An Enhancement of HASBE Scheme Setting up Access Control with Hierarchical Identity based Encryption in Cloud Computing

[1]Ch V V Narasimha Raju, [2]P Amarendra Reddy

[1]Dept of CSE,Marri Laxman Reddy Institute of Technology ,Dundigal,Hyderabad-500043, A.P, INDIA

[2] Dept of CSE, Marri Laxman Reddy Institute of Technology ,Dundigal, Hyderabad-500043, A.P, INDIA

Abstract— At present cloud computing is going to be very famous technology in IT enterprises. For a company, the data stored is huge and it is very precious. In this era, even sensitive data is stored and shared on the internet using trusted third parties and service providers. We propose hierarchical attribute-set-based encryption (HASBE) by extending cipher text-policy attribute-set-based encryption (ASBE) with a hierarchical structure of users. It is implemented using cipher text policy by encrypting and decrypting the data in the cloud so that the cloud system becomes more scalable and flexible by enforcing data owners to share their data with data consumers controlled by the domain authority. We implement our scheme and show that it is both efficient and flexible in dealing with access control for out sourced data in cloud computing with comprehensive experiments.

Keywords—cloudcomputing; Attributesetbased encryption (ASBE); Access Control; ciphertext policy.;

I. Introduction

Today for many organizations they need to store their enormous amount of data. Network storage providers are giving the resources for these organizations on demand. Among these, Cloud computing is a new computing paradigm that is built on virtualization, parallel and distributed computing, service-oriented architecture, and utility computing. The advantages of cloud computing comprise decreased costs and capital expenses, scalability, increased operational, immediate time to promote, flexibility, and so on. Different service-oriented cloud computing models have been designed, Platform as a Service (PaaS), including Infrastructure as a Service (IaaS), and Software as a Service (SaaS). Frequent commercial cloud computing systems have been built at different levels, e.g., Amazon's EC2, Amazon's S3, and IBM's Blue Cloud areIaaS systems, while Google App Engine and Yahoo Pig are representative PaaS systems, and Google's Apps and Sales force's Customer Relation Management (CRM) System be owned by SaaS systems. The ABE scheme used an user's identity as attributes, and a set of attributes were used to encrypt and decrypt data. The ABE scheme can result the problem that data owner needs to use every authorized user's public key to encrypt data. The KP-ABE scheme can achieve fine grained access control and more flexibility to control users than ABE scheme. But the disadvantage of KP-ABE is that the access policy is built into a user's private key, so data owner can't choose who can decrypt the data except choosing a set of attributes which can describe this data. In a CP-ABE scheme, the roles of cipher texts and decryption keys are switched; the cipher text is encrypted with a tree access policy chosen by an encrypt or while the corresponding decryption key is created with respect to a set of attributes. As long as the set of attributes associated with a decryption key satisfies the tree access policy associated with a given cipher text, the key can be used to decrypt the cipher text. Since users' decryption keys are related with a set of attributes, CP-ABE is practically closer to traditional access control models such as Role-Based Access Control (RBAC). Thus, it is more natural to apply CP-ABE, instead of KP-ABE, to enforce access control of encrypted data.

II. Related Work

From the internet through web-based tools and applications, a model by which information technology services being delivered and resources are retrieved, rather than direct connection to a server where the Data and software packages are amassed in servers. In survey on several schemes such as Cipher text-Policy Attribute-Based Encryption, Key-Policy Attribute-Based Encryption, Cipher text Policy Attribute Set Based Encryption, Hierarchical Identity Based Encryption, Fuzzy Identity-Based Encryption, Hierarchical Attribute-Based Encryption and Hierarchical Attribute-Set-Based Encryption for access control of outsourced data are conversed. In presented a survey on various encryption methods that gives security, scalable and flexible fine grained access control. As the data is divided over the network, it is required to be encrypted. Distribution of data signifies 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 users access the data and the system.

A. *Attribute based encryption (ABE):-*

Sahai and Waters 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. The new access control scheme that is 'Attribute Based Encryption (ABE)' scheme was introduced which consist of key policy attribute based encryption (KP-ABE). In ABE scheme both the user secret key and the cipher text 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. They are Key-Policy ABE (KP-ABE) scheme and Cipher text-Policy ABE (CPABE) scheme. That can be discussed further.

B. Key Policy Attribute Based Encryption(KP-ABE):-

To enable more general access control, V. Goyal, O.Pandey, A. Sahai, and B. Waters proposed a key-policy attribute-based encryption (KP-ABE) scheme. In cloud computing, an access control mechanism based on KP-ABE together with a re-encryption techniques used for efficient user revocation. This scheme enables a data owner to reduce most of the computational overhead to cloud servers. The use of this encryption scheme KP-ABE 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 corresponding to a set of attributes in KP-ABE, which is generated corresponding to an access structure. The data file that is encrypted is stored with the corresponding attributes and the encrypted DEK.

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 cipher text 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 cipher text 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.

Limitations of KP-ABE:-

Encrypt or cannot decide who can decrypt the encrypted data. It can only choose descriptive attributes for the data, and has no choice but to trust the key issuer. KP-ABE is not naturally suitable to certain applications. For example, sophisticated broadcast encryption where users are described by various attributes and in this, the one whose attributes match a policy associated with a cipher text, it can decrypt the cipher text. KP-ABE scheme supports user secret key accountability. It is providing fine grained access but has no longer with flexibility and scalability.

c. Cipher Text Policy Attribute Based Encryption:-

In several distributed systems a user should only be able to access data if a user possesses a certain set of credentials or attributes. The only method for enforcing such policies is to employ a trusted server to store the data and mediate access control. However, basic CP-ABE schemes are far from enough to support access control in modern enterprise environments, which require considerable flexibility and efficiency in specifying policies and managing user attributes. In a CP-ABE scheme, 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.

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 cipher text 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 cipher text 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 cipher text CT. In CP-ABE depends how attributes and policy are associated with cipher texts and users' decryption keys. In a CP-ABE scheme, a cipher text is associated with a monotonic tree access structure and a user's decryption key is associated with set of attributes.

Limitations of CP-ABE:-

However, basic CP-ABE schemes are still not fulfilling the enterprise requirements of access control which require considerable flexibility and efficiency. CP-ABE has limitations in specifying policies and managing user attributes. In a CP-ABE scheme, 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. For realizing complex access control on encrypted data and maintaining confidential-ability, CP-ABE can be used. Encrypted data can be kept confidential even if the storage server is un-trusted; moreover, our methods are secure against collusion attacks. KP-ABE uses attributes to describe the encrypted data and built policies into user's keys. In other hand CP-ABE, attributes are used to describe a user's credentials. Data encryptor determines a policy for who can decrypt.

III. Proposed Work

The objective of this work is to expand HASBE scheme is to realize scalable, supple, and fine-grained access control in cloud computing. The HASBE method flawlessly integrates a hierarchical structure of scheme customers by concerning an allocation algorithm to ASBE. HASBE not only maintains compound attributes due to flexible attribute set combinations, but also attains efficient user revocation because of multiple value assignments of attributes. We properly proved the security of HASBE based on the security of CP-ABE.In this paper contributes in multiform. Initially ,we show how ASBE algorithm is been enhanced by HASBE with a hierarchical structure with the better features like flexibility ,scalability and the common feature of fine grained access control of ASBE.

A. Ciphertext Policy Attribute-Set Based Encryption (CPASBE):-

Cipher text 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. Specifically CP-ASBE allows, 1) user attributes to be organized into a recursive family of sets and 2) policies that can selectively restrict decrypting users to use attributes from within a single set or allow them to combine attributes from multiple sets. In a CP-ABE scheme, 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, cipher text-policy attribute-set-based encryption (CP-ASBE or ASBE for short) is introduced. ASBE is an extended form of CP-ABE which organizes user attributes into a recursive set structure.

Limitations:-The challenge in constructing a CP-ASBE scheme is in selectively allowing users to combine attributes from multiple sets within a given key. There is challenge for preventing users from combining attributes from multiple keys. Now challenge for preventing users from combining attributes From multiple keys can be generated by the Identity Based Encryption (IBE) and Hierarchical Identity Based Encryption (HIBE).

B. Identity based Encryption (IBE) and Hierarchical Identity based Encryption(HIBE).

In an identity-based encryption scheme, an arbitrary key is used as the key for data encryption and for decryption; a key is mapped by a key authority. Hierarchical Identity Based Encryption (HIBE) is the hierarchical form of a single IBE. The concept of HIBE scheme can help to explain the definition of security. In a regular IBE (1-HIBE) scheme; there is only one private key generator (PKG) that distributes private keys to each users, having public keys are their primitive ID (PID) arbitrary strings. Private key PK of any user in their domain can be computed by Domain PKGs, provided they have previously requested their domain secret key-SK from the root PKG. Similarly, is for number of sub-domains. There also includes a trusted third party or root certificate authority that allows a hierarchy of certificate authorities: Root certificate authority issues certificates for other authorities or users in their respective domains. The original system does not allow for such structure.

However, a hierarchy of PKGs is reduces the workload on root server and allows key assignment at several levels. In this paper, we are going to implement scheme for access control in cloud computing using HIERARCHICAL ATTRIBUTE SET BASED ENCRYPTION (HASBE).HASBE extends the cipher text-policy attribute-set-based encryption (CP-ASBE, or ASBE for short) scheme proposed by Bobba et al. with system users having hierarchical structure, to achieve flexible, scalable, and access control.

C. Access Control Solutions for Cloud Computing

The traditional method to protect sensitive data outsourced to third parties is to store encrypted data on servers, while the decryption keys are disclosed to authorize users only. However, there are several drawbacks about this trivial solution. First of all, such a solution requires an efficient key management mechanism to distribute decryption keys to authorized users, which has been proven to be very difficult.

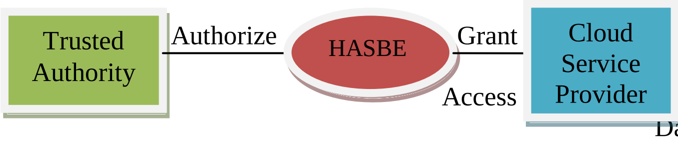


Fig 1. Cloud service Provider Access.

New File Creation:

To protect data stored on the cloud, a data owner first encrypts data files and then stores the encrypted data files on the cloud. As in [16], each of the file is encrypted with a symmetric data encryption key that is in turn encrypted with HASBE scheme. Before uploading to the cloud, a data file is handled by the data owner as follows:

- Pick a unique ID for this data file.
- Randomly pick a symmetric data encryption key DEK←K , where is the key space, and encrypt the data.
- Define a tree access structure for the file and encrypt (PK, DEK, T) With using algorithm of HASBE which returns cipher text. Finally, the encrypted data file is stored on the cloud. Encrypt (PK, DEK, T). M is the message to encrypt. In the *New File Creation* operation, M is the DEK of a data file. T is the tree access structure. Encrypt algorithm is the same as that of ASBE. The algorithm associates a polynomial with each node in the tree, which is chosen randomly in a top-down manner from the root node. This algorithm computes the Cipher text as follows:

$CT=+ (T.C=M.e\,(g.g)^{\alpha .}C=h_1^{*}, C=h_2^{*}$, ¥y€Y; $C_y=g^{y}{}_{x}{}^{(0)}$, $C^{t}{}_{y}=H(att(y))^{g}{}_{x}{}^{(0)}$,¥x€X; $C_x=h_2^{q}{}_{x}{}^{(0)}$.

Where Y denotes the set of leaf nodes in, X denotes the set of translating nodes in the access tree.

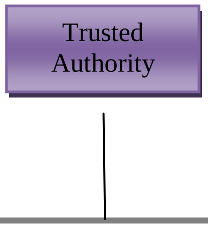
D. Developing the environment

Cloud computing system under concern consists of five types of parties: cloud service provider, data owners, data consumers, domain authorities, and trusted authority. The cloud service supplier administers a cloud to provide data storage service. Data proprietors encrypt their data records and store them in the cloud for sharing with data consumers. To entrance the joint data files, data consumers download encrypted data files of their attention from the cloud and then decrypt them. Each data owner/consumer is monitored by a domain authority.

By the parent domain authority or the trusted authority, a domain authority is managed. Domain authorities, data owners, data consumers, and the trusted authority are organized in a hierarchical way. The conditioned authority is the origin authority and in charge for managing top-level domain authorities. Each top-level domain authority matches to a top-level association, such as an amalgamated enterprise, whereas each lower-level domain authority communicates to a lower-level organization, such as associated company in a federated organization.

Data owners/consumers may correspond to employees in an organization. Every domain authority is responsible for managing the domain authorities at the next level or the data owners/consumers in its domain. This study proposes a Business Model for Cloud Computing Based on a Separate Encryption and Decryption Service. In this business model, Encryption/Decryption as a Service and Storage as a Service (SaaS) are not provided by a single operator. In addition, the SaaS provider may not store unencrypted user data and, once the provider of Encryption/Decryption as a Service has finished encrypting the user data and handed it off to an application (e.g. a CRM system), the encryption/decryption system must delete all encrypted and decrypted user data.

The concept of dividing authority is often applied in business management. For example, responsibility for a company’s finances is divided between the accountant and cashier. In business operations, the accountant is responsible for keeping accounts, while the cashiers responsible for making payments. By keeping these two functions separate, the company can prevent the accountant from falsifying accounts and embezzling corporate funds. Official documents frequently need to be stamped with two seals (i.e., the corporate seal and the legal representative’s seal), thus preventing a staff member from abusing his position to issue fake documents, and these seals are normally entrusted to two different people. These examples of the division of authority are designed to avoid a concentration of power which could raise operational risks. To illustrate the concept of our proposed business model presents an example in which the user uses separate cloud services for CRM, storage and encryption/decryption. The trusted authority is the root authority and responsible for managing top-level domain authorities. Each top-level domain authority corresponds to a top-level organization, such as a federated enterprise, while each lower-level domain authority corresponds to a lower-level organization,



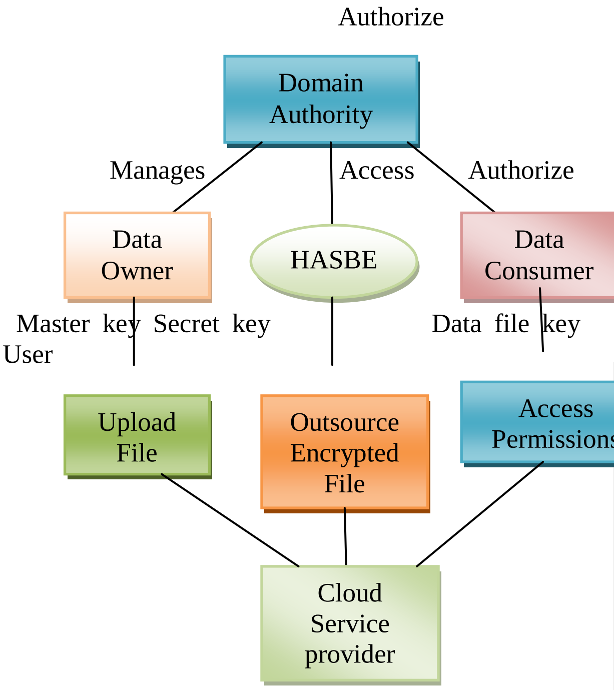


Fig 2. Cloud environment Development

such as an affiliated company in a federated enterprise. Data owners/consumers may correspond to employees in an organization. Each domain authority is responsible for managing the domain authorities at the next level or the data owners/consumers in its domain.

The traditional method to protect sensitive data outsourced to third parties is to store encrypted data on servers, while the de- cryption keys are disclosed to authorized users only. The cloud computing system under consideration consists of five types of parties: a cloud service provider, data owners, data consumers, number of domain authorities, and a trusted authority

IV. System model

Data characterizes an extremely important asset for any group of organization, and endeavor users will face serious consequences if its confidential data is disclosed to their business competitors. Thus, cloud users in the first place want to make sure that their data are kept secret to outsiders, together with the cloud provider and their possible contestants. This is the first data security requirement.

Even though the great profits brought by cloud computing paradigm are exciting for IT companies, academic researchers, and possible cloud users, security problems in cloud computing turn out to be serious obstructions which, devoid of being suitably addressed, will prevent cloud computing widespread applications and practice in the future. One of the famous safety concerns is data security and privacy in cloud computing due to its Internet-based data storage and management. Users have to give up their data to the cloud service provider for storage and business operations in cloud environment, while the cloud service supplier is usually a commercial enterprise which cannot be totally trusted.

In this system, neither data owners nor data consumers will be always online. They come online only when essential, while the cloud service provider, the trusted authority, and domain authority are always online. The cloud is unspecified to have abundant storage capacity and computation power. In addition, we take for granted that data consumers can access data files for interpretation only.

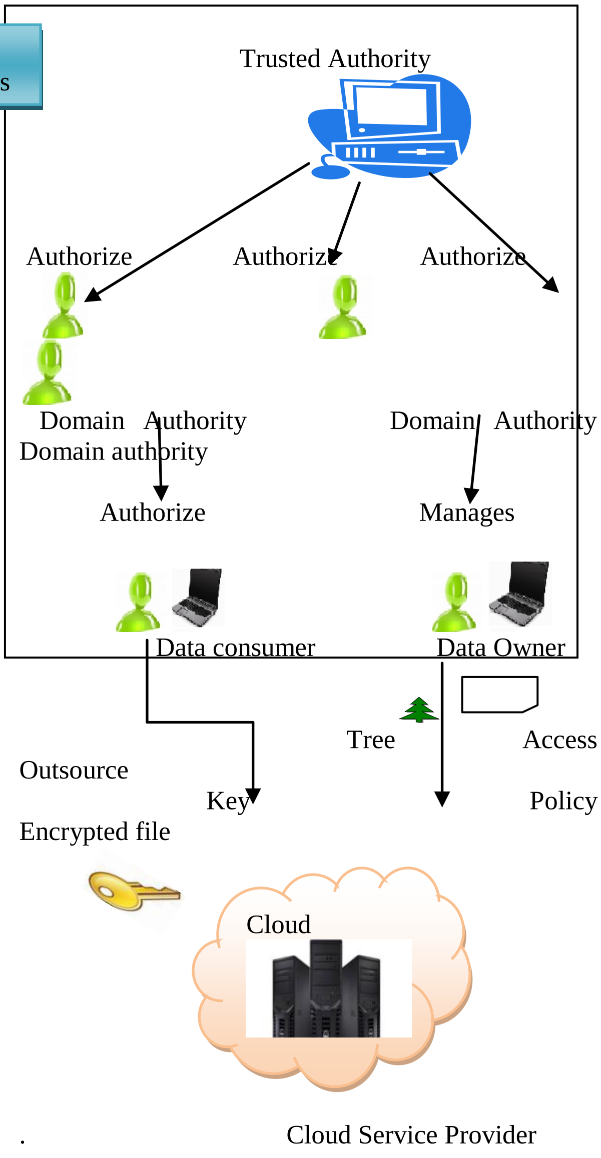


Fig 3. System Architecture

- *HASBE scheme:* The proposed HASBE method effortlessly expands the ASBE scheme to handle the hierarchical structure of system users. Recall that our system model consists of a trusted authority, multiple domain authorities, and numerous users equivalent to data owners and data consumers.

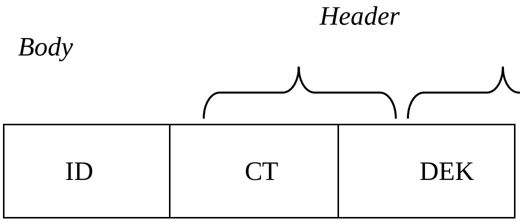


Fig 4. Format of a data file on the cloud.

The trusted authority is accountable for generating and distributing system parameters and root master keys as well as authorizing the top-level domain authorities. A domain influence is accountable for delegating keys to lesser domain authorities at the next level or users in its domain. Each user in the system is allocated a key structure which specifies the attributes associated with the user's decryption key. Represents data file format of cloud. When the system is set up, the conditioned authority selects a bilinear group and some random numbers. When Public Key (PK) and MasterSecretKey (MK0) may be generated and also there will be several exponentiation operations.

V.CONCLUSION AND FUTURE ENHANCEMENT

In this paper, we introduced the HASBE scheme for realizing scalable, flexible, and fine-grained access control in cloud computing. The HASBE scheme seamlessly incorporates a hierarchical structure of system users by applying a delegation algorithm to ASBE. HASBE not only supports compound attributes due to flexible attribute set combinations, but also achieves efficient user revocation because of multiple value assignments of attributes.

We formally proved the security of HASBE based on the security of CP-ABE by Bethencourt *et al*. Finally, we implemented the proposed scheme, and conducted comprehensive performance analysis and evaluation, which showed its efficiency and advantages over existing schemes.

REFERENCES

[1] D.Boneh and M. Franklin. "Identity Based Encryption from the Weil Pairing." In Proc. of CRYPTO'01, Santa Barbara, California, USA, 2001.

[2] B. Barbara, "Salesforce.com: Raising the level of networking," Inf. Today, vol. 27, pp. 45–45, 2010.

[3] T. Yu and M. Winslett, "A unified scheme for resource protection in automated trust negotiation," in Proc. IEEE Symp. Security and Privacy Berkeley, CA, 2003.

[4] A.Sahai and B. Waters. "Fuzzy Identity-Based Encryption." In Proc. of EUROCRYPT'05, Aarhus, Denmark, 2005.

[5] V. Goyal, O. Pandey, A. Sahai and B. Waters, "Attribute Based Encryption for Fine-Grained Access Conrol of Encrypted Data", ACM conference on Computer and Communications Security (ACM CCS), 2006.

[6] M. Pirretti, P. Traynor, P. McDaniel and B. Waters, "Secure Attribute-Based Systems", ACM conference on Computer and Communications Security (ACM CCS), 2006.

[7] Ross, —Technical perspective: A chilly sense of security,‖Commun. ACM, vol. 52, pp. 90–90, 2009.

[8] D. E. Bell and L. J. LaPadula, Secure Computer Systems: Unified Exposition and Multics Interpretation The MITRE Corporation, Tech. Rep., 1976.

[9] K. J. Biba, Integrity Considerations for Secure Computer Sytems the MITRE Corporation, Tech. Rep., 1977.

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

[11] Chittaranjan Hota, Sunil Sanka,"Capability-based Cryptographic Data AccessControlinCloudComputing",Int. J. Advanced Networking and Applications, Volume: 03; Issue: 03; Pages: 1152-1161 (2011).

[12] V.Suma, K.Vijay Kuma,"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.

[13] Zhiguo Wan, Jun'e Liu, and Robert H. Deng, "HASBE: A Hierarchical Attribute-Based Solution for Flexible and Scalable Access Control in CloudComputing"IEEETransactions On Information Forensics And Security, Vol. 7,No. 2, April 2012.

[14] G.Wang, Q. Liu, and J.Wu, "Hierarchical 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.

[15] H. Harney, A. Colgrove, and P. D. McDaniel, "Principles of policy in secure groups," in Proc. NDSS, San Diego, CA, 2001.

[16] D. E. Bell and L. J. LaPadula, Secure Computer Systems: Unified Exposition and Multics Interpretation The MITRE Corporation, Tech. Rep., 1976.

[17] L. M. Vaquero. 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.

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

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

[20] 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.

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