International Journal of Grid Distribution Computing
Vol.7, No.6 (2014), pp.137-148
http://dx.doi.org/10.14257/ijgdc.2014.7.6.11

Quality Based Solution for Adaptable and Scalable Access Control in Cloud Computing

A. Varalakshmi Harika, Haleema P. K., R. Jaya subalakshmi, N. Ch. S. N. Iyengar

School of Computing Science and Engineering, VIT University, Vellore, T N, India
avharikka@yahoo.com,haleema@vit.ac.in,suba_2026@gmail.com,
nchsniyr@vit.ac.in

Abstract

Cloud Computing Environment, the data presides over a set of networked resources and these data centers may be located in any part of the world and access of the data provided through Internet. Cloud computing facilitates computing assets on demand by the use of a service provider. In the Current Scenario, Security and privacy challenges are facing in this cloud environment. We implement our scheme and show that it is both efficient and flexible in dealing with access control for outsourced data in cloud computing with comprehensive experiments using the technique Hierarchical Attribute Based Encryption to protect data of the users and analyze its performance.

Keywords: *Cloud Computing, ABE, HASBE, Cloud Services, Jelastic Server*

1. Introduction

Cloud Computing is a current user trusted technology accessing through Internet at “Any time anywhere”. Without Installing Software’s, it allows the Consumers and Business to use the application like Storage, Processing and Bandwidth using Central Remote Servers.

To keep up the client information secure in outsider Servers, It is needed to enforce Strict Security Policies and also require additional trust in clients to use the cloud services.

By having a web-based application, bringing new locales and suppliers up on to the framework gets to be much speedier and easier. Also, quality is more turning a collaborative process. Encryption Techniques for Storing the User data and key Management, Self Encrypting drive to protect the data from the unauthorized access in case of maintenance of servers of the cloud.

The Aim of the project undertaking improving the data security storage using Attribute Based Encryption technique for encrypting and decrypting the data and authentication levels of security is provided to the secure storage and access the data through cloud computing.

2. Surveying Techniques

Surveying techniques is analyzed in two ways, the techniques used for implementing for the project and cloud services (SAS, PAS, and IAS) provided by the companies for accessing through cloud servers .Firstly, the technique/ Concept used for the Project is discussed briefly

2.1. Attribute Based Encryption (ABE)

The concept of ABE is a type of Public Key (P_K) Encryption and the Cipher Text (C_t) depends upon the Set of Attributes (S_a). Decryption is possible only the attributes of the User Key (U_k) match’s with Cipher Text attribute.

ISSN: 2005-4262 IJGDC

Features

ABE holds the multiple keys to access the data, at least one individual key is required to access the Encrypted data.

Types

ABE is classified into different types, the following are explained below:

(1) Key-Policy ABE [KPABE]

Goyal [1] Introduced the technique associated with C_t is provided with $S_{a\ and}$ users in the form of accessing method are Single access represent in the form of tree structure. S_a to the message encrypted corresponds to the P_k. User can able to access the data, if the key match's in the form of access tree structure.

Disadvantage:

- Scalability (Managing S_a with multiple users).
- Flexibility (To access the data multiple level of attribute authorities).

(2) Cipher-Text Policy ABE [CPABE] and Cipher Text Policy Attribute Set Based Encryption[CPASBE]

Bethencourt [2] proposed the concept of CPABE similar to Identity Based Encryption (IBE). Because it contains the P_k and Master Private Key (M_k) and rules to Decrypt the data using M_k / P_k which have attributes of the users.

To solve the problem with the CPABE introduced the concept on the CPASBE is representing in the form of unchanging structure that does not permit individual variation and access to represent as dynamic constraints. Sa is representing in the form of recursive structure. Based on the rules it allows Sa allowed to combine the attributes form multiples and decrypt to use the attribute in a single access.

(3) Hierarchical Attribute Set Based Encryption [HASBE]

Wang [3] comparing the concept of the HIBE and CPABE and derived the concept, It is a Technique used for cloud storage services with the combination of CPABE and Bobba, *et al.* [4] states that the, HIBE (Hierarchical Identity Based Encryption), it contains Private key Generator (P_k) and domain $P_{k,}$ Users, associated with Key ID (K_i). To access the data from cloud storage it has some restrictions in the form of different levels. The Main access is the root authority responsible for the domain level authority like admin, User.

Wang, *et al.* [5] proposed the concept of HASBE for the security level of the data storage in the cloud with the encrypted and decrypted along with fewer failures and more scalable and flexibility.

2.1.1 Analysis of Attribute Based Encryption [ABE] Techniques

The implementation of the algorithm for this application is done based on the analysis of the concept of ABE. The following Table 1 shows the analysis of ABE Techniques used in Real time authentication service in cloud for storing data in cloud servers.

Table 1. Analysis of ABE techniques based on the Access control, Efficiency, Computation Overhead

S.NO.	Techniques	Access control	Efficiency	Computation overhead
1	KPABE	Low, High	Average	Reduces
2	CPASBE	Better	Better	Lower
3	HASBE	Better	Flexible	Less

Sacha, *et al.* [6] proposed the Distributed ABE [DABE], to overcome the problem of authorities to maintain the independent attributes, different types of entities are introduced using the algorithm CPABE as a part responsible for distributing the M_k to access the storage of the data. Drawback of DABE is access policy of attributed based encryption in distributed environment.

Shucheng Yan, *et al.* [7] states the solution for the challenge issues in ABE and protect the data storing at the untrusted servers and also privileges in sharing the user key's to access the data from the cloud. Drawback of ABE to communicate with blob in the database first it has to communicate with public key Infrastructure (PKI).

Wang, *et al.* [8] states the security problem in the storage and proposed the solution using the techniques HIBE and CPABE to improve the performance tradeoff and applying the Proxy re-encryption technique. Drawback of CPABE, encrypt the data severely limits the ability of the users.

Patil, *et al.* [9], analysis the techniques in ABE and makes the comparison between the HIBE and HASBE from this they concluded that, HASBE generate the key in the form of hierarchal attribute and provides the M_k to the user to access the data more securely.

2.2. Cloud Services

Secondly, the cloud services provided by the company to access through cloud is discussed in below,Most of the Top IT companies are provided the cloud services to the users. Some of the companies like Google, Sales Force, and Amazon and so on.

Cloud services can be distributed/Accessing/utilizing by the user in three ways

1. Platform as a service(PAS)
2. Software as a service(SAS)
3. Infrastructure as a service(IAS)

From the above three services, it is categorized by the company in different ways and provide services to the users.

The following diagram shows the Cloud services in current Real time operating services for the users to access.

The Following Cloud services are explained and also real time cloud services provided by some companies are defined:

1. Testing-as-a-service [TAAS]: Using the remotely hosted testing software's, hardware's have the access to test the cloud applications, websites, systems, enterprise like SOASTA, Cognizant testing services, Impetus.

2. Management-Governance-as-a-service [MGAAS]: To manage more than one cloud service management service is used. Governance will assign the policy and security restriction for access and usage of the data by the users.

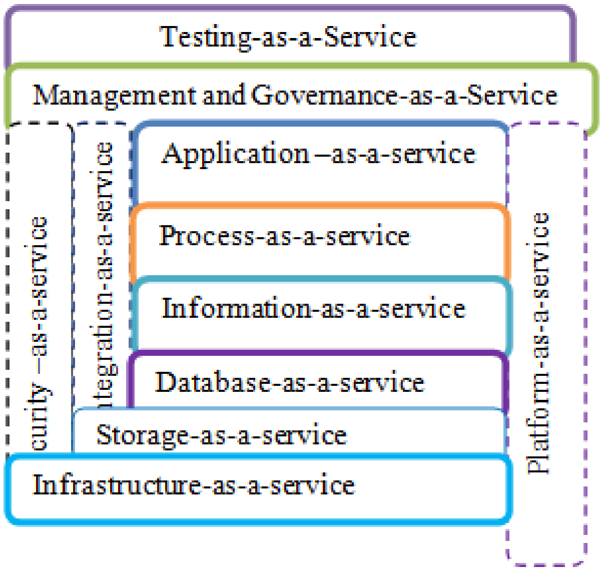


Figure 1. General Architecture view of cloud service provided by the companies in the current scenario

3. Application-as-a-service [AAS]: It is a service, using the cloud platform, they can access any software's Paid version, from the cloud at the lowest and develop the application without purchasing and installing software's installing in system. Service provided by some of the companies like salesforce.com, office tool, Google app engine and so on.

4. Process-as-a-service [PRAAS]: E-Commerce, Business services delivers services over the internet and access that service using devices like Smartphone, Computers, and so on. The popular Google providing business service to the user like Google-Ad-sense, and also IBM Blue Live Works and so on.

5. Information-as-a-service [IFAAS]: Access the service using single application using API [Application Program Interface] through remotely hosted information. For example, live updates of Stock Market

6. Database-as-a-service [DAAS]: Remotely hosted database can be accessed through internet and connected to the application to store the data in cloud servers. Some of the popular companies like Google cloud, Cloud Bee, Oracle Cloud and so on.

7. Storage-as-a-service [SAAS]: Storage user files, documents, photos in the cloud secure storage encrypted format and can access the data through authentication process, such as Drop Box, Google Cloud, and Media fire and so on.

8. Infrastructure-as-a-service [IAAS]: IT companies now a days, most preferable service is infrastructure, they are creating their own private /public cloud, create the infrastructure according to the requirements like network, storage, manage, processing and making control over the operating environment to deploy and run, develop the products and deliver to the customers. These services also provided by some other companies like Rack Space, Sky tap and so on.

9. Security-as-a-service [SCAAS]: Security provided to the databases, storage data in cloud with authentication levels to access the data. It can be provided remotely over the networks. Popular companies like McAfee, Panda Cloud antivirus and so on.

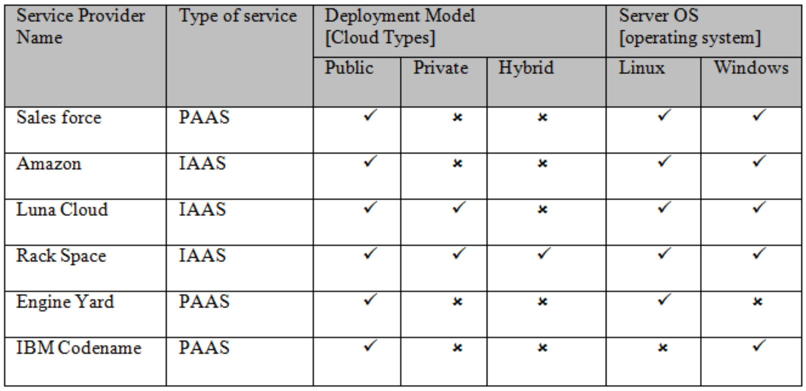
10. Integration-as-a-service [IGAAS]: To develop, Maintain, Manage the customer information in the cloud, Integration provides the complete services associated to the application. Leading Companies like Mule Soft, DELL and so on.

11. Platform-as-a-service [PAAS]: Platform service offers the complete service to the users to develop the application, deploying, testing, storage, Using cloud operating systems and access the service for the development of product. Some of the companies like Google APP Engine, Windows Azure, Realistic, Amazon web service and so on.

2.2.1. Analysis of current cloud computing services

Most common services (SAAS, IAAS, and PAAS) in the cloud provided by the company is analyzed and shown in the form of the Table 2.

Table 2. Analysis of cloud service providers based on the type of the service, cloud type and server operating system used to provide services



Service Provider Name	Type of service	Deployment Model [Cloud Types]			Server OS [operating system]	
		Public	Private	Hybrid	Linux	Windows
Sales force	PAAS	✓	×	×	✓	✓
Amazon	IAAS	✓	×	×	✓	✓
Luna Cloud	IAAS	✓	✓	×	✓	✓
Rack Space	IAAS	✓	✓	✓	✓	✓
Engine Yard	PAAS	✓	×	×	✓	×
IBM Codename	PAAS	✓	×	×	×	✓

3. Motivation

The Proposed system for HASBE presents regarding designation instrument and enhanced proficiency. It gives productively impart private information on cloud servers and likewise providing security in the cloud, which decide on the structure &semantics of their properties storage data in the cloud databases, access through the set of attributes in level of authentication's, provides the flexibility and scalability.

4. Architecture

Note:

Level 1-states the Admin Authority, provide access to the user for service

Level 2- Domain Authority, access the service provided by the admin using login credentials.

Level 3- Cloud service used to deploy the application in the cloud environment

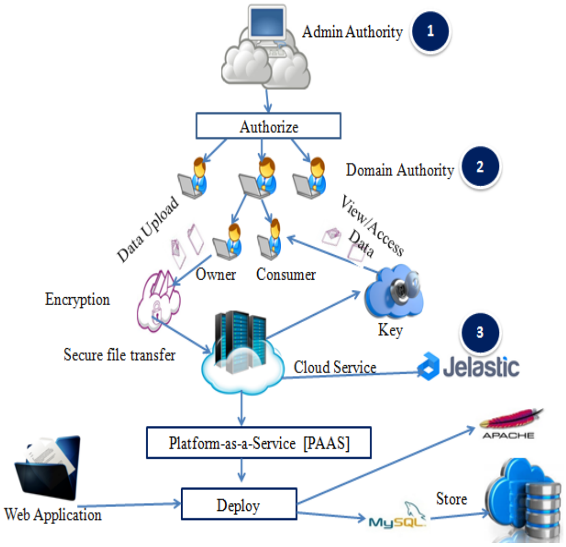


Figure 2. Architecture of the proposed system using cloud service, the representing of the diagram in three levels

5. Explanation of the functionalities

The Implementation of this concept is carried out in three levels for providing security to user data stored in cloud servers. Encryption and decryption process is implemented for the uploaded and downloaded to protect from the unauthorized access.

Module 1: [Admin Authority]

Admin Authority is the owner of the cloud, providing services to the users for accessing and storage in the cloud database.

User has to register to access the cloud service, using Login credentials. After completing the registering process, User can access the service for uploading and downloading data.

Module 2: [Domain Authority, Data Consumer]

In this Module, the process of storing and accessing again defined in two terms

2.1. Domain Authority

Particular Domain user will upload the data in the cloud servers, once the data is uploaded, the data is encrypted without accessing the data from the unauthorized users. The M_k is generated after the data uploading is done is cloud database servers.

Login authentication process can be done, after Domain Authority will upload the data in database. Once the data is uploaded the file encrypted and then update in the database. Unauthorized access is not processed through the security of the data stored. The M_k is generated, once the data uploaded, the uploaded data file is linked up with the $M_{k,}$ to download and save the file from cloud to the operating system.

2.2. Data Consumer

User has to use the M_k to access the data uploaded by the Domain. The M_k checks the status of the using key is valid or invalid. If it is valid, the data is decrypted and user can download, otherwise Invalid reports the error.

Consumer has the authentication process through login, once the registration. Consumer selects the appropriate file to download and enter the key to perform the decrypt operation of the particular file to view/ access the data.

Encryption and decryption process in the form of levels of security to access the set of attributes of the users from the cloud servers.

Module 3: [Cloud Service]

Finally, Cloud service [Jelastic] is used for the web application for deploying the application through web browser, accessing and storing the data in database.

Jelastic Cloud provides the IAAS and PAAS service's to the users from the cloud. Create the own Cloud environment in Jelastic cloud servers and supported the software's required to run the project and plug-in the Jelastic to the net beans software connected to the cloud and deploy the developed web application in cloud web browsers, to identify and detect the error in the application and compile the data is done. Process the application, the data is stored to the Mysql database hosted through the Jelastic cloud database servers and run through using the cloud services.

6. Methodology

The methodology used in the project for encrypting and decrypting the data in cloud is implemented using the algorithm Hierarchical Attribute Set Based Encryption [HASBE]. The Proposed HASBE is combination of CPABE, HIBE to provide the access in the security based level for the set of attribute users and generate the M_K. The Encrypted data generates the key in form of the assigned key structure to access and download the data from the database.

Table 3. Description of the keys used in the algorithm for implementing algorithm

Keys	Description
M_k	Master Key
P_k	Public Key
P_{ki}	Private Key
C_t	Cipher Text
S_a	Set of Attributes
U_k	User Key

Algorithm :

In the HASBE scheme, there are multiple keys with different usages. Then, we define the HASBE scheme, by presenting randomized polynomial time algorithms as follows:

Step 1: Start the process

Step 2: The process organized and generates a public key of P_k and M_k.

Step 3: Structure of key generates a private key of P_{ki} and M_k.

Step 4: Depending upon the root level authority, private key [P_k] is generated to the new Domain Authority.

Step 5: Pk, attribute, subset generates a new P_k, which contains the new attribute.

Step 6: Encrypt the file and relative M_k is generated to access the users.

Step 7: Using M_k, the content of the file is decrypted.

Note: The content of the encrypted data stored in the database only decrypted based on the M_k.

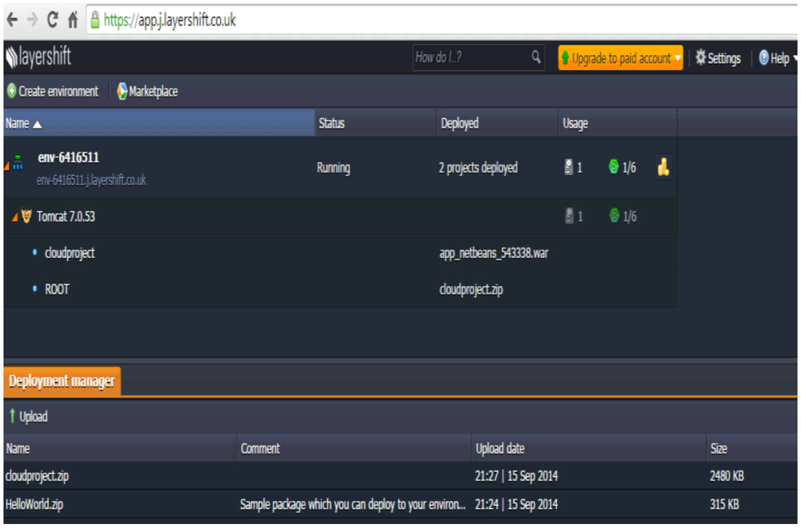
Step 8: Stop the process.

7. Experimentation Results and Performance Evaluation

7.1.1. Jelastic server

Jelastic server is a cloud service. It provides two types of service IAAS, PAAS. Implementation of this concept access the service type is PAAS. First creating the environment in the clod according to the requirements of the project, Tomcat 7.0 and Mysql 5.6 environment is created. Access the service the using Netbeans 7.4 and plugin this service in the IDE and execute the web application.

In this cloud service user has to create the environment of the cloud according to the project requirements and then plug-in jelastic in the net bean IDE. After installing the plug-in, login with cloud service authentication with the username and password. Upload the project in the cloud of the jelastic server. In the project implementation, run the project as jelastic environment plug-in. Build and deploy the application in the cloud server.The following shows the experimental results of the Jelastic cloud server and the net beans IDE monitoring the process is show in Figure 3.



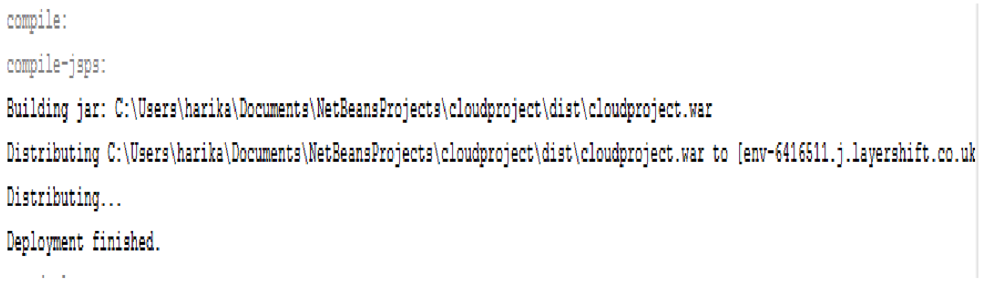
Name ▲	Status	Deployed	Usage
env-6416511 env-6416511.j.layershift.co.uk	Running	2 projects deployed	1 1/6
Tomcat 7.0.53			1 1/6
cloudproject		app_netbeans_543338.war	
ROOT		cloudproject.zip	

Name	Comment	Upload date	Size
cloudproject.zip		21:27 | 15 Sep 2014	2480 KB
HelloWorld.zip	Sample package which you can deploy to your environ...	21:24 | 15 Sep 2014	315 KB

Figure 3. compilation using the cloud service and accessing the tomcat 7.0 web servers and Mysql 5.6 database for accessing through Net beans IDE for compilation of the web application and storing in the database

7.1.2. Deployment stage in net beans

Execution of the web application is done successfully, the following web page is shown, and environment of the project along with the service and project filename is shown in the Figure 4.

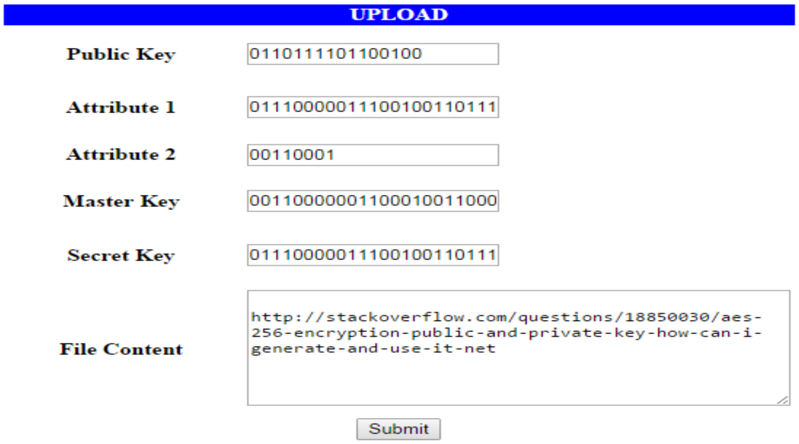


```
compile:
compile-jsps:
Building jar: C:\Users\harika\Documents\NetBeansProjects\cloudproject\dist\cloudproject.war
Distributing C:\Users\harika\Documents\NetBeansProjects\cloudproject\dist\cloudproject.war to [env-6416511.j.layershift.co.uk
Distributing...
Deployment finished.
```

Figure 4. Environmental setup using jelastic server access and compiled project successfully access the cloud service

7.1.3 Encryption process of Owner Authority Module

Owner Authority module upload the text file, once the file is uploaded. Public Key and 2 attributes sets, master key, secret key is generated and file content is shown in Figure 5.



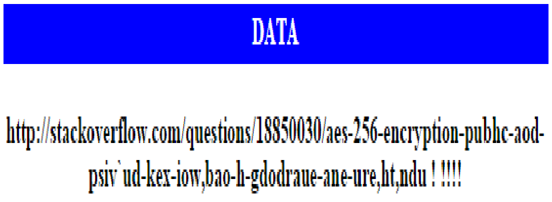
UPLOAD

Public Key	0110111101100100
Attribute 1	01110000011100100110111
Attribute 2	00110001
Master Key	00110000001100010011000
Secret Key	01110000011100100110111
File Content	http://stackoverflow.com/questions/18850030/aes-256-encryption-public-and-private-key-how-can-i-generate-and-use-it-net

Figure 5. Encryption process of upload by Owner Authority

7.1.4 Decryption process of Consumer Authority Module

Decryption process is accessed by the consumer and select the file and Secret key is in binary format is entered. Both the given input matches and content of the encrypted data is decrypted and respected data is shown in Figure 6.



DATA

http://stackoverflow.com/questions/18850030/aes-256-encryption-pubhc-aod-psiv`ud-kex-iow,bao-h-gdodraue-ane-ure,ht,ndu ! !!!!

Figure 6. Decryption process using the secret key consumed by the Consumer Authority

7.2 Performance Evaluation

Performance evaluation of the three different types of algorithms, *i.e.*, HASBE, CPABE, HIBE encryption process is shown in two graphs Figure 7 and Figure 8. Comparative Analysis of performance of three algorithms shows that the HASBE improves the execution time when compare to the HIBE and CPABE. Level of Access Tree also decreased when implemented in HASBE algorithm. The Observation State by the performance Analysis, HASBE Algorithm will give more security and storage and increases the performance level in the cloud Storage.

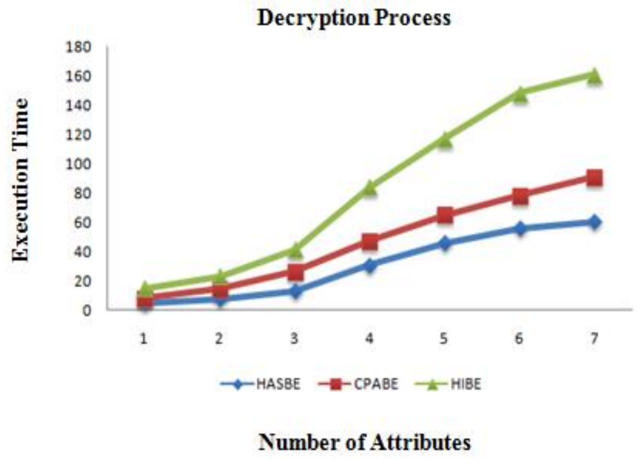


Figure 7. Graphical representation of decryption process can be calculated in terms of execution time and number of attributes

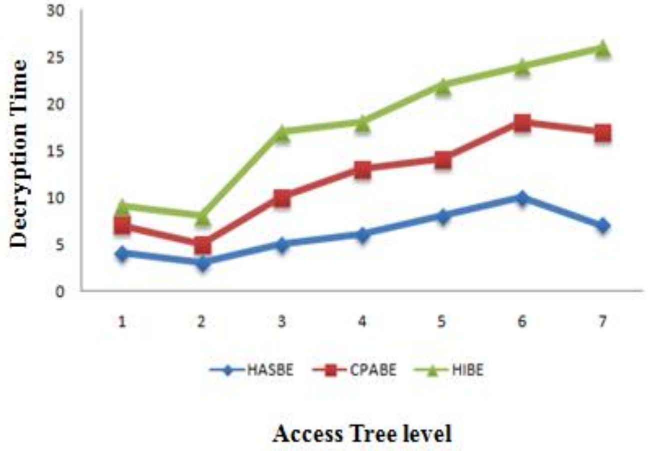


Figure 8. Graphical representation of decryption process can be calculated in terms of access tree level and decryption time

8. Conclusion

Cloud computing is the fastest growing technology in current scenario. Popular companies providing the cloud service to the users using low level encryption algorithm techniques, This leads to problematic for user storage data stored in the cloud. The proposed algorithm defines the newest level to protect the security for the cloud storage users with the multi level authentication's and the key authorization to decrypt the data in secure process. As the cloud users and trusting on the cloud increased day-by-day, companies has to provide the more security algorithm techniques to the data stored in the cloud servers.

References

[1] P. Goyal, A. Sahai and A. Saha, "Attribute-based encryption for fine-grained access control of encrypted data", Proceedings of the 13th ACM conference on Computer and communications security, **(2006)**,October 30-November 3, Alexandria, USA.

[2] J. Bethencourt, A. Sahai and B. Waters, "Ciphertext-Policy Attribute-Based Encryption", Proceedings of IEEE Security and Privacy, **(2007)**, Oakland.

[3] G. Wang, Q. Liu and J. Wu, "Hierarchical Attribute-Based Encryption for Fine-Grained Access Control in Cloud Storage Services", Proceedings of the 17th ACM conference on Computer and communications security, **(2010)**, Chicago, USA.

[4] R. Bobba, H. Khurana and M. Prabhakaran, "Attribute-Sets: A Practically Motivated Enhancement to Attribute-Based Encryption", Proceedings of the 14th European conference on Research in computer security, **(2009)**, Heidelberg.

[5] G. Wang, Q. Liu, J. Wu and M. Guo, "Hierarchical attribute-based encryption and scalable user revocation for sharing data in cloud servers", Computers & Security, vol. 30, Issue 5, **(2011)** July, pp. 320–331.

[6] S. Muller, S. Katzenbeisser and C. Eckert, "Distributed Attribute-Based Encryption", in International Conference on Information Security and Cryptology, **(2008)** December 3-5, Seoul, Korea.

[7] S. Yu, C. Wang, K. Ren and W. Lou, "Attribute Based Data Sharing with Attribute Revocation", 5th ACM Symposium on Information, Computer and Communications Security, **(2010)** April 13 – 16, Beijing, China.

[8] G. Wang, Q. Liu and J. Wu, "Hierarchical attribute-based encryption for fine-grained access control in cloud storage services", Proceedings of the 17th ACM conference on Computer and communications security, **(2010)** October 4-8, New York, USA

[9] P. Rohini, "Data Security Technique in cloud storage", IJCST, vol. 4, **(2013)**, pp. 113-119.

Authors

A Varalakshmi is currently pursuing post-graduation at VIT University Vellore, Tamil Nadu in Computer Science and Engineering stream. She has done Bachelor of Engineering in Computer Science and Engineering from Annamacharya Institute of Engineering and Technology, Tirupati. Her major interest work area is Cloud Computing, Big data Analytics, Android development.

Haleema (M.C.A., M.Phil,, M.Tech) is an Assistant Professor (Senior) in the School of Social Sciences and Languages and pursuing her Ph.D. research work in the School of Computing Science and Engineering. Her area of research is "Software Agent based computing".

R. Jaya Subalakshmi is an Assistant Professor in the School of Computing Science and Engineering at VIT University, Vellore-632014, Tamil Nadu, India. She did M.S.(By Research) in VIT University. Her research area is Cryptography, Data Privacy and Agent based Distributed Computing.

Dr. N. Ch. S. N. Iyengar (b 1961) currently Senior Professor at the School of Computing Science and Engineering , VIT University, Vellore-632014, Tamil Nadu, India .He had 30 yrs of teaching experience. His research interests include Agent-Based Distributed secure Computing, Intelligent Computing , Network Security, Cloud Computing and Fluid Mechanics. He has authored several textbooks and had nearly 172 research publications in reputed peer reviewed International Journals. He delivered many keynote /invited lectures and served as PCM//TCM/reviewer for many International Conferences. He is Editor in Chief for International Journal of Software Engineering and Application (IJSEA) of AIRCC, Guest Editor for SI on Cloud Computing and Services of *Int'l J. of Communications, Network and System Sciences* and Editorial Board member for International Journals like **IJAST of SERSC, IJConvC of Inderscience** and many more.