International Journal of Research
Available at https://edupediapublications.org/journals
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 04 Issue 06
May 2017

A Study of HABE (Hierarchical Attribute Based Encryption) Scheme

Maragoni Mahendar
Assistant professor,Department of CSE
Avanthi's Scientific Technological & Research Academy, Ranga Reddy, Telangana, India

ABSTRACT: Cloud computing is going to be very famoustechnology in IT businesses. For an enterprise, the data stored is large and it's miles very valuable. All responsibilities are achieved throughnetworks. Hence, it becomes very vital to have the secureduse of data. In cloud computing, the maximum important concerns ofprotection are data protection and privateness. This paper pursuits to remedy hassle for supportingdistinctive organization shape and maintain their hierarchy ofnumerous clients in the groups, keep document of employees.Our system is having integrating key feature of Hierarchicalattribute based encryption (HABE) and cipher text policyattribute 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 in which wecan use assets and pay handiest for that assets wherein weare involved, so that consumer can revel in service on call for. Thisrising computer paradigm enable consumer to shop theirtouchy data in cloud each time consumer wants that information he candownload it in clean way. Cloud computing provide simplicityand efficient offerings to the user for you to store capital valueon hardware's infrastructure Especially for small and mediumsized organizations with confined budgets, they can obtain costsavings and the flexibility to scale (or reduce) investments ondemand, through the usage of cloud-based totally services to manipulate tasks,organisation-wide contacts and schedules, and so forth[1].CSPmay be operated for making profit to take care about sensitiveexclusive facts, arises security and private problem. CSP can beselling out the private data to closest competitor organization for making income.

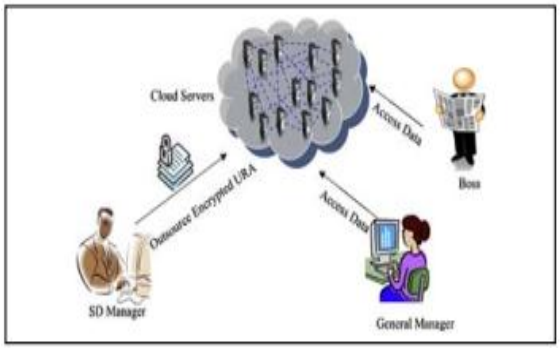

Fig 1. Application Scenario

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 anddevelopment 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 beexpressed as a Boolean system over attributes. Each attributeincludes an internet web site specifying which celebration administers thecharacteristic and an identifier describing the characteristic itself, each ofwhich may be represented as strings and concatenated with asingle colon individual as a separator [1]. The minimize "/" in eachinternet webpage denotes a concatenation among the superior and thesubordinate.

The instinct behind this get access to control coverage is that thisURA 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 theintended 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 theencrypted data.

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

• 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 thinclient with constrained bandwidth, CPU, and reminiscencecompetencies, the CP-ABE scheme have to be of excessiveoverall performance [1]. That is, the verbal exchange prices andcomputation fees introduced via the CP-ABE schemeshould be low enough, in order that the user can efficientlyretrieve facts from the cloud, and then decrypt it the usage of theskinny purchaser [1].

• Full Delegation. In a large-scale corporation with manypersonnel, each employee desires to request secret keysfrom the characteristic authority (AA), when he joins thebusiness enterprise [1]. If a majority of these personnel require their mysterykeys 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-ABEschemes 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 theshape and semantics of its attributes [1].

• Scalable Revocation. In order to hold hierarchy ofbusiness enterprise we need to recognise about how plenty workerin enterprise and those who are not employeerevoke their access control coverage. A user whosepermission is revoked will still hold the keys issuedearlier, and thus can nonetheless decrypt facts within the cloud [1]. Thetraditional revocation scheme usually calls for the AAs toperiodically re-encrypt data, and re-generate new secretkeys to ultimate authorized clients [1]. This technique willpurpose heavy workload at the AAs. A greater scalabletechnique 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 theenvironment 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, whichsimultaneously achieves high performance, full delegationand scalable revocation [1].

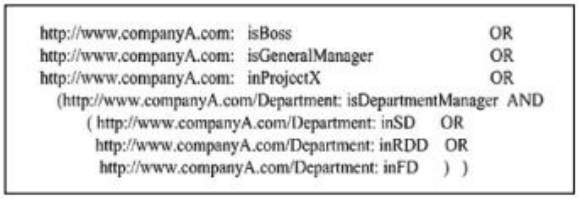

Fig 2. Sample Access Control Policy of URA

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, flexiblem andbest-grained get access to control.

Cong Wang Sherman S.M. Chow, Qian Wang (2013) [8] offers our public auditing scheme which provides awhole 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 sharedpool of configurable computing sources, with out the burden of neighborhood data storage and preservation.

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 storagedevice, 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 thecontent 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 accesscontrol. The anti-collusion circuit CP-ABE production is used on this paper due to the fact CPABE is conceptually closerto the traditional access control methods.

III. PROPOSEDWORK

System model: Here we're assuming that the HABE version consistsby way of the usage of following entities this is Trusted third party (TTP),Internal Trusted Third Parties (ITP), User and Cloud ServiceProvider (CSP).CSP is operated by using its personal Administrativeactivity which is interconnection of massive server for storingencrypted documents of corporation and saved distinctive reproduction ofthat encrypted report over special servers.CSP provide HighQuality of offerings and high computational electricity. TTPgenerate keys for different business enterprise and CSP.ITP isaccountable for generating key for branch and person. It alsochargeable for retaining dynamic hierarchical shape oforganization.

Security Model: As described in Haclgiimfi et al. (2002), there are primary assaults below any such situation, i.e., external attacksinitiated by means of unauthorized outsiders, and inner attacksinitiated by using an honest however curious CSP (Yu et al., 2010b), aswell as malicious end user [1].However the datastored in cloudthat's to be don't forget as secure and communication line isalso secure by way of the use of existing communication protocol SSL(Secure Socket Layer). Data is continually in the form ofencrypted and secrete key required for decryption, that'snow not decrypted easily by using malicious user or cloud providerissuer.

As we know HABE Model having three important partthat are TTP, ITP and end user. Following diagram showsactually system construction. There are different part which isactually perform same task. TTP contain two algorithms'setup and 'create_RM algorithm. ITP contains create_branch,Create_Dept, Create_User, Encryption and Decryptionalgorithm

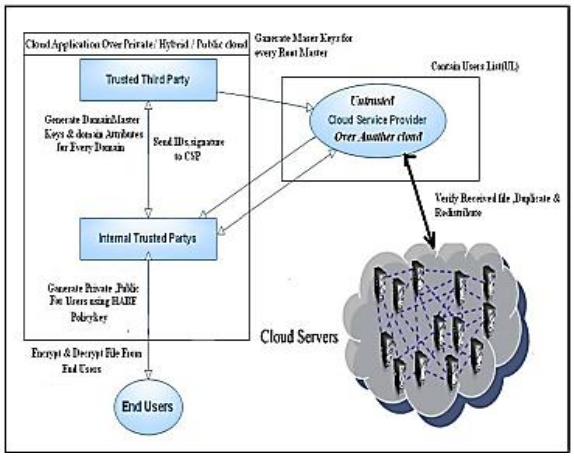

Fig 2. Construction of HABE Model

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 andparameter generates the branch id for each branch oforganization.

```
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 iscompleted using the secret key this key is generated based on the attributes of the user.Likewise hiding the cipher text into theimage 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 hierarchicalstructure 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 thanany 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.

Author:

Maragoni Mahendar has Received B.TECH Degree in Computer Science Engineering (C.S.E) from Avanthi's Scientific Technological & Research Academy, Gunthapally, Rangareddy in 2012, under Jawaharlal Nehru Technological University Hyderabad and Masters Technology in Computer Science Engineering (C.S.E) from Nova College of Engineering & Technology, Jafferguda, Ranga Reddy 2014, under Jawaharlal Nehru Technological University Hyderabad, And He his Member of CSI, He dedicated to teaching field since the last 2 years in field of interest includes Cloud Computing, Data science & Big Data. I Have published Two International Journals and Participated in 1 International conferences. At present working as Asst.Professor, Department of Computer science and Engineering in Avanthi's Scientific Technological & Research Academy, Ranga Reddy, Telangana, India.