ISSN 2347-3983

International Journal of Emerging Trends in Engineering Research, Vol.3. No.10, Pages : 356 - 361 (2015)
Special Issue of ICACSSE 2015 - Held on October 30, 2015 in St. Ann's College of Engineering & Technology, Chirala, AP, India
http://www.warse.org/IJETER/static/pdf/Issue/icacsse2015sp74.pdf

Customizable Compact Key framework for secure cloud access control

S. Rama Krishna[1],
Associate Professor[1],
Head Of the Department, CSE[1],
Vycet, Chirala[1],
9346949121[1],
ramakrishna.ss@gmail.com[1],

Dr. B. Padmaja Rani[2],
Professor[2],
Department of CSE[2],
Jntuceh, Hyderabad[2],
9885447701[2],
padmaja_jntuh@yahoo.co.in[2],

K. Sai Vijaya Lakshmi[3]
Assistant Professor[3]
Department of CSE[3]
Vycet, Chirala[3]
9700857137[3]
vijayakommanaboyina@gmail.com[3]

ABSTRACT

Cloud Computing is no more a buzzword today. Several Reasons are pushing corporate companies into cloud technologies. Initial investment, scalability, availability, performance, uptime are some of the major among several reasons. One side it is proving to be most enticing on the other side still questions remains unanswered about its implementation. Virtualization technology, speed of internet, lack of trust, security are topping among this list of these questions.

This paper brings a framework for access control in cloud with two properties collision resistance and key compaction. This algorithm is inspired from attribute based encryption and key aggregation. It addresses problems like flexibility, efficiency, fine graininess over attribute based encryption. Attribute based encryption points to collusion resistance, fine graininess but key is large and lacks in compactness. Key aggregation is designed to build the compactness in key by merging several keys and bringing the impact of all the keys in one. Keeping these major aspects here we attempted to build our algorithm aggregated key attribute based encryption.

Keywords
Cloud, Virtualization technology, collision resistance, key compaction, fine graininess, attributes based encryption.

1. INTRODUCTION

In view of the features such as elastic service, resource pooling, Service on demand cloud computing becomes more popular. By using these resources in the cloud, user can minimize initial establishment cost. Cloud computing has amazing features but facing many challenges. In those major challenges are multi tenancy, virtualization, average speed of internet, access control and Security [1, 17].

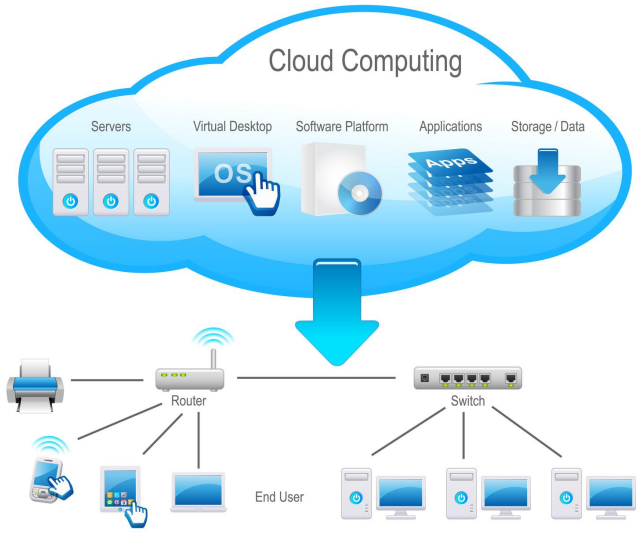

Figure 1: Simple Cloud Model

In multi tenancy [23], many users will share virtual storage space on cloud as shown in figure 1. There is possibility of hi-jacking essential data. This may cause a potential damage in corporate world [24]. Hence the cloud has several questions left with it about confidentiality of data [18]. Several authors try to address these security issues raised in multi

ISSN 2347-3983
International Journal of Emerging Trends in Engineering Research, Vol.3. No.10, Pages : 356 - 361 (2015)
Special Issue of ICACSSE 2015 - Held on October 30, 2015 in St. Ann's College of Engineering & Technology, Chirala, AP, India
http://www.warse.org/IJETER/static/pdf/Issue/icacsse2015sp74.pdf

tenancy [25]. Access control is the key technique for data protection because it allows only the genuine users and prohibits the other users to access the data [13]. Even by providing the access rights to genuine users still we have to believe the trusted server, for this reason users want to encrypt their data before keeping their data in cloud [11]. Cloud storage, which assures properties like CIA will increase trust in cloud users [20, 21, 22].

2. LITERATURE REVIEW

Access control models generally include Discretionary Access control (DAC), Mandatory Access control (MAC), Role based Access control (RBAC). In DAC the object owner maintains the access control mechanism to limit the number of users [7]. Only those users specified by the owner may have the access permissions like Read, write and executable properties, where as in MAC access control decisions are made by the central authority, not by the individual owner of particular object and the owner has no right to change the access permissions. RBAC model assigns the access permissions to a particular role, and assigns appropriate roles to users according to the users job in their organization [8, 15]. Role is the bridge between the user and the access permissions. But all these methods are based on centralized access control and it becomes bottle neck.[2] In these access controls we maintain a trusted server to store the data. However, if the number of users increases to store the data then we replicate all the data into many trusted servers. So here we lose data confidentiality property. So we go for encryption mechanism. Traditionally, we have public key encryption, in this we encrypt the data and generate private keys for particular users. So, it takes more time and not expressive.

Sahai and water invented Attribute Based Encryption method (ABE) [3, 12]. Here it does not allow the data to encrypt per a particular user. Whereas it encrypts the based attributes or a policy on attributes. A user can decrypt the data, if there is a match between the private key and the cipher text. Threshold Attribute Based Encryption (TABE) System [3], in which cipher text were labelled with set of attributes and user private key is associated with attributes also with the threshold parameters. If user wants to decrypt the data then he must satisfy the attributes also with the threshold parameter.

This design was motivated from Identity Based Encryption [4, 5, 6] which uses biometric identities [16]. TABE is also not expressive and it is complicated for more general systems. So, we go for Policy Based Attribute Based Encryption [14] in that first is Key Policy Attribute Based Encryption (KPABE). As the name specifies here the users' key is associated with an access structure and the data is encrypted with a set of attributes [9]. Access structure means user key is embedded with a general secret sharing scheme. Cipher text Policy Attribute Based Encryption (CPABE), is a converse to KPABE where as cipher text is associated with an access structure and the users key will be associated with an arbitrary no of attributes[10].

If multiple users collude, only one user can decrypt the data, we do not allow the colluders can decrypt the data by combining their attributes. Suppose user1 has read and user2 has write permissions then we allow user1 for read and user2 for write, we do not allow read, write for both users by combining read write attributes. So, in CPABE we embed the secret sharing scheme into each users private key to avoid this [10]. By adding this access structure mechanism we can achieve the Collusion Resistance. In Hierarchical Attribute Based Encryption (HABE), we mainly contain Root Master and Domain Master. Root Master is responsible for generating keys and Domain Master is responsible for distributing the keys [26].Here if the number of attributes increases automatically the length of the key also increases. User decrypts the message if there is a match between the access structure and the cipher text. In Key Aggregation Crypto System (KAC) we keep the size of the key as constant.

ISSN 2347-3983
International Journal of Emerging Trends in Engineering Research, Vol.3. No.10, Pages : 356 - 361 (2015)
Special Issue of ICACSSE 2015 - Held on October 30, 2015 in St. Ann's College of Engineering & Technology, Chirala, AP, India
http://www.warse.org/IJETER/static/pdf/Issue/icacsse2015sp74.pdf

3. PROPOSED SYSTEM

The design of this new algorithm is to achieve both the collusion resistance and to customize the key length. For this we introduce a new parameter Level Aggregator (λ) by means of which we can customize variable key length, key compression technique for reducing the length of the key and then apply Attribute Based Encryption for certain level to avoid collisions.

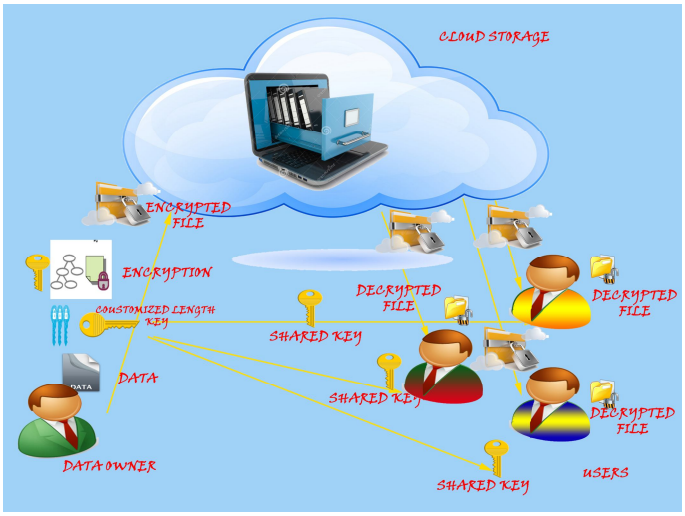

Figure 2: Architecture of Proposed System

Figure 2 describes about the architecture of the proposed system, where the data owner encrypts the data with the help of Shared Master Secret Key (SMSK). The encrypted data will be stored in cloud. Data owner sends a Secret Key which is generated from SMSK to the user. User can decrypt the data with the help of secret key.

• **Setup (SP):** The setup algorithm takes Security Parameters (SP) as input. Security parameters include attributes and Level Aggregator (λ) It gives public parameters (PP) as output.

• **KeyGen (PP):** KeyGen algorithm takes public parameters (PP) as input. Here the key is generated by the data owner. It gives a Shared Master Secret Key (SMSK) as an output.

•**Encrypt (SMSK, Mes, A, λ):** The Encryption Algorithm takes Shared Master Secret Key (SMSK),a message (Mes), Level Aggregator(λ),and an access policy (A) will be constructed for an arbitrary set of attributes is represented as A. Here, first we compress the key by using key compression technique [27] up to Level Aggregator (λ) then we apply ABE. Finally the algorithm converts the plaintext into cipher text and it gives the Cipher Text (CT) as an output.

•**SecretKeyGen (SMSK, C):** The SecretKeyGen algorithm takes Shared Master Secret Key (SMSK), set of classes(C) correspond to users as input and executed by the data owner. It gives secret key (SK) as an output.

• **Decrypt (SK, CT):** The decrypt key algorithm takes Cipher Text and Secret Key (SK) as input and decrypts the data into plain text and gives plain text as an output.

Technical terms used in the algorithms as

SP-Security Parameters
PP-Public Parameters
SMSK-Shared Master Secret Key
Mes-Message
A-Access Policy
λ-Level Aggregator
CT-Cipher Text
C-Set of Classes
SK- Secret Key

3.1 Performance Analysis

Graph drawn by considering the above algorithms by taking Accessing Ratio(AR) on X-axis and Key compression ratio(KC) on Y-axis, if we increase the Access ratio(AR) increases respective Key Compression level also increases which is shown in figure 3. Here the access ratio is the ratio between

ISSN 2347-3983
International Journal of Emerging Trends in Engineering Research, Vol.3. No.10, Pages : 356 - 361 (2015)
Special Issue of ICACSSE 2015 - Held on October 30, 2015 in St. Ann's College of Engineering & Technology, Chirala, AP, India
http://www.warse.org/IJETER/static/pdf/Issue/icacsse2015sp74.pdf

accessing power of cipher text classes with the total no of classes(C).

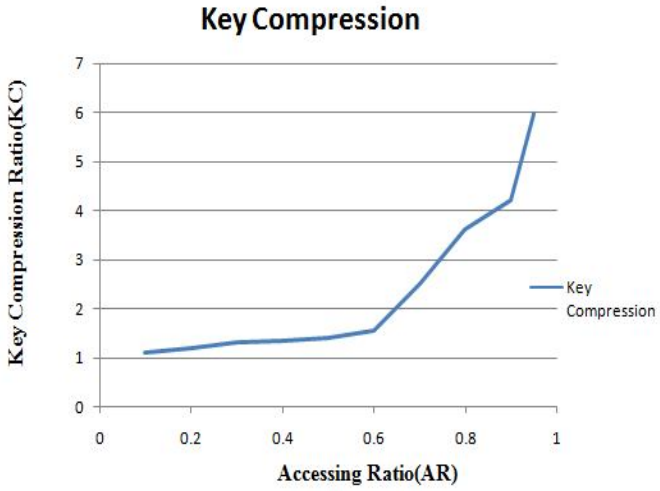

Figure 3: Represents the relation between the Access Ratio and Key Compression ratio

Figure 4 represents the relation between Key length and Level Aggregator (λ) where Key length on y-axis and Level Aggregator on x-axis, if we increase the Level Aggregator then the respective Key length also increases.

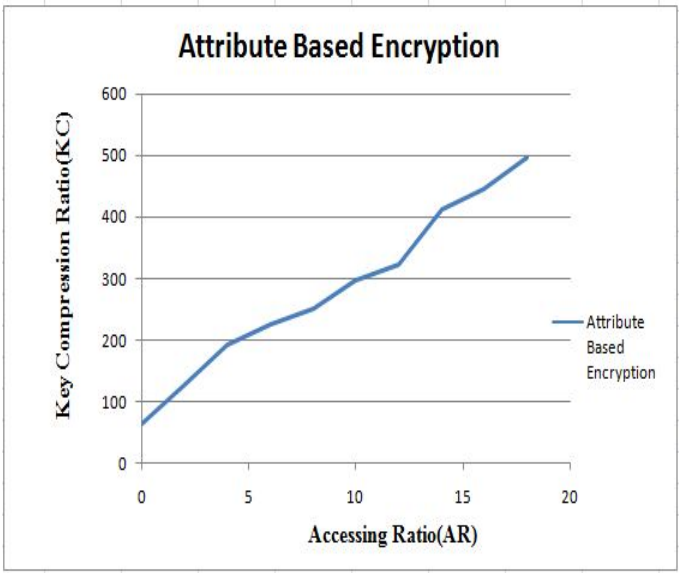

Figure 5: Represents the variation of key length with the use of Attribute Based Encryption and Key Compression techniques.

In figure 5 we try to Portrait changes happened in both Attribute Based Encryption (ABE) as well as Key Compression, by taking accessing ratio and no of keys generated into comparison factor.

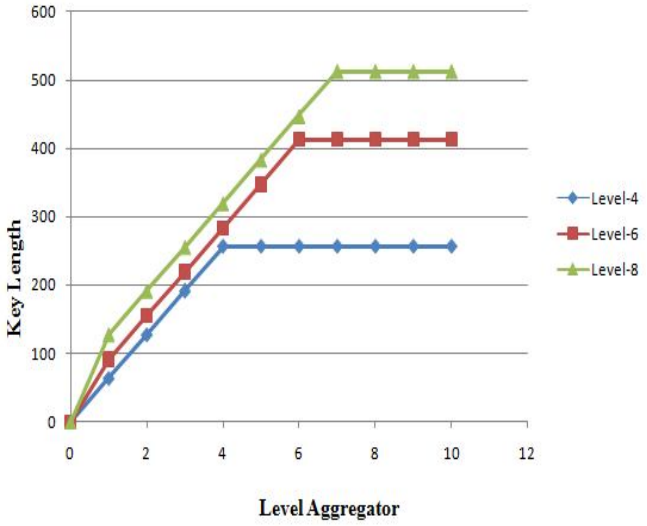

Figure 6: Represents the customized key length with the use of Level Aggregator

In figure 6 we observe the length of the key is increasing as specified in Attribute Based Encryption introduction of Level Aggregator(λ) in our algorithm, we can customize the length of the key to certain levels. Here the data owner provided the flexibility in defining Level Aggregator (λ) hence the length of the key. So here the Level Aggregator is the key factor for defining the key length.

3.2 Experimental Setup

Experiment was carried by setting up a data owner machine, cloud machine, 10 users with variable _le sizes and key lengths were recorded. For Data owner machine we used dual core processor, 2GB RAM, Windows Operating System. A private cloud was setup using eucalyptus 4.1 cloud operating System, which is installed on i5 processor with 8 GB RAM for cloud controller, 2 nodes were clustered with a configuration Pentium dual core 2.7 GHz processor and 2 GB RAM connected over LAN. 10 Client machines were having configuration of dual core

ISSN 2347-3983

International Journal of Emerging Trends in Engineering Research, Vol.3. No.10, Pages : 356 - 361 (2015)
Special Issue of ICACSSE 2015 - Held on October 30, 2015 in St. Ann's College of Engineering & Technology, Chirala, AP, India
http://www.warse.org/IJETER/static/pdf/Issue/icacsse2015sp74.pdf

processor, 1GB RAM with Windows or MAC Operating System.

4. CONCLUSION

The scope of this paper limited the discussion regarding the data confidentiality and access control which is a major challenge. In this paper we focus on the data protection by providing flexible fine grained access control with the customizable key length by data owner. This can be achieved by compressing the key with key compression technique, our Level Aggregator (λ) is used for providing customizability. It also avoids the collusions between the users hence allows only the genuine users to access and visualize the data.

5. REFERENCES

[1] Li, Xinlu, and Xiaoxia Zhao. "Survey on access control model in cloud computing environment." 2013 International Conference on Cloud Computing and Big Data (CloudCom-Asia). IEEE, 2013.

[2] Ausanka-Crues, Ryan. "Methods for access control: advances and limitations." Harvey Mudd College 301 (2001).

[3] A. Sahai and B.Waters. Fuzzy Identity Based Encryption. In Advances in Cryptology AS Eurocrypt, volume 3494 of LNCS, pages 457 A S473. Springer, 2005.

[4] A. Shamir. Identity Based Cryptosystems and Signature Schemes. In Advances in Cryptology S CRYPTO, volume 196 of LNCS, pages 37 _S53. Springer, 1984.

[5] D. Boneh and M. Franklin. Identity Based Encryption from the Weil Pairing. In Advances in Cryptology S CRYPTO, volume 2139 of LNCS, pages 213-229. Springer, 2001.

[6] C. Cocks. An identity based encryption scheme based on quadratic residues. In IMA Int. Conf., pages 360-363, 2001.

[7] Osborn, Sylvia, Ravi Sandhu, and Qamar Munawer. "Con_guring role-based access control to enforce mandatory and discretionary access control policies." ACM Transactions on Information and System Security (TISSEC) 3.2 (2000): 85-106.

[8] Tang, Bo, Qi Li, and Ravi Sandhu. "A multi-tenant RBAC model for collaborative cloud services." Privacy, Security and Trust (PST), 2013 Eleventh Annual International Conference on. IEEE, 2013.

[9] Goyal, Vipul, et al. "Attribute-based encryption for fine-grained access control of encrypted data." Proceedings of the 13th ACM conference on Computer and communications security. Acm, 2006.

[10] Bethencourt, John, Amit Sahai, and Brent Waters. "Ciphertext-policy attribute-based encryption." Security and Privacy, 2007. SP'07. IEEE Symposium on. IEEE, 2007.

[11] Chu, Cheng-Kang, et al. "Key-aggregate cryptosystem for scalable data sharing in cloud storage." Parallel and Distributed Systems, IEEE Transactions on 25.2 (2014): 468-477.

[12] Ruj, Sushmita. "Attribute Based Access Control in Clouds: A Survey."

[13] Chen, Yi-Ruei, et al. "Cloudhka: A cryptographic approach for hierarchical access control in cloud computing." Applied Cryptography and Network Security. Springer Berlin Heidelberg, 2013.

[14] Gitanjali, Gitanjali, Sukhjit Singh Sehra, and Jaiteg Singh. "Policy Speci_cation in Role based Access Control on Clouds." International Journal of Computer Applications 75.1 (2013): 39-43.

[15] Saidi, Mustapha Ben, and Abderrahim Marzouk. "Access Control Protocol for Cloud Systems Based On the Model TOrBAC."

[16] Suryadevara, Sowmya, et al. "Tongue as a Biometric Visualizes New Prospects of Cloud

Computing Security." Proceedings of International Conference onInformation and Network Technology (ICINT 2011). 2011.

[17] Mukundrao, Joshi Ashay, and Galande Prakash Vikram. "Enhancing Security in Cloud Computing." Information and Knowledge Management. Vol. 1. No. 1. 2011.

[18] Wang, Cong, et al. "Privacy-preserving public auditing for secure cloud storage." Computers, IEEE Transactions on 62.2 (2013): 362-375.

[19] Khawale, Rashmi, and Omprakash Tembhurne. "A Review on Data Sharing Across Cloud Storage Using Key Aggregate Cryptosystem."

[20] Subashini, Subashini, and V. Kavitha. "A survey on security issues in service delivery models of cloud computing." Journal of network and computer applications 34.1 (2011): 1-11.

[21] Christodorescu, Mihai, et al. "Cloud security is not (just) virtualization security: a short paper." Proceedings of the 2009 ACM workshop on Cloud computing security. ACM, 2009.

[22] Mather, Tim, Subra Kumaraswamy, and Shahed Latif. Cloud security and privacy: an enterprise perspective on risks and compliance. " O'Reilly Media, Inc.", 2009.

[23] Rimal, Bhaskar Prasad, Eunmi Choi, and Ian Lumb. "A taxonomy and survey of cloud computing systems." INC, IMS and IDC, 2009. NCM'09. Fifth International Joint Conference on. Ieee, 2009.

[24] Espadas, Javier, et al. "A tenant-based resource allocation model for scaling Software-as-a-Service applications over cloud computing infrastructures." Future Generation Computer Systems 29.1 (2013): 273-286.

[25] Mietzner, Ralph, et al. "Variability modeling to support customization and deployment of multi-tenant-aware Software as a Service applications." Proceedings of the 2009 ICSE Workshop on Principles of Engineering Service Oriented Systems. IEEE Computer Society, 2009.

[26] Wang, Guojun, Qin Liu, and Jie Wu. "Hierarchical attribute-based encryption for fine-grained access control in cloud storage services." Proceedings of the 17th ACM conference on Computer and communications security. ACM, 2010.

[27] Bhalerao, R. S., and S. M. Rokade. "Securely Sharing Of Data with Others in Cloud Storage Using Public Key Cryptosystem."

Author's Biographies

S. Rama Krishna M.Tech is working as Associate Professor in the Department of Computer Science & Engineering, VYCET, Chirala.

Dr. B Padmaja Rani M.Tech, Ph.D is working as Professor & Head of department in Computer Science &Engineering at JNTUH College of Engineering Hyderabad (Autonomous). She has done extensive research in the areas like Information Retrieval Embedded Systems. Official Email: padmaja jntuh@jntuh.ac.in

K.Sai Vijaya Lakshmi M.Tech is working as Assistant Professor in the Department of Computer Science & Engineering, VYCET, Chirala.