UACEE International Journal of Advances in Computer Networks and its Security – IJCNS
Volume 3 : Issue 2 [ISSN 2250 – 3757]
Publication Date : 05 June 2013

# Privacy Preserving Access Control and Multi-Authority in Cloud with Efficient Authentication, Encryption and Revocation

**A.BLESSY[1] , S.SATHYALAKSHMI[2]**

***SCHOOL OF COMPUTING SCIENCES, HINDUSTAN UNIVERSITY, CHENNAI***

**blessy2789@gmail.com[1] , slakshmi@hindustanuniv.ac.in[2]**

***Abstract*---- Cloud computing is location-independent computing, whereby shared servers provide resources, software, and data to computers and other devices on demand. It describes a new supplement, consumption, and delivery model for IT services based on the Internet. Details are abstracted from consumers, who no longer have need for expertise in, or control over, the technology infrastructure "in the cloud" that supports them. Cloud computing is still considered in its infancy, there are many challenging issues waiting for tackling. The cloud suffers much from data loss, privacy, security and revocation problems. To overcome these problems an efficient Knowledge Based - Click Point Authentication (KB-CPA) and Multi-Authority Ciphertext-Policy Attribute Based Encryption (MA-CP-ABE) is proposed with some modifications. *(Abstract)***

***Keywords*---- Fuzzy Identity Based Encryption (F-IBE) ; Multi-Authority Attribute Based Encryption (MA-ABE); Key-Policy Attribute Based Encryption (KP-ABE); Click Point Authentication (CPA); Ciphertext-Policy Attribute Based Encryption (CP-ABE); Knowledge Based Authentication (KBA); Knowledge Based - Click Point Authentication (KB-CPA); Multi-Authority Ciphertext-Policy Attribute Based Encryption (MA-CP-ABE); Pseudo Random Key Generator (PRKG); Global Identifier (GID); Global Attribute List (GAL) *(keywords)***

## I. Introduction

Cloud computing is internet based computing. which involves the provision of dynamically scalable and often virtualized resources. The serious issue to be faced in cloud nowadays is security and privacy. Even though these issues are solved by many authentication and encryption schemes, there still some challenges are to be faced.

Fuzzy Identity Based Encryption (F-IBE) scheme proposed in [19] maintains a certain threshold access structure which is both error-tolerant and secure against collusion attacks. However it is more complex to be implemented. Multi-Authority Attribute Based Encryption (MA-ABE) scheme proposed in [3][12][13], allows any polynomial number of independent authorities which reduces heavy computation overhead on central authority but privacy of the user is traced. Key-Policy Attribute Based Encryption (KP-ABE) scheme proposed in [2], falls short of flexibility in attribute management and scalability in dealing with multiple-levels of attribute authorities. Ciphertext-Policy Attribute Based Encryption (CP-ABE) proposed in [2][9][12][21], suffers from collusion attack which arises when users combine their attributes to obtain the attributes of the owner. Attribute Revocation proposed in [6][10] [16] [21] suffers from periodical key reissuing and updation of entire system.

Knowledge Based Authentication (KBA) defined in [7][18] includes both text-based and picture-based passwords providing more security but lacks in usability. Passpoint Authentication is proposed in [8], in which 5 points in an image with 200*200 pixels along with that image is used as a password with 10*10 pixels error tolerant. It is less secure and requires a lot of memory. Cued Click Point Authentication proposed in [5] is more secure but requires more amount of memory and time consuming. Persuasive Cued Click Point Authentication proposed in [4] highlights the unpredictable part of the image so that security gets increased but user is not allowed to chose of his own choice and increases memory and time consumption.

### A. Cloud Computing

Cloud computing is internet based computing, which describes a new supplement, consumption, and delivery model for IT services based on the Internet, and it typically involves over-the-Internet provision of dynamically scalable and often virtualized resources.

### B. Click Point Authentication

For an efficient authentication, comparing to text based password a graphical password scheme is used for its larger password space and its resistance against password attacks. However it suffers from the drawback of much memory requirements and time consumption, the proposed work overcomes this by Click Point Authentication (CPA) which is a combined scheme of Recognition Based and Recall Based Graphical Techniques.

### C. Multi-Authority Ciphertext-Policy Attribute Based Encryption

For an efficient encryption to preserve security and privacy of the user, to resist collusion attack, comparing to other public key encryption method, to handle expressive types of encrypted access control, Multi-Authority - Ciphertext-Policy Attribute Based Encryption is used with some modifications. Here, a unique decryption key is issued randomly based on Pseudo Random Key Generator (PRKG)[19] when a set of attributes are registered with the authorities. The number of authorities is decided by the owner's attribute set. The owner's attribute set can be of Resource set, Subject set, Service set, etc.,

Based on Multi-Authority Attribute based Encryption (MA-ABE), depending on the authority number, the attributes are distributed to the user from the owner's registered attribute set. Again based on Ciphertext-Policy Attribute Based Encryption (CP-ABE) on a Threshold Access Structure, the ciphertext is encrypted with a k number of attributes randomly chosen among the distributed user's attributes. As long as the set of attributes associated with a decryption key satisfies the tree access policy associated with a given ciphertext, the key can be used to decrypt the ciphertext. For owner and user each authority randomly issue 8 bit and 4 bit secret key independently. These are done by using a PRKG in a Linear Congruential Method in which a seed value with the incrementor and modulo value will be initialized to generate a random number.

### D. Global Identifier (GID) and Global Attribute List (GAL)

To resist collusion attack, for a owner's content all the users will be issued with the same attribute set depending on the authority number and different 4 bit key from each authority. Therefore there is no chance for multiple users to combine their attributes and track the user. Here GID is used to tie all the secret keys issued by authorities together to make authorities unaware of the secret key and (n-2) number of corrupted authorities can be tolerated. GAL is additionally used to avoid distribution of attribute set every time to the user. Using GAL, the user should select their attributes among the given ones to decrypt their ciphertext. It is more natural to apply CP-ABE, instead of Key Policy-Attribute Based Encryption (KP-ABE), to enforce access control of encrypted data.

### E. Attribute Revocation

To solve Revocation issues, the day before expiration time user or owner will be given warning signal, and then if they wish they can extend their time or revoke. In case of owner the attributes will be revoked after the expiration time else they can extend their expiration time of the same secret key. In case of user, the user's secret key will be revoked after the expiration time else they can extend their usage time by requesting another secret key.

## II. Existing System

Generally, cloud suffers hardly from security problems even if it is solved by many authentication and encryption schemes, problems still there persist and raise some issues making them inefficient. In the existing system text based password is used which is less secure as it can't resist against many attacks due to its small password space.

However graphical password overcomes this problem with large password space, existing algorithm lacks usability due to their high memory requirements, time consumption and computation.

Then, even though the KP-ABE scheme used in existing system preserves privacy, the encryptor exerts no control over who has access to the data

she encrypts, except by her choice of descriptive attributes for the data. Rather, she must trust that the key-issuer issues the appropriate keys to grant or deny access to the appropriate users. It also falls short of flexibility in attribute management and scalability in dealing with multiple-levels of attribute authorities. GID, which is used in KP-ABE to resist collusion attack, is more complex when used without a central authority.

The compromisation of server and corruption of authorities weaken the privacy of user. The attribute revocation in KP-ABE is cumbersome as, the other users using those attributes will suffer when it gets revoked.

# III. DESIGNING PRIVACY PRESERVING ACCESS CONTROL & MULTI-AUTHORITY IN CLOUD

## A. *Basic Architecture*

From Fig. 1, owners and users register with the cloud after creating an account and then enter the cloud through CPA. After getting authenticated, to encrypt the original data, which is to be stored in the cloud, MA-CP-ABE scheme on a threshold access structure is done. When the time for expiration arrives attribute revocation is done in the cloud for users and owners in a different fashion.

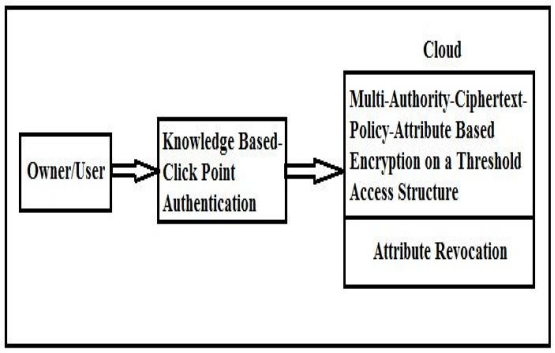


Fig. 1 Basic Architecture

## B. *Module Management System*

The privacy preserving access control and multiple authority in cloud with secure authentication, encryption and revocation scheme consists of several modules which can be seen in Fig. 2:

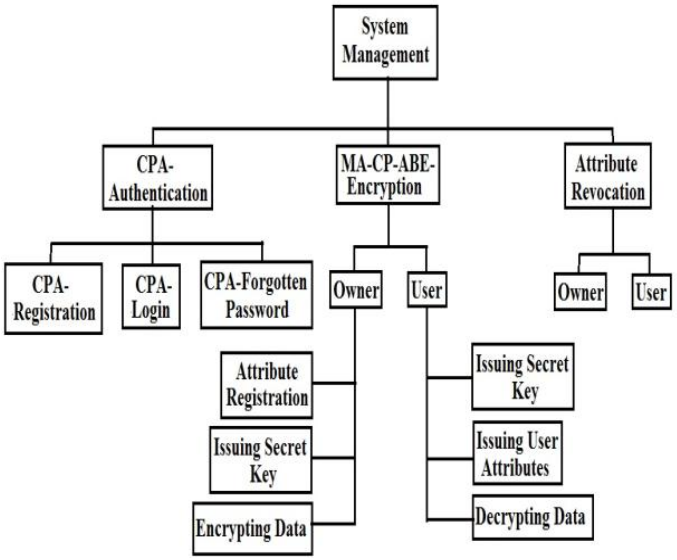


Fig. 2 Module Management System

### *1) Click Point Authentication*

Click Point Authentication is a Knowledge Based Authentication. Here owners and users are registering their account with a security question and answer and, creating the password using recognition based in which they are selecting an image which can be used as a password along with its image code and then, using recall based they are clicking on a pixel part of the image using mouse to generate a coordinate which is also added as the password. As soon as the recall based password is generated it will be send to the user along with its random image code.

After registration, the owner or user login using CPA by entering the username, choosing an image from the given list and entering the pixel point and image code using virtual keyboard.

If a user/owner has forgotten or lost his recall based password they will be asked for the security question and answer they previously registered and if it is right their coordinates will be send to them else it will display an error message saying security question and answer is wrong. After they received the pixel point, they enter it in forgotten page. If the pixel point entered is right they will be provided with their image code. But image will not be given as it is proved that a legitimate user won't be able to forget the chosen images. Then the login page will be opened in which the authentication is done.

### *2) MA-CP-ABE of Owner*

For using a central authority, multi authorities are used to reduce the overload in computation and

tolerate (n-2) corrupted authorities. MA-CP-ABE scheme is used with some modification where owners register a set of attributes of different domains separately with the multi authorities and there will be no communication between the authorities. These registered attributes will be stored in a Global Attribute List, where all owners' attributes are tied together and in a Owner's Attribute Set, which is maintained for each owner.

After registering attributes, using a PRKG in a Congruential Linear Method each domain independent authorities will issue 8 bit random key by padding or concatenation and will be placed in GID separately, where they are tied together and sent to the owner's email id.

After the key issuing process to the owner, based on the attributes that are selected on a threshold access structure from the $dk^{th}$ number of user's attributes, the data are encrypted and stored in the cloud database.

### *3) MA-CP-ABE of User*

When a user selects the data from the cloud, the authority selects a $dk^{th}$ number of attributes based on the authority number from the data's Owner's Attribute Set and sends it to the user's email id. After distribution of attributes to the user, using a PRKG each domain independent authorities issue 4 bit random key to the user by padding or concatenation and these keys are tied together in a Global Identifier separately for each user and GID will be send to the user's email id.

While logging in, as soon as the key is entered, the user of that key will be provided with global list of attributes of all the users. Then the legitimate user will select his attributes in it. According to threshold access structure, it will be checked whether in the selected attributes the randomly chosen k number of attributes is there.If all the specific attributes specified in threshold access structure are there, then the data will be decrypted.

### *4) MA-CP-ABE Attribute Revocation of Owner*

The day before expiration time, owner will be given warning signal, then if they wish they can extend their service time of same secret key by providing their GID to authority to modify the Service Time attributes, else their attributes will be revoked.

### *5) MA-CP-ABE Attribute Revocation of User*

The day before expiration time user will be given warning signal, then if they wish they can extend their usage by requesting another secret key else their key will be revoked.

## IV. Proposed System

In the proposed work, CPA is used with MA-CP-ABE-r on a Threshold Access Structure to make the content of the owner secure, private and indirectly under the control of him. CPA is a graphical password authentication scheme that provides much resistance against password attacks and requires less memory and time consumptions with less computation comparing to the existing system. MA-CP-ABE is an efficient ABE scheme, which enhances the security by encrypting the original data using specific set of attributes among the users's attribute set on a threshold access structure and randomized secret key of owner using multi authorities. Multi Authority reduces the computation overhead, network overload and provides (n-2) tolerance in corruption of authorities. CP-ABE on threshold access structure is used to enforce access control of encrypted data for its efficiency, scalability, flexibility and simplicity. In CP-ABE, the encryptor intelligently decides who should or should have access to the data that she encrypts. GID is used to tie all the secret keys issued by each authority together for both user and owner. GAL is used in which all the owner's entire attribute set are placed in it. PRKG is used which uses Linear Congruential Method to generate random keys from each authority. These three mechanisms are followed to enhance the privacy of user and resist the collusion attack. Efficient Revocation is done separately with different mechanisms for both user and owner without affecting other users and the system.Therefore the security, data loss, privacy preserving, access control and attribute revocation issues are solved efficiently using CPA and MA-CP-ABE with some modifications.

## V. Implementation and Operational Environment

A cloud will be developed in which a CPA registration and login page will be designed and once the password is forgotten recovery

mechanism is also done. MA-CP-ABE scheme is implemented for encrypting and decrypting data. Attribute Revocation is done for both user and owner in a different fashion after their expiration time. These schemes are developed in a eclipse using JSP with a MY SQL database as a backend.

# VI. Conclusion

In this work of privacy preserving access control and multi-authority in cloud with efficient authentication, encryption & revocation, KB-CPA and MA-CP-ABE scheme is used with some modification to ensure security and privacy in the cloud by tackling collusion attack, revocation issue and computation overhead.

## *References*

[1] Amiya Nayak, !, Milos Stojmenovic, and Sushmita Ruj (2011), "Privacy Preserving Access Control with Authentication for Securing Data in Clouds" in proceedings: 2012 12th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing.

[2] Bethencourt.J, Sahai.A, and Waters.B (May 20-23 2007), "Ciphertext-policy attribute-based encryption," in Proceedings: IEEE Symposium on Security and Privacy (S & P'07), (Oakland, California, USA), pp. 321–34, IEEE.

[3] Chase.M (February 21-24 2007), "Multi-authority attribute based encryption," in Proceedings: Theory of Cryptography Conference-TCC'07 (S. P. Vadhan, ed.), vol. 4392 of Lecture Notes in Computer Science, (Amsterdam,The Netherlands), pp. 515–534, Springer.

[4] Chiasson.S, Biddle.R, Forget.A and van Oorschot.P (. Feb. 2011), "Persuasive Cued Click-Points: Design, Implementation, and Evaluation of a Knowledge-Based Authentication Mechanism," Technical Report TR-11-03, School of Computer Science, Carleton Univ.

[5] Chiasson.S, Biddle.R and van Oorschot.P (Sept. 2007), "Graphical Password Authentication Using Cued Click Points," Proc. European Symp. Research in Computer Security (ESORICS), pp. 359-374.

[6] Cong Wang, Kui Ren, and Shucheng Yu (April 13–16, 2010), "Attribute Based Data Sharing with Attribute Revocation" in proceedings: ASIACCS'10, Beijing, China.

[7] De Angeli.D, Coventry.L, Johnson.G, and Renaud.K (2005), "Is a Picture Really Worth a Thousand Words? Exploring the Feasibility of Graphical Authentication Systems," Int'l J. Human-Computer Studies, vol. 63, nos. 1/2, pp. 128-152.

[8] Dirik.A, Menon.N, and Birget.J, (July 2007), "Modeling User Choice in the Passpoints Graphical Password Scheme," Proc. Third ACM Symp. Usable Privacy and Security (SOUPS).

[9] Herranz.J, Laguillaumie.F, and R´afols.C (May 26-28 2010), "Constant size ciphertexts in threshold attribute-based encryption," in Proceedings: Public Key Cryptography-PKC'10 (P. Q. Nguyen and D. Pointcheval, eds.), Lecture Notes in Computer Science, (Paris, France), pp. 19– 34, Springer.

[10] Hur.J and Noh.D.K. (2011), "Attribute-based access control with efficient revocation in data outsourcing systems," IEEE Transactions on Parallel and Distributed Systems, vol. 22, no. 7, pp. 1214–1221.

[11] Lewko.A and Waters.B (May 15-19 2011), "Decentralizing attribute - based encryption," in Proceedings: Advances in Cryptology-EUROCRYPT'11 (K. G. Paterson, ed.), vol. 6632 of Lecture Notes in Computer Science, (Tallinn, Estonia), pp. 568–588, Springer.

[12] Li.J, Huang.Q, Chen.X, Chow.S.S.M, Wong.D.S, and Xie.D, (2011), "Multi-authority ciphertext-policy attribute-based encryption with accountability," in Proceedings: ACM Symposium on Information, Computer and Communications Security-ASIACCS'11, pp. 386–390, ACM.

[13] Lin.H, Cao.Z, Liang.X, and Shao.J (December 14-17 2008), "Secure threshold multiauthority attribute based encryption without a central authority," in Proceedings: International Conference on Cryptology in India-INDOCRYPT'08 (Kharagpur, India), vol. 5365 of Lecture Notes in Computer Science, pp. 426–436, Springer.

[14] M¨uller.S, Katzenbeisser.S, and Eckert.C (December 3-5 2008), "Distributed attribute based encryption," in Proceedings: Information Security and Cryptology-ICISC'08 (P. J. Lee and J. H. Cheon, eds.), vol. 5461 of Lecture Notes in Computer Science, (Seoul, Korea), pp. 20–36, Springer.

[15] Naor.M, Pinkas.B, and Reingold.O (May 2-6 1999), "Distributed pseudo - random functions and KDCs," in Proceedings: Advances in Cryptology - EUROCRYPT'99 (J. Stern, ed.), vol. 1592 of Lecture Notes in Computer Science, (Prague, Czech Republic), pp. 327–346, Springer.

[16] Nikita Borisov, Prateek Mittal, and Sonia Jahid (March 22–24, 2011)," EASiER: Encryption based Access Control in Social Networks with Efficient Revocation in Proceedings: ASIACCS '11, Hong Kong, China.

[17] Ostrovsky.R, Sahai.A, and Waters.B (October 28-31 2007), "Attribute- based encryption with non-monotonic access structures," in Proceedings: ACM Conference on Computer and Communications Security-CCS'07 (P. Ning, S. D. C. di Vimercati, and P. F. Syverson, eds.), (Alexandria, Virginia, USA), pp. 195–203, ACM.

[18] Owen.G.S, Suo.X, Zhu.Y, (2005), \Graphical passwords: A survey", 21st Annual Computer Security Applications Conference (ACSAC'05) 463-472.

[19] Sahai.A, and Waters.B (May 22-26 2005), "Fuzzy identity-based encryption," in Proceedings: Advances in Cryptology - EUROCRYPT'05 (R. Cramered.), vol. 3494 of Lecture Notes in Computer Science, (Aarhus,Denmark), pp. 457–473, Springer.

[20] Taeho Jung, Xiang-Yang Li and Zhiguo Wan (2012), "Privacy Preserving Cloud Data Access With Multi-Authorities" in proceedings: Advances in Cryptology - EUROCRYPT'99 (J. Stern, ed.), vol. 1592 of Lecture Notes in Computer Science , (Prague, Czech Republic), pp. 327–346, Springer.

[21] Xiaohui Liang, Rongxing Lu, Xiaodong Lin, and Xuemin (Sherman) Shen (2010),"Ciphertext Policy Attribute Based Encryption with Efficient Revocation"in proceedings: In ACM Conference on Computer and Communication.