International Journal of Research
e-ISSN: 2348-6848 & p-ISSN 2348-795X Vol-5, Special Issue-11
International Conference on Multi-Disciplinary Research - 2017 held in February, 2018 in Hyderabad, Telangana State, India organised by GLOBAL RESEARCH ACADEMY - Scientific & Industrial Research Organisation (Autonomous), Hyderabad.

A Novel Integrity-Verification based Secured ABE model for cloud computing

Kranthi Kumar Singamaneni
Research Scholar
Department of CSE
GITAM University,
Vishakhapatnam, India

P.Sanyasi Naidu
Associate Professor
Department of CSE
GITAM University,
Vishakhapatnam, India

Abstract**—** Cloud environment has emerged as a flexible, computational cost and scalable to solve the problems of increasing on-demand requirements on shared computing resources. Data security and access control are the major issues in the cloud environment, as users often store their sensitive data by the third party authorities. Attribute based encryption and decryption models have been widely used in the cloud server for not only hiding the data but also provide user access control. Many cloud based privacy protection solutions have been implemented in the literature, however most of them only focus on limited data size and storage format. With the increase in attribute and user policies, tree size growth also exponentially increases which is very difficult to the user to access the information. In constant based attribute based encryption communication overhead occurs due to the increase in users network access. In this proposed work a pattern based access policy is introduced to reduce the communication overhead and time to access the information. This approach includes three phases i.e Setup phase, Key Generation Phase, Encryption and Decryption. This system uses hash based policy access structure with homomorphic encryption mechanism. Experimental results proved that proposed model has high efficiency in terms of computation overhead, time to generate secret key, time to access the shared information and storage overhead .

Keywords— ABE, Cloud security, Encryption and Decryption Algorithm

I. INTRODUCTION

With the rapid development of the distributed computing and internet architectures, there is an exponential demand for data processing and sharing resources in the cloud environment. The third party provider needs to implement trusted access control and confidentiality for the cloud customers. Also, it is highly recommendable for the large scale applications to support one to many communications to reduce the data encryption and decryption mode. Since the cloud applications such as Google apps, Microsoft 360,and cloud infrastructures such as Eucalyptus, Amazon's EC2 and platforms such as Amazon' s s3 and window's Azure have different configurations and different services . As the size of the client data stored in cloud environment increasing, it becomes highly sensitive to store against un-authorized third party applications and users; for instance, social networks and medical records. Privacy and security are the major challenges in cloud computing[1][2]. The traditional cryptosystem framework based on public key infrastructure (PKI) can achieve data security, confidentiality and non-repudiation along with limitations. In order to encrypt data, the third party provider needs to obtain the authorized user's public keys and then communicate the cipher data to the individual authorized user, which increases the bandwidth and processing overhead.

Instead of encrypting the data once for each user, it would be advantageous to be able to encrypt only once for all cloud users. This process is known as ABE. In this approach, each user has a set of authorized attribute-sets, policies and a privacy key[3]. Several attributes based encryption schemes have been proposed in the last few decades. As the size of the key space and attributes set were fixed in the setup phase, data size of the attribute space is quadratically limited to security measures. In an basic ABE procedure , secret key, private key and cipher text are decrypted with the access tree structures [4]. Users are able to decrypt cipher text if and only if the respective attributes satisfy the access policy. The idea of CP-ABE is just reverse mechanism of KP-ABE. CP-ABE acts as the basic unit for many other schemes because of its flexible nature. KP-ABE has the disadvantage of no control on decryption rights. This issue of previous approach is resolved here. It has also implementation in real world scenario. This proposed scheme faces also a severe problem, that is:- It cannot be implemented in enterprise scenario. This flaw occurs because of low flexibility and inefficiency/ poor efficiency. The whole process of decryption requires attributes of single set. Thus, users are eligible to select single attribute or combination of attributes from that specified set. Later this disadvantage of CP-ABE scheme was encountered and overcome by another newly developed approach, i.e., CP-ASBE (Cipher text Policy Attribute Set Based Encryption).

Hierarchical attribute-based encryption model was developed using ABE model. The whole model was represented by hierarchical structure. Key generation process is carried out by a root master, that interacts with several different domain masters. Every domain master again interacts with numbers of enterprise users. The said model has its applications in cloud enterprise domain and in proxy re-encryption. This scheme is theoretical one and it's impossible and too expensive to implement practically. Conjunctive clause attributes are managed by same domain authority, whereas similar attributes are managed by multiple domain authorities.

In KP-ABE scheme, the cipher text is integrated with the attributes ,policies and private keys with tree access structure as shown in Figure 1.

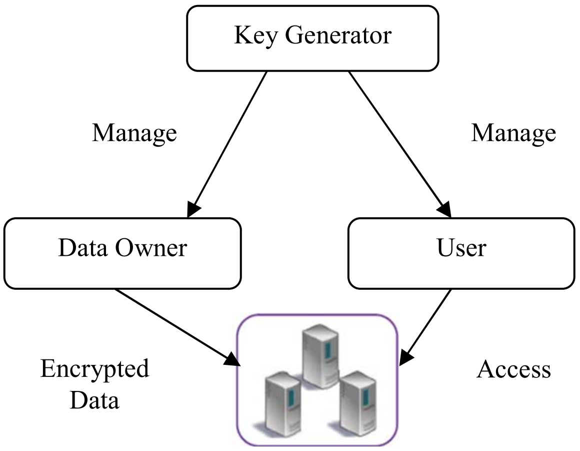

Fig 1: Cloud Data

Various security frameworks with protecting data both from cloud side and client side are implemented in the literature for data security. But computational requirements and processing speed play a vital role in deployment of these cloud security models in cloud computing environment. Public-key cryptography makes it possible to do asymmetric cryptography. Using the public key, anyone can encrypt messages that can only be decrypted if one possesses the private key or decryption key. A special form of public-key cryptography, called Attribute-Based Encryption, allows users to decrypt messages if their decryption key satisfies the access policy defined in the ciphertext.By using encryption, data can be protected against unauthorized access without the need of an on-line verifier authorizing data requests[5][6][7].

Access structures are used to define which users have access to which resources. In the case of attribute-based authentication, attributes determine the authorization level of the user. An access structure can be regarded as a collection of sets of attributes. Each single set describes which attributes are needed to be granted access. As long as the user's attributes satisfy at least one set in the collection, the user is granted access. There are two kinds of access structures: monotonic and non-monotonic. Monotonic access structures ensure that whenever a user would be granted access based on a subset of his attributes, he will be granted access based on all his attributes. This means that no negations of attributes are possible. Nonmonotonic access structures do allow such negation of attributes.

[8] proposed a fuzzy Identity based encryption scheme in which a descriptive attributes set are considered as identity for encryption and decryption process. For the privacy or secret key k_{AS} corresponds to the attribute set S. We can decrypt the data using $k_{AS'}$ corresponds to the attribute set $'$ and satisfies the condition $|S \cap S'| < d$,where d is the minimum number of attributes.

Access Control Mechanism in Cloud Environment

Role based access control models assigns the user access control permissions and roles according to the business function in the organization. Role is the mapping between the user and the access permissions. Basically, user access control permission is divided into two steps: Association of role and user, and association of access permissions. Cloud Computing role based access control model has three constraints they are environment, type of servers and resource limitation[8][9].

Task based access control models were the improved model of role based access control mechanism. It provides dynamic authority assignment in task contextual information and graded access control via a role.

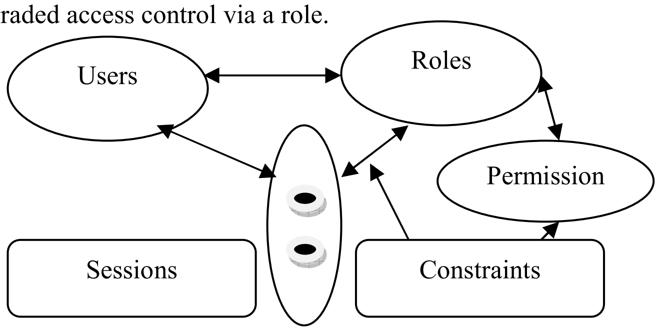

Fig 2: Encryption session interaction

View based access control mechanism is the enhancement of access control mechanism which is based on traditional access matrix procedures with views as matrix values and roles as subjects. As shown in Fig 2., views on objects are assigned to principals. Principal can access the complete operations of an object , if he or she has a view on the object with the valid permission.

Integrity and authentication of data in cloud environment are essential issues to ensure that data confidentiality and privacy preserving to the customer's data or queries. Problem of dealing with user's queries and encrypted data over cloud environment were discussed widely in research literature.[2-5] try to memory integrity checking to address integrity issues by applying Hash tree over memory content. An integrity verification approach [4] in hybrid clouds is applied to support the data migration and scalability service is implemented on limited data.

Main Problems in CP-ABE and KP-ABE: Require a number of exponential generators for private key computation which is a significant computation ovehead.Also it requires Random oracle model which is less secure than other standard models. Both the cipher texts and private keys are labeled with an policy set and attribute set , the decryption will succeed only if there exist at least k common attributes between the cipher text and a private key.

Sno	Method	Setup attributes	Problems
1	Outsourced Provable Data [7]	RSA based homomorphism linear-model	It may leak user's data to the third party users
2	ABE[8]	Setup, Public and secret keys	Doesn't support secure communication in cloud environment
3	CP-ABE[9]	Attributes,Policies,Key Generators	As the number of attributes size or storage space increases, computational time also increases.
4	KP-ABE[10]	Key policies, Attributes, Key generation	Fail to construct the access policy patterns for multiple cloud storage services.

The traditional models ensure data security by using encryption is not optimal in the cloud virtual machines of cloud providers. Since administrators manage the remote system access to servers and infrastructure, if the cloud administrator is an attacker then he can gain remote access to the user's cloud data [4-6]. Although the trusted third party authorities are aware of the malicious insider, they assume that they have limited solutions to overcome these issues. A minimized cost-effective solution, secured, multi-cloud storage method is implemented in cloud environment which controls an economical distribution of information among the available cloud instances to provide the customers with secure storage and data availability. A high performance cloud computing service is implemented that integrates the parallel processing framework and checkpoint infrastructure such as Message passing interface for virtual machines. In the cloud server attacks, the length of the overlapping runtime of the cloud instances and malicious virtual machines is important to find the network bandwidth. Since limiting the overlapping execution times may degrade the network performance and increase the error rate.

Basic requirements of attribute and key based access mechanisms in a cloud environment are as follows:

- The implemented approach should be scalable and efficient in design which prevents runtime computation.
- This system should be high secured against collision.
- Each user decrypt the data from the cloud server using the decryption process through the access tree mechanism.
- It should support forward and backward access control model.
- Forward Access Privacy: describes that a cloud user cannot open any encrypted data which was stored in the cloud server in hidden form.
- Backward access control means that a authorized cloud user cannot decode any encrypted cloud data that is hosted in the cloud.

Problems in Traditional Attribute Encryption Methods:

1. Key policy attribute based encryption is that it cannot decide cloud user's decrypting data which is in cipher form.
2. Key policy attributes encryption can only choose limited attributes for access control mechanism.
3. In cipher text policy encryption schemes are difficult to represent the policies and manage authorized client attributes.
4. Achieving the large attributes and key space are challenging factors in a cloud environment.
5. Traditional ABE schemes suffer with revocation issue in multiple cloud servers.
6. Identity based Encryption scheme suffers with one to many communication problems. That is, if the sender wants to share his data with multiple receivers, he must know all the receiver's identities.

3.Mathematical Cloud Security Attack Detection Model in Distributed Network

A new mathematical cost model was implemented by [8] to find the energy usage in man in the middle detection. Let us consider un-directed graph $G=(V_m,E,C_{vm})$, where V_m = {0,1,2, …..,N} is a set of cloud nodes representing Virtual Machine instances. Here they assume node V_0 represents the request dispatcher, whereas nodes $V_1,V_2,V_3..V_m$ represent available client instances.

Let E = { $(i,j):i,j\in V_m,i\neq j$ } is a set of edges joining the virtual machine instances, with ant travel distance or cost.

Let C_{vm} = { $c_{ij}:i,j\in V_m,i\neq j$ } is the cost of traversing between the virtual machine instances (nodes).

Let ψ be the total number of ants in PSO model, each with capacity ψ_c and task assignment to virtual machine instances based on the stochastic demands and variables. Here, a VM client instance holds the stochastic parameters ρ_1, where I = {0,1,… n}, which are independent variables with known data normalization. The total request of each Virtual Machine is not known until the ant is not arriving at the VM instance. Therefore, they consider the demand ρ_1 does not exceed the ψ_c and follows a normal distribution with probability mass function(pmf).

$$\text{pmf} = \text{Probabililty}(\rho_1 = d)\ ,$$

Where d is total demand of VM instance $d\in w:\text{whole number}$.

Pmf= $\sum_{i=1} P(d_i)$, in case of discrete model

Pmf= $\int f(d_i)dx$, in case of continuous model

According to the VM instances, node demand of the ant resolves whether to continue to the next VM instance or to go back to the user task execution for re-stocking of new task.

$B_{i,j,k}$ = Binary flow variable

$B_{i,j,k}$ =1, if the path between (i and j) is travelled by k^{th} agent.

$B_{i,j,k}$ =0, otherwise

$J_{i,k}$, Task components uploaded at i^{th} virtual machine instance by k^{th}.

ψ : Total number of ants initiated by the task controller.

η : Remaining unallocated tasks of the ants.

C_j : Capacity of tasks carried by the ants.

$\alpha^{p}_{j,k}(\eta)$: Predicted cost of forward task actions.

$\alpha^{r}_{j,k}(\eta)$: Predicted cost of restocking tasks.

If $\alpha_{j,k}(\eta)$ is the task allocated to the j^{th} VM instance by the k^{th} agent, then the objective function can be formulated as:

$$\alpha_{j,k}(\eta) = \min(\alpha^{p}_{j,k}(\eta), \alpha^{r}_{j,k}(\eta))$$

Where

$$\alpha^{p}_{j,k}(\eta) = c_{j,j+1} + \sum \alpha_{j+1,k}(\eta - d)\,p_{i+1}, if\ d \le \eta$$

And

$$\alpha^{p}_{j,k}(\eta) = \sum 2c_{aj+1,0} + (\eta + c_j - d)\alpha_{j+1,k}\,p_{i+1,d}, if\ d > \eta$$

$$\alpha^{r}_{j,k}(\eta) = C_{0,j+1} + \sum \alpha_{j+1,K}(C_j - d)\,p_{j+1,d} + C_{j,0}$$

$$\int_{C} \alpha^{r}_{j,k}(\eta) = C^{2}{}_{j,0} + C^{2}_{0,j+1} + C_{j,0} \sum \alpha_{j+1,K}(C_j - d)\,p_{j+1,d}$$

III. Proposed ABE Scheme in Cloud Environment

Bi-linear Group in ABE model:

Let G be a cyclic group of prime order p generated by group element g. Let G_p be the group of prime order p. Let a map $m: G \times G \rightarrow G_p$ is said to be bilinear maps if it satisfies the following conditions:

1. $m(e1^x, e2^y) = m(e1, e2)^{xy}$

   for all e1,e2 $\in$ G and x,y $\in G_p$

   and x, y$\in Z_p$
2. m is efficiently computable.
3. Non- Degenerate
   a. $m(g, g) \ne 1$

Most of the ABE schemes have four steps as shown in Fig 3:

Setup: This phase setup public key parameters of the user using the mathematical group theory functions.

Key Generation: This phase generates private key as secret key , depending on the set of user's attribute and policies.

Cloud Data Encryption: Each cloud user encrypts the data using his public key along with the credentials[11-12].

Cloud Data Decryption: This phase enables a receiver with the matching attributes and polices to decrypt the cloud data as shown in Figure 2.

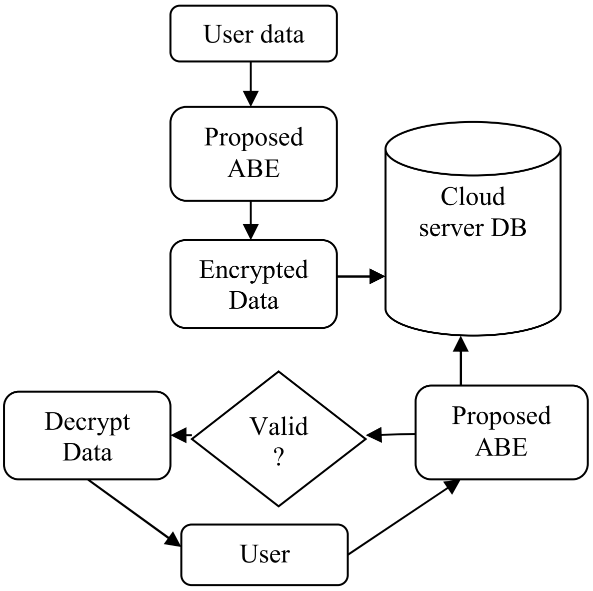

Fig 3: Proposed Model

Key Generation :

Key Generation algorithm will take set of attributes , Policies and hash value as input and returns Secret key as output.

Each user is associated with secret key and it will be generated using three pattern keys as

Public Key:={ S', $g(p), g(q), g(r)$, $G_{\alpha 1}, G_{\alpha 2}, G_{\alpha 3}$, $H^{1}_{AK}, H^{2}_{SK}, H^{3}_{(Policies)}$; };

Master key:={ $\alpha 1, \alpha 2, \alpha 3$ }; known to T.A

$K_{1,i} = g_{(P)}^{1/(S'+\alpha 1)}$; i=0…..Pattern1.length;

$K_{1,j} = g_{(q)}^{1/(S'+\alpha 2)}$; j=0….. Pattern2.length;

$K_{1,k} = g_{(r)}^{1/(S'+\alpha 3)}$; k=0…. Pattern3.lenght;

Secret key:={Policies, $H^{1}_{AK}, H^{2}_{SK}, H^{3}_{(Policies)}$; , $K_{1,i}, K_{1,j}, K_{1,k}$ };

Encryption Process:

Input: Public key, Attributes, User-Policy, Cloud data;

PublicKey:={ S', $G_{\alpha 1}, G_{\alpha 2}, G_{\alpha 3}$ $g(p), g(q), g(r)$, ,

$H^{1}_{AK}, H^{2}_{SK}, H^{3}_{(Policies)}$; };

Calculations:

$C(S^{'},i)_0 = g_{(p)}^{S^{'}}$

$C(i)_0^{'} = g_{(p)}^{(\alpha 1+\alpha 2+\alpha 3)}$;

Where $\alpha 1, \alpha 2, \alpha 3 \in G_{\alpha 1}, G_{\alpha 2}, G_{\alpha 3}$;

$C(i)_1 = g_{(p)}^{H^2_{(SK)}+H^3_{(Policies)}} . g_{(p)}^{H^1_{(AK)}+\alpha 1}$ i:=0……pat1.length;

$C(j)_2 = g_{(p)}^{H^1_{(AK)}+H^3_{(Policies)}} . g_{(p)}^{H^2_{(SK)}+\alpha 2}$; j:=0……pat2.length

$C(k)_3 = g_{(p)}^{H^1_{(AK)}+H^2_{(SK)}} . g_{(p)}^{H^3_{(Policies)}+\alpha 3}$; k:=0…...pat3.length;

Encryption algorithm encrypts the message using policy pattern structures. Algorithm uses three patterns with homomorphic encryption and decryption process. Additive and Multiplicative homomorphism takes two inputs and generate secure encrypted values as output. Homomorphism encryption and decryption uses $\psi(i)_0 , \psi(i)_0^{'}$ as input.

Additive Homomorphic Encryption

$EncD(I_1+I_2) = EncD(I_1) + EncD(I_2)$;

Multiplicative Homomorphic Encryption

$EncD(I_1 .I_2) = Enc(I_1).Enc(I_2)$;

$\psi(i)_0$=EncD(I_1):=EncD(I_1)=($I_1+\gamma*\beta$)mod n where n=$\alpha*\beta$;

$\psi(i)_0^{'}$=EncD(I_2):=Enc(I_2)=($I_2+\gamma*\beta$)mod n where n=$\alpha*\beta$;

$EncD(I_1+I_2)$:= Enc($\psi(i)_0$)+Enc($\psi(i)_0^{'}$);

$EncD(I_1+I_2)$:=($I_1+\gamma*\beta$)mod(n)+($I_2+\gamma*\beta$)mod n

EncD($I_1.I_2$):=EncD($\psi(i)_0$).EncD($\psi(i)_0^{'}$);

:=($I_1+\gamma*\beta$)mod n. +($I_2+\gamma*\beta$)mod n;

Cipher Text CT
{
Total patterns TP,
$H^1_{AK}, H^2_{SK}, H^3_{(Policies)}$; ,.e($EncD(I_1+I_2)$,EncD($I_1.I_2$) ,{ $\psi(i)_0 , \psi(i)_0^{'}$ },Cipher text C
};

Cipher Text CT is publicly available to all the attribute policy holders. This CT will be decrypted only those users who has exact policy matching patterns keys.

Decryption Process:

Input(CT,Secret Key):

Secret key:={Policies, $H^1_{AK}, H^2_{SK}, H^3_{(Policies)}$; , $K_{1,i}, K_{1,j}, K_{1,k}$ };

Cipher Text CT
{
Total patterns TP,
$H^1_{AK}, H^2_{SK}, H^3_{(Policies)}$; ,.e($EncD(I_1+I_2)$,EncD($I_1.I_2$) ,{ $\psi(i)_0 , \psi(i)_0^{'}$ },Cipher text C
};

Decryption Process:

Consider

M.e($EncD(I_1+I_2)$,Enc($I_1.I_2$).e($C(i)_1 , K_{1,i}$).e($C(j)_2$ $K_{1,j}$).e($C(k)_3 , K_{1,k}$) to extract added pattern policy.

$EncD(I_1+I_2)=$

Enc($\psi(i)_0+\psi(i)_0^{'}$)=Enc($\psi(i)_0$)+Enc($\psi(i)_0^{'}$);

:=($\psi(i)_0+\gamma*\beta$)mod n+($\psi(i)_0^{'}+\gamma*\beta$)mod n

EncD($I_1.I_2$):=Enc($\psi(i)_0.\psi(i)_0^{'}$)

:=Enc($\psi(i)_0$).Enc($\psi(i)_0^{'}$);

:=($\psi(i)_0+\gamma*\beta$)mod n. +($\psi(i)_0+\gamma*\beta$)mod n;

Dec($EncD(I_1+I_2)$):=(EncD($\psi(i)_0+\psi(i)_0^{'}$)) mod α

:= (($\psi(i)_0+\gamma*\beta$)mod n+($\psi(i)_0^{'}+\gamma*\beta$)mod n) mod α

:= I_1+I_2 -----> (1)

Dec(EncD($I_1.I_2$)):=(EncD($\psi(i)_0.\psi(i)_0^{'}$):=EncD($\psi(i)_0$).Enc($\psi(i)_0^{'}$))mod α;

:=(($\psi(i)_0+\gamma*\beta$)mod n. +($\psi(i)_0^{'}+\gamma*\beta$)mod n) mod α;

:= $I_1.I_2$ --------> (2)

Solving eq-(1) and eq (2) we will get I_1, I_2.

$\alpha=\alpha 1$

$\beta=\alpha 2$

$\gamma=\alpha 3$

$\{H_1^{'}, H_2^{'}, H_3^{'}\} = \{H^1_{AK}, H^2_{SK}, H^3_{(Policies)}\}$

Now e($Enc(M_1+M_2)$,Enc($M_1.M_2$))=e($\psi(i)_0 , \psi(i)_0^{'}$)

:=e($g_p^{S^{'}} , g_p^{(\alpha+\beta+\gamma)}$)

$:= e(g_p, g_p)^{S^{'}(\alpha+\beta+\gamma)}$

Consider

$$\prod_{i=1}^{n} e(C_{1,i}, K_{1,i}) = e(g_p^{H_2^{'}+H_3^{'}} . g_p^{H_1^{'}+\alpha}, g_p^{1/(S^{'}+\alpha)})$$

$$= e(g_p^{H_2^{'}+H_3^{'}+H_1^{'}+\alpha}, g_p^{1/(S^{'}+\alpha)})$$

$$=e(g_p^{S'+\alpha}, g_p^{1/(S'+\alpha)})$$
$$=e(g_p, g_p)^{(S'+\alpha)/(S'+\alpha)}$$
$$=e(g_p, g_p)=1$$

$$\prod_{j=1}^{n} e(C_{2,j}, K_{1,j}) = e(g_p^{H_2'+H_3'}.g_p^{H_1'+\beta}, g_p^{1/(S'+\beta)})$$
$$=e(g_p^{H_2'+H_3'+H_1'+\beta}, g_p^{1/(S'+\beta)})$$
$$=e(g_p^{S'+\beta}, g_p^{1/(S'+\beta)})$$
$$=e(g_p, g_p)^{(S'+\beta)/(S'+\beta)}$$
$$=e(g_p, g_p)=1$$

$$\prod_{k=1}^{n} e(C_{3,k}, K_{1,k}) = e(g_p^{H_1'+H_2'}.g_p^{H_3'+\gamma}, g_p^{1/(S'+\gamma)})$$
$$=e(g_p^{H_1'+H_2'+H_3'+\gamma}, g_p^{1/(S'+\gamma)})$$
$$=e(g_p^{S'+\gamma}, g_p^{1/(S'+\gamma)})$$
$$=e(g_p, g_p)^{(S'+\gamma)/(S'+\gamma)}$$
$$=e(g_p, g_p)=1$$

$$e(g_p, g_p)^{S'(\alpha+\beta+\gamma)}.\prod_{i=1}^{n} e(C_{1,i}, K_{1,i}).\prod_{j=1}^{n} e(C_{2,j}, K_{1,j}).$$
$$\prod_{k=1}^{n} e(C_{3,k}, K_{1,k})$$
$$\Rightarrow M.\ e(g_p, g_p)^{S'(\alpha+\beta+\gamma)}.1.1.1$$
$$\Rightarrow M.\ e(g_p, g_p)^{S'(\alpha+\beta+\gamma)} \text{ -----} > (3)$$

Now Based on the user entered policy A and D parameters may vary as

If user entered policy is in pattern1 then

$$D_{1,i} = g_p^{\alpha}$$
$$A_{1,i} = g_p^{\beta+\gamma}$$

If user entered policy is in pattern2 then

$$D_{2,j} = g_p^{\beta}$$
$$A_{2,j} = g_p^{\alpha+\gamma}$$

If user entered policy is in pattern3 then

$$D_{3,k} = g_p^{\gamma}$$
$$A_{3,k} = g_p^{\alpha+\beta}$$

If user entered policy is in patter1 then decryption follows:

Decryption:= M. $e(g_p, g_p)^{S'(\alpha+\beta+\gamma)}$ /e(C,D*A)

$$:= M.\ e(g_p, g_p)^{S'(\alpha+\beta+\gamma)} / e(g_p^{S'}.g_p^{\alpha}.g_p^{\beta+\gamma})$$
$$:= M.\ e(g_p, g_p)^{S'(\alpha+\beta+\gamma)} / e(g_p^{S'}.g_p^{\alpha+\beta+\gamma})$$
$$:= M.\ e(g_p, g_p)^{S'(\alpha+\beta+\gamma)} / e(g_p, g_p)^{S'(\alpha+\beta+\gamma)}$$
$$:= M$$

Similarly other policies can decrypt the original message M.

Experimental Results

All experiments are executed with the aws cloud server with third party libraries amazon aws, cpabe, abe ,jama.etc.

Table 2: Time complexity of proposed model to the existing ABE models.

Models	Encryption Time	Decryption Time	Communication Time
ABE	8767	7598	3977
CPABE	7824	7293	3740
KPABE	6988	7193	3498
Proposed	6294	7019	3142

Table 2, describes the computation efficiency of proposed model to the existing models in terms of time. From the table ,it was clear that proposed model has less time compared to ABE, CPABE and KPABE models.

Table 3: Uploading Runtime

Algorithm	instances	HashSize	UploadTime
CPABE	4	1024	6533
KPABE	4	1024	6498
FHEncrytion	4	1024	5824
Proposed	4	1024	5251

From the Table2, it is clear that Proposed ABE encryption and decryption model has less upload runtime compared to traditional models ABE on cloud environment.

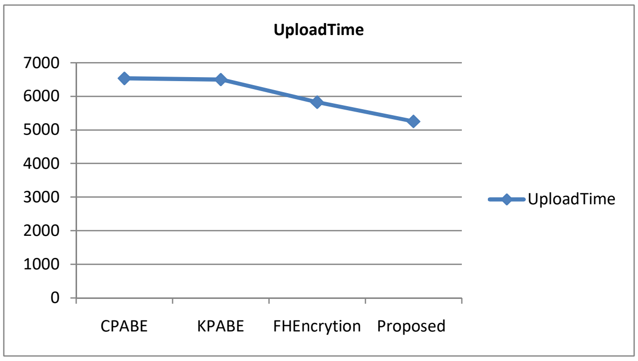

Fig 4: Uploading Runtime

From the Fig 4, it is clear that Proposed ABE encryption and decryption model has less upload runtime compared to traditional models ABE on cloud environment.

II. CONCLUSION

Cipher policy based encryption schemes consume high computation overhead for each user in the encryption and decryption process. In this proposed work , a robust attribute based algorithm is designed for secure sharing of data between users. Traditional cipher policy based models are independent of hash integration in the encryption and decryption process. Also, cpabe and kpabe models initialize static parameters for key setup and master key generation. Multiuser authentication and integration take more time to encrypt and decrypt the large amount of data to the remote cloud server. This proposed approach performs well for small as well as large datasizes. This system takes constant time for encryption and decryption process as well as key generation process. For encryption and decryption this system uses homomorphic schemes for policy verification process. In the future work, an optimized hardware based attribute encryption and decryption model will be used to overcome the traditional limitations of the CPABE and KPABE schemes.

References

[1] Junbeom Hur,"Improving Security and Efficiency in Attribute-Based Data Sharing",IEEE TRANSACTIONS ON KNOWLEDGE AND DATA ENGINEERING, VOL. 25, NO. 10, OCTOBER 2013.

[2]Zhiguo Wan, Jun’e Liu,"HASBE: A Hierarchical Attribute-Based Solution for Flexible and Scalable Access Control in Cloud Computing",IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 7, NO. 2, APRIL 2012.

[3]Mohamed Nabeel,"Privacy Preserving Delegated Access Control in Public Clouds",IEEE TRANSACTIONS ON KNOWLEDGE AND DATA ENGINEERING, VOL. 26, NO. 9, SEPTEMBER 2014.

[4] Kan Yang,"Expressive, Efficient, and Revocable Data Access Control for Multi-Authority Cloud Storage",IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 25, NO. 7, JULY 2014.

[5]Zhibin Zhou,"Efficient Privacy-Preserving Ciphertext-Policy Attribute Based-Encryption and Broadcast Encryption",IEEE,2015.

[6]Junzuo Lai,"Attribute-Based Encryption With Verifiable Outsourced Decryption",ACM,2013.

[7] Stefano Guarino,"Provable Storage Medium for Data Storage Outsourcing",IEEE TRANSACTIONS ON SERVICES COMPUTING,2014.

[8] Jinguang Han,"Improving Privacy and Security in Decentralized Ciphertext-Policy Attribute-Based Encryption",IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 10, NO. 3, MARCH 2015.

[9] Jianting Ning,"White-Box Traceable Ciphertext-Policy Attribute-Based Encryption Supporting Flexible Attributes",IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 10, NO. 6, JUNE 2015.

[10] Changji Wang,"An Efficient Key-Policy Attribute-Based Encryption Scheme with Constant Ciphertext Length",Hindawi Publishing Corporation Mathematical Problems in Engineering Volume 2013, Article ID 810969

[11] T. Jung, X. Li, Z. Wan and M. Wan, "Control cloud data access privilege and anonymity with fully anonymous attribute-based encryption", IEEE Trans. on Info. Forensics and Security, vol. 10, no. 1, pp. 190-199, 2015.

[12]J. Li, X. Huang, J. Li, X. Chen and Y. Xiang, "Securely outsourcing attribute-based encryption with checkability", IEEE Trans. on Parallel and Distributed Systems, vol. 25, no. 8, pp. 2201-2210, 2014