ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 2, Issue 3, May 2013

HASBE: A Hierarchical Attribute-Based Solution for Flexible and Scalable Access Control by Separate Encryption/Decryption in Cloud Computing

[1]S. Gokuldev, [2]S.Leelavathi
[1]Associate Professor, [2]PG Scholar
[1,2]Department of Computer Science and Engineering
[1,2]SNS College of Engineering, Coimbatore, India

Abstract-Cloud computing has emerged as one of the most important paradigms in the IT industry for last few years. In general data owners and service providers are not in the same trusted domain in cloud computing. Service providers should not be a trusted one anyhow they are all third party. The system focuses on a novel technique to Hierarchical Attribute Set Based Encryption (HASBE); it is driven by the Cipher Policy attribute-based encryption (CP-ABE) with a hierarchical structure of cloud users. This approach not only achieves scalability, it achieves both flexibility and fine-grained access control of data in cloud. The work for storing the data in encrypted form is a common method of information privacy protection. Cloud system is responsible for both tasks on storage and encryption or decryption of data. Introduce a new business model for cloud computing based on the concept of separating the encryption and decryption service from the storage service. The proposed work focuses CRM (Customer Relationship Management) for business model that is driven by the category of Software as a Service (Saas) method in cloud. Using this scheme it achieves the flexible, scalable and fine grained access control of data. It also achieves high secure and effective user revocation in cloud environment.

Keywords: **Cipher Policy attribute-based encryption (CP-ABE), Hierarchical Attribute Set Based Encryption (HASBE), Cloud Computing, Customer Relationship Management (CRM), Software as a Service (Saas).**

I. INTRODUCTION

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 are IaaS 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 cloud service supplier directs a cloud to offer data storage service. Data owners encrypt their statistics files and store them in the cloud for sharing with data customers. To contact the shared data files, data customers download encrypted data files of their interest from the cloud and then decrypt them. Each data owner/consumer is managed by a domain influence. A domain authority is directed by its parent domain authority or the believed authority. Data owners, domain authorities, data consumers, and the conditioned authority are prearranged in a hierarchical way**.** The confidences authority is the root authority and responsible for organization top-level domain authorities.

Data owners/consumers may communicate 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.In our system, neither data owners nor data customers will be forever online. They arrive online only when essential, whereas the cloud service provider, the confidences authority, and domain authorities are always online. The cloud is unspecified to have plentiful storage capacity and computation power. Additionally, we suppose that data customers can right of entry data files for reading only.

This paper deals with a novel business model for cloud computing supported on a separate encryption and decryption service in Fig. 1. 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

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 2, Issue 3, May 2013

user data. Once the provider of Encryption/Decryption as a Service has completed, encrypting user data supplied it off to an application (e.g. a CRM system). The encryption/decryption system must delete all encrypted and decrypted user data.

The observation of separating authority is often applied in business management. For example, responsibility for a company's finances is divided between the accountant and cashier. In business processes, the accountant is responsible for keeping accounts, while the cashier is in charge for making payments. By keeping these two functions divide, the company can prevent the accountant from misrepresenting accounts and embezzling corporate finances. Authorized documents frequently need to be stamped with two seals (i.e., the corporate seal and the legal representative's seal), thus avoiding a staff member from abusing his position to issue fake documents, and these seals are normally delegated to two dissimilar people. These examples of the division of authority are designed to avoid a concentration of power which could raise operational risks.

In a cloud computing environment, the user usually uses cloud services with exact purposes, e.g., Salesforce.com's CRM service, SAP's ERP services, etc. Data generated while using these services is then stored on storage facilities on the cloud service. This work highlights the addition of an independent encryption/decryption cloud service. This type of business model, with the result that two service providers split responsibility for data storage and data encryption/decryption. Fig 1 illustrates the concept of our proposed business model. It presents an example in which the user utilizes separate cloud services for CRM, storage and encryption/decryption. According to the user's needs, CRM Cloud Services could be transferred for other function-specific application services (e.g., ERP Cloud Services, Account Software Cloud Services, Investment Portfolio Selection and Financial Operations Cloud Services).

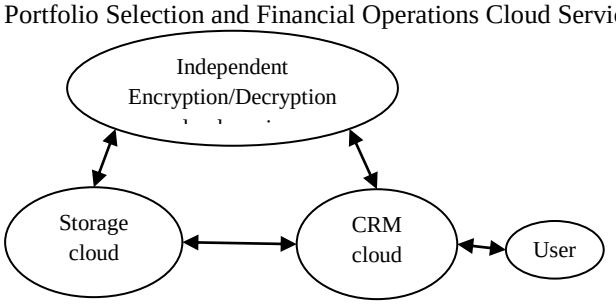

Fig 1: Business model concept integrating separate cloud services for Data encryption or decryption, CRM and storage

The rest of the paper is organized as follows. Section II provides an overview on related work. The Section III deals with proposed work. In Section IV analyze the experimental results. Lastly, we conclude the paper in Section V.

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 [1] 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 [2] 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 user's access the data and the system.

In [3] discussed a new form of cloud computing environment that represent attribute based access control mechanism. It shows the way to propose of attribute based access control instrument for cloud computing. Yan Zhu et.al [4] proposed an efficient temporal access control encryption scheme for cloud services with the assist of cryptographic integer contrasts and a proxy-based re-encryption mechanism on the current time. It also offered a dual proportional appearance of integer choices to enlarge the power of attribute expression for implementing various temporal constraints.

Shucheng Yu et.al [5] paper addressed this demanding open concern by, on one hand, defining and enforcing access policies based on data attributes and on the other, the data owner to delegate most of the computation

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 2, Issue 3, May 2013

tasks involved in fine-grained data access control to untrusted cloud servers without disclosing the underlying data contents. We achieve this goal by combining techniques of attribute-based encryption (ABE), proxy re-encryption, and lazy re-encryption. The suggested method also has most important properties of user access privilege privacy and user secret key accountability. Guojun Wang et.al [6] proposed a hierarchical attribute-based encryption scheme (HABE) by combining a hierarchical identity-based encryption (HIBE) scheme and a ciphertext-policy attribute-based encryption (CP-ABE) scheme.

The literature encloses many clarifications of cloud computing [12]. After compiling learned descriptions of cloud computing, Vaquero, Rodero-Merino, Cancers, and Lindner proposed that cloud computing could be described as the incorporation of virtual resources according to user requirements, flexibly combining resources including hardware, development platforms and various applications to create services [13].

In a cloud computing environment, the user normally utilizes cloud repairs with specific functions, e.g., Salesforce.com's CRM service [14], SAP's ERP services [15], etc. Data produced while using these services is then stored on storage facilities on the cloud service. This study emphasizes the addition of an independent encryption/decryption cloud service to this type of business model, with the result that two service providers divide responsibility for data storage and data encryption/decryption.

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. To end with, we realized the suggested proposal, and accomplished complete performance analysis and evaluation, which demonstrated its effectiveness and benefits over obtainable schemes. The scope of the project is to build up a new computing technology necessitates users to hand over their precious data to cloud providers, thereby raising safety and confidentiality concerns on outsourced data.

Several methods utilizing attribute-based encryption (ABE) have been proposed for access control of outsourced data in cloud computing; though, most of them suffer from hardness in implementing complex access control policies. 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.

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.

A. Developing the cloud Environment

Fig. 2 represents a 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 an 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.

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 2, Issue 3, May 2013

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.

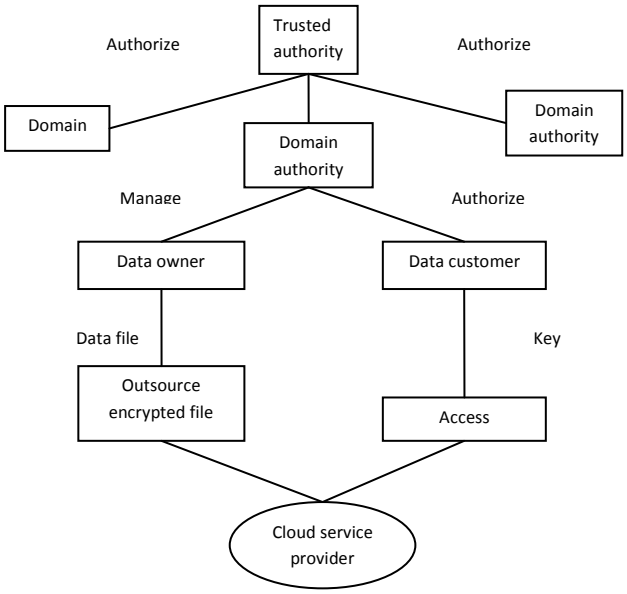

Fig 2: Cloud environment development

B. Design the security model

This work, assumes that the cloud server supplier is untrusted in the sense that it may collude with spiteful users (short for data owners/data consumers) to yield file comfortable accumulated in the cloud for benefit. In the hierarchical structure of the system users, each party is related with a public key and a private key, with the latter being reserved clandestinely by the party.

The conditioned authority acts as the root of trust and allows the top-level domain authorities. A domain authority is trusted by its lesser domain authorities or users that it controls, but may try to get the private keys of users outside its domain. Users may trying to access data files either within or outside the scope of their access privileges, so malevolent users may collude with each other to get sensitive files beyond the privileges.

C. 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.

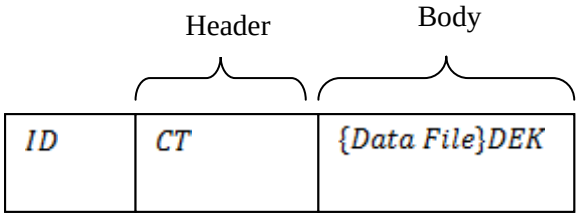

Fig 3: Format of a data file on the cloud

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. Fig. 3 represents data file format of cloud.

The main operation can be described as HASBE: System Setup, Top-Level Domain Authority Grant, New Domain Authority/User Grant, New File Creation, User Revocation, File Access, and File Deletion.

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 2, Issue 3, May 2013

*System Setup***:** When the system is set up, the conditioned authority selects a bilinear group and some random numbers. When Public Key (PK) and Master Secret Key (MK_0) may be generated and also there will be several exponentiation operations.

Top-Level Domain Authority Grant: A domain authority is associated with a unique ID and a recursive attribute set $A = \{A_0, A_1, \ldots..A_m\}$, where $A_i = \{a_{i,1}, a_{i,2}, \ldots\ldots, a_{i,n}\}$ with $a_{i,j}$ being the j^{th} attribute in A_i and n_i being the number of attributes in .When a new top-level domain authority wants to join the system, then the trusted authority will first verify whether it is a valid domain authority. If so, the trusted authority calls CreateDA to generate the master key for DA_i. After getting the master key, DA can authorize the next level domain authorities or users in its domain.

New Domain Authority/User Grant: In this operation, a new user/new domain authority is linked with an attribute set, which is the set of higher level domain authority. The main computation overhead of this operation is rerandomizing the key.

*New File Creation***:** In this operation, the data owner needs to encrypt a data file using the symmetric key DEK and then encrypt DEK using HASBE. The complexity of encrypting the data file with Data Encryption Key (DEK) depends on the size of the data file and the underlying symmetric key encryption algorithm. Encrypting DEK with a tree access structure T consists of two exponentiations per leaf node T in and one exponentiation per translating node in T.

User Revocation: In this operation, a domain authority just maintains some state information of users' keys and assigns new value for expiration time to a user's key when updating it. When re-encrypting data files, the data owner just needs two exponentiations for ciphertext components associated with Expiration-time the attribute.

File Access: In this method, the decrypted operation of encrypted data files has been done. A user first obtains DEKs with the Decrypt algorithm and then decrypt data files using DEKs. We will discuss the computation complexity of the Decrypt algorithm. The cost of decrypting a ciphertext varies depending on the key used for decryption. Even for a given key, the way to satisfy the associated access tree may be various. The Decrypt algorithm consists of two pairing operations for every leaf node used to satisfy the tree, one pairing for each translating node on the path from the leaf node used to the root and one exponentiation for each node on the path from the leaf node to the root. So the computation complexity varies depending on the access tree and key structure

File Deletion*:* This operation is executed at the request of a data owner. If the cloud can verify the requestor is the owner of the file, the cloud deletes the data file.

D. Encryption/Decryption as a Separate Cloud Service Business Model

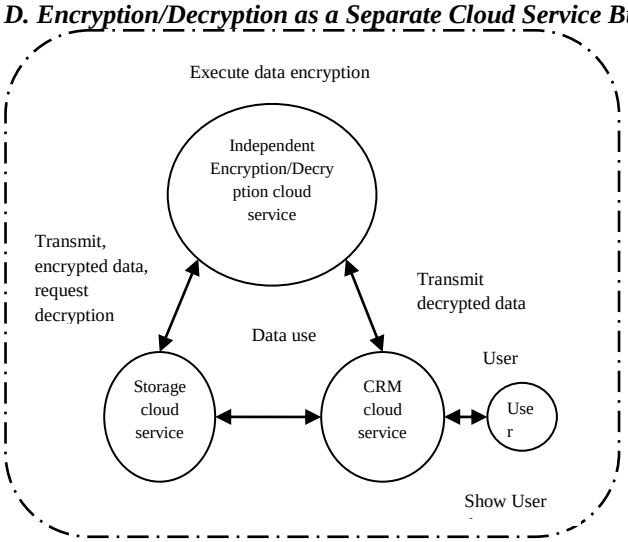

Fig 4: Encryption/Decryption as a Separate Cloud Service Business Model

- Step 1: This step can use current e-commerce or other services which have already securely verified the user's registration, such as symmetric key-based challenge and reply login verification, or through a One-Time Password.
- Step 2: In this step, the CRM Service System transmits the user ID to the Storage Service System where it searches for the user's data. This data is encrypted so, once found, a request must be sent to the Encryption/Decryption Service System along with the user ID.

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 2, Issue 3, May 2013

- Step 3: It shows the Storage Service System executing the transmission of encrypted client data and the user ID to the Encryption/Decryption Service System.
- Step 4: The Encryption/Decryption Service System uses the received user ID to index the user's data decryption key, which is then used to decrypt the received data. Using the correct decryption key to decrypt the data is critical to restoring the data to its original state.
- Step 5: The decrypted client data is provided to the CRM Service System which then displays the client data to the user.
- Step 6: The implementation of the Data Retrieval Program. Earlier to distribution the decrypted client data, the Encryption/Decryption Service System and the CRM Service System can launch a secure data transmission channel to securely broadcast the decrypted client data. After the decrypted client data is sent, the Encryption/Decryption Service System is not permitted to preserve the decrypted data and any unencrypted data must be deleted to avoid the encrypted data and the decryption key from being stored in the equivalent system. This is a critical factor in ensuring the privacy of user data.
- Step 7: Retrieval process vice versa of the above process.

These seven steps are shows in Fig. 4.

IV. EXPERIMENTAL RESULTS

With the control, a field authority DA can carry out New User/Domain Authority Grant for a new user or one more domain authority in his domain. The charge depends on the number of subsets and attributes to be entrusted. Suppose the domain authority DA has a private key with some number of attributes. When DA wants to delegate some amount of the attributes, the cost produces linearly with the number of subsets to be assigned. This has been implemented by a HASBE scheme based on the CP-ABE which uses the Pairing-Based Cryptography.

A. Setup Time

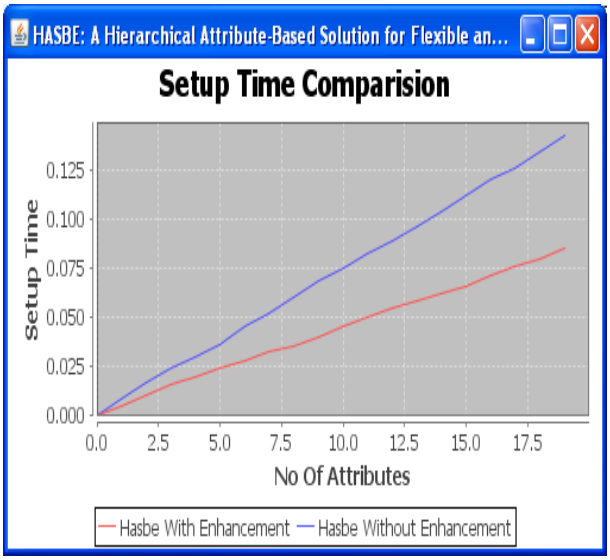

Fig 5: Setup time comparison

Fig. 5 shows the time required to set up the system for a varying number of attributes. The cost of this operation increases linearly with the number of attributes, and the setup can be completed in constant time for a given number of attribute. From which we can infer the setup time for HASBE without enhancement is larger than HASBE with enhancement. Thus the proposed system can be quickly initialized over the existing system.

B. Key Generation Time

The cost is determined by the number of subsets and attributes in the key structure. When there is only one subset in the key structure, the cost grows linearly with the number of attributes as Fig. 6 shows.

While the number of attributes is varied from 0 to 40, the time also increases linearly. But still the key generation time for HASBE without enhancement is higher than the proposed HASBE with enhancement of separate model.

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 2, Issue 3, May 2013

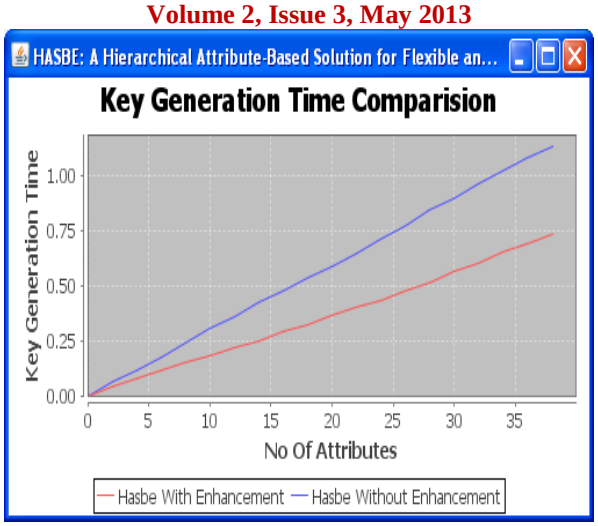

Fig 6: Key generation time comparison

C. Key Update Time

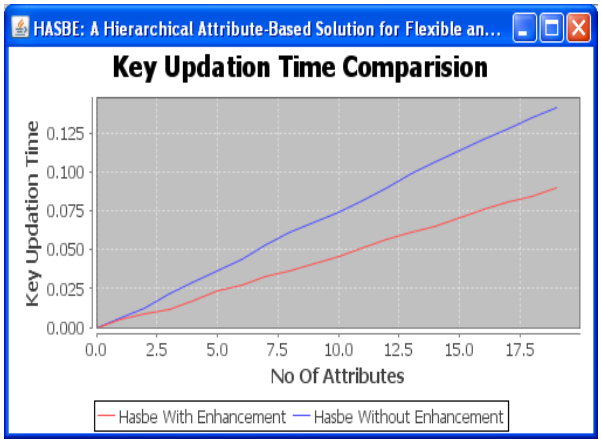

Fig 7: Key update time comparison

The root authority or domain authority can assign a new attribute to the user or domain authority. If the new attribute needs to be assigned to several subsets, the cost of key update is linear with the number of the subsets, as shown in Fig. 8. Time taken for key update in the existing system is higher than that of the proposed system.

D. Decryption Time

The time for this decryption operation depends on the access tree structure. The time of decryption is different depending on the access tree and key structure. It assumes that there is just 1 subset with 40 attributes in the key structure associated with the private key. As shown in Fig. 7, the decryption time is proportional to the number of leaf nodes needed for decryption, and the level of the access tree has no impact on the decryption time. Obviously here also the time taken to perform the operation of the proposed system is less compared to that of existing.

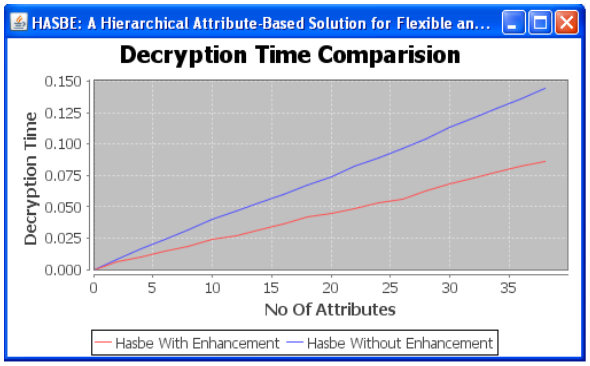

Fig 8: Decryption time comparison

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 2, Issue 3, May 2013

V. CONCLUSION

The existing system provides the cloud service provider to facilitate both encryption and decryption service and storage service as a single unit. In order to enhance the encryption and decryption standards and storage services, it's required to separate encryption and decryption standard and storage services as separate unit. To address this, a business model for cloud computing need to the introduced so as to increase the service performance of both the units. The proposed system handles this business model and the performance of separate encryption and decryption service and storage service is enhanced. In future HASBE scheme can be extended to sustain any depth of the key structure also system can be improved during new algorithms and techniques

REFERENCES

[1] K.Priyadarsini, C.Thirumalai selvan,"A Survey on Encryption Schemes for Data Sharing in Cloud Computing", (IJCSITS), ISSN: 2249-9555,Vol. 2, No.5, October 2012.

[2] Neena Antony, A. Alfred Raja Melvin," A Survey on Encryption Schemes in the Clouds for Access Control", International Journal of Computer Science and Management Research Vol 1 Issue 5 December 2012.

[3] Abdul Raouf Khan,"Access Control in Cloud Computing Environment", ARPN Journal of Engineering and Applied Sciences, Vol. 7, No. 5, May 2012 Issn 1819-6608.

[4] Yan Zhu, Hongxin Huy, Gail-Joon Ahny, Dijiang Huangy, and Shanbiao Wang," Towards Temporal Access Control in Cloud Computing", INFOCOM 2012.

[5] Shucheng Yu, Cong Wang, Kui Ren, and Wenjing Lou," Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing", INFOCOM10.

[6] Guojun Wang, Qin Liu, Jie Wub, Minyi Guo,"Hierarchical attribute-based encryption and scalable user revocation for sharing data in cloud servers", Jul 1, 2011.

[7] 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.

[8] Chittaranjan Hota, Sunil Sanka,"Capability-based Cryptographic Data Access Control in Cloud Computing", Int. J. Advanced Networking and Applications, Volume: 03; Issue: 03; Pages: 1152-1161 (2011).

[9] 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.

[10] R. Kandukuri, V, R. Paturi and A. Rakshit, "Cloud security issues," in Proceedings of the 2009 IEEE International Conference on Services Computing, pp. 517-520, September 2009.

[11] R. Sterritt, "Autonomic computing," Innovations in Systems and Software Engineering, vol. 1, no. 1, Springer, pp. 79-88. 2005.

[12] R. Buyya, C. S. Yeo, S. Venugopal, J. Broberg, and I. Brandic, "Cloud computing and emerging IT platforms: vision, hype, and reality for delivering computing as the 5th utility," Future Generation Computer Systems, vol. 25, issue 6, pp. 599-616, June 2008.

[13] L. M. Vaquero,L. 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.

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

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

[16] 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.