A Hierarchical Third Party Based Model for Security & Integrity in Multi Cloud Computing Environment - A Survey

Ankit Prajapati[1]
[1]Student
[1]Department of Computer Science & Engineering
[1]Narnarayan Shastri Institute of Technology, Jetalpur

Abstract— It has been observed that the concept of cloud computing is increasing day by day in the world of IT industry in recent years. Data Owners are progressively counting on the cloud services for storing their data, backing up their data and use it in real time when ever needed. Since the data stored is online it requires data owners to entrust their valuable data to cloud service providers, so there ought to be increased security and privacy concerns on data. In this paper, various attribute based encryption schemes are explained such as key - policy attribute base encryption scheme , cipher - policy attribute based encryption scheme , cipher - policy attribute set based encryption scheme, Hierarchical identity based encryption scheme , Hierarchical attribute based encryption scheme and hierarchical attribute set based encryption scheme for providing security , integrity and fined grained access control of the outsourced data along with their strength and weaknesses. Also a new mechanism is presented, a hybrid model for providing security in cloud computing environment. This model combines the advantages of two most popular existing cloud security models.

Key words: cloud computing , data security , data integrity , attribute based encryption , fined grained access control , HASBE

I. Introduction

Cloud computing is a new computing paradigm that is built on virtualization, parallel and distributed computing, utility computing, and service-oriented architecture. In the last several years, cloud computing has emerged as one of the most influential paradigms in the IT industry, and has attracted extensive attention from both academia and industry. Cloud computing holds the promise of providing computing as the fifth utility [1] after the other four utilities (water, gas, electricity, and telephone). The benefits of cloud computing include reduced costs and capital expenditures, increased operational efficiencies, scalability, flexibility, immediate time to market, and so on .

Different cloud delivery models have been proposed, including Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) [20]. The Fig 1 represents these delivery models with example.

A. *Software as a Service (SaaS):*

Here interaction between the consumer and the service is hosted as part of the service in the cloud. Salesforce's Customer Relation Management (CRM) System is SaaS System.

B. *Platform as a Service (PaaS):*

Here consumer can deploy their own software's and applications in the cloud. Google

C. *Infrastructure as a Service (IaaS):*

In this service model consumer can control and manage the system but they can't control the infrastructure of the cloud.

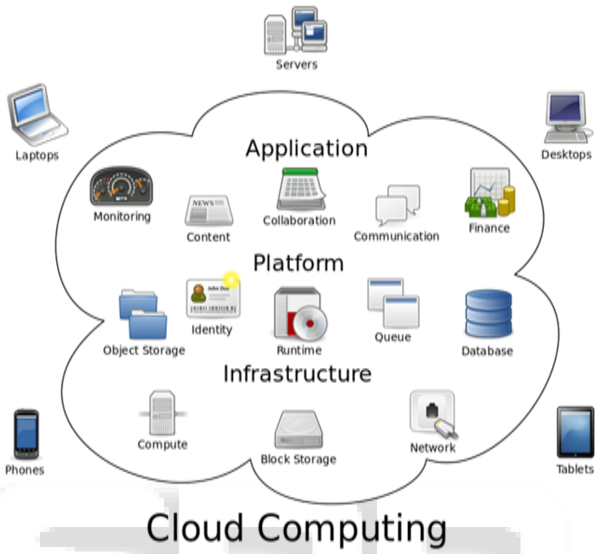

Fig. 1: represent these delivery models with example

Numerous commercial cloud computing systems have been built at different levels, e.g., Amazon's EC2 [2] , Amazon's S3 [3], and IBM's Blue Cloud [4] are IaaS systems, while Google App Engine [5] and Yahoo Pig are representative PaaS systems, and Google's App [6] and Salesforce's Customer Relation Management (CRM) System [7] belong to SaaS systems. With these cloud computing systems, on one hand, enterprise users no longer need to invest in hardware/software systems or hire IT professionals to maintain these IT systems, thus they save cost on IT infrastructure and human resources; on the other hand, computing utilities provided by cloud computing are being offered at a relatively low price in a pay-as-you-use basis.

Although cloud computing has brought many benefits to the IT companies, but the most important drawback concerning the cloud is security and privacy of the outsourced data so cloud data security is a major concern for data owners while using cloud services. While using cloud services the users got to hand over their data to cloud service providers. The cloud service provider is a commercial entity which cannot be totally trusted. Data is an extremely important property of a data owner, an organization or any enterprise so security of the data is the major concern. So data owners will first certify that their data is kept confidential from unauthorized personal. Not only security but other issues that are important is data confidentiality, flexibility and fine grained access control in cloud computing environment.

Access control is also a crucial issue and numerous models are proposed for it. Bell-La padula(BLP) [8] and Biba [9] are two famous security models. To achieve a fine grained access control the number of schemes [10]-[13] have been presented but this schemes are only applicable to the systems in which data owners and the service providers are on the same trusted domain . Since data owners and service providers are usually on different trusted domain this scheme cannot be applied , a new scheme called attribute based encryption [14] was proposed.

In this paper, we study all the attribute based encryption schemes such as key - policy attribute base encryption scheme(KP-ABE) , cipher - policy attribute based encryption scheme(CP-ABE) , cipher - policy attribute set based encryption scheme(CP-ASBE), Hierarchical identity based encryption scheme(HIBE) , Hierarchical attribute based encryption scheme and hierarchical attribute set based encryption scheme(HASBE).We will also study the HASBE scheme in detail and propose a future work on the basis of it.

II. RELATED WORK

In this section we review the concept of Attribute Based Encryption and provide a brief overview of the all the attribute based scheme. After that we examine the existing HASBE scheme in detail.

A. *Attribute - Based Encryption:*

The concept of attribute-based encryption was first proposed in a landmark work by Amit Sahai and Brent Waters [15] and later by Vipul Goyal, Omkant Pandey, Amit Sahai and Brent Waters [14]. It is a type of public-key encryption in which the secret key of a user and the ciphertext are dependent upon attributes of the user (e.g. the country he lives, or the kind of subscription he has). In such a system, the decryption of a ciphertext is possible only if the set of attributes of the user key matches the attributes of the ciphertext [15].

B. *Key Policy Attribute - Based Encryption:*

The concept of KP-ABE was introduced by Vipul Goyal, Omkant Pandey, Amit Sahai and Brent Waters [14] in which the ciphertext is associated with set of the attributes of the user and user's decryption scheme is dependent on monotonic tree access structure. Decryption is only possible if the attributes associated to the ciphertext satisfies the tree access structure. KP-ABE scheme is a public key encryption technique that is desinged for one to many communications. The use of this scheme provides fine grained access control as this scheme reduces the most of the computational overhead to the cloud servers.

C. *Cipher Policy Attribute - Based Encryption:*

In CP-ABE Scheme [16] the roles of ciphertext and decryption keys are reversed than the KP-ABE scheme. The ciphertext is encrypted using the tree access policy and decryption key of the user is depended on the set of attribute set. As long as the set of attributes of decryption key satisfies the tree access policy associated with the ciphertext ,user can decrypt the ciphertext.

In this scheme decryption keys only support user attributes that are organized locally as a single

Set so user can only use all the possible combination of attribute in a single set issued in their keys to satisfy policies [17]. This is the main draw-back of the CP-ABE scheme so Bobba [17] introduced a new scheme CP-ASBE or ASBE that is an extended version of the CP-ABE.

D. *Cipher Policy Attribute Set - Based Encryption:*

CP-ASBE is an extended form of CP-ABE which organizes user attributes into a recursive set structure. The following is an example of a key structure of depth 2, which is the depth of the recursive set structure:

{Employee: VQUBE, Post: Developer, Software Engineer,
{Project Id: 11, Post: Developer}
{Project Id: 23, Post: Software Engineer}}

The above example represents the recursive employee structure of depth 2, One Employee of VQUBE Company can be Developer for ProjectId11 and he can be also work as a Software Engineer for ProjectId23. So a single attribute-Post can be assigned to multiple values. So from the above example we can say that ASBE support flexibility [20]. ASBE can enforce dynamic constraints on combining attributes to satisfy a policy which results in greater flexibility in access control. As a recursive attribute set is assigned to a user in the ASBE scheme, attributes from the same set can be easily combined, while attributes from different sets can only be combined with the help of translating items using ASBE. This problem can be solved simply by assigning multiple values of the group of attributes in different sets. Existing ABE schemes are not suitable for some applications where efficient ciphertext policy encryption of ABSE is more effectively used. ASBE’s capability of assigning multiple values for the same attribute enables it to solve the user revocation problem efficiently, which is difficult in CP-ABE [21].

E. *Hierarchical Identity Based Encryption Scheme:*

Hierarchical Identity based encryption Scheme (HIBE) is that the hierarchic variety of IBE[19]. The conception of HIBE theme will facilitate to elucidate the definition of security. In a regular IBE (1-HIBE) ,there is only 1 private key generator (PKG) that distributes private keys to every users, having public keys area unit their primitive ID (PID) absolute strings. A two-level HIBE (2-HIBE) theme consists of a root PKG, domain PKGs and users, all of that area unit related to PID’s. A users public key consists of their PID and their domains. during a 2-HIBE, users retrieve their private key from their domain PKG. The private key PK is compute by Domain PKGs of any user in their domain, their domain secret key-SK are often provided and antecedently requested from the foundation PKG. Similarly, is for variety of sub-domains. There conjointly includes a trusted third party or root certificate authority that permits a hierarchy of certificate authorities: Root certificate authority problems certificates for alternative authorities or users in their various domains. The initial system doesn't yield such structure. However, a hierarchy of PKG is reduces the employment on root server and permits key assignment at many levels. But the main problem of the system is the key management as letting each user obtain the key from owner [20].

F. Hierarchical Attribute Set Based Encryption Scheme:

Hierarchical attribute set based encryption scheme is proposed by extending the ciphertext policy attribute set based encryption scheme [18]. In HASBE scheme the user keys are associated with attribute set and ciphertext are associated with the tree access structure. If attributes of user key match with access structure of ciphertext then only the user can decrypt the ciphertext [18]. HASBE scheme provides flexible, scalable and fine grained access control over the outsourced data. The main entities in the HASBE scheme are trusted third party auditors , domain/sub domain authorities and cloud service providers. In HASBE scheme trusted authority is subdivided into sub domain authorities which manages the data owners and data users respectively.

Parameters	KP-ABE	EKP-ABE	CP-ABE	CP-ASBE	HIBE	HASBE
Access Control	Low	Better than KP-ABE	Moderate	Better than CP-ABE	Respectively Very low	Flexible High
Security	Low	Better than KP-ABE	Moderate	Better than CP-ABE	High	High
Computatio-nal overhead	High	Low	Moderate	Low	High	High
Efficiency	Moderate	Higher than KP-ABE	Moderate	Low	Low	Low
Scalability	Low	Low	Low	High	Low	High

Table 1: Comparison Between attribute based encryption schemes

III. EXISTING SYSTEM

The cloud computing system consists of five types of parties: a cloud service provider, data owners, data consumers, a number of domain authorities, and a trusted authority. The cloud service provider is responsible for providing the data storage facilities and other resource services to the cloud users. Data owners store their files on the cloud after encrypting the files for sharing it with the data users or data consumers. To access the shared data files, data consumers download encrypted data files of their interest from the cloud and then decrypt them[18]. Each data owner/consumer is managed by a domain authority. A domain authority is managed by its parent domain authority or the trusted authority. Data owners, data consumers, domain authorities, and the trusted authority are organized in a hierarchical manner as shown in Figure [18].

The trusted authority is the root level authority which is responsible for managing the top level domain authorities and each domain authority is responsible for managing the domain authorities at the next level/sub domain authorities or the data owners/consumers in its domain.

In cloud system, neither data owners nor data consumers will be always online. They come online only when necessary, while the cloud service provider, the trusted authority, and domain authorities are always online. The cloud is assumed to have abundant storage capacity and computation power. In addition, we assume that data consumers can access data files for reading only.

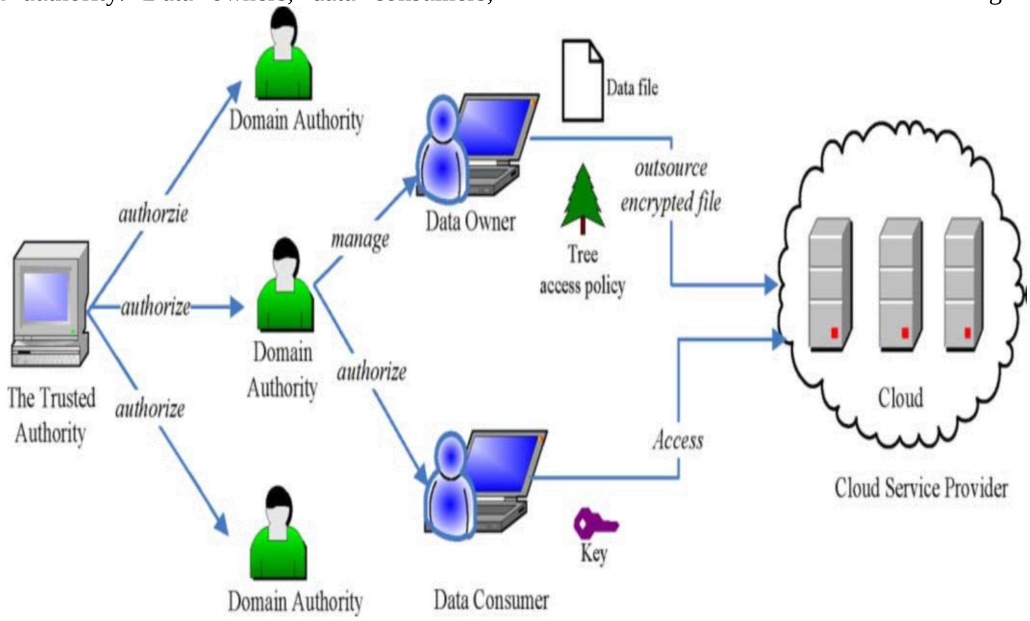

Fig. 2: Existing System

A. Limitations of Existing System:

Although the present model/HASBE scheme overcomes the limitations of the third party auditors based scheme. But it is very complex hierarchical structure. Also presence of multiple domain authority creates ambiguity. It is inferred that user has no control over the integrity of the data as the data stores in on the cloud. The domain authority/Service providers modifies or deletes the data on the cloud without the permission of the user. In the existing system the single third party auditor is responsible for maintaining the different cloud we can say multiple clouds also[21]. So, if the third party auditor is compromised in any means than data might be leaked from all the clouds linked with the third party auditors also if any unauthorized user can get the access to data than the confidentiality, privacy and integrity of the data might be compromised which creates a serious problem.

IV. Proposed Methodology

So, In this paper new mechanism is proposed to have TPA (Third Party Auditor) on the same cloud of the service providers. The HASBE Scheme will be used on the cloud by the trusted authority to maintain the integrity of the data and the data of the users will be managed by the trusted authority itself providing a more secure mechanism, reduce computational overhead, Authenticate Data Security ,Scalability , Expressiveness.

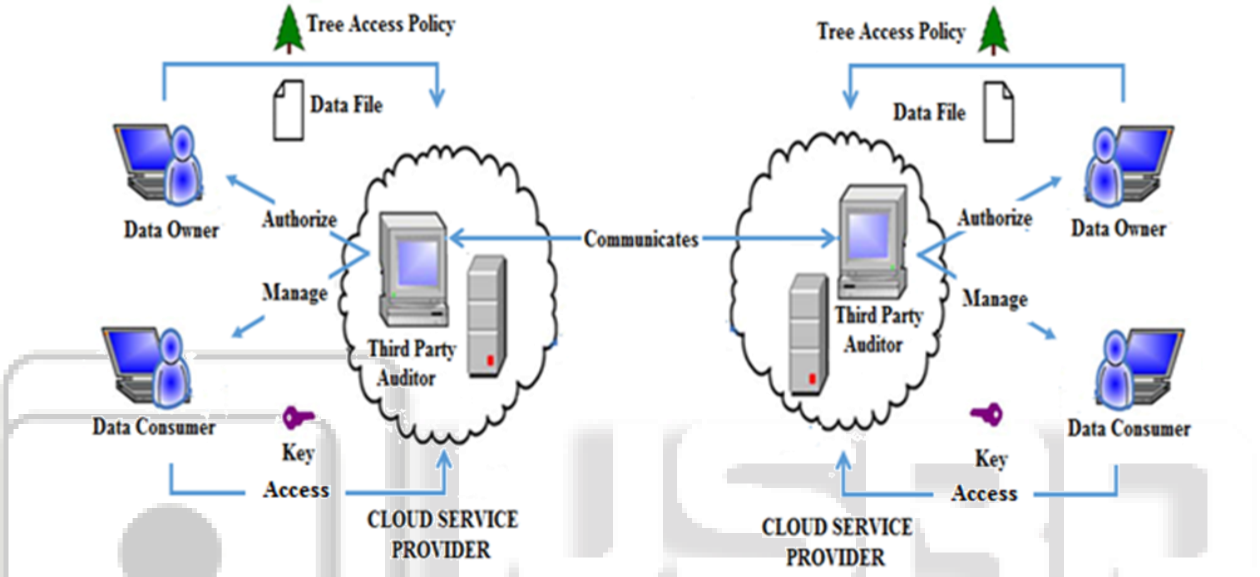

Fig. 3: Proposed Methodology

In our proposed model, the client or user interacts with the third party auditor. The third party auditor is an authorized person appointed by the owner of the cloud. In our model, both data and auditor are present at the cloud servers site. It is responsible for performing functions at all the three layers.

(1) The first layer is USER AUTHENTICATION.
(2) The second layer is DATA ENCRYPTION AND DATA PROTECTION.
(3) The third layer is DATA DECRYPTION.

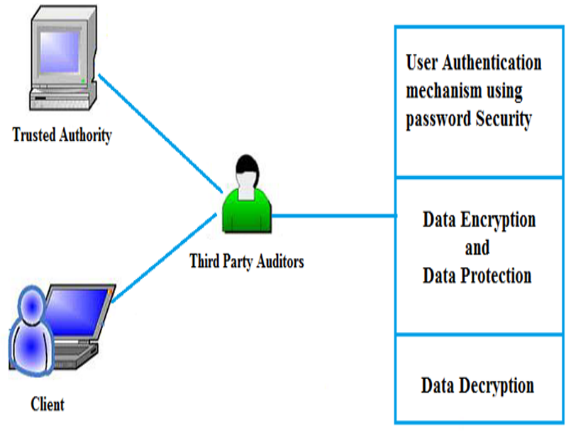
Trusted Authority
Third Party Auditors
Client
User Authentication mechanism using password Security
Data Encryption and Data Protection
Data Decryption

Fig. 4: Layer Architecture

V. Conclusion

In this paper, comparison of the different attribute based encryption methods are done from the previous papers and identified the HASBE scheme provides the best security and integrity than others. Also here a new model/technique is presented for the cloud security using HASBE scheme. Which combines the features of present hierarchical model and the third party auditor based model. Moreover, future planning is to implement this new mechanism in practical to improve the security and integrity in cloud.

VI. Acknowledgement

I would like to thanks all the authors whom I have referred for giving their suggestions and making the material available for us to refer.

References

[1] Cloud computing and emerging it platforms: vision, hype and reality for delivering computing as the 5th utility. R. Buyya, C. Shin Yeo, J. Broberg, and I. Brandie. s.l.: Future Generation Computer Systems, 2009, Vol. 25, pp. 599-616.
[2] Amazon Elastic Compute Cloud (Amazon EC2) [online]. https://aws.amazon.com/ec2/. [Online]
[3] Amazon web services (AWS).

https://s3.amazonaws.com/. [Online]

[4] Martin, R. IBM brings cloud computing to earth with massive new data centers, Information week. http://www.informationweek.com/news/hardware/data_centers/209901523. [Online] 2008.

[5] Google App Engine. http://code.google.com/appengine/. [Online]

[6] Like technology from an advanced alien culture: Google apps for education at ASU. Lane, K. Barlow and J. s.l.: ACM New York, NY, USA ©2007, 2007, pp. 8-10.

[7] Salesforce.com: Raising the level of networking. Barbara, B. s.l.: Inf. Today, 2010, Vol. 27, pp. 45-45.

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

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

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

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

[12] 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.

[13] J. Li, N. Li, and W. H. Winsborough, "Automated trust negotiation using cryptographic credentials," in Proc. ACM Conf. Computer and Communications Security (CCS), Alexandria, VA, 2005.

[14] 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.

[15] A. Sahai and B. Waters, "Fuzzy identity based encryption," in Proc. Acvances in Cryptology—Eurocrypt, 2005, vol. 3494, LNCS, pp. 457–473.

[16] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute based encryption," in Proc. IEEE Symp. Security and Privacy, Oakland, CA, 2007.

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

[18] Zhiguo Wan, Jun'e Liu , Robert H. Deng. A Hierachical Attribute Based Solution For Flexible and Scalable Access Control in Cloud Computing. 2, s.l.: IEEE, 2012, Vol. 7, pp. 743-754.

[19] D. Bonech and M. Franklin. "Identity-Based Encryption from the weil Pairing." Proc. of CRYPTO'01 , Santa Barbara, California, USA, 2001

[20] Survey on Multi Authority Attribute Based Encryption for personal Health Record in Cloud Computing. Vahidhunnisha J, Ramasamy S, Balasubramaniam T. 2, s.l.: International Journal of latest trends in engineering and technology, 2013, Vol. 3. 2278-621X.

[21] Ensuring Integrity Proof in Hierarchial Attribute Encryption Scheme Using Cloud Computing. Dr. R Aparna, Pallavi R. 1, s.l. : International Journal of Cognitive Science, Engineering and Technology, 2013, Vol. 1.