. Youssef and Manal Algae" A Framework for Secure Cloud Computing" , IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 4, No 3, July 2012 ISSN (Online): 1694-0814.

[13] Mohit Marwaha , Rajeev Bedi "Applying Encryption Algorithm for Data Security and Privacy in Cloud Computing", IJCSI International Journal of Computer Science Issues, Vol. 10, Issue 1, No 1, January 2013 .ISSN (Print): 1694-0784 | ISSN (Online): 1694-0814 .

[14] Mohammad Manzurul Islam , Sarwar Morshed and Parijat Goswami, "Cloud Computing: A Survey on its limitations and Potential Solutions", IJCSI International Journal of Computer Science Issues, Vol. 10, Issue 4, No 2, July 2013.ISSN (Print): 1694-0814 | ISSN (Online): 1694-0784 .

[15] J.-M. Do, Y.-J. Song, and N. Park, "Attribute based proxy re-encryption for data confidentiality in cloud computing environments," in Proceedings of the 1st International Conference on Computers, Networks, Systems and Industrial Engineering. Los Alamitos, CA, USA: IEEE Computer Society, 2011, pp. 248–251.

[16] Ruj, S., Stojmenovic, M., & Nayak, A. 2012, May. Privacy Preserving Access Control with Authentication for Securing Data in Clouds. In Cluster, Cloud and Grid Computing (CCGrid), 12th IEEE/ACM International Symposium on (pp. 556-563). IEEE.

[17] M. Nabeel and E. Bertino, "Towards attribute based group key management," in Proceedings of the 18th ACM conference on Computer and communications security, Chicago, Illinois, USA, 2011.

[18] K. P. N. Puttaswamy, C. Kruegel, and B. Y. Zhao, "Silverline: toward data confidentiality in storage-intensive cloud applications," in Proceedings of the 2nd ACM Symposium on Cloud Computing, ser. SOCC '11. New York, NY, USA: ACM, 2011, pp. 10:1–10:13.

[19] Nuttapong Attrapadung, Benoit Libert, and Elie de Panafieu, "Expressive Key-Policy Attribute-Based Encryption with Constant-Size Cipher texts", 14th International Conference on Practice and Theory in Public Key Cryptography, Taormina, Italy, March 6-9, 2011.

[20] Li, Qinyi, Hu Xiong, Fengli Zhang, and Shengke Zeng. "An Expressive Decentralizing KP-ABE Scheme with Constant-Size Cipher text." *IJ Network Security* 15, no. 3 (2013): 161-170.

[21]J.Bethencourt, A.Sahai, B.Waters,"Cipher text-policy attribute based encryption," in SP '07: Proceedings of the 2007 IEEE Symposium on Security and Privacy. Washington, DC, USA: IEEE Computer Society, 2007, pp.321–334.