International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 04 Issue-17
December 2017

An EFH: Hybrid-Based Attribute Technique In Cloud Computing

P Naveena, Dr.M.Purushothsam, Dr.Suresh Akella
[1]M.Tech Computer Science Engineering Sreyas Institute of Engineering and Technology, Beside INDU Aranya,Nagole, Hyderabad
[2]M.Tech.,M.S.PhD. Associate Professor, Department of Computer Science And Engineering Sreyas Institute of Engineering and Technology, Beside INDU Aranya,Nagole, Hyderabad
[3]Principal, Sreyas Institute of Engineering and Technology, Beside INDU Aranya,Nagole, Hyderabad

ABSTRACT: *Cloud computing is continuing to be very famous technology in IT businesses. For an enterprise, where the data stored is very large and it's miles very valuable. All responsibilities are achieved through networks. Hence, it becomes very vital to have the secured use of data. In cloud computing, the maximum important concerns of protection are data security and privateness. This paper pursuits to remedy hassle for supporting distinctive organization shape and maintain their hierarchy of numerous clients in the groups, keeping document of employees. Our proposed system is integrating the key feature of Hierarchical attribute based encryption (HABE) and cipher text policy attribute based encryption (CP-ABE) device, so as not handiestfinished excessive performance and first-rate grained get access to, user revocation scheme while user are not longer worker ofenterprise.*

KEYWORDS-Access control, Attribute based encryption, Keypolicy, ciphertext policy, hierarchical-ASBE

I. INTRODUCTION

cloud computing is a computational surroundings wherein we can use belongings and pay handiest for that assets wherein we are involved, in order that patron can experience service on call for. thisrising computer paradigm permit consumer to shop theirtouchy statistics in cloud whenever consumer wants that facts he candownload it in smooth manner. cloud computing provide simplicity and green offerings to the consumer a good way to keep capital valueon hardware's infrastructure mainly for small and mediumsized corporations with restrained budgets, they could obtain cost savings and the power to scale (or reduce) investments on demand, through the usage of cloud-primarily based absolutely offerings to govern obligations,company-extensive contacts and schedules, and so on[1].csp may be operated for making earnings to take care about sensitive exclusive information, arises security and personal hassle. csp can be selling out the personal records to closest competitor business enterprise for making income.

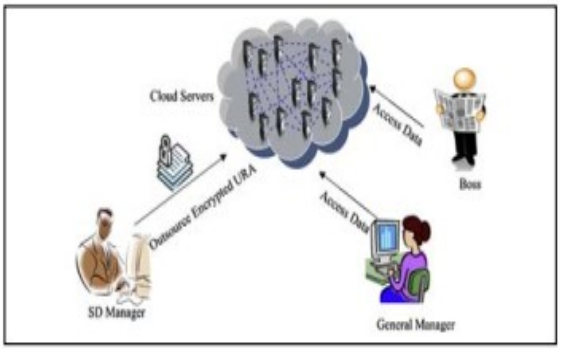

Fig 1. Application Scenario

We keep in mind the following utility scenario (see Fig. 1):Company A can pay a CSP for sharing company data in cloudservers. Suppose the sales department(SD), the research and development department (RDD), and the finance branch(FD) are taking part in Project X [1]. The SD supervisorwants to save an encrypted person requirement analysis (URA)within the cloud, so that best the employees that have certaincertificate can get right of entry to the report. For example, the SDsupervisor may also specify an access manage coverage for this URA, asshown in Fig. 2[1].

In Fig. 2, the get admission to control coverage may be expressed as a Boolean system over attributes. Each attribute includes an internet web site specifying which celebration administers the characteristic and an identifier describing the characteristic itself, each of which may be represented as strings and concatenated with asingle colon individual as a separator [1]. The minimize "/" in each

internet webpage denotes a concatenation among the superior and thesubordinate.

The instinct behind this get access to control coverage is that this URA should handiest be accessed by the boss and the general supervisor of the organization, the contributors of Project X, and allthe department managers who are concerned in Project X[1].Furthermore, the party that administers attributes "isBoss","isGeneralManager", and "inProjectX" is advanced to the birthday partythat administers attributes "isDepartmentManager", "inSD","inRDD", and "inFD"[1]. In the above application state of affairs,the encrypter does no longer recognize the exact identities of the intended recipients, however as an alternative he simplest has a way to explainthem the usage of certain descriptive attributes [1]. Therefore, thefollowed encryption device ought to guide an attribute-basedaccess structure. Flexible encryption schemes which includes ciphertext-policy characteristic-primarily based encryption (CP-ABE), may befollowed to provide a nice grain get access to manipulate for the encrypted data.

CP-ABE permits encrypting records specifying an access control coverage over attributes, so that most effective users with a set ofattributes pleasing this policy can decrypt the corresponding data [1]. For example, the data encrypted the usage of the get right of access to shape "a1^a2" way that only the user with attributes a1and a2, can decrypt the data [1]. In order to offer safety CPABE scheme offer following properties.

• High Performance. In the cloud-computing surroundings,users may also get access to data whenever and anywhere the usage of anydevice [1]. When a user wants to get right of access to data using a thin client with constrained bandwidth, CPU, and reminiscence competencies, the CP-ABE scheme have to be of excessive overall performance [1]. That is, the verbal exchange prices and computation fees introduced via the CP-ABE scheme should be low enough, in order that the user can efficiently retrieve facts from the cloud, and then decrypt it the usage of the skinny purchaser [1].

• Full Delegation. In a large-scale corporation with many personnel, each employee desires to request secret keys from the characteristic Attribute authority (AA), when he joins the business enterprise [1]. If a majority of these personnel require their mystery keys from one Attribute Authority (AA), there will be aoverall performance bottleneck at the AA [1].

To reduce the workload on the AA, a few CP-ABE schemes offer key delegation between clients, which allows

• A user to generate attributes mystery keys containing asubset of his own characteristic secret keys for different customers [1].

Full delegation way key delegation between AAs,wherein every AA independently makes selections on the shape and semantics of its attributes [1].

• Scalable Revocation. In order to hold hierarchy of business enterprise we need to recognise about how plenty workerin enterprise and those who are not employee revoke their access control coverage. A user whosepermission is revoked will still hold the keys issued earlier, and thus can nonetheless decrypt facts within the cloud [1]. Thetraditional revocation scheme usually calls for the AAs to periodically re-encrypt data, and re-generate new secret keys to ultimate authorized clients [1]. This technique will purpose heavy workload at the AAs. A greater scalable technique is to take advantage of the considerable assets ina cloud by allowing the AAs to delegate the CSP to reencrypt records and re-generate keys to clients, underneath the environment that the CSP knows nothing about the dataand keys based on the above-mentioned analysis, it's milesneeded to suggest a comfortable data-sharing scheme, which simultaneously achieves high performance, full delegation and scalable revocation [1].

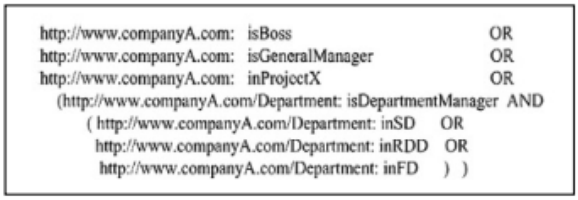

Fig 2. Sample Access Control Policy of URA

II. RELATED WORKS

Zhiguo Wan, Jun'e Liu, and Robert H. Deng (2012) [6] proposed the approach HASBE (Hierarchical Attribute-

setbased Encryption).HASBE extends the ciphertext-policy characteristic-set-based totally encryption (CP-ASBE, or ASBE forbrief) scheme through Bobbaet al. With a hierarchical structure of deviceclients, as a way to achieve scalable, flexible and best-grained get access to control.

Cong Wang Sherman S.M. Chow, Qian Wang (2013) [8] offers our public auditing scheme which provides a whole outsourcing solution of data not handiest the statistics itself, however also its integrity checking. Using cloud storage,clients can remotely shop their data and revel in the on-denmand for remarkable programs and services from a shared pool of configurable computing sources, with out the burden of neighbourhood data storage and preservation.

J. Bethencourt, Amit Sahai, Brent Waters [11], a system for realizing complex access control on encrypted data that we call Ciphertext-Policy Attribute-Based Encryption. By using our techniques encrypted data can be kept confidential even if the storage server is untrusted; moreover, our methods are secure against collusion attacks. Previous Attribute Based Encryption systems used attributes to describe the encrypted data and built policies into user's keys; while in our system attributes are used to describe a user's credentials, and a party encrypting data determines a policy for who can decrypt. Thus, our methods are conceptually closer to traditional access control methods such as Role-Based Access Control (RBAC). In addition, we provide an implementation of our system and give performance measurements. The system allows for a new type of encrypted access control where user's private keys are specified by a set of attributes and a party encrypting data can specify a policy over these attributes specifying which users are able to decrypt. The system allows policies to be expressed as any monotonic tree access structure and is resistant to collusion attacks in which an attacker might obtain multiple private keys. In the future, it would be interesting to consider attribute-based encryption systems with different types of expressibility.

Dijiang Huang (2015) [7] has mentioned get right of access to control the usage of Constant-length Ciphertext Policy Comparative AttributeBased Encryption. CCP-CABE achieves the performance as it generates consistent-size keys and ciphertextno matter the variety of involved attributes, and it additionally keeps the computation value consistent on lightweightmobile devices.

Jianan Hong(2015) [10] proposed that Ciphertext-Policy Attribute-primarily based Encryption (CP-ABE) is seemed as one amongthe maximum appealing cryptographic strategies for data get access to control in cloud storage device, due to its finegrained information access manipulate policy and direct control of facts for statistics proprietors. In CP-ABE, the user can get right of access to the content of the ciphertext, only if his/her attributes satisfy the ciphertext's preset access policy.

JieXu, Qiaoyan Wen, Wenmin Li and Zhengping Jin(2015) [9] have been proposed Circuit Ciphertext-policy Attribute based Hybrid Encryption with Verifiable Delegation in Cloud Computing to maintain data personal and attain access control. The anti-collusion circuit CP-ABE production is used on this paper due to the fact CP-ABE is conceptually closer to the traditional access control methods.

III. PROPOSEDWORK

System model: Here we're assuming that the HABE version consists by way of the usage of following entities this is Trusted third party (TTP),Internal Trusted Third Parties (ITP), User and Cloud Service Provider (CSP).CSP is operated by using its personal Administrative activity which is interconnection of massive server for storing encrypted documents of corporation and saved distinctive reproduction of that encrypted report over special servers.CSP provide High Quality of offerings and high computational electricity. TTP generate keys for different business enterprise and CSP.ITP is accountable for generating key for branch and person. It also chargeable for retaining dynamic hierarchical shape of organization.

Security Model: As described in Haclgiimfi et al. (2002), there are primary assaults below any such situation, i.e., external attacks initiated by means of unauthorized outsiders, and inner attacks initiated by using an honest however curious CSP (Yu et al., 2010b), as well as

International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 04 Issue-17
December 2017

malicious end user [1].However the data stored in cloud that's to be don't forget as secure and communication line is also secure by way of the use of existing communication protocol SSL(Secure Socket Layer). Data is continually in the form of encrypted and secrete key required for decryption, that's now not decrypted easily by using malicious user or cloud provider issuer.

As we know HABE Model having three important part that are TTP, ITP and end user. Following diagram shows actually system construction. There are different part which is actually perform same task. TTP contain two algorithms' setup and 'create_RMalgorithm.ITPcontainscreate_branch,Create_ Dept,Create_User,Encryptionand Decryptionalgorithm

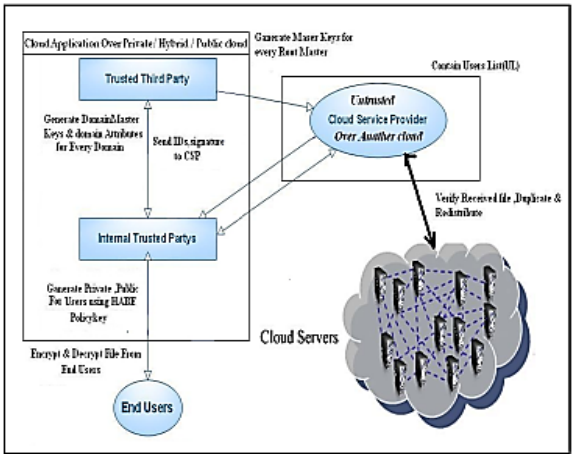

Fig 2. Construction of HABE Model

For construction of System we need to know algorithm which is follows.

A. Setup Algorithm

Setup algorithm takes a same parameter and generate master
key for each organization and CSP.

```
Setup (parameter)
{
//generate master key for Each Root master
Generate (Mki);
}
```

B. Create Branch Algorithm

This algorithm takes a master key of each organization and parameter generates the branch id for each branch of organization.

```
create_branch(Mki,parameter)
{
Generate (Bki);
//Bki is for each branch of organization
}
```

C. Create Dept Algorithm

This algorithm takes a Mki,Bki,Ref_id and parameter togenerate department wise key i.e. Dki.

```
Create_dept (Mki,Bki,Ref_id,parameter)
{
//Dki is department wise key
// Ref_id is id of parent node
Generate (Dki);
}
```

D. Create User Algorithm

This algorithm takes a Mki,Bki,Dki and parameter o generate User id Uid.

```
Create_User(MK,Bid,Dki,parameter)
{
If (true) Generate (uid);
Else error;
}
```

E. Encryption Algorithm

This algorithm takes a plane text file F and valid user accesspolicy on that file and generate cipher text file and it will bestored on cloud service provider. A is disjoined normal form(DNF) policy.

```
Encryption (F,Pka|aεA)
{
If(Pk is true)
{
Generate (cipher text file)
}
Else
{
Error;
}
}
```

F. Decryption Algorithm

This algorithm takes cipher text (CT), Secrete key (SK) εConjunctive clause and generates plaintext.

```
Decryption (CT,Ski|aεCCi)
{
If (Ski is true)
{
Generate (plaintext file F);
```

}
Else
{
Error;
}
}

IV. CONCLUSION

In this paper the suggested work is confirmed to be secured using the hybrid encryption concept. Encrypting the data is completed using the secret key this key is generated based on the attributes of the user.Likewise hiding the cipher text into the image is an additional security for both the data owner and the use. HASBE pools the functionalities of HIBE and ASBE.HASBE scheme seamlessly incorporates a hierarchical structure of system users. It customs a delegation algorithm toASBE. Out of these schemes, the HASBE scheme offers extra scalable, flexible and fine-grained access control than any other schemes in cloud computing

REFERENCES

[1] Guojun Wanga,*, Qin Liu a,b, Jie Wub, Minyi Guo-Hierarchicalattribute-based encryption and scalable user revocation for sharing datain cloud servers. In Proceeding of CCS 3 0 (2 0 1 1) 3 2 0 e3 3 1.

[2] Wang G, Liu Q, Wu J. Hierarchical attribute-based encryption for finegrained access control in cloud storage services. In: Proceedings ofCCS-2010 (Poster), pp. 735e737.

[3] Bethencourt J, Sahai A, Waters B. Ciphertext-policy attributebasedencryption. In: Proceedings of ISSP; 2007. p. 321e34.

[4] aws.amazon.com/documentation/ec2

[5] s3.amazonaws.com/awsdocs/EC2/2008-12.../ec2-dg-2008-12-01.pdf

[6] Z. Wan,s J. Liu, and R. H. Deng, ―HASBE: A Hierarchical attributebased solution for flexible and scalableaccess control in cloud computing,‖ IEEE Trans. Inf. Forensics Security, vol. 7, no. 2, pp. 743–754, Apr. 2012.

[7] Zhijie Wang, Student Member, IEEE, Dijiang Huang, Senior Member, IEEE, Yan Zhu, Member, IEEE, Bing Li,Student Member, IEEE, and Chun-Jen Chung, Student Member, IEEEEfficient Attribute-Based Comparable DataAccess ControlVOL. 64, NO. 12, DECEMBER 2015.

[8] Cong Wang, Member, IEEE, Sherman S.M. ChowPrivacy-Preserving Public Auditing for Secure CloudStorage VOL. 62, NO. 2, FEBRUARY 2013.

[9] JieXu, Qiaoyan Wen, Wenmin Li and ZhengpingJinCircuitCiphertext-policy Attribute-based HybridEncryption with Verifiable Delegation in Cloud Computing DOI 10.1109/TPDS.2015.2392752.

[10] Jianan Hong, KaipingXue, Member, IEEE, andWei Li Comments on ―DAC-MACS: Effective Data AccessControl for Multiauthority Cloud Storage SystemsSecurity Analysis of Attribute Revocation in MultiauthorityData Access Control for Cloud Storage Systems VOL. 10, NO. 6, JUNE 2015.

[11] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in Proc. IEEE Symp. Secur. Privacy, May 2007,pp. 321–334.