# HASBE: Hierarchical Attribute-based solution for Flexible and Scalable Access Control in Cloud computing.

**Gayathri. D[1], Anusha.B [2], Sathya Anjusha.P [3], Madhuri.N [4]**

Dept. of CSE, BITM Bellari, Karnataka - 583104

[1]gayathridvr@gmail.com,[2] anushakuttyb@gmail.com, [4]madhuriin705@gmail.com

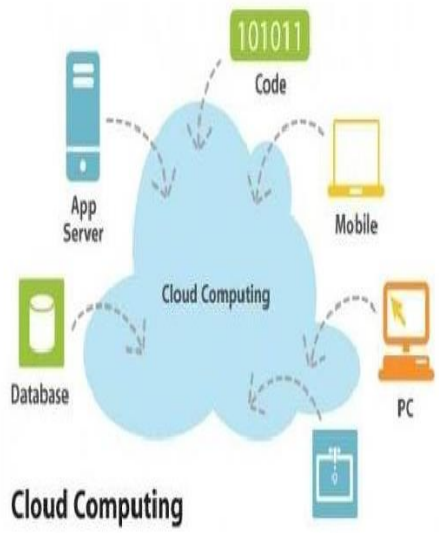
***ABSTRACT:***
***Cloud is used for virtualization, parallel and distributed computing, utility computing, and service oriented architecture to store user data. the benefits of cloud computing are reduced data leakage, decrease evidence acquisition time, they eliminate or reduce service downtime, they forensic readiness, they decrease evidence transfer time. main factor to be discussed is security of cloud computing, which is a risk factor involved in major computing fields. Cloud computing is basically an internet based network made up of large number of servers – mostly based on open standards, modular and inexpensive.***

## *I. INTRODUCTION*

Cloud computing is internet-("CLOUD") based development and use of computer technology ("COMPUTING"). It is a general term for anything that involves delivering hosted services over the internet.

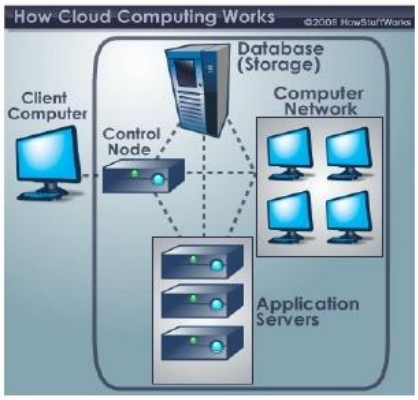
User of the cloud only care about the service or information they are accessing – be it from their PCs, mobile devices, or anything else connected to the Internet – not about the underlying details of how the cloud works.

It is used to describe both a platform and type of application. It also describes applications that are extended to be accessible through the internet. These cloud applications use large data centres and powerful servers that host web applications and web services. Anyone with a suitable internet connection and a standard browser can access a cloud application.




## *II. WORKING OF CLOUD COMPUTING*

Super computers today are mainly used by the military, government intelligence agencies, universities and research labs, and large companies to tackle enormously complex calculations for such tasks as simulating nuclear explosions, predicting climate change, designing airplanes, and analysing which proteins in the body are likely to bind with potential new drugs. Cloud computing aims to apply that kind of power –measured in the tens of trillions of computation per second- to problems like analysing risk in financial portfolios, delivering personalized medical information, even powering immersive computer games, in a way that users can tap through the web. It does that by networking large groups of servers that often use low cost consumer PC technology, with specialised connections to spread data processing chores across them. By contrast, the newest and most powerful desktops PCs process only about 3 billion computations a second. Let's say you're an executive at a large corporation. Your particular responsibilities include making sure that all of your employees have the right hardware and software they need to do their jobs. Buying computers for everyone isn't enough—you also have to purchase software or software licenses to give employees the tools they require. Whenever you have a new hire, you have to buy more software or make sure your current software license allows another user. It's so stressful that you find it difficult to go.



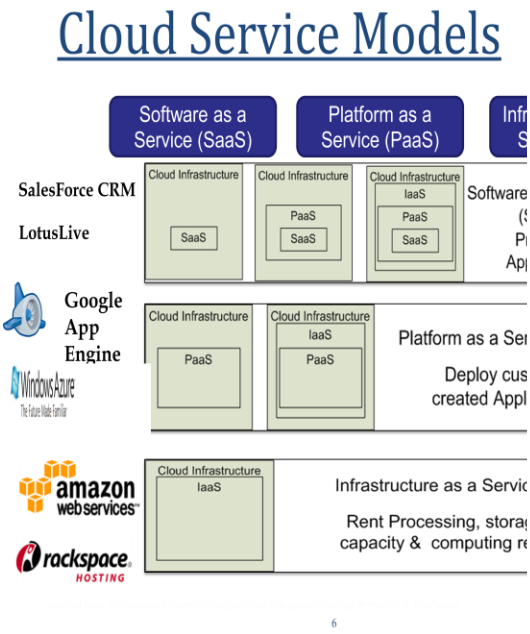

## III. *CLOUD SERVICES*:

- Infrastructure-as-a-service:
  Infrastructure-as-a-service like Amazon web services provides virtual servers with unique IP address and blocks of storage on demand. Customers benefit from an API from which they can control their servers. Because customers can pay for exactly the amount of service they use, like for electricity or water, this service is also called utility computing.

- Platform-as-a-service:
  Platform-as-a-service is a set of software and development tools hosted on the provider's servers. Developers can create applications using the providers APIs. Google apps is one of the most famous Platform-as-a-service provider's .Developers should take notice that there aren't any interoperability standards(yet), so many providers may not allow you to take your application and put it on the other platform.

- Software-as-a-service:

Software-as-a-service is a broadest market. In this case the provider allows the customer only to use it applicants. The software interacts with the user through a user interface. These applicants can be anything from web based email, to applicants like Twitter and Last.fm.




## *IV. BENEFITS OF CLOUD COMPUTING:*

- Accelerate innovation and business agility by providing faster ways to build and scale new apps and services to go from local to global in no time
- Speed IT delivery to match the pace of business. Spend less time managing hardware and more time focusing on high-priority investments
- Reduce capital expenses—hardware, facilities, operations, and even power—with computing on-demand
- Choose the solution that best meets the needs of your organization across on-premises, hosting provider, and Microsoft Azure.

## *V. APPLICATION*

A cloud application leverages cloud computing in software architecture, often eliminating the need to install and run the application on the customer's own computer, thus alleviating the burden of software maintenance, ongoing operation, and support. For example:

- Peer-to-peer/volunteer computing (BOINC, Skype)
- Web applications (Webmail, Face book, Twitter, You tube, Yammer)
- Security as a Service ( Google Apps, Sales force, Nivio ,Learn.com, Zoho )
- Software plus services (Microsoft Online Services)
- Storage [distributed]
- Content distribution (Bit Torrent, Amazon Cloud Front)
- Synchronisation (Drop box, Live Mesh, Spider Oak, Zumo Drive)

## *VI. HASBE:*

To provide additional security for the data stored in the cloud. Various cryptographic techniques has been used for secure outsourcing of data. The proposed HASBE is used for enhanced security settings. In this we use bilinear mapping techniques to enhance secure key exchange of the data.

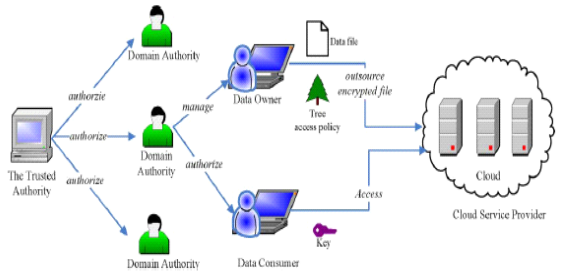



Fig. 1. System model.

The 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 manages a cloud to provide data storage service. Data owners encrypt their data files and store them in the cloud for sharing with data consumers. To access the shared data files, data consumers download encrypted data files of their interest from the cloud and then decrypt them. Each data owner/consumer is administrated 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 the figure.

## *VII. KEYWORDS:*

Attribute-based encryption, access control, cloud computing, hierarchical attribute-based encryption., software as a Service (Saas).

## *VIII. ADVANTAGES*

- Low initial capital investment
- Shorter start-up time for new services
- Lower maintenance and operation costs
- Higher utilization through virtualization
- Easier disaster recovery.

## *IX. HASBE SCHEME*

Our system model consists of a trusted authority, multiple domain authorities, and numerous users corresponding to data owners and data consumers. The trusted authority is responsible for generating and distributing system parameters and root master keys as well as authorizing the top-level domain authorities.

## *X. IMPLEMENTATION*

➢ ALGORITHMS USED

- **hasbe -setup**: Generates a public key (PK) and a master key (MK)
- **hasbe -keygen**: Given PK and MK , generates a private key for a key structure. The key structure with depth 1 or 2 is supported
- **hasbe-enc**: Given PK , encrypts a file under an access tree policy .
- **hasbe-dec**: Given a private key, decrypts a file.
- **hasbe-rec**: Given PK, a private key and an encrypted file, re-encrypt the file.

➢ *OPERATIONS*

- Data Owner Module

In this module, the data owner uploads their data in the cloud server. For the security purpose the data owner encrypts the data file and then store in the cloud. The data owner can change the policy over data files by updating the expiration time. The Data owner can have capable of manipulating the

encrypted data file. And the data owner can set the access privilege to the encrypted data file.

- Data Consumer Module

  In this module, the user can only access the data file with the encrypted key if the user has the privilege to access the file. For the user level, all the privileges are given by the Domain authority and the Data user's are controlled by the Domain Authority only. Users may try to access data files either within or outside the scope of their access privileges, so malicious users may collude with each other to get sensitive files beyond their privileges.

- Cloud Server Module

  The cloud service provider manages a cloud to provide data storage service. Data owners encrypt their data files and store them in the cloud for sharing with data consumers. To access the shared data files, data consumers download encrypted data files of their interest from the cloud and then decrypt them.

- Attribute based key generation Module

  The trusted authority is responsible for generating and distributing system parameters and root master keys as well as authorizing the top-level domain authorities. A domain authority is responsible for delegating keys to subordinate domain authorities at the next level or users in its domain. Each user in the system is assigned a key structure which specifies the attributes associated with the user's decryption key.The trusted authority calls the algorithm to create system public parameters PK and master key MK. PK will be made public to other parties and MK will be kept secret. When a user sends request for data files stored on the cloud, the cloud sends the corresponding ciphertexts to the user. The user decrypts them by first calling decrypt(CT,SK) to obtain DEK and then decrypt data files using DEK.

## *XI. SECURITY AND PERFORMANCE*

We assume that the cloud server provider is untrusted in the sense that it may coperate with malicious users (short for data owners/data consumers) to harvest file contents stored in the cloud for its own benefit. In the hierarchical structure of the system users given in Fig. 1, each party is associated with a public key and a private key, with the latter being kept secretly by the party. The trusted authority acts as the root of trust and authorizes the top-level domain authorities. A domain authority is trusted by its subordinate domain authorities or users that it administrates, but may try to get the private keys of users outside its domain. Users may try to access data files either within or outside the scope of their access privileges, so malicious users may collude with each other to get sensitive files beyond their privileges. In addition, we assume that communication channels between all parties are secured using standard security protocols, such as SSL.

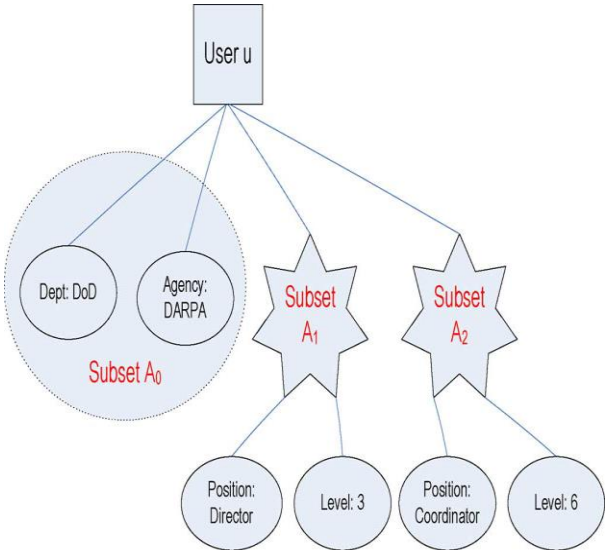



Fig. 2. Example key structure.

We analyze the computation complexity for each system operation in our scheme as follows.

- System Setup.
- Top-Level Domain Authority Grant.
- New User/Domain Authority Grant.
- New File Creation
- User Revocation.
- File Access.
- File Deletion.

## *XI SCOPE*

HASBE employs multiple value assignments for access expiration time to deal with user revocation more efficiently than existing schemes. The security of HASBE based on security of the cipher text-policy attribute-based encryption (CP-ABE) scheme and analyze its performance and computational complexity.

## *XII CONCLUSION*

In this paper, we introduced HASBE for providing addition security for the data stored in the cloud. HASBE algorithm is used for encryption, through RSA and DES algorithm we can easily debug the key concept, So that user can easily understand the encrypted data. To avoid this we have proposed HASBE. We formally prove the security of HASBE .Finally, we implemented the proposed scheme, evaluation, which showed its performance and advantages.

## *XIII REFERENCES*

[1] Amazon Elastic Compute Cloud (Amazon EC2) [Online]. Available: http://aws.amazon.com/ec2/.

[2] Amazon Web Services (AWS) [Online]. Available: https://s3.amazonaws.Com.

[3] G.Wang, Q. Liu, and J.Wu, "Hierachical attibute-based encryption for fine-grained access control in cloud storage services," in *Proc. ACM Conf. Computer and Communications Security (ACM CCS)*, Chicago, IL, 2010.

[4] S. Yu, C. Wang, K. Ren, and W. Lou, "Achiving secure, scalable, and fine-grained data access control in cloud computing," in *Proc. IEEE INFOCOM 2010*, 2010.

[5] Introduction to cloud computing wikipedia

[6] Web guild.org
http://www.webguild.org/

[7] How stuff works.com
http://communication.howstuffworks.com/

[8] Cloud security.org
http://cloudsecurity.org/