International Journal of Research
Available at https://edupediapublications.org/journals

e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue 12
April 2018

Cloud based Hierarchical Multi User Data Shared Attribute based Encryption

[1]K. Praveena. [2]K. Sai Pranay, [3]P. Anil Kumar, [4]D. Prathyusha
[1]Assistant Professor, [2,3,4]B.Tech,
[1,2,3,4]Department of Computer Science and Engineering,
[1,2,3,4]Vignan Institute of technology and Science.

ABSTRACT

With the thriving growth of the cloud computing, the security and privacy concerns of outsourcing data have been increasing dramatically. However, because of delegating the management of data to an untrusted cloud server in data outsourcing process, the data access control has been recognized as a challenging issue in cloud storage systems. One of the preeminent technologies to control data access in cloud computing is Attribute-based Encryption (ABE) as a cryptographic primitive, which establishes the decryption ability on the basis of a user's attributes. This paper provides a comprehensive survey on attribute-based access control schemes and compares each scheme's functionality and characteristic. We also present a thematic taxonomy of attribute-based approaches based on significant parameters, such as access control mode, architecture, revocation mode, revocation method, revocation issue, and revocation controller. The paper reviews the state-of-the-art ABE methods and categorizes them into three main classes, such as centralized, decentralized, and hierarchal, based on their architectures. We also analyzed the different ABE techniques to ascertain the advantages and disadvantages, the significance and requirements, and identifies the research gaps. Finally, the paper presents open issues and challenges for further investigations.

INTRODUCTION

Cloud computing is a computing paradigm in which the application software and databases are moved to the centralized large data centers. Cloud computing differs from existing hosting services. Services are based on consumption and the technology infrastructure is optimized for hosting several customers. Cloud Computing has been envisioned as the next-generation architecture of IT Enterprise. It is receiving more and more attentions, from both industrial and academic community. Cloud computing separates usage of IT resources from their management and maintenance, so that clients can focus on their core business and leave the expensive maintenance of IT services to cloud service provider. However clients of outsourced storage are at the mercy of their storage providers for the continued availability of their data. Even Amazon's S3, the best-known storage service, has experienced significant downtime. Here we are considering scenarios where clients may have concerns of the data security and survivability of their data stored in the cloud storage.

The management of the data and services may not be fully trustworthy. Trust Access of clients on identity and behaviors is significant for Network Services. In Trust Environment, security and survivability must be provided on network services. The client's behaviors should be monitored and some abnormal behaviors should be handled. In order to increase the data storage security and to provide trust environment in cloud, we propose architecture with Hierarchical Attribute-based secure outsourcing to monitor data flow to ensure data storage security and survivability thereby providing trust environment to the clients. Cipher text-policy attribute-based encryption (CP-ABE), as one of the most promising encryption systems in this field allows the encryption of data by specifying an access control policy over attributes so that only users with a set of attributes satisfying this policy can decrypt the corresponding data.

However a CP-ABE system may not work well when enterprise users outsource their data for sharing on cloud servers due to the following reasons: First, one of the biggest merits of cloud computing is that users can access data stored in the cloud anytime and any- where using any device such as thin clients with limited bandwidth, CPU, and memory capabilities. Therefore the encryption system should provide high performance. Second, in the case of a large-scale industry a delegation mechanism in the generation of keys inside an enterprise is needed. IBE provides a public key encryption mechanism where a public key is an arbitrary string. In this paper construct two efficient Identity Based Encryption (IBE) systems that are selective identity secure
without the random oracle and these system include an efficient CCA2 public key cryptosystem. Although some CPABE schemes support delegation between users which enables a user to generate attribute secret keys containing a subset of this own attribute secret keys for other users.

We hope to achieve a full delegation that is a delegation mechanism between attribute authorities (AAs) which independently make decisions on the structure and semantics of their attributes. Third, in case of a large-scale industry with a high turnover rate, a scalable revocation mechanism is a must. In this paper, we propose first a hierarchical attribute based encryption (HABE) model by combining a HIBE system and a CP-ABE system Based on the HABE model we construct a HABE scheme by making a performance expressivity trade-off to achieve high performance.

Traditionally trust can be established based on identities. Obtain local identities from system in order to access system service. Under assumption of that entities in the systems are already known each other. On open system like Internet strangers can make connection and establish trust together obviously establishing trust based on ID is not a feasible approach. Parties may come from different security domain and often do not have any pre-existing relationship.

Therefore, the properties of the participants will be most relevant. The approach of automated trust negotiation differs from traditional identity-based access control systems mainly in the following aspects:

1) Trust between two strangers is established based on parties' properties. It is proven through disclosure of digital credentials.

2) Every party can define access control policies to control outsider's access to their sensitive resources.

3) Instead of a one-shot authorization and authentication trust is established incrementally through a sequence of bilateral credential disclosures.

4) Less sensitive first. More sensitive disclosed later on as level of trust increase.

5) When it comes to SaaS and PaaS authentication thenticate users with your identity provider and use federation for trust with the SaaS vendor.

6) Interestingly the CSA recommends enabling the use of a single set of credentials valid across multiple sites for individual users and to void vendor proprietary methods.

LITERATURE SURVEY

[1] Vipul et al. published ―Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data.‖ which states that as more sensitive data is shared and stored by third-party sites on the Internet, there will be a need to encrypt data stored at these sites. One drawback of encrypting data is that it can be selectively shared only at a coarse-grained level (i.e., giving another party your private key). A new cryptosystem is developed for fine-grained sharing of encrypted data that we call Key-Policy Attribute-Based Encryption (KP-ABE). In the cryptosystem, ciphertexts are labeled with sets of attributes and private keys are associated with access structures that control which ciphertexts a user is able to decrypt. It demonstrates the applicability of the construction to sharing of audit-log information and broadcast encryption. The construction supports delegation of private keys which subsumes Hierarchical Identity-Based Encryption (HIBE).

[2] Rakesh et al. published ―Attribute-Sets: A Practically Motivated Enhancement to Attribute-Based Encryption.‖ elaborates that in distributed systems users need to share sensitive objects with others base on the recipients ability to satisfy a policy. Attribute- Based Encryption (ABE) is a new paradigm where such policies are specified and cryptographically enforced in the encryption algorithm itself. Ciphertext-Policy ABE (CP- ABE) is a form of ABE where policies are associated with encrypted data and attributes are associated with keys. In this work focus is on improving the flexibility of representing user attributes with keys. Specifically, it proposes the Ciphertext Policy Attribute Set Based Encryption (CP-ASBE) - 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. It shows that

the proposed scheme is more versatile and supports many practical scenarios more naturally and efficiently. It provides a prototype implementation of the scheme and evaluates its performance overhead.

[3] Pankaj et al. published ―Cloud Computing Security Issues in Infrastructure as a Service.‖ explains that cloud computing promises to cut operational and capital costs and the more important thing is it lets IT departments focus on strategic projects instead of keeping datacenters running. It is much more than simple internet. It is a construct that allows user to access applications that actually reside at location other than users own computer or other Internet-connected devices. There are numerous benefits of this construct. For instance other company hosts user application. This implies that they handle cost of servers, they manage software updates and depending on the contract user pays less i.e. for the service only. Confidentiality, Integrity, Availability, Authenticity, and Privacy are essential concerns for both Cloud providers and consumers as well. Infrastructure as a Service (IaaS) serves as the foundation layer for the other delivery models, and a lack of security in this layer will certainly affect the other delivery models, i.e., PaaS, and SaaS that are built upon IaaS layer. It presents an elaborated study of IaaS components security and determines vulnerabilities and countermeasures. Service Level Agreement should be considered very much importance.

[4] John et al. published ―Ciphertext-Policy Attribute-Based Encryption (CP-ABE).‖ explains that in several distributed systems a user should only be able to access data if a user possesses 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. However, if any server storing the data is compromised, then the confidentiality of the data will be compromised. In this paper we present a system for realizing complex access control on encrypted data that we call Ciphertext-Policy Attribute-Based Encryption. By using this technique encrypted data can be kept confidential even if the storage server is untrusted; moreover, the methods are secure against collusion attacks. Previous Attribute-Based Encryption systems used attributes to describe the encrypted data and built policies into users keys; while in this system attributes are used to describe the users credentials, and a party encrypting data determines a policy for who can decrypt. Thus, these methods are conceptually closer to traditional access control methods such as Role-Based Access Control (RBAC). In addition, it provides an implementation of system and gives performance measurements.

[5] Suhair et al. Published ―Designing a Secure Cloud-Based EHR System using Ciphertext-Policy Attribute-Based Encryption. ―which shows that as more and more healthcare organizations adopt electronic health records (EHRs), the case for cloud data storage becomes compelling

for deploying EHR systems; not only is it inexpensive but it also provides the flexible, wide-area mobile access increasingly needed in the modern world. However, before cloud-based EHR systems can become a reality, issues of data security, patient privacy, and overall performance must be addressed. As standard encryption (including symmetric key and public-key) techniques for EHR encryption/decryption caused increased access control and performance overhead, the scheme proposes the use of Ciphertext-Policy Attribute-Based Encryption (CP-ABE) to encrypt EHRs based on healthcare providers' attributes or credentials; to decrypt EHRs, they must possess the set of attributes needed for proper access. It motivates and presents the design and usage of a cloud-based EHR system based on CP-ABE, along with preliminary experiments and analysis to investigate the flexibility and scalability of the proposed approach.

[6] Ayad et al. published ―Enabling Data Dynamic and Indirect Mutual Trust for Cloud Computing Storage System.‖ which proposes a cloud-based storage scheme that allows the data owner to benefit from the facilities offered by the CSP and enables indirect mutual trust between them. The proposed scheme has four important features: (i) it allows the owner to outsource sensitive data to a CSP, and perform full block-level dynamic operations on the outsourced data, i.e., block modification, insertion, deletion and append, (ii) it ensures that authorized users (i.e., those who have the right to access the owners file) receive the latest version of the outsourced data, (iii) it enables indirect mutual trust between the owner and the CSP, and (iv) it allows the owner to grant or revoke access to the outsourced data. The security issues of the proposed scheme are discussed. Besides, it justifies its performance through theoretical analysis and experimental evaluation of storage, communication, and computation overheads.

[7] Chandana et al. published ―GASBE: A Graded Attribute-Based Solution for Access Control in Cloud Computing.‖ which states that cloud computing is an emerging computing paradigm in which resources of the computing infrastructure are provided as services over the Internet. As promising as it is, this paradigm also brings forth many new challenges for data security and access control when users outsource sensitive data for sharing on cloud servers, which are not within the same trusted domain as data owners. To keep sensitive user data confidential against un-trusted servers, existing solutions usually apply cryptographic methods by disclosing data decryption keys only to authorized users. However, in doing so, these solutions inevitably introduce a heavy computation overhead on the data owner for key distribution and data management when _ne grained data access control is desired, and thus do not scale well. The problem of simultaneously achieving fine-graininess, scalability, and data confidentiality of access control still remains unresolved. It addresses this challenging open issue by defining and enforcing access policies based on data

attributes on one hand and allowing the data owner to delegate most of the computation tasks involved in fine grained data access control to untrusted cloud servers without disclosing the underlying data contents, on the other hand. It achieves this goal by exploiting and uniquely combining techniques of attribute-based encryption (ABE), proxy re-encryption, and lazy re-encryption.

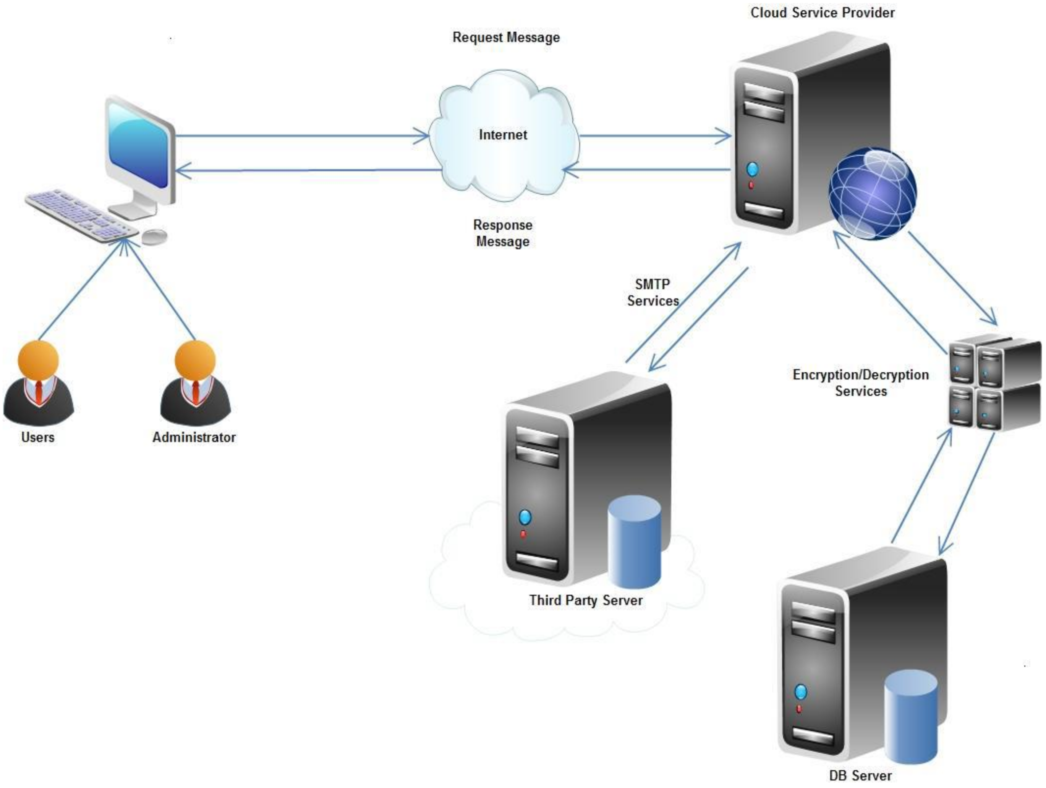
[8] Guojun et al. published ―Hierarchical attribute-based encryption and scalable user revocation for sharing data in cloud servers.‖ which explains that with rapid development of cloud computing, more and more enterprises will outsource their sensitive data for sharing in a cloud. To keep the shared data confidential against untrusted cloud service providers (CSPs), a natural way is to store only the encrypted data in a cloud. The key problems of this approach include establishing access control for the encrypted data and revoking the access rights from users when they are no longer authorized to access the encrypted data. It aims to solve both problems. First, it proposes a hierarchical attribute-based encryption scheme (HABE) by combining a hierarchical identity-based encryption (HIBE) system and a ciphertext-policy attribute-based encryption (CP-ABE) system, so as to provide not only fine-grained access control, but also full delegation and high performance. Then, it proposes a scalable revocation scheme by applying proxy re-encryption (PRE) and lazy re-encryption (LRE) to the HABE scheme, so as to efficiently revoke access rights from users.

[9] Qin et al. published ―Hierarchical Attribute-Based Encryption for Fine-Grained Access Control in Cloud Storage Services.‖ which states that cloud computing, as an emerging computing paradigm, enables users to remotely store their data into a cloud so as to enjoy scalable services on-demand. Especially for small and medium-sized enterprises with limited budgets, they can achieve cost savings and productivity enhancements by using cloud-based services to manage projects, to make collaborations, and the like. However, allowing cloud service providers (CSPs), which are not in the same trusted domains as enterprise users, to take care of confidential data, may raise potential security and privacy issues. To keep the sensitive user data confidential against untrusted CSPs, a natural way is to apply cryptographic approaches, by disclosing decryption keys only to authorized users. However, when enterprise users outsource confidential data for sharing on cloud servers, the adopted encryption system should not only support fine-grained access control, but also provide high performance, full delegation, and scalability, so as to best serve the needs of accessing data anytime and anywhere, delegating within enterprises, and achieving a dynamic set of users. In this it propose a scheme to help enterprises to efficiently share confidential data on cloud servers. The goal is achieved by first combining the hierarchical identity-based encryption (HIBE) system and the ciphertext-policy

attribute-based encryption (CP-ABE) system, and then making a performance-expressivity tradeoff, finally applying proxy re-encryption and lazy re-encryption to our scheme.

[10] Patrick et al. published ―Methods and Limitations of Security Policy Reconciliation.‖ which explains that a security policy is a means by which participant session requirements are specified. However, existing frameworks provide limited facilities for the automated reconciliation of participant policies. It considers the limits and methods of reconciliation in a general-purpose policy model. It identifies an algorithm for efficient two-policy reconciliation, and show that, in the worst-case, reconciliation of three or more policies is intractable. Further, it suggests efficient heuristics for the detection and resolution of intractable reconciliation. Based upon the policy model, it describes the design and implementation of the Ismene policy language. The expressiveness of Ismene, and indirectly of the model, is demonstrated through the representation and exposition of policies supported by existing policy languages. It concludes with brief notes on the integration and enforcement of Ismene policy within the Antigone.

SYSTEM ARCHIRECTURE



IMPLEMENTATION

Attribute based encryption (ABE):- First introduced the attribute based encryption (ABE) for enforced access control through public key cryptography. The main goal for these models is to provide security and access control. The main aspects are to provide flexibility, scalability and fine grained access control. In classical model, this can be achieved only when user and server are in a trusted domain. But what if their domains are not trusted or not same? So, the new access control scheme that is „Attribute Based Encryption (ABE)‟ scheme was introduced which consist of key policy attribute based encryption (KP-ABE). As compared with classical model, KP-ABE provided fine grained access control. However it fails with respect to flexibility and scalability when authorities at multiple levels are considered. In ABE scheme both the user secret key and the ciphertext are associated with a set of attributes. A user is able to decrypt the cipher-text if and only if at least a threshold number of attributes overlap between the cipher-text and user secret key. Different from traditional public key cryptography such as Identity-Based Encryption, ABE is implemented for one-to many encryption in which cipher-texts are not necessarily encrypted to one particular user, it may be for more than one number of users. In Sahai and Waters ABE scheme, the threshold semantics are not very expressive to be used for designing more general access control system. Attribute-Based Encryption (ABE) in which policies are specified and enforced in the encryption algorithm itself. The existing ABE schemes are of two types. They are Key-Policy ABE (KP-ABE) scheme and Ciphertext-Policy ABE (CPABE) scheme. That can be discussed further.

Key Policy Attribute Based Encryption (KP-ABE):- It is the modified form of classical model of ABE. Exploring KP-ABE scheme, attribute policies are associated with keys and data is associated with attributes. The keys only associated with the policy that is to be satisfied by the attributes that are associating the data can decrypt the data. Key Policy Attribute Based Encryption (KP-ABE) scheme is a public key encryption technique that is designed for one-to-many communications. In this scheme, data is associated with the attributes for which a public key is defined for each. Encrypter, that is who encrypts the data, is associated with the set of attributes to the data or message by encrypting it with a public key. Users are assigned with an access tree structure over the data attributes. The nodes of the access tree are the threshold gates. The leaf nodes are associated with attributes. The secret key of the user is defined to reflect the access tree structure. Hence, the user is able to decrypt the message that is a ciphertext if and only if the data attributes satisfy the access tree structure. In KP-ABE, a set of attributes is associated with ciphertext and the user's decryption key is associated with a monotonic access tree structure. When the attributes associated with the ciphertext satisfy the access tree structure, then the user can decrypt the ciphertext. In the cloud computing, for efficient revocation, an access control mechanism based on KP-ABE and a encryption technique used together. It enables a data owner to reduce most of the computational overhead to the servers.

The KP-ABE scheme provides fine-grained access control. Each file or message is encrypted with a symmetric data encryption key (DEK), which is again encrypted by a public key, that is corresponding to a set of attributes in KP-ABE, which is generated corresponding to an access tree structure. The encrypted data file is stored with the corresponding attributes and the encrypted DEK. If and only if the corresponding attributes of a file or message stored in the cloud satisfy the access structure of a user's key, then the user is able to decrypt the encrypted DEK. That can be used to decrypt the file or message. KP-ABE scheme consists of the following four algorithms:

1. Setup: This algorithm takes as input a security parameter κ and returns the public key PK and a system master secret key MK. PK is used by message senders for encryption. MK is used to generate user secret keys and is known only to the authority.

2. Encryption: This algorithm takes a message M, the public key PK, and a set of attributes as input. It outputs the ciphertext E.

3. Key Generation: This algorithm takes as input an access structure T and the master secret key MK. It outputs a secret key SK that enables the user to decrypt a message encrypted under a set of attributes if and only if matches T.

4. Decryption: It takes as input the user's secret key SK for access structure T and the ciphertext E, which was encrypted under the attribute set . This algorithm outputs the message M if and only if the attribute set satisfies the user's access structure T.

Cipher Text Policy Attribute Based Encryption:- It introduced the concept of another modified form of ABE called CP-ABE that is Ciphertext Policy Attribute Based Encryption. In CP-ABE scheme, attribute policies are associated with 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. CP-ABE works in the reverse way of KP-ABE. In CP-ABE the ciphertext is associated with an access tree structure and each user secret key is embedded with a set of attributes. In ABE, including KP-ABE and CP-ABE, the authority runs the algorithm Setup and Key Generation to generate system MK, PK, and user secret keys. Only authorized users (i.e., users with intended access structures) are able to decrypt by calling the algorithm Decryption. In CP-ABE, each user is associated with a set of attributes. His secret key is generated based on his attributes. While encrypting a message, the encryptor specifies the threshold access structure for his interested attributes. This message is then encrypted based on this access structure such that only those whose attributes satisfy the access structure can decrypt it. With CP ABE technique, encrypted data can be kept confidential and secure against collusion attacks. CP-ABE scheme consists of following four algorithms:

1. Setup : This algorithm takes as input a security parameter κ and returns the public key PK as well as a system master secret key MK. PK is used by message senders for encryption. MK is used to generate user secret keys and is known only to the authority.

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

3. Key-Gen: This algorithm takes as input a set of attributes associated with the user and the master secret key MK. It outputs a secret key SK that enables the user to decrypt a message encrypted under an access tree structure T if and only if matches T.

4. Decrypt: This algorithm takes as input the ciphertext CT and a secret key SK for an attributes set . It returns the message M if and only if satisfies the access structure associated with the ciphertext CT. In CP-ABE depends how attributes and policy are associated with cipher texts and users‟ decryption keys. In a CP-ABE scheme, a ciphertext is associated with a monotonic tree access structure and a user's decryption key is associated with set of attributes. In this scheme, the roles of ciphertexts and decryption keys are switched as that in KP-ABE.

Ciphertext Policy Attribute-Set Based Encryption (CPASBE):- As compared to CP-ABE scheme in which the decryption keys only support user attributes that are organized logically as a single set, so users can only use all possible combinations of attributes in a single set issued in their keys to satisfy policies. To solve this problem, ciphertext-policy attribute-set based encryption (CP-ASBE or ASBE for short) is introduced. ASBE is an extended form of CPABE which organizes user attributes into a recursive set structure. Ciphertext Policy Attribute Set Based Encryption (CP-ASBE) is a modified form of CP-ABE. It differs from existing CP-ABE schemes that represent user attributes as a monolithic set in keys. It 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. The CP-ASBE consists of recursive set of attributes. The desirable feature and the recursive key structure is implemented by four algorithms, Setup, KeyGen, Encrypt, and Decrypt.

1. Setup: Here is the depth of key structure. Take as input a depth parameter „d‟. It outputs a public key PK and master secret key MK.

2. Key-gen: Takes as input the master secret key MK, the identity of user u, and a key structure A . It outputs a secret key SK for user u.

3. Encrypt: Takes as input the public key PK, a message M, and an access tree T . It outputs a ciphertext CT.

4. Decrypt: Take as input a ciphertext CT and a secret key SK for user u. It outputs a message m If the key structure A associated with the secret key SK, satisfies the access tree T, associated with the ciphertext CT, then m is the original correct message M. Otherwise, m is null. Specifically CP-ASBE allows- User attributes are organized into a recursive family of sets and Allowing attributes to combine from multiple sets. Thus, by grouping user attributes into sets and no restriction on how they can be combined, CP-ASBE can support compound attributes. More flexibility and fine grained access is provided by AP-ASBE. Similarly, multiple numerical assignments for a given attribute can be supported by placing each assignment in a separate set as well as placing it into a single set.

CONCLUSION

The paper proposed a modified HABE scheme by taking advantages of attributes based encryption (ABE) and hierarchical identity based encryption (HIBE) access control processing. The proposed access control method using MHABE is designed to be utilized within a hierarchical multiuser data-shared environment, which is extremely suitable for a mobile cloud computing model to protect the data privacy and defend unauthorized access. Compared with the original HABE scheme, the novel scheme can be more adaptive for mobile cloud computing environment to process, store and access the enormous data and files while the novel system can let different privilege entities access their permitted data and files. The scheme not only accomplishes the hierarchical access control of mobile sensing data in the mobile cloud computing model, but protects the data from being obtained by an untrusted third party.

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] Rakesh Bobba, Himanshu Khurana and Manoj Prabhakaran, ―Attribute- Sets: A Practically Motivated Enhancement to Attribute-Based Encryption‖, July 27, 2009 S. Zhang, C. Zhu, J. K. O. Sin, and P. K. T. Mok, ―A novel ultrathin elevated channel low-temperature poly-Si TFT,‖ *IEEE Electron Device Lett.*, vol. 20, pp. 569–571, Nov. 1999.

[3] 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.

[4] J.Bethencourt, A. Sahai, and B. Waters. ―Ciphertext-Policy Attribute- Based Encryption.‖ In Proc. of SP'07, Washington, DC, USA, 2007.

[5] Zhibin Zhou, Dijiang Huang‖ On Efficient Ciphertext-Policy Attribute Based Encryption and Broadcast Encryption‖.

[6] R.Ostrovsky, A. Sahai, and B. Waters. ―Attribute-based encryption with non-monotonic access structures‖. In Proc. of CCS'06, New York, NY, 2007

[7] D.Boneh and M. Franklin. ―Identity-Based Encryption from the Weil Pairing.‖ *In*

Proc. of CRYPTO'01, Santa Barbara, California, USA, 2001.

[8] Guojun Wang, Qin Liu , Jie Wu ―Hierarchical attribute-based encryption and scalable user revocation for sharing data in cloud services‖, 2011.

[9] G.Wang, Q. Liu, and J.Wu, ―Hierachical attibute-based encryption for fine-grained access control in cloud storage services,‖ in *Proc. ACM Conf. Computer and Communications Security (ACM CCS)*, Chicago, IL, 2010.

[10] P. D. McDaniel and A. Prakash, ―Methods and limitations of security policy reconciliation,‖ in *Proc. IEEE Symp. Security and Privacy*, Berkeley, CA, 2002.

[11] A.Sahai and B. Waters. ―Fuzzy Identity-Based Encryption.‖ In Proc. Of EUROCRYPT'05, Aarhus, Denmark, 2005..

[12] Zhiguo Wan, Jun'e Liu, and Robert H. Deng, ―HASBE:A Hierarchical Attribute-Based Solution for Flexible and Scalable Access Control in Cloud Computing‖ *IEEE Transactions On Information Forensics And Security*, Vol. 7, No.2,April2012.