SURVEY: ABE Based Secured Cloud Storage

N. Poornima, S.N. Shanmugai, S.Swathi, K.Vidhya
KPR Institute of Engineering and Technology, Coimbatore, Tamil Nadu, India

Abstract: **- Cloud provides offer for several storage services for their users in efficient manner. Cloud users are allowed to store data in cloud server using cloud storage and reduce the risk in storing and retrieving in local machine. The data can be shared by a user in a group and the facility shakes the integrity of the shared data due to access by many users in the field. It is necessary to ensure the integrity of shared data before using that data for some process and the correctness of the cloud storage. Public auditing mechanism is employed to ensure the correctness of the shared data. Both data owner and the Third Party Auditor (TPA) can examine shared data integrity without downloading the data from cloud server. The cloud computing, strengthen the capabilities of the hardware resources by optimal and shared utilization. Even the critical infrastructure, for example, power generation and distribution plants are being migrated by the cloud computing paradigm. However, the services deployed by third-party cloud service providers entail additional security threats. The migration of user's assets outside the administrative control in a shared environment where numerous users are collocated escalates the security concerns. Moreover, the survey presents the solutions presented in the literature to counter the security issues. Furthermore, a brief view of security vulnerabilities measures in the mobile cloud computing are also highlighted. In the end, the discussion of the open issues and future research directions is also presented. This research paper attempts to point out various techniques to solve the privacy and security issues of the data in public auditing method in cloud environment.**

I. INTRODUCTION

In Cloud Computing, The cloud is a term referring to accessing computer, Information Technology (IT), and software applications through a network connection, often by accessing data centers using Wide Area Networking (WAN) or Internet connectivity. In this we discuss about Cloud Computing based on cloud. Cloud computing is a common shared pools of configurable computer system resources and higher-level services that can be rapidly provisioned with minimal management effort, often over the Internet and relies on sharing of data to achieve coherence and economies of scale, similar to a public utility. Third-party clouds user enable an organization to focus on their core businesses instead of expending resources on computer infrastructure and maintenance of the system. Advocates notes that cloud computing allows companies either avoid or minimize up-front IT infrastructure costs. Proponents also claims a cloud computing to enterprises to get their applications up and running faster, with improved manageability and less maintenance, and that it enables IT teams to more rapidly adjust resources to achieve fluctuating and unpredictable demand. Cloud providers typically use "pay-as-you-go" technologies, which can lead to unexpected operating expenses if administrators are not familiarized with cloud-pricing models.[1]

1.1. Characteristics

- **Device and location independence** enable the users to access systems using a web browser regardless of their location or what device they use (e.g., PC, mobile phone).
- **Maintenance** of cloud computing is easier in the cloud service system, because they do not need to be installed on each user's computer and can be accessed from different places (e.g., different work locations, while travelling, etc.).[2]
- **Multi-tenancy** enables the sharing of resources and costs across a large pool of users thus allowing for centralization, peak-load capacity, utilization.
- **Performance** is monitored by the IT experts from the service provider, and consistent and loosely coupled architectures are constructed using web services as the system interface.
- **Productivity** may be increased when multiple users can work on the same data simultaneously, rather than waiting for that data to be saved and emailed.
- **Reliability** improves with the use of multiple redundant sites, which makes well-designed cloud computing suitable for business continuity and disaster recovery.
- **Scalability and elasticity** via dynamic ("on-demand") provisioning of resources on a fine-grained, self-service basis in near real-time without users having to engineer for peak loads. This gives the ability to scale up when the usage need increases or down if resources are not being used.
- **Security** can be improved due to centralization of data, increased security-focused resources, etc., but concerns can persist about loss of control over certain sensitive data, and the lack of security for stored kernels. Security is often good or better than other traditional systems, in part because service providers are able to devote resources to solving security issues that many customers cannot afford to tackle or which they lack the technical skills to address.[3]

The National Institute of Standards and Technology's (NIST) definition of cloud computing identifies "five essential characteristics":

- *On-demand self-service:* A consumer can be unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring the human interaction with each service provider.
- *Broad network access:* Capabilities are available over the network and accessed through the standard mechanisms that can promote by heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops, and workstations).
- *Resource pooling:* The provider's computing resources are pooled to the serve for multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to a consumer demand.
- *Rapid elasticity:* Capabilities can be elastically provisioned and released, in some cases automatically, to scale the resources rapidly outward and inward commensurate with the demand. To the consumer, the capabilities available for resource provisioning often appear unlimited and can be appropriated in any quantity at any time.
- *Measured service:* Cloud systems automatically control and optimize the resource use by leveraging a metering capability at some level of the abstraction appropriate to the type of service provided(e.g., storage, processing, bandwidth, and active user accounts).[4]

II. SERVICE MODELS

Though service-oriented architecture advocates "everything as a service" (with the acronyms EaaS or XaaS, or simply aas), cloud-computing providers offer their "services" according to different models, which of the three standard models are classified as Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS)..[5] The below figure 1 represents the service models of cloud.

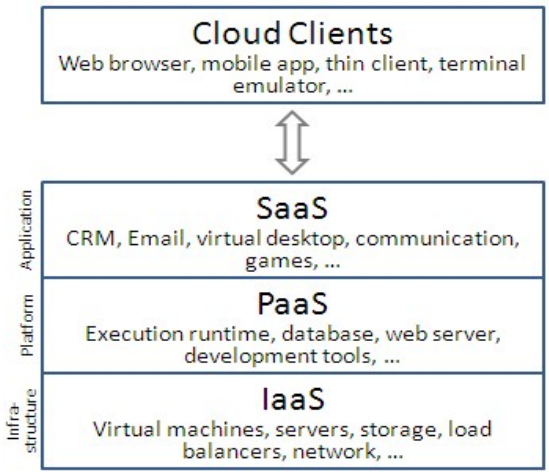

Figure 1 SERVICE MODELS

Infrastructure as a service (IaaS)

"Infrastructure as a service" (IaaS) referred as an online services platform that provide high-level interface that is used to dereference various low-level interface details of underlying network infrastructure like physical computing resources, location, data partitioning, scaling, security, backup etc. A hypervisor runs the virtual machines as guests.[6]

Platform as a service (PaaS)

The NIST's definition of cloud computing defines the Platform as a Service as: The capability provided to the consumer is to deploy the cloud infrastructure consumer-created or acquired applications created using the programming languages, libraries standards, services, and tools supported by the providers.[7]

Software as a service (SaaS)

The NIST's definition of cloud computing defines the Software as a Service as: The capability provided to the consumer to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either in a thin client interface, such as a web browser (e.g., web-based email), or a program interface.[8]

2.1. Deployment Clouds

One of the key elements of Cloud Computing is the deployment model in the system. There are a number of different methodologies to define the elements of Cloud. So far there are no unambiguously definitions or standards in cloud. Therefore there are different understandings of deployment models in which no one being better than another, but we are seeing some dominant definitions of cloud computing. The below figure 2 mention the deployment model of cloud computing..[9]

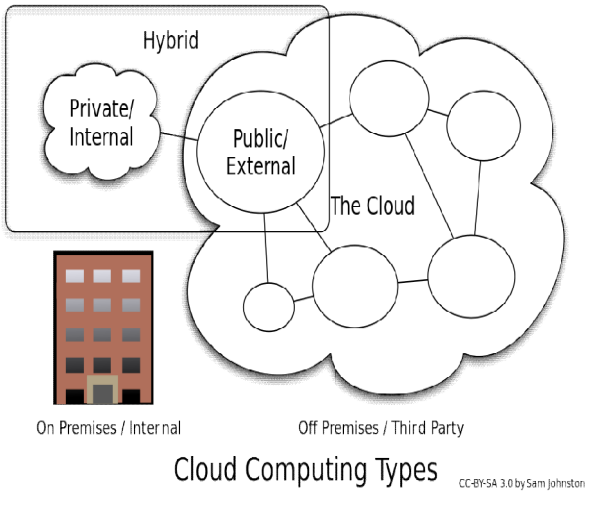

FIGURE 2 DEPLOYMENT MODELS

Private Cloud

Private cloud is the cloud infrastructure operated solely for a single organization, whether managed internally or by a third party, and hosted either internally or externally.[10]

Public Cloud

A cloud is called as a "public cloud" when the services are rendered over a network that is open for public use by cloud. Public cloud services may be free when publically used. Technically there may be little or no difference between public and private cloud architecture.[11]

Hybrid Cloud

Hybrid cloud is a composition of two or more clouds services (private, community or public) that remain distinct entities but are bound together in the system, offering the benefits of multiple deployment models. Hybrid cloud can also mean the ability to connect collocation, managed and/or dedicated services with cloud resources.[12]

III. CLOUD STORAGE

Cloud storage is:

Made up of many distributed resources, but still acts as one, either in a federated or a cooperative storage architecture

Highly fault tolerant through the redundancy and distribution of data resources.

Highly durable through the creation of versioned copies of resources.

Typically eventually consistent with regard to data replicas.

The cloud storage is an extensible storage, so cloud can store more data as much it is needed for future use.

Advantages of Cloud Storage:

1. Usability: All cloud storage services reviewed, have desktop folders for Mac's and PC's. This allows the users to drag and drop files between the cloud storage and its local storage.

2. Bandwidth: It can avoid emailing files to individuals and instead send a web link to recipients through your email.

3. Accessibility: The files which are stored can be accessed from anywhere via Internet.

4. Disaster Recovery: It is highly recommended the businesses have an emergency backup plan ready in the case of an emergency.

5. Cost Savings: Businesses and organizations can often reduce annual operating costs by using cloud storage; cloud storage costs about 3 cents per gigabyte to store data internally.

Disadvantages of Cloud Storage

1. Usability: To be careful when using drag/drop to move a document into the cloud storage folder. This will be permanently move your document from its original folder to the cloud storage location.

2. Bandwidth: Several cloud storage have a specific bandwidth allowance. If an organization of cloud services surpasses the given allowance, the additional charges could be significant.

3. Accessibility: If there is no internet connection, you have no access to your data.

4. Data Security: There are some concerns with the safety and privacy of important data stored remotely.

5. Software: If you want to be able to manipulate your files locally through multiple devices, you'll need to download the service on all devices.[13]

IV. SECURITY RISKS OF CLOUD STORAGE

1. Data Breaches

Cloud computing and services are relatively new, yet data breaches in all forms have existed for years. A study conducted by the Ponemon Institute entitled the "Man In Cloud Attack" reports that over 50 percent of the IT and security professionals surveyed believed their organization's security measures to protect data on cloud services are low.

2. Hijacking of Accounts

The growth and implementation of the cloud in many organizations has opened a whole new set of issues in account hijacking.

3. Insider Threat

An attack from inside the organization may seem unlikely, but the insider threat does exist. Employees can use their *authorized* access to an organization's cloud-based services to misuse or access information such as customer accounts, financial forms, and other sensitive information.

4. Malware Injection

Malware injections are scripts or code embedded into the cloud services that act as "valid instances" and run as SaaS to cloud servers. This means that malicious code can be injected into cloud services and viewed as part of the software or service that is running within the cloud servers themselves.

5. Abuse of Cloud Services

The expansion of cloud-based security services has made it possible for both small and enterprise-level organizations to host vast amounts of data easily. However, the cloud's unprecedented storage capacity has also allowed both

hackers and authorized users to easily host and spread malware, illegal software, and other digital properties.

6. Shared Vulnerabilities

Cloud security is a shared responsibility relationship between the provider and the client. The partnership between client and provider requires the client to take preventative actions to protect their data. While major providers like Box, Drop box, Microsoft, and Google do have standardized procedures to secure their side, fine grain control is up to you, the client.

7. Data Loss

Data on cloud services can be lost through a malicious attack, natural disaster, or a data wipe by the service provider..[14]

V. TECHNOLOGY SUPPORT

In Cloud Computing security, the technologies are discussed by their performance, algorithm and their pros and cons.

5.1. Attribute- Based Encryption

5.1.1. About ABE

Attribute-based encryption is a type of public key in which the secret key of a user and the cipher text are dependent upon attributes of the phrase. In such a system, the decryption of a cipher text is possible only if the set of attributes of the user key matches the attributes of the cipher text.

5.1.2. Concept of ABE

ABE concept is very powerful and a promising mechanism, ABE systems suffer mainly from two drawbacks: non-efficiency and non-existence of attribute revocation mechanism. A crucial security aspect of attribute-based encryption is collusion-resistance: An adversary that holds multiple keys should only be able to access data if at least one individual key grants access.

5.1.3. Performance of 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. 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 the system.

5.1.4. Pros and Cons of ABE

The problem with an attribute based encryption (ABE) scheme is that the data owner needs to use every authorized user's public key to encrypt data. The application of this scheme is restricted in the real environment because it uses the access of monotonic attributes to control user's access in the system..[15][16]

5.2. Key Policy Attribute-Based Encryption (KP-ABE)

5.2.1. About KP-ABE

Key Policy Attribute Based Encryption (KP-ABE) is the modified form of classical model of ABE. Users are assigned in the access structure (AS) over the data attributes. To reflect the access structure the secret key of the user is defined in attributes. Cipher texts are labeled with the sets of attribute and private keys are associated with an monotonic access structure that control which cipher texts a user is able to decrypt. Key policy Attribute Based Encryption (KP-ABE) scheme is designed for one to-many communications.

5.2.2. Concept of KP-ABE

In KP-ABE, users' secret keys are generated based on an access tree that defines the privileges scope of the concerned user, and data are encrypted over a set of attributes.

5.2.3. Performance of KP-ABE

KP-ABE scheme consists of the following four algorithms:

1. Setup: This algorithm takes as input with 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 the user secret keys and is known as 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 an input in an access structure T and the master secret key is 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 attribute.

4. Decryption: It takes an input to the user's secret key SK for an 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.

5.2.4. Pros and Cons of KP-ABE

The problem with KP-ABE scheme is encrypt or cannot decide who can decrypt the encrypted data. It can only choose descriptive attributes for the data, it is unsuitable in some application because a data owner has to trust the key issuer.[]

5.3. Cipher Text Policy Attribute-Based Encryption (CP-ABE)

5.3.1. About CP-ABE

In a CP-ABE scheme, every cipher text is associated with an access policy on attributes, and every user's private key is

associated with a set of attributes. A user is able to decrypt a cipher text only if the set of attributes associated with the user's private key satisfies the access policy associated with the cipher text. CP-ABE works in the reverse way of KP-ABE.

5.3.2. Concept of CP-ABE

In the CP-ABE, the encryptor controls access strategy. The main research work of CP-ABE is focused on the design of the access structure.

5.3.3. Performance of CP-ABE

CP-ABE scheme consists of following four algorithms:

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

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

3. Key-Gen: This algorithm takes an input a set of attributes associated with the user and the master secret key MK in the system. It outputs the 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.

5.3.4. Pros and Cons of CP-ABE

However, the CP-ABE schemes are still not fulfilling the enterprise requirements of the access control which require considerable flexibility and efficiency. CP-ABE has limitations in specifying the policies and managing the user attributes. In the CP-ABE scheme, a decryption keys only support the 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.[18]

5.4. Hierarchical Attribute-Based Encryption

5.4.1. About HABE

Hierarchal attribute-based encryption (HABE) is derived by Wang et al. The HABE model consists of a root master (RM) that corresponds the third trusted party(TTP),multiple domain masters(DMs) in which the top-level DMs corresponds to a multiple enterprise users, and numerous users that corresponds to all the personnel in an enterprise software. This scheme used the property of hierarchal generation if keys in HIBE scheme to generate keys. Then HABE scheme is defined by presenting randomized polynomial time algorithm. The below figure 3 represents the Hierarchal structure.

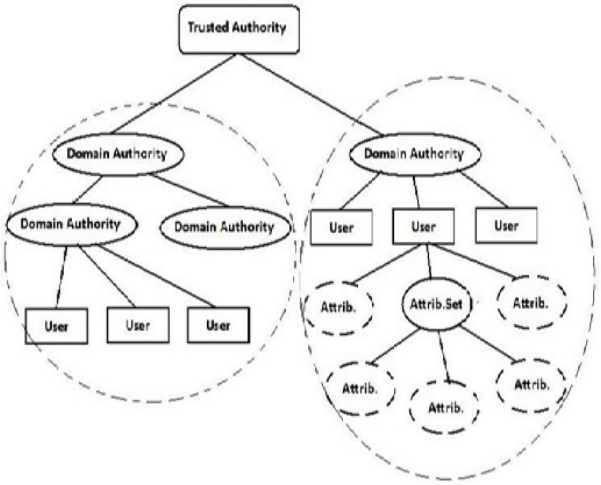

Figure 3 HIERARCHAL STRUCTURE

5.4.2. Concept of HABE

In the HABE scheme, there are multiple keys with different usages of resources. Therefore, we first provide a summary of the most relevant keys to serve as a quick reference.

5.4.3. Performance of HABE

Then, HABE scheme is defined by presenting the randomized polynomial time algorithms as follows:

1. Setup (K) (params,MK0): The RM takes a sufficiently large security parameter K as input, and outputs system parameters params and root master key MK0.

2. Create DM (params , MKi, PKi+1) (MKi+1): Whether the RM or the DM generates master keys for the DMs directly under it using params and its master key.

3. CreateUser(params,MKi, PKu, PKa) (SKi,u, SKi,u,a): The DM first checks whether U is eligible for a, which is administered by itself. If so, it generates the user identity secret key and the user attribute secret key for U, using params and its master key; otherwise, it outputs will be"NULL".

4. Encrypt(params; f ;A; {PKa|a E A})(CT): A user takes a file f, a DNF access control policy A, and public keys of all attributes in A, as inputs, and outputs a cipher text CT.

5. Decrypt(params, CT, SKi,u, {SKi, u, a|aECCj}□(f):The user, whose attributes which satisfy the j-th conjunctive clause CCj, takes the params, ciphertext, the user identity secret key, and the user attribute secret keys on all attributes in CCj, as inputs, to recover the plaintext.

5.4.4. Pros and Cons of HABE

In practice, it is unsuitable to implement. Since all attributes in one conjunctive clause in this scheme may be administered by the same domain authority, the same attribute may be administered by multiple domain authorities.[19]

5.5. Multi-Autthority Attribute-Based Encryption

5.5.1. About MABE

Multi-authority attribute-based encryption scheme uses the multiple parties to distribute attributes for users in the resources. A Multi Authority ABE system which composed of K attributes authorities and one central authority. Each attribute authority is also assigned a value dk.

5.5.2. Concept of MABE

A randomized algorithm which must be run by some trusted third party authority (e.g. central authority).Takes as input the security parameter K. In outputs a public key, the secret key pair for each of the attribute authorities(PKa , SKa), and also outputs a system public key and a master secret key which will be used by the central authority(PKca , SKca).

5.5.3. Performance of MABE

For Attribute Key Generation algorithm takes an input the authority's secret key, the authority's value dk, the user's GID, and a set of attributes in the authority's domain AkC and the outputs of the secret key for the user. The Encryption is done by an randomized algorithm run by the sender it takes a set of attributes for each authority, a message, and the system public key as input and outputs of the cipher text. A decryption algorithm run by the user takes a cipher text as input, which was encrypted under the attribute set A and the decryption keys for an attribute set Au and outputs a message M. It allows any polynomial number of an independent authorities to monitor the attributes and the distributed private keys and tolerate any number of a corrupted authorities. In this model, a recipient is defined not by a single string, but by a set of attributes.

5.5.4. Pros and Cons of MABE

Complication in multi-authority scheme required that each authority's attribute set be disjoint .[20]

VI. COMPARISON

The table represents the comparison of KP-ABE,CP-ABE, HABE ,MABE.[21]

S.NO	ALGORITHM	KP-ABE	CP-ABE	HABE	MABE
1	Setup	(K) (PK ,MK)	(K) (PK ,MK)	RM(K) (Params,MK)	(K) (PKa,SKa,SPKca MSKca)
2	Encryption	(M,PK,A) (CT)	(M,PK,AS) (CT)	(f,DNF,AS,PK) (CT)	(A ,M,SPK) (CT)
3	Key Generation	(MK,AS,PK) (SK)	(A, MK) (SK)	DM(PK,MKi,PKi+1) (MKi+1). USER(P K; MKi; P Ku; PKa) SKu	AKG(SKa,dk,GID,AKC) (SKu) CKG(MSKca,GID) (SKu)
4	Decryption	(SK,CT,PK) (M)	(CT,SK) (M)	(Params,CT,SK,A) (M)	(CT,DK) (M)
5	Limitation	It cannot decide who can encrypt data.	Decrypt key only support user attribute that are organized logically.	Unsuitable to implement	Each authority attribute set should be disjoint
6	Component	Data is associated with an access policy.	CT is associated with an access policy .	Hierarchical generation of key.	Multiple authorities
7	Efficiency	Average	Average	Better	Scalable
8	Secured access control	Low	Average	High	Average
9	Computational overhead	High	Average	More	More
10	Data confidentiality	No	Yes	Yes	Yes
11	User accountability	No	no	No	Yes
12	Scalability	No	yes	No	Yes
13	User revocation	No	no	Yes	Yes
14	Collusion Resistent	Yes	Yes`	Yes	Yes

VII. COMPARATIVE ANALYSIS

(I) Based On Usage Count

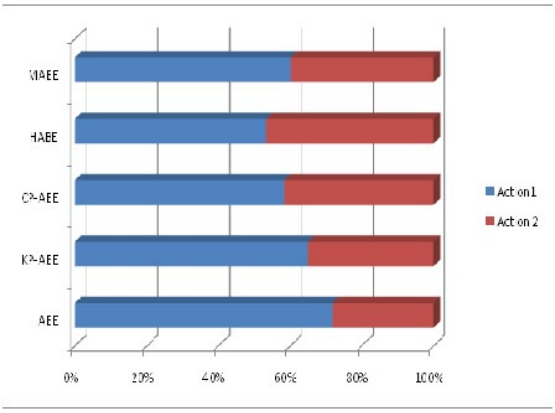

FIGURE 4 BASED ON USAGE COUNT

(ii) Based On Performance

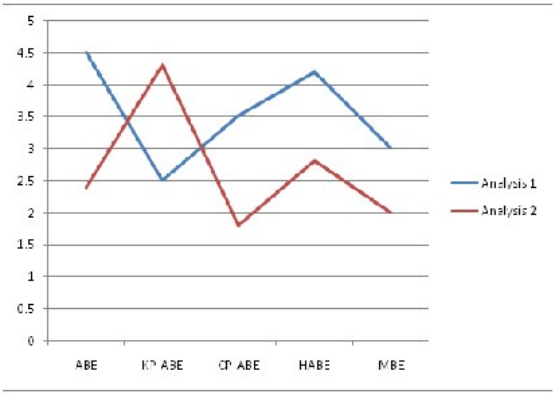

FIGURE 5 BASED ON PERFORMANCE

VIII. CONCLUSION

In this paper, we have overviewed different attributes based encryption (ABE) schemes that can be used in cloud systems for flexible, scalable and fine grained access control. In ABE scheme, there are both the 'secret key' and 'ciphertext' are associated with a set of attributes. ABE is further modified into KP-ABE that provides fine grained access control. In KP-ABE, attribute policies are associated with keys and data is associated with the attributes. Keys associated with the policy that is satisfied by the attributes can decrypt the data. Moreover, we have explored CP-ABE and CP-ASBE. The CP-ABE scheme differs from KP-ABE in such a way that in CP-ABE, ciphertext is associated with an 'access tree structure' and each user 'secret key' is embedded with a 'set of attributes'. 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. HASBE combines the functionalities of HIBE and ASBE.

REFERENCES

[1]. Duan, Yucong; Fu, Guohua; Zhou, Nianjun; Sun, Xiaobing; Narendra, Nanjangud; Hu, Bo. *"Everything as a Service (*XaaS*) on the Cloud: Origins, Current and Future Trends". IEEE*.3
[2]. Amies, Alex; Sluiman, Harm; Tong, Qiang Guo; Liu, Guo Ning (July 2012). "Infrastructure as a Service Cloud Concepts". *DevelopingandHosting Applications on the Cloud*. IBM Press. *ISBN 978-0-13-306684-5*.
[3]. *Boniface, M.; et al. (2010). Platform-as-a-Service Architecture for* Real-Time Quality of Service Management in Clouds. 5th International Conference on Internet and Web Applications and Services (ICIW).
[4]. "Definition of: SaaS". *PC Magazine Encyclopedia*. Ziff Davis. Retrieved 14 May 2014.
[5]. Zhang, R., Lee, M., & Liu, L. (2010). Security models and requirements for healthcare application clouds. In 3rd International Conference on Cloud Computing. doi:10.1109/CLOUD.2010.62
[6]. "There's No Such ThingAs APrivate Cloud Cloud-computing -". 2013-01-26. Archived from the original on 2013-01-26
[7]. *Rouse, Margaret.* "What is public cloud?". *Definition from Whatis.com.* Retrieved 12 October 2014.
[8]. *Désiré Athow.* "Hybrid cloud: is it right for your business?". *TechRadar*. Retrieved 22 April 2015.
[9]. Mu-Hsing Kuo, A. (2011). Opportunities and challenges of cloud computing to improve health care services. Journal of Medical Internet Research. PMID:21937354
[10]. Kresimir Popovic and Zeljko Hocenski. Cloud computing security issues and challenges, in: MIPRO, 2010 Proceedings of the 33rd International Convention, 2010.p.344-349.
[11]. Rakesh Bobba, Himanshu Khurana and Manoj Prabhakaran, "Attribute- Sets: A Practically Motivated Enhancement to Attribute-Based Encryption", July 27, 2009.
[12]. V. Goyal, O. Pandey, A. Sahai, and B. Waters. "Attribute-Based Encryption for Fine-grained Access Control of Encrypted Data". In Proc. of CCS'06, Alexandria, Virginia, USA, 2006.
[13]. Nuttapong Attrapadung, Benoit Libert and Elie de Panafieu, "Expressive key-policy attribute-based encryption with constantsize ciphertexts," Research Center for Information Security, AIST (Japan), Universitecatholique de Louvain, ICTEAM – Crypto Group (Belgium), Ecoleno rmale superieure, Cachan (France).
[14]. J.Bethencourt, A. Sahai, and B. Waters. "Ciphertext-Policy Attribute-Based Encryption." In Proc. of SP'07, Washington, DC, USA, 2007.
[15]. 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, April 2012.
[16]. Chase Melissa, "Multi-authority attribute based encryption", In Theory of Cryptography, pp. 515-534, 2007.
[17]. Ziefle, M., & Rocker, C. (2010). Acceptance of pervasive healthcare systems: A Comparison of Different Implementation Concepts. In 4th international conference on pervasive computing.
[18]. J.Bethencourt, A. Sahai, and B. Waters. "Ciphertext-Policy Attribute-Based Encryption." In Proc. of SP'07, Washington, DC, USA, 2007.
[19]. 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, April 2012.
[20]. Chase Melissa, "Multi-authority attribute based encryption", In Theory of Cryptography, pp. 515-534, 2007.
[21]. Ziefle, M., & Rocker, C. (2010). Acceptance of pervasive healthcare systems: A Comparison of Different Implementation Concepts. In 4th international conference on pervasive computing.