International Journal of Computing Communication and Information System(IJCCIS)
Vol 6. No.3 – July-September 2014 Pp. 96-105
©gopalax Journals, Singapore
available at : www.ijcns.com
ISSN: 0976–1349

# AN ANALYSIS ON ATTRIBUTE-BASED SOLUTION FOR ADAPTABLE AND SCALABLE SECURITY ACCESS CONTROL IN CLOUD COMPUTING

[1]S. Artheeswari [2]Dr.RM. Chandrasekaran
[1]Research Scholar, [2]Professor (CSE) / Director DDE,
[1,2]Department of Computer Science
[1,2]Annamalai University, Annamalainagar,Chidambaram
[1]art.arthe@gmail.com [2]aurmc@hotmail.com

## ABSTRACT

*Cloud computing is a well-known technology in IT enterprises. The data stored is enormous and it is very valuable for an enterprise. All tasks are done through networks. Hence, it is significant to have the protected use of data. In cloud computing, the most important concerns are data privacy and security. And also flexible, scalable and fine grained access control must be preserved in the cloud systems. There are policy based schemes that have been proposed. In this work, we are going to explore various schemes for encryption that contains Attribute Based encryption (ABE) and its types KP-ABE and CP-ABE. Further discussion consists of an improvement in CP-ABE to CP-ASBE and to HASBE. A comparison table has been enclosed for comparative study of these techniques.*

*Keywords: Cloud computing, Scalability, Access Control, Privacy and Security*

## 1. INTRODUCTION

Cloud computing technology consists of the use of computing resources that are delivered as a service over a network. In cloud computing model, users are allowed to store the data and perform the specified business operations. Hence cloud service provider must provide trust and security, since the valuable and sensitive data is stored in huge amount in clouds. For this purpose, there have been many of the schemes, proposed for encryption such as simple encryption technique. In this paper we have discussed about the Attribute-Based Encryption(ABE) schemes[2] and how it has been developed and modified further into Key Policy Attribute based encryption (KP-ABE), Cipher-text Policy Attribute Based Encryption (CP-ABE)[4], CP-ASBE, HABE and HASBE so on.

### 1.1 Challenges in cloud security

***1) Data protection***: To be considered protected, data from one customer must be correctly segregated from that of another. It must be stored securely when “at rest” and it must be able to change securely from one location to another. Cloud providers have systems to prevent data leaks or access by third parties [3]. The proper separation of duties should ensure that auditing and/or monitoring cannot be defeated, even by privileged users of the cloud provider.

***2) Access Control and Accounting:*** Heterogeneity in cloud computing demands fine-grained access management policies. Particularly, access management services ought to be versatile enough to capture dynamic, context or attribute-based or credential-based access necessities and to enforce the principle of smallest privilege [3].

***3) Identity management***:
Every enterprise will have its own identity management system to control access to information and computing resources. SSO technology is used to integrate the identity management of the customer or provides by its own a solution for identity management.

***4) Secure-Service Management:***
In cloud computing environments, cloud service suppliers and service integrators compose services for their customers. The service integrator offers a platform that lets freelance service suppliers orchestrate and inter work services and cooperatively provide supplementary services that have customers’ protection needs [3].

***5) Physical and personnel security:***
The provider should assure the security of physical machines and that access to these machines as well as all relevant customer data is not only restricted but that access is documented[23].

***6) Availability:***
Customers are assured by cloud providers to have regular and predictable access to their data and applications.

***7) Application security:***
Cloud providers make sure that applications available as a service via the cloud are protected by outsourced implementation and acceptance procedures and testing of outsourced or packaged application code [23]. It also requires application security measures (application-level firewalls) to be in place in the production environment.

### 1.2 The Pros and Cons of Cloud Computing

#### 1.2.1 The Pros of Computing Cloud

Cloud computing offers the possibility of extending the information system of an enterprise at the request of the latter, according to the intended use. Services provided in the cloud are wide. Particularly, the Company may benefit from the capacity of processing information, infrastructure, storage capacity and storage as well as computer applications.

#### 1.2.2 The Cons of Cloud Computing

Cloud computing seems to promise a great future. Many people or companies are in contradiction of this notion, as the famous Richard Stallman (founder of the "Free Software Foundation") [4] who start from cloud computing as a trap.

The problem that derives up most is related security. How to guarantee the security of information stored in the cloud? More broadly Cloud Computing leads to the loss of control over the life cycle of applications.

## 2. LITERATURE SURVEY

Using the net via web based applications resources are retrieved from where they are stored. Survey on many schemes like Cipher Text-Policy ABE, Key-Policy ABE, Cipher Text Policy Attribute Set Based encryption, Hierarchical Identity primarily based encryption, Fuzzy Identity-Based Encryption, ranked Attribute-Based Encryption and ranked Attribute-Set-Based Encryption access control of outsourced data are conversed.

In [23], a survey is presented based on various encryption methods that provides security, scalable and flexible fine grained access control. Since the resources are accessed through internet the data should be protected and data signifies that the data should be protected and proper access control should be maintained. There are many encryption systems that offer security and access control in clouds that ensure that authorized user's access the data and the system. In [2], a new form of cloud computing environment that represent attribute based access control mechanism is presented. It proposes an attribute based access control instrument for cloud computing. Yan Zhu et.al [24] planned an encryption scheme, efficient temporal access control for cloud services with the assist of cryptographic integer contrasts and a proxy-based re-encryption mechanism within the current time. It also enlarges the power of attribute expression for implementing various temporal constraints.

Shucheng Yu et.al [16] paper addressed this demanding open concern by, on one hand, defining and imposing access policies supported based on attributes and on the opposite, {the data|the info|the information} owner to delegate most of the computation tasks concerned in fine-grained data access control to untrusted cloud servers while not revealing the underlying data contents. We accomplish this goal by combining techniques of attribute-based encryption (ABE), proxy re-encryption and lazy re-encryption. The proposed technique also has most important properties of user access privilege privacy and user secret key accountability.

Guojun Wang et.al [21] planned a ranked attribute-based encryption scheme (HABE) by combining a ranked identity-based encryption (HIBE) scheme and a cipher text-policy attribute-based encryption (CP-ABE) scheme. The literature encloses several explanations of cloud computing [14]. once compiling learned descriptions of cloud computing, Cancers, Lindner, Rodero-Merino, and Vaquero planned that cloud computing may well be described because the incorporation of virtual resources in step with user requirements, flexibly combining resources as well as hardware, development platforms and numerous applications to form services [17]. During a cloud computing surroundings, the user normally utilizes cloud repairs with specific functions, e.g., Salesforce.com's CRM service [15], SAP's ERP services [18], etc. The data of these services are stored on the cloud. This allows us to associate encryption/decryption cloud service to this form of business model, with the result that two service suppliers divide responsibility for information storage and data encryption/decryption.

The literature survey that continuing study of different schemes available in Attribute Based encryption(ABE) are KP-ABE, CP-ABE, Attribute-based Encryption Scheme with Non-Monotonic Access Structures, ABE and MABE. Also it includes advantage, disadvantage and a comparison table of each scheme based on fine grained access control, collusion resistant, computational overhead and efficiency.

### 2.1 Hierarchical identity-based encryption

(Boneh and Franklin, 2001) proposed an identity-based encryption (IBE) system where there is only one private key generator (PKG) to distribute private keys to each user, which is undesirable for a large network because PKG has a burdensome job [4].

Gentry and Silverberg (2002), who have been dedicated to reduce the workload on the root PKG, introduced a HIBE scheme [4]. The scheme with total collusion resistance at an arbitrary number of levels has chosen Cipher text security under the random oracle model and the Bilinear Diffiee Hellman (BDH) assumption.

A subsequent construction by Boneh and Boyen (2004) proposed a HIBE system with selective-ID security under the BDH assumption without random oracles [4].

Boneh et al. (2005) for better performance proposed an efficient HIBE system which requires only a constant length of Cipher text and a constant number of bilinear map operations during decryption.

In recent work, Gentry and Halevi (2009) proposed a fully secure HIBE scheme by using identity-based broadcast encryption with key randomization, and Waters (2009) achieved full security in systems under a simple assumption by using a dual system encryption.

### 2.2 Attribute based encryption (ABE):

An attribute based encryption scheme introduced by Sahai and Waters in 2005 is to provide security and access control. Attribute-based encryption (ABE) is a public-key based encryptions which allows users to encrypt and decrypt data based on user attributes. In which the secret key of a user and the Cipher text are dependent upon attributes (e.g. the country she lives, or the kind of subscription she has). In such a system, the decryption of a cipher text is possible only if the set of attributes of the user key matches the attributes of the cipher text. Decryption is only possible when the number of matching is at least a threshold value d. Collusion-resistance is a crucial security feature of Attribute-Based Encryption. An adversary that holds multiple keys should only be able to access data if at least one individual key grants access. The problem with attribute based encryption (ABE) scheme is that data owner needs to use every authorized user's public key to encrypt data. The application of this scheme is restricted in the real environment because it uses the access of monotonic attributes to control user's access in the system.

Sahai and Waters (2005) introduced the notion of attribute based encryption (ABE). Based on their work, Goyal et al. (2006) proposed a fine-grained access control ABE scheme, which supports any monotonic access formula. Their scheme is characterized as key-policy ABE (KP-ABE) since the private key specifies the access structure and the encrypted text describes the attributes.[1].

A subsequent construction by Ostrovsky et al. (2007) allows for non monotonic access structures [4]. Bethencourt et al. (2007) introduced a Cipher text-policy ABE (CP-ABE) scheme, private key specifies the attributes and the encrypted text describes the access structure.

Muller et al. (2008) constructed an efficient distributed Attribute - based encryption (DABE) scheme that requires a constant number of bilinear map operations during decryption, using disjunctive normal form (DNF) policy.[4] Both DABE and DNF of CP-ABE schemes provide a proof of selective security under the generic bilinear group model and the random oracle model [4].

A conjunctive fuzzy and precise identity-based encryption (FPIBE) (Wang et al.) scheme is proposed for secure data sharing in cloud servers [1]. The FPIBE achieve a flexible access control by separating the access control policy into two parts: an attribute-based access control policy [1] and a recipient identity (ID) set. Using the FPIBE scheme, a user can encrypt data by specifying an ID of recipients, or implementing a policy over access control, so that only the user whose ID belonging to the ID set or attributes filling the access control policy can decrypt the corresponding data. However, it does not address the scalability issue.

### 2.3 Key Policy Attribute Based Encryption (KP-ABE)

It is the adapted form of classical model of ABE. Users are assigned with an access tree structure over the data attributes. Threshold gates are the nodes of the access tree. The attributes are associated by leaf nodes. To reproduce the access tree structure the secret key of the user is defined. Cipher texts are labeled with sets of attributes and private keys are associated with monotonic access structures that control which cipher texts a user is able to decrypt. Key Policy Attribute Based Encryption (KP-ABE) scheme is designed for one-to-many communications.

Following four algorithms are implemented in KP-ABE:

**Setup:** Algorithmic rule takes input K as a security parameter and returns PK as public key and a system master secret key MK. The public key PK is used by message senders for encryption. Master Secret Key MK is used with user secret keys and is understandable only by authority.

**Encryption:** Algorithmic rule takes a message M, the public key PK, and a collection of attributes as input. It results the cipher text E.

**Key Generation:** Algorithmic rule takes as input an access structure T and also the master secret key MK. It results a secret key SK that enables the user to decrypt a message encrypted beneath a collection of attributes if and only if matches T.

**Decryption:** It takes as input the user’s secret key SK for access structure T and also the cipher text E, that was encrypted beneath the attribute set. This rule outputs the message M if and as long as the attribute set satisfies the user’s access structure T.

The KP-ABE scheme can achieve fine-grained access control and more flexibility to control users than ABE scheme. The problem with KP-ABE scheme is that the encryptor cannot decide who can decrypt the encrypted data. KP-ABE selects only descriptive attributes for the data, it is inappropriate in some application because a data owner has to trust the key issuer.

### 2.4 Cipher text Policy Attribute Based Encryption

Another modified form of ABE called CP-ABE introduced by Sahai. In a CP-ABE scheme, every cipher text is related to an access policy on attributes, and each user’s private key is related to a set of attributes. A user is able to decrypt a cipher text only if the set of attributes associated with the user’s private key satisfies the access policy associated with the cipher text. CP-ABE works in the reverse way of KP-ABE. The access structure of this system or algorithm, is the same method used in KP-ABE to build. And the access structure built on the encrypted data can let the encrypted data choose which key can recover the data, it means the user's key with attributes just satisfies the access structure of the encrypted data. And the concept of this scheme is similar to the traditional access control schemes. The encryptor specifies the threshold access structure for his interested attributes while encrypting a message. Based on this access structure message it is then encrypted such that only those whose attributes satisfy the access structure can decrypt it. The most existing ABE schemes are derived from the CPABE scheme.

Following four algorithms are implemented in CP-ABE:

**Setup:** This algorithm takes as input a security parameter K and returns the public key PK moreover as a system master secret key MK. the public key PK is employed by message sender for encryption and also the master secret key MK is employed to get user secret keys and is thought only to the authority.

**Encrypt:** This algorithm takes as input an access structure T, the public parameter PK, and a message M. It outputs the cipher text CT.

**Key-Gen:** This algorithm takes as input a set of attributes related to the user and the master secret key MK. It outputs a secret key SK that permits the user to decrypt a message encrypted beneath an access tree structure T if it matches T.

**Decrypt:** This algorithm takes as input the cipher text CT and a secret key SK for an attributes set. It returns the message M if and as long as satisfies the access structure related to the cipher text CT. It improves the disadvantage of KP-ABE that the encrypted data will not select who can rewrite. It will support the access control in the real setting. additionally, the user's private key during this scheme, a mix of a set of attributes, so a user only use this set of attributes to satisfy the access structure in the encrypted data. Drawbacks of the most existing CP-ABE schemes are still not fulfilling the enterprise needs of access control that need considerable flexibility and efficiency. CPABE has limitations in terms of specifying policies and managing user attributes. In a CP-ABE scheme, decryption keys only support user attributes that are organized logically as one set, that the users will only use all possible combinations of attributes in a single set issued in their keys to satisfy policies. Then cipher text - policy attribute set based encryption (CP-ASBE or ASBE for short) is introduced by Bobba, Waters et al [10]. ASBE is an extended sort of CP-ABE. It organizes user attributes into a recursive set primarily based structure and permits users to impose dynamic constraints on however those attributes may be combined to satisfy a policy. The CP-ASBE consists of algorithmic set of attributes. The challenge in constructing a CP-ASBE scheme is allowing users to combine attributes from multiple sets within a given key. There's a task for preventing users from combining attributes from multiple keys.

### 2.5 Attribute-based Encryption Scheme with Non-Monotonic Access Structures

Previous ABE schemes were limited to expressing only monotonic access structures and there is no satisfactory method to represent negative constraints in a key access formula. Ostrovsky et al. proposed an attribute-based encryption with non-monotonic access structure in 2007. Non-monotonic access structure can use the negative word to describe every attributes in the message, but the monotonic access structure cannot.

This scheme contains four algorithms:

**Setup(d):** In the construction of basic, a parameter d specifies what number of attributes each cipher text has.

**Encryption (M, ¥ã, PK):** To encrypt a message M ¥å GT under a set of d attributes ¥ã C Zp, choose a random values s ¥å Zp and output the cipher text E.

**Key Generation (A, MK, PK):** This algorithm outputs a key D that enables the user to decrypt an encrypted message only if the attributes of that cipher text satisfy the access structure.

**Decrypt(CT, D):** Input the encrypted data CT and private key D, if the access structure is satisfied it generates the original message M. It enables non-monotonic policy, i.e. policy with negative attributes.

The problem with Attribute-based Encryption Scheme with Non-Monotonic Access Structures is that there are numerous negative attributes in the encrypted data, but they don't narrate it. It means that each attribute adds a negative word to describe it, but these are useless for decrypting the encrypted data. It can cause the encrypted data overhead becoming vast. It is inefficient and complex. Each cipher text needs to be encrypted with d attributes, where d is a system-wise constant.

## 3. COMPARATIVE ANALYSIS IN BETWEEN THE DIFFERENT APPROACHES

### 3.1 Decryption and Re encryption

The Decryption and Re encryption process analyzed with several approaches is shown in following figure.

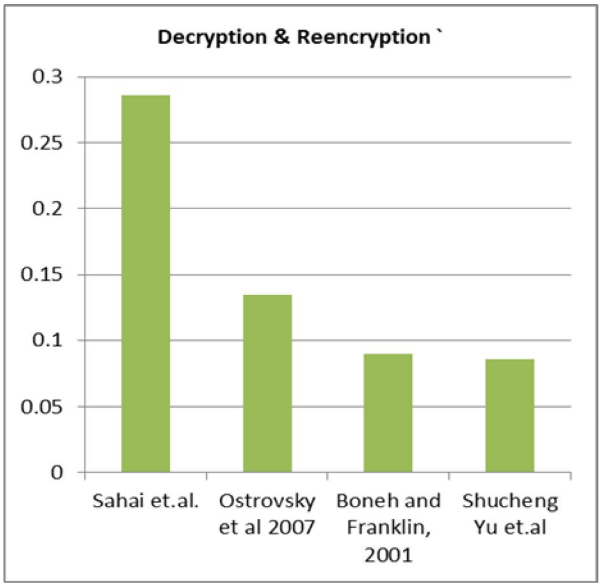

**Figure : 1. Decryption and Reencryption analysis in between the different approaches.**

The decryption and re-encryption process has applied in several approaches and all the values in table.

### 3.2 Time Cost

The Time Cost process analyzed with several approaches is shown in following figure. The Time Cost of the several approaches is analyzed, the Shucheng et.al is better than the other approaches.

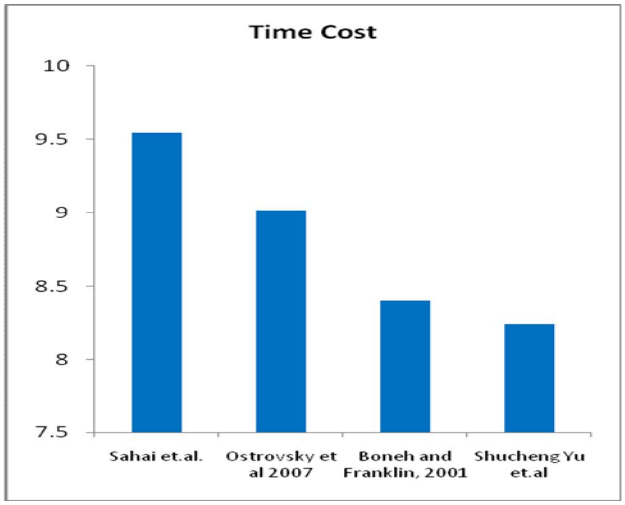

**Figure :2. Time Cost analysis in between the different approaches.**

The Sahai et.al and Ostrovsky et.al is also nearly same time cost values.

### 3.3 Analysis with the Different Approaches

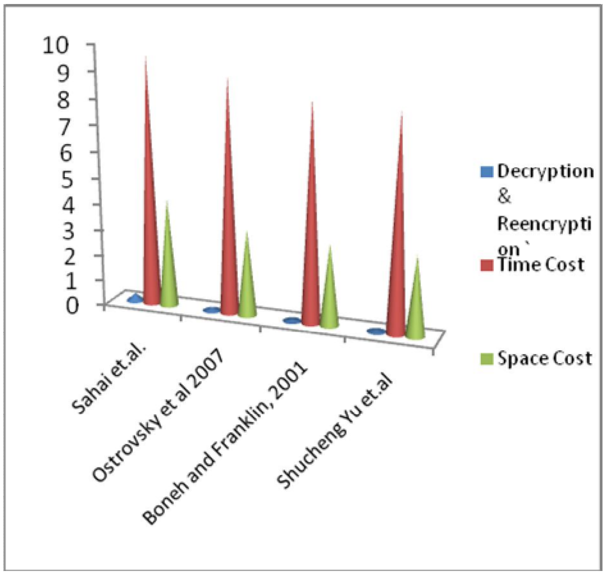

**Figure :3. Comparison of Metrics of different approaches.**

.

The figure also explains the different approaches with the metrics like decryption & Re encryption, Time Cost and Space cost.

## 4. CONCLUSION

In this work we have overviewed different attributes based encryption (ABE) schemes that can be used in cloud systems for adaptable, scalable and security access control. In ABE scheme, both the ‘secret key’ and ‘cipher text’ are associated with a set of attributes. ABE is further modified into KP-ABE that provides fine grained access control. In KP-ABE, attribute policies are associated with keys and data is associated with the attributes. Keys associated with the policy that is satisfied by the attributes can decrypt the data. Moreover, we have explored CP-ABE and CP-ASBE. The CP-ABE scheme differs from KP-ABE in such a way that in CP-ABE, Cipher text is associated with an ‘access tree structure’ and each user ‘secret key’ is embedded with a ‘set of attributes’. Attribute policies are associated with the data and attributes are associated with keys and only those keys that the associated attributes satisfy the policy associated with the data are able to decrypt the data. HASBE combines the functionalities of HIBE and ASBE. HASBE scheme seamlessly incorporates a hierarchical structure of system users. It uses a delegation algorithm to ASBE. Out of these schemes, the HASBE scheme provides more flexible, scalable and fine-grained access control than any other schemes in cloud computing.

## REFERENCES

[1] R. Sterritt, “Autonomic computing,” Innovations in Systems and Software Engineering, vol. 1, no. 1, Springer, pp. 79-88. 2005.

[2] V. Goyal, O. Pandey, A. Sahai, and B.Waters”Attribute-based encryption for fine-grained access control of encrypted data," in Proceedings of the 13th ACM conference on Computer and communications security, pp. 89-98, 2006.

[3] M. Pirretti, P. Traynor, P. McDaniel, and B. Waters. “Secure attribute-based systems”. In Proceedings of the 13th ACM conference on Computer and communications security, pages 99-112. ACM Press New York, NY, USA, 2006.

[4] J.Bettencourt, A. Sahai, and B.Waters”Ciphertext-policy attribute based encryption “in Proceedings of IEEE Symposium on Security and Privacy, pp. 321-334, 2007.

[5] R. Ostrovsky and B. Waters.“Attribute based encryption with nonmonotonic access structures”.In Proceedings of the 14th ACM conference on Computer and communications security, pages 195-203. ACM New York, NY, USA, 2007.

[6] D. Benslimane, S. Dustdar, and A. Sheth, "Services mashups: the new generation of web applications". IEEE Internet Computing, vol. 12, no. 5, pp. 13–15, 2008.

[7]Muller, S. Katzenbeisser, and C.Eckert, “Distributed attribute-based encryption," in Proceedings of ICISC, pp. 20-36, 2008.

[8]R. Buyya, C. S. Yeo, S. Venugopal, J. Broberg, and I. Brandic, “Cloud computing and emerging IT platforms: vision, hype, and reality for delivering computing as the 5th utility,” Future Generation Computer Systems, vol. 25, issue 6, pp. 599-616, June 2008.

[9]L. M. Vaquero, L. Rodero-Merino, J. Caceres, and M. Lindner, “A break in the clouds: towards a cloud

definition," ACM SIGCOMM Computer Communication Review, vol. 39, no. 1, pp. 50-55, January 2009.

[10]RakeshBobba, HimanshuKhurana and ManojPrabhakaran, "AttributeSets: A Practically Motivated Enhancement to Attribute-Based Encryption", July 27, 2009

[11]R. Kandukuri, V, R. Paturi and A. Rakshit, "Cloud security issues," in Proceedings of the 2009 IEEE International Conference on Services Computing, pp. 517-520, September 2009.

[12]Salesforce.com, Inc., "Force.com platform," Retrieved Dec. 2009, from http://www.salesforce.com/tw/.

[13]SAP AG., "SAP services: maximize your success," Retrieved Jan. 2010, from http://www.sap.com/services/index.epx.

[14]S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving secure, scalable, and fine-grained data access control in cloud computing," in Proc. IEEE INFOCOM 2010, 2010.

[15]A. B. Lewko, T. Okamoto, A. Sahai, K. Takashima, Waters, "Fully secure functional encryption: Attribute based encryption and (hierarchical) inner product encryption," in Proc.EUROCRYPT, 2010, pp. 62–91

[16]Shucheng Yu, Cong Wang, KuiRen, and Wenjing Lou," Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing", INFOCOM10.

[17]B. Waters, "Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization," in Proc. Public Key Cryptography, 2011, pp. 53–70.

[18]T. Okamoto and K. Takashima, "Fully secure functional encryption with general relations from the

[19]M. Green, S. Hohenberger, and B. Waters, Outsourcing the decryption of ABE ciphertexts," in Proc. USENIX Security Symp, San Francisco, CA, USA, 2011.

[20]M. Bellare and P. Rogaway, "Random oracles are practical: A paradigm for designing efficient protocols," in Proc. ACM Conf. Computer and Communications Security, 1993, pp. 62–73.

[21]Guojun Wang, Qin Liu, JieWub, MinyiGuo,"Hierarchical attribute-based encryption and scalable user revocation for sharing data in cloud servers", Jul 1, 2011.

[22]ChittaranjanHota, Sunil Sanka,"Capability-based Cryptographic Data Access Control in Cloud Computing", Int. J. Advanced Networking and Applications, Volume: 03; Issue: 03; Pages: 1152-1161 (2011).

[23]V Bozovic, D Socek, R Steinwandt, and V. I. Villanyi, "Multiauthority attribute-based encryption with honest-but-curious central authority" International Journal of Computer Mathematics, vol. 89, pp. 3, 2012.

[24]Q. Liu, G. Wang, and J. Wu, "Time based proxy re-encryption scheme for secure data sharing in a cloud environment," Information Sciences .In Press, 2012.

[25]A. Sahai and B. Waters, "Fuzzy identity-based encryption," inProc.EUROCRYPT, 2005, pp. 457-473

[26]G. Wang, Q. Liu, and J.Wu, "Hierachicalattibute-based encryption for fine-grained access control in cloud storage services," in Proceedings of the 17th ACM conference on Computer and communications security.

[27]Ding, W. and Marchionini, G. 1997 A Study on Video Browsing Strategies. Technical Report.University of Maryland at College Park. Computing

[28]K.Priyadarsini, C.Thirumalaiselvan,"A Survey on Encryption Schemes for Data Sharing in Cloud Computing", (IJCSITS), ISSN: 2249-9555, Vol. 2, No.5, October 2012.

[29] Neena Antony, A. Alfred Raja Melvin," A Survey on Encryption Schemes in the Clouds for Access Control", International Journal of Computer Science and Management Research Vol 1 Issue 5 December 2012.

[30]Abdul RaoufKhan,"Access Control in Cloud Computing Environment", ARPN Journal of Engineering and Applied Sciences, Vol. 7, No. 5, May 2012 ISSN:1819-6608.

[31]Yan Zhu, HongxinHuy, Gail-JoonAhny, DijiangHuangy, and Shanbiao Wang," Towards Temporal Access Control in Cloud Computing", INFOCOM 2012.

[32]Miss. Rehana Begum, Mr. R.Naveen Kumar, Mr. VoremKishore,"Data Confidentiality Scalability and Accountability (DCSA) in Cloud Computing ", Volume 2, Issue 11, November 2012.

[33] V.Suma, K.VijayKuma,"An Efficient Scheme For Cloud Services Based On Access Policies", International Journal of Engineering Research & Technology (IJERT),Vol. 1 Issue 8, October – 2012,ISSN: 2278-0181.

[34] Zhiguo Wan, Jun'e Liu, and Robert H. Deng, Senior Member, IEEE."A Hierarchical Attribute-Based Solution for Flexible and Scalable Access Control in Cloud Computing ",IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 7, APRIL 2012

**Author Profile**

**Mrs. S. Artheeswari** is working as Assistant Professor in Mailam Engineering College, Mailam, Tamilnadu. She has 8 years of experience in academic field. She completed her Bachelor of Technology(IT) in Madras University and Master of Engineering(CSE) in Anna University. Now, doing as a Research Scholar in Annamalai University in the field of Computer Science. Her area of Interest includes Cloud computing, Data Structures, Security and Database Management System. She also has life member for several association and society.

**Dr. RM. Chandrasekaran** is currently working as a Professor, Department of Computer Science & Engineering and also jointly as Director, Directorate of Distance Education. Annamalai University. He obtained his Bachelor of Engineering in Computer Science and Master of Engineering from Anna University and Master of Business Administration from Annamalai University. Completed his PhD in Computer Science from Annamalai University, Annamalainagar, India. He has 23 years of teaching experience and 5 years of experience in Research & Development. He also worked as a Registrar in Anna University, Trichy for 3 Years. He worked as software consultant in USA. Also, he has co-organized two Workshops and two conferences. His area of interest includes Computer Algorithms, Text Data Mining and Software Metrics. He published 10 papers in National Journal and 10 papers in International Journals. He also published many papers in national and international conferences.