ISSN 2320-9984

Volume 5 Issue 1 | March 2017

ISSN: 2320-9984 (Online)

International Journal of Modern Engineering & Management Research

Website: www.ijmemr.org

Fuzzy & Attribute Identity Encryption Schemes with Non Monotonic Structures in Cloud Computing – A Comprehensive Study

Himani Tiwari
M. Tech. Research Scholar
Takshshila Institute of Engineering & Technology
Jabalpur (M.P.), [INDIA]
Email:himani.tiwari03@gmail.com

Abhishek Pandey
Assistant Professor
Department of Computer Science Engineering
Takshshila Institute of Engineering & Technology
Jabalpur (M.P.), [INDIA]
Email: abhishekpandey@takshshila.org

Abstract—*An Attribute-Based Encryption (ABE) scheme that allows a user's private key to be expressed in terms of any access formula over attributes. Previous ABE schemes were limited to expressing only monotonic access structures. We provide a proof of security for our scheme based on the Decisional Bilinear Diffie-Hellman (BDH) assumption. In several distributed systems a user should only be able to access data if a user posses a certain set of credentials or attributes. Currently, the only method for enforcing such policies is to employ a trusted server to store the data and mediate access control. Attribute-Based Encryption (ABE) is a new paradigm where such policies are specified and cryptographically enforced in the encryption algorithm itself. Cipher text-Policy ABE (CP-ABE) is a form of ABE where policies are associated with encrypted data and attributes are associated with keys. A new form of CP-ABE - which, unlike existing CP-ABE schemes 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.*

Keywords:—*Attribute-based encryption, Identity-based encryption, Cloud computing, Encryption schemes, Cloud services.*

1. INTRODUCTION

Lots of distributed file and information systems require complex access-control mechanisms, where access decisions depend upon attributes of the protected data and access policies assigned to users. Traditionally, such access-control mechanisms have been enforced by a server that acts as a trusted reference monitor; the monitor will allow a user to view data only if his access policy allows it.

In many situations, when a user encrypts sensitive data, it is imperative that she establish a specific access control policy on who can decrypt this data. For example, suppose that the FBI public corruption offices in Knoxville and San Francisco are investigating an allegation of bribery involving a San Francisco lobbyist and a Tennessee congressman.

There are different types of clouds based on their location:

Public Cloud : A public cloud is one in which the services and infrastructure are provided off -site over the Internet. Standardized workload for applications is used by lots of people, such as e -mail. Need to test and develop application code. It has SaaS (Software as a Service) applications from a vendor who has a well-implemented security strategy. Need incremental capacity (the ability to add computer capacity for peak times).

Private Cloud : A private cloud is one in which the services and infrastructure are maintained on a private network. Therefore, control and security are inevitable. Business is part of an industry that must conform to strict security and data privacy issues. Company is large enough to run a next generation cloud data center efficiently and effectively on its own.

Community Cloud : The benefits of a public cloud are multi-tenancy and pay-as- you-go billing structure. The community cloud uses all these benefits as well as the private cloud features such as privacy, security and policy compliance. The community cloud can governed by the participating organizations or by a third-party managed service provider (MSP).

Hybrid Cloud : A type of cloud that has multiple service providers with a variety of features of the other two clouds. This is the most efficient platform to keep the data for a company that use a SaaS application but is concerned about security. The SaaS dealer can create a private cloud just for a company inside their firewall. They can provide with a virtual private network (VPN) for more security.

The encryption is the method used to convert the data over the network in a non-readable format as well as will be accessible by the users authorized to it. The encryption is done based on the keys used to encode the message. Based on that there are two types of encryption scheme:

1. Public key encryption
2. Private key encryption

All the encryption schemes available now falls in either of these two categories. The public key encryption scheme uses key pairs for the encoding of the message. It uses the receiver's public key to encode the data and the same could be decoded with the receiver's private key which is known only to the owner. Whereas in the latter only a single key is used for both encryption as well as decryption. The cryptographic technologies are used in the cloud computing in order to secure the data getting tampered from the unauthorized accesses. So the data is encrypted before it is uploaded to the cloud. Only the authorized users will be able to decrypt and download the file. The main security goals of any system include the following:

Confidentiality: ensures that the authorized users will be only able to access the files.

Integrity: ensures that the data sent by the sender is same as that received by the receiver

Authentication: Verify the identity of the entities that communicate over the network.

Non-repudiation: Assures that a party in a communication cannot falsely deny that a part of the actual communication occurred.

2. LITERATURE SURVEY

ABE Scheme Concluded **-**In showing how to construct an Attribute-Based Encryption system with non-monotone access formulas, we begin by describing a "core" construction, in which the we assume that every cipher text is annotated with exactly d attributes.

Ciphertext-Policy Concluded-In this research paper author created a system for Ciphertext-Policy Attribute Based Encryption. Our system allows for a new type of encrypted access control where user's private keys are specified by a set of attributes and a party encrypting data can specify a policy over these attributes specifying which users are able to decrypt. Our system allows policies to be expressed as any monotonic tree access structure and is resistant to collusion attacks in which an attacker might obtain multiple private keys. Finally, we provided an implementation of our system, which included several optimization techniques.

Motivated Enhancement Concluded-Attribute -Based Encryption (ABE) ushers in a new paradigm where such policies are specified and cryptographically enforced in the encryption algorithm itself. Existing ABE schemes come in two complimentary forms, namely, Key-Policy ABE (KP-ABE) schemes and Ciphertext-Policy ABE (CP-ABE) schemes. In KP-ABE schemes [11, 12, 14, 16], as the name indicates, attribute policies are associated with keys and data is annotated with attributes. Only those keys associated with a policy that is satisfied by the attributes annotating the data are able to decrypt the data. In CP-ABE schemes [2, 6, 10, 13], on the other hand, attribute policies are associated with data and attributes are associated with keys.

Motivation-The ability to group attributes into sets and to frame policies that can selectively restrict the decrypting key to use attributes belonging to the same set is a powerful feature more than one might realize initially. In this section we illustrate its versatility by solving various problems in different contexts which did not have any reasonably efficient solutions prior to this.

Evaluation-In this section we discuss the efficiency of CP-ASBE scheme instantiated with two levels, describe its implementation and evaluate its performance overhead relative to BSW CP-ABE.

Efficiency. It is straightforward to estimate the efficiency of our key generation and encryption algorithms. In terms of computation, our key generation algorithm requires two exponentiations for every attribute in the key issued to the user and two exponentiations for every set (including recursive sets for a scheme with levels > 2) in the key.

Time Require for Encryption-In this graph time require for encryption by proposed system are shown. It shows that reduction in time and since using Rijndael algorithm encryption process is to strong.[17]

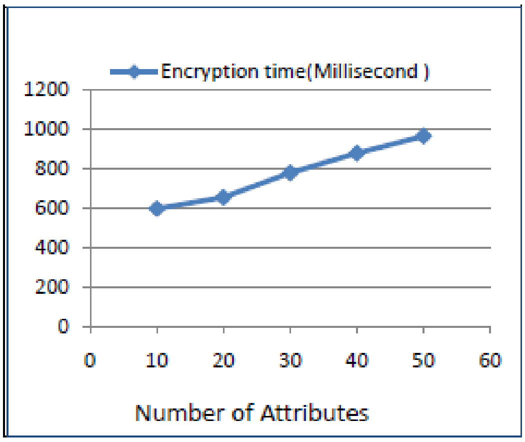

Figure 1. Time required by Rijndael in the Proposed Hierarchical CP-ABE system

Time require for Decryption-In this graph time require for decryption by proposed system figure 5.2 where user's private key which is generated on the based attribute assigned to user. So while decryption process no need to decrypt all attribute so it require less time than existing system.[17]

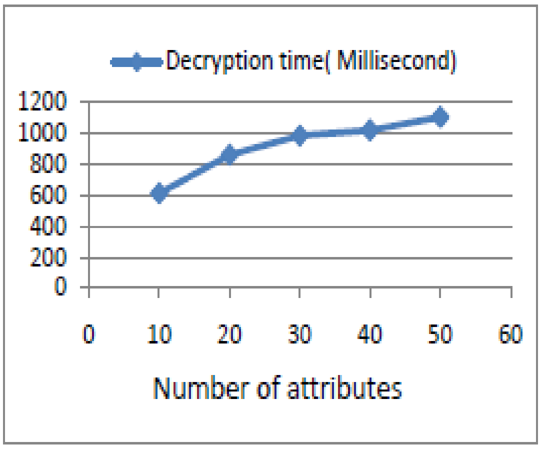

Figure 2. Time required to decrypt attributes by the Proposed Hierarchical CP-ABE System

3. ENCRYPTION SCHEMES

Attribute based Encryption (ABE)

The attribute based encryption is a one to many public key encryption technique[15][16] which performs encryption and decryption based on some user attributes that are selected by the one who performs encryption form the attribute set. In this scheme the secret key as well as the cipher text are dependent upon attributes. A user will be able to decrypt the cipher text only when user key matches with the attributes of the cipher text [2].The encryption schemes that comes under the mentioned one are listed below:

Key-Policy Attribute Based Encryption (KP-ABE) Capable of sharing data for users in the cloud in an enterprise environment. Also, it can be used to achieve proxy re-encryption[4]. This scheme uses the property of hierarchical generation of keys in HIBE scheme to generate keys.

Multi-Authority Attribute Based Encryption (MA-ABE)

The scheme uses multiple parties to distribute attributes for users [2]. The system is composed of one central authority and K attribute authorities and the attribute authority is also assigned with a value dk. It consists of many authorities to manage the attributes and the distribution of the secret keys. The user who wish to download the information will request

Identity Based Encryption (IBE)

This is a modified version of classical ABE[3]. Here users are assigned with an access tree structure over the data attributes. The nodes of the access tree represents the threshold gates. The leaf nodes denote the attributes. The cipher texts are marked with set of attributes whereas the private keys are associated with monotonic access structures which decides which all users will be able to decrypt the cipher text. The scheme is designed for one -to-many communications. In a KP-ABE scheme, cipher texts are labelled with sets of attributes and access policies over these attributes are associated with users' private keys.

Cipher Text Policy Attribute *Based Encryption (CP-ABE)*- CP- ABE[3] is also a modified form of the classical ABE. In this scheme, every users' private key is associated with a set of attributes and every cipher text is associated with an access policy. The decryption of the cipher text is possible only when the set of attributes associated with the users' private key satisfies the access policy associated with the cipher text. The access structure of the scheme inherits the same method used in the KP-ABE scheme. The access structure provides the encrypted data decide which key can recover the data. The encryptor is the one who can set the access controls while encrypting a message. Currently, most existing ABE schemes are derived from CP-ABE schemes.

Attribute-based Scheme with Non- Monotonic Access Structures

The prior ABE methods fail to express monotonic access structures and there are no particular methods to represent negative constraints in a key's access formula. This method can use negative word to define every attribute in the message, whereas the monotonic access structure cannot[7]. It enables non-monotonic policy which is the policy with negative attributes.

Hierarchical attribute-based Encryption-

The scheme satisfies properties such as fine grained access control[11], full delegation and scalability. The method is the decryption keys from the attribute authority.

IBE is a public key encryption system which uses an arbitrary string as the public key [8]. The security demand is semantic security against an adaptive chosen cipher text attack. No polynomial bound adversary wins the following game with non-negligible advantage. The sender who has access to the public parameters of the system can encrypt a message.

Hierarchical Identity Based Encryption (HIBE)

It has two level scheme [6], that consists of a root private key generator (PKG), users and domain PKGs, which all are associated with the primitive Ids (PIDS) which are arbitrary strings. The scheme also includes a trusted third party and allows a hierarchy of certificate authorities: the root certificate authority will issue certificates for other certificate authorities, who can in turn issue certificates for users in their respective domains.

Hierarchical Attribute Set Based Encryption (HASBE)

In HASBE, fine grained access control in cloud storage services is obtained by combined hierarchical identity based encryption(HIBE) and CP-ABE. It follows a hierarchical structure to the scheme. HASBE[5] being an extension of cipher-text attribute set-based encryption (ASBE)[9] derives the features such as access control and flexibility.

Homomorphic Encryption

The method [13] allows computations on the cipher text to get the encrypted result. When the same is decrypted, the result will be a set of computations that are applied on the plain text. It allows the chaining of different services without exposing the data to each other. The fully homomorphic scheme is built upon the lattice cryptography[14].

3. PROOF OF SECURITY

We prove that the security of our main construction in the attribute-based selective-set model reduces to the hardness of the Decisional BDH assumption.

Bettencourt, Sahai and Waters [3] proposed two methods that are derived from attribute based encryption based on the difference in the deployment. Both works with the same algorithms as in the case of attribute based encryption. The algorithm has four phases as explained in the previous method. Setup, Encryption, Key Generation and Decryption. The key policy based attribute based encryption scheme can attain fine-grained access control and flexibility than ABE. The drawback with the scheme is that the encrypt or cannot decide who can decrypt the encrypted data. The same is unsuitable for some application as the data owner need to trust the key issuer.

With the case of cipher text policy based attribute based encryption, the scheme overcomes the drawbacks of KP- ABE ie, the encrypted data could choose who can decrypt. The user’s private key is a combination of a set of attributes. The flaws of the existing CP-ABE schemes are not fulfilling the enterprise requirements of the access control that need efficiency and flexibility. In CP-ABE decryption keys only support user attributes that are organized logically as a single set so that users could use all the possible combinations of the same. The CP-ASBE consists of recursive set of attributes. There is challenge for preventing users from combining attributes from multiple keys.

R. Ostrovsky and B. Waters [7] proposed another ABE scheme with non- monotonic access structure. The can use negative word to define every attribute in the message, whereas the monotonic access structure cannot. The mentioned scheme being ABE works as same as the classical ABE scheme consisting of the four algorithms. Being non monotonic ABE the encryption phase as well as the decryption phase are slightly different from that of the classical ABE. In the encryption phase, rather than taking the access structure as input the algorithm takes non-monotonic access structure as input. And in the decryption phase, the plain text is derived from the cipher text based on the same non-monotonic access structure.

The problem with ABE scheme over non - monotonic access structures is that there are many negative attributes in the encrypted data. It can cause the encrypted data overhead to huge. It is inefficient and complex that each cipher text needs to be encrypted with d attributes, d is a system-wise constant.

Wang et al.[8] proposed the hierarchical attribute based encryption in which it uses the property of hierarchical generation of keys. Also, it can be used to achieve proxy re-encryption[4]. Proxy re-encryption schemes are the cryptosystems that are used to alter the cipher text that has been encrypted by one user so that the same could be decrypted by another user. The method employs two algorithms instead of key generation. The algorithms are Setup, Create domain masters, Create users, Encryption and Decryption. But the same is impractical to implement. As all of the attributes in one conjunctive clause in this scheme may be managed by the same domain authority, the same attribute may be managed by multiple domain authorities.

V Bozovic, D Socek, R Steinwandt, and Vil-lanyi [2] proposed Multi-Authority Attribute Based Encryption in which the scheme employs the following algorithms. Setup, Attribute Key Generation, Central key generation, Encryption and Decryption. The setup algorithm is a randomized algorithm run by a third party and it gives a master key as output. In the attribute key generation phase the secret key is generated as output taking the users' GID, the authority's value dk and a set of attributes in the authority's domain and the randomized algorithm is run by the attribute authority.

Y. Reng and D. Gu [6] has put forward another identity based encryption method ie, hierarchical identity based encryption. In a 2-HIBE, users retrieve their private keys from their domain PKG. It can compute the private key of any user in their domain. The scheme also includes a trusted third party and allows a hierarchy of certificate authorities: the root certificate authority will issue certificates for other certificate authorities, who can in turn issue certificates for users in their respective domains.

The scheme comprise of four algorithms. The first phase is the Setup phase in which the algorithm which takes random parameter as input and give master key and public parameters. The next phase is the key generation phase to generate private key for the identity it takes the public parameters and a random number from the integer set. The next phase being the encryption phase, the algorithm takes the parameters, identities as well as the message as input to give the cipher text as output. The decryption phase takes private key as well as the cipher text as input to give the plain text as output. HIBE is a scheme that has good efficiency and access control compared to IBE. But it is high in case of computational overhead.

Z. Wan, J. Liu, and R. H. Deng [5] introduced the concept of Hierarchical Attribute Set Based Encryption which combines the concept of the HIBE as well as CP-ABE schemes. It comprises of five types of parties: data owners, data consumers, a cloud service provider, a number of domain authorities and a trusted authority. Cloud service provider is to provide a data storage service. Data owners will encrypt their data files and store them in the cloud. Data consumers will download the encrypted data files to access shared data files. Each domain authority is responsible for managing the data owners/consumers in its domain or the domain authorities at the next level. Root authority is the trusted authority and is responsible for managing top-level domain authorities. ASBE's capability of assigning more values to the same attribute enables it to solve the user revocation problem efficiently, which is not capable in CP-ABE.

C Fontaine, F Galand [13] discusses about homomorphic encryption. Homomorphic encryption is the encryption scheme which is used to apply operations on the encrypted data. It can be applied in any system by using various public key algorithms. The Homomorphic encryption is a scheme with four functions. It can be represented as H = {Key Generation, Encryption, Decryption, Evaluation}. Key generation is used to generate a key pair of secret key and public key used for the encryption of the plain text. Encryption and decryption phases works as normal. Evaluation is used by the server which has a function f to evaluate the cipher text using the public key pk.

The above desirable feature and the recursive key structure is implemented by four algorithms: Setup phase takes the depth of the key as the input to provide the public key and the master key as the output. The next phase is the keygen phase which take the identity, the master key and the key structure as the input to give the secret key for the user as the output. The encryption and decryption phases work as is that is for providing the cipher text and the plain text respectively. The HASBE scheme can easily and efficiently manage the user revocation as it employs multiple values for access expiration time. The scheme is easily scalable due to the hierarchical structure whereas on the other hand, the computation overhead is high as the data decryption keys are disclosed only to authorized keys.

There are many encryption schemes that come under the Homomorphic encryption. The various schemes include Paillier, RSA, BGV encryption scheme, Gorti's Enhanced Homomorphic Cryptosystem (EHC), Non-interactive Exponential Homomorphic Encryption Scheme [NEHE], Algebra Homomorphic Encryption Scheme Based On Updated ElGamal (AHEE) etc. Paillier can be used for preserving the additive property of homomorphic encryption while ElGamal and RSA can be used for multiplicative property. Each of the above mentioned schemes could be used in various applications like-voting system, Banking, For the security of integer polynomials, Efficient Secure Message Transmission in Mobile Ad Hoc Networks, Active networks and e-commerce based on mobile agent, electronic voting and mobile cipher respectively.

Sahai [4] proposed the supposition of IBE based on Fuzzy Logic and named fuzzy Identity-Based Encryption, which permits tolerance of fault among the distinctiveness of a private and the public keys, they gave realistic uses of Fuzzy-IBE of encryption in the area biometrics and ABE.

The proposed scheme that uses the concepts of distance metrics & Bilinear Decisional Diffie-Hellman supposition. This was most suitable schemes to ways data access manage in public clouds for it can assurance data owners' direct control over their data and provide a fine-grained access control service.

Amit [9], developed a structure for CP-ABE. The developed system permits for a novel kind of encrypted way in manage where client's private keys are précised by a set of elements and a party encrypting data can identify a strategy over these elements indicating which users are proficient to decrypt. The developed system permits policies to be articulated as any monotonic tree access configuration and is anti to conspiracy attacks in which an assailant might gain manifold private keys. as a final point, they made available an accomplishment of there system, which incorporated more than a few optimization skills.

Bobba,[12] proposed Ciphertext Policy Attribute Set Based Encryption (CP-ASBE), an extended version of conventional CP-ABE. which, distinct existing CP-ABE schemes that signify customer elements as a monolithic set in keys, systematize user element into a recursive set based structure and allows users to inflict dynamic restraints on how those attributes may be pooled to gratify a strategy. According to CP-ASBE,

a. Client characteristics are ordered into a recursive ancestors of sets.

b. strategies that can selectively confine decrypting the clients to use characteristics from contained by a solitary set or permit them to merge characteristics from manifold sets.

4. COMPARISON OF ENCRYPTION SCHEMES

In the schemes mentioned above, the Attribute-based methods are widely used. The attribute based encryption are easy to implement and it can efficiently handle the complex cipher texts easily. The comparative study of all the encryption schemes used in cloud computing is given in Table I. The least commonly used scheme is the identity based one. As it is based on identities the mentioned one cannot efficiently handle the encryption. In the case of the attribute based scheme the encryption is based on the access policy that is derived from the attribute list set by the sender. HASBE is not commonly used as it is difficult to implement.

5. CONCLUSIONS AND FUTURE DIRECTIONS

The paper are presents a survey on various encryption techniques used in cloud computing. Most of the above mentioned methods has their roots either in the identity based encryption or attribute based encryption. Identity based encryption is not much used now a days. cipher text length as well as the same is easy to implement.

We presented the first Attribute-Based Encryption system that supports the expression of non-monotone formulas in key policies. We achieved this through a novel application of revocation methods into existing ABE schemes. In addition, the performance of our scheme compares very favorably to that of existing, less-expressive ABE systems.

An important goal in ABE systems is to create even more expressive systems. Our work took a significant step forward by allowing key policies that can express any access formula. Eventually, we would like to have systems that can express. CP-ASBE a form of CP-ABE that organizes user attributes into a recursive family of sets and allows users to impose dynamic constraints on how attributes may be combined. We demonstrated how CP-ASBE can naturally support compound attributes, and numerical attributes with multiple value assignments. We showed that it achieves this versatility with very little overhead through efficiency analysis and performance evaluation of a prototype implementation any access circuit.

Other directions for future work are the design of efficient CP-ASBE schemes that are secure in the standard model and extending CP -ASBE to a multi-authority setting.

Table 1 : Comparative Study of Encryption Scheme

Sr. No.	***Encryption schemes***	***Features***	***Advantages***	***Disadvantages***
1.	ABE[1]	Main goal to achieve security and access control, Encryption based on attributes set by the sender	Collusion resistance – security feature, Easy to implement	The data owner use authorized public key for encryption, The application of the scheme is restricted in the real environment, High computational overhead
2.	KP-ABE[3]	Modified classical ABE, for one-to-many communications	Gain fine grained access control and flexible than ABE, Monotonic access structures-enables the encrypt or to decide who can decrypt the data	unsuitable for some application as the data owner need to trust the key issuer, Low access control and high computational overhead
3.	CP-ABE[3]	Private key is associated with a set of attributes, Cipher text is associated with access policy	Better than ABE and KP-ABE, Encrypt or can decide who can decrypt the data, Encrypt or can set the access controls over the encrypted data	Not suitable to meet enterprise requirements, Challenge: preventing users from combining attributes from multiple keys
4.	ABE with Non-monotonic Access structures[7]	Can use negative words to define attributes in the message	It enables non-monotonic Policy	cause encrypted data overhead due to too many negative words

Table 2: Comparative Study Comparison of Different Encryption Scheme

Technique	ABE	CP-ABE	CP-ASBE
Access Control	Very Low	Average Realization of complex access Control	Higher than CP-ABE, ABE
Efficiency	Medium	Average Not efficient for modern environments	Better than CP-ABE Less collision Atta cks
Computational Overhead	Very Low	Average	Lower Than CP-ABE

REFERENCES:

[1] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attibute-based encryption for fine-grained access control of encrypted data," in Proc. ACM Conf. Computer and Communications Security (ACM CCS), Alexandria, VA, 2006.

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

[3] J. Bettencourt, A. Sahai, and B.Waters "Ciphertext-policy attribute based encryption" in Proceedings of IEEE symposium on Security and Privacy, pp. 321V334, 2007.

[4] 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.

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

[6] Yanli Ren and Dawu Gu, "Efficient Hierarchical Identity Based Encryption Scheme in the Standard Model" in Proc. Informatica 32 (2008),pp 207?211.

[7] 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 195203. ACM New York, NY, USA,2007.

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

[9] R. Bobba, H. Khurana, and M. Prabhakaran, "Attribute-sets: A practically motivated enhancement to attribute-based encryption," in Proc. ESORICS, Saint Malo, France, 2009.

[10] A. Sahai and B. Waters, "Fuzzy identity based encryption," in Proc. Advances in Cryptology-Eurocrypt, 2005, vol. 3494,LNCS, pp. 457?473.

[11] Adi Shamir. Identity-based cryptosystems and signature schemes. In Proceedings of CRYPTO 84 on Advances in cryptology,pages 47?53. Springer-Verlag New York, Inc.,1985.

[12] 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, pp. 534-542.

[13] Fontaine C, Galand F. "A survey of homomorphic encryption for non specialists". EURASIP Journal on Information Security 2007. 2007 Jan; 1?15

[14] Daniele Micciancio, Oded Regev, "Lattice-based Cryptography", Jul 2008

[15] Mr. Anup R. Nimje, "Attribute-Based Encryption Techniques in Cloud Computing Security : An Overview", International Journal of Computer Trends and Technology- volume4Issue3 - 2013,http://oaji.net/articles/2015/2028-1433398925.pdf

[16] R.Nitya Lakshmi, "Analysis of Attribute Based Encryption Schemes", International Journal of Computer Science and Engineering Communications Vol.3, Issue 3, 2015, http://www.ijcttjournal.org/Volume4/issue-3/IJCTT-V4I3P143.pd

[17] Secure Data Retrieval based on Attribute-based Encryption in Cloud Chaudhari Swapnil H. (Student) B.R Associate Professor SSVPS's BS Deore College of Engineering, Dhule, 424005, India