P. Nirupama E. et al. International Journal of Recent Research Aspects ISSN: 2349-7688, Vol. 4, Issue 2, June 2017, pp. 185-189

Public Key Based One to Many Encryption with Provable Decryption

P. Nirupama E.[1], Madhusudhana Reddy[2]

[1]Research Scholar,BU,Coimbator RK College of Engineering & Technology, Hyderabad

[2]Professor, CSE, RK College of Engineering & Technology, Hyderabad,

***Abstract*—This paper presents Attribute Based Encryption (ABE) is a new public key based one to many encryption that enables access control over encrypted data stored in the cloud, using some access polices and ascribed attributes associated with private key and cipher text. One of the main efficiency drawbacks of the existing ABE schemes is that decryption involves expensive pairing operations and the nu mber of such operations grows with the complexity of the access policy. In Existing System, ABE system with outsource decryption that largely removes the decryption overhead for the user. In these schemes user provide untrusted server, say a proxy operate by a cloud service provider, with a transformation key that allows the cloud to translate any ABE cipher text by the user attribute into a simple cipher text, there is a small computational over head for the user to recover the plaintext from transformed cipher text. In these paper user provides proxy server that allow private key to translate any ABE cipher text into plaintext based on the user attribute. Security of an ABE system with outsourced decryption ensures that an adversary (including a malicio us cloud) will not be able to learn anything about the encrypted message. To provide a security of the data as well as it is easy to encrypt and decrypt the data.**

Keywords – Attribute based encryption, outsourced decryption, certifiable.

I. INTRODUCTION:

Cloud computing is the use of computing resources (hardware and software) that are delivered as a service over a network (typically the Internet). The name comes from the common use of a cloud-shaped symbol as an abstraction for the complex infrastructure it contains in system diagrams. Cloud computing entrusts remote services with a user's data, software and computation. Cloud computing consists of hardware and software resources made available on the Internet as managed third-party services. These services typically provide access to advanced software applications and high-end networks of server .

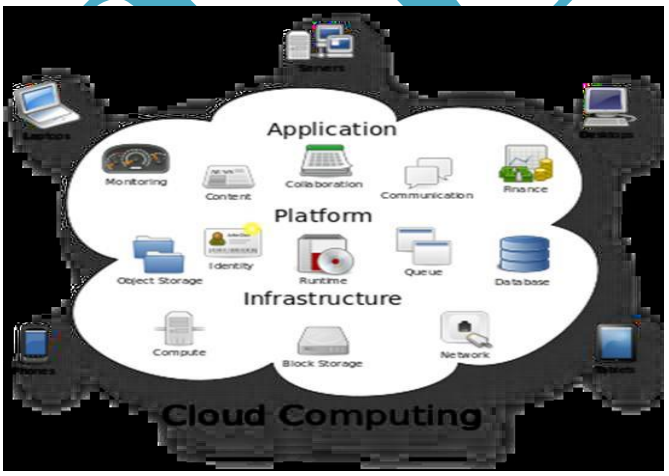


Figure 1: Structure of Cloud Computing

How Cloud Computing Works?

The goal of cloud computing is to apply traditional supercomputing, or high-performance computing power, normally used by military and research facilities, to perform tens of trillions of computations per second, in consumer-oriented applications such as financial portfolios, to deliver personalized information, to provide data storage or to power large, immersive computer games.

The cloud computing uses networks of large groups of servers typically running low-cost consumer PC technology with specialized connections to spread data-processing chores across them. This shared IT infrastructure contains large pools of systems that are linked together. Often, virtualization techniques are used to maximize the power of cloud computing.

Characteristics and Services Models:

The salient characteristics of cloud computing based on the definitions provided by the National Institute of Standards and Terminology (NIST) are outlined below:

On-demand self-service: A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service's provider.

Broad network access: Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, laptops, and PDAs).

Resource pooling: The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location-independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or data center). Examples of resources include storage, processing, memory, network bandwidth, and virtual machines.

Rapid elasticity: Capabilities can be rapidly and elastically provisioned, in some cases automatically, to quickly scale out and rapidly released to quickly scale in. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be purchased in any quantity at any time.

Measured service: Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be managed, controlled, and reported providing transparency for both the provider and consumer of the utilized service.

Figure 2 : Characteristics of cloud computing

Services Models:

Cloud Computing comprises three different service models, namely Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), and Software-as-a-Service (SaaS). The three service models or layer are completed by an end user layer that encapsulates the end user perspective on cloud services. The model is shown in figure below. If a cloud user accesses services on the infrastructure layer, for instance, she can run her own applications on the resources of a cloud infrastructure and remain responsible for the support, maintenance, and security of these applications herself. If she accesses a service on the application layer, these tasks are normally taken care of by the cloud service provider.

Figure3: Structure of service models

Benefits of cloud computing:

- **Achieve economies of scale** – increase volume output or productivity with fewer people. Your cost per unit, project or product plummets.
- **Reduce spending on technology infrastructure.** Maintain easy access to your information with minimal upfront spending. Pay as you go (weekly, quarterly or yearly), based on demand.
- **Globalize your workforce on the cheap.** People worldwide can access the cloud, provided they have an Internet connection.
- **Streamline processes.** Get more work done in less time with less people.
- **Reduce capital costs.** There's no need to spend big money on hardware, software or licensing fees.
- **Improve accessibility.** You have access anytime, anywhere, making your life so much easier!
- **Monitor projects more effectively.** Stay within budget and ahead of completion cycle times.
- **Less personnel training is needed.** It takes fewer people to do more work on a cloud, with a minimal learning curve on hardware and software issues.
- **Minimize licensing new software.** Stretch and grow without the need to buy expensive software licenses or programs.
- **Improve flexibility.** You can change direction without serious "people" or "financial" issues at stake.

Advantages:

- **Price:** Pay for only the resources used.
- **Security**: Cloud instances are isolated in the network from other instances for improved security.
- **Performance:** Instances can be added instantly for improved performance. Clients have access to the total resources of the Cloud's core hardware.
- **Scalability:** Auto-deploy cloud instances when needed.
- **Uptime:** Uses multiple servers for maximum redundancies. In case of server failure, instances can be automatically created on another server.
- **Control:** Able to login from any location. Server snapshot and a software library lets you deploy custom instances.
- **Traffic:** Deals with spike in traffic with quick deployment of additional instances to handle the load.

B **Related Work:**

Previously this paper implemented ABE with verifiable decryption is mainly focus on CP-ABE system. It is a new public key based one too many encryption that is single sender can encrypt the multiple data for the same key(master key) each and every file contains a new key that is used to decrypt the data.

The encrypted data is stored in the cloud using some access polices and ascribed attributes user satisfied attribute then only user takes cipher text with transformation key from the cloud and it is send to the proxy server that contains a decryption algorithm it take input as the cipher text , transformation key . It produces output is plain text and send

to the user. Here the private keys are the attributes the files are created with the help of the AND OR gates.

II. EXISTING SECURITY SYSTEM

Green *et al.* proposed an ABE system with outsourced decryption that largely eliminates the decryption overhead for users. In such a system, a user provides an untrusted server, say a cloud service provider, with a transformation key that allows the cloud to translate any ABE ciphertext satisfied by that user's attributes or access policy into a simple ciphertext, and it only incurs a small computational overhead for the user to recover the plaintext from the transformed cipher text.

Consider a cloud based electronic medical record system in which patients' medical records are protected using ABE schemes with outsourced decryption and are stored in the cloud. In order to efficiently access patients' medical records on her mobile phone, a doctor generates and delegates a transformation key to a proxy in the cloud for outsourced decryption; Given a transformed ciphertext from the proxy, the doctor can read a patient's medical record by just performing a simple step of computation. If no verification of the correctness of the transformation is guaranteed, however, the system might run into the following two problems: 1) for the purpose of saving computing cost, the proxy could return a medical record transformed previously for the same doctor; 2) due to system malfunction or malicious attack, the proxy could send the medical record of another patient or a file of the correct form but carrying wrong information. The consequence of treating the patient based on incorrect information could be very serious or even catastrophic.

A Disadvantages of Existing System:

One of the main efficiency drawbacks of the most existing ABE schemes is that decryption is expensive for resource-limited devices due to pairing operations, and the number of pairing operations required to decrypt a cipher text grows with the complexity of the access policy. At the cost of security, only proven in a weak model (i.e., selective security), there exist several expressive ABE schemes where the decryption algorithm only requires a constant number of pairing computations.

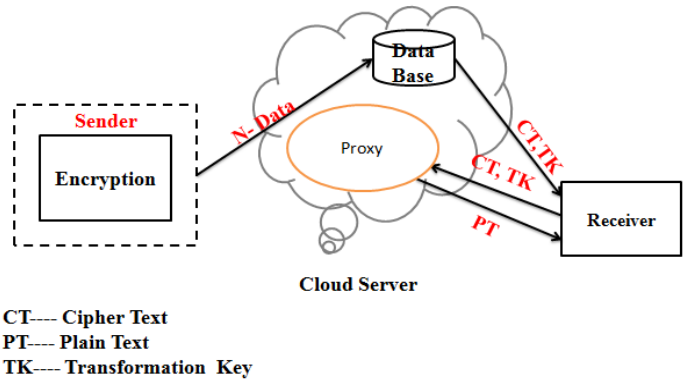
III. PROPOSING SECURITY SYSTEM

In this paper, we first modify the original model of ABE with outsourced decryption in existing system to allow for verifiability of the transformations. After describing the formal definition of verifiability, we propose a new ABE model and based on this new model construct a concrete ABE scheme with verifiable outsourced decryption. Our scheme does not rely on random oracles.

An Advantages Of Proposed System:

- ✓ Proposed scheme does not rely on random oracles
- ✓ The scheme substantially reduced the computation time required for resource-limited devices to recover plaintexts.
- ✓ In these paper user provides proxy server that allow private key to translate any ABE cipher text into plaintext based on the user attribute .To provide a security of the data as well as it is easy to encrypt and decrypt the data.

The project has implemented in a java and text data is encrypt as well as decrypt based on the user attribute with the help of the private keys.



CT---- Cipher Text
PT---- Plain Text
TK---- Transformation Key

Figure 4: Proposed System Architecture.

IV NEW MODEL OF CP-ABE SCHEME

A Setup Unit:

The setup algorithm is used to take input of two parameter that consists of size of the group and universal descriptor .The group size is used the group of a prime order p for each and every attribute we need to calculate the public key that contain different parameters to provide a more security of the data .The output of the algorithm is the public key which is used to encrypt the data from the user side.

A.1 Definition of a Bilinear Map:

Let be G an algorithm that takes as input a security parameter λ and outputs a tuple (p,G,Gt,e) where G and Gt are the multiplicative cyclic group of p and e : G1XG2 → G3 is a map such that

1) **Bilinearity:** $e(u^a,v^b) = e(u,v)^{ab}$ for all and (g , h) ϵ G and a , b ϵ zp*

2) **Nondegeneracy:** e(g,h)=^{z}2) **Nondegeneracy:** e(g,h) ≠ 1 whenever .(g , h) ≠ Ig

3) **Computable:** An efficient computability for any input pair. We refer to the tuple (p,G,Gt,e) as a bilinear group.

The setup algorithm working procedure can be explained below in the following steps

Setup(λ,U)

1. This algorithm take input as two parameters λ,U Where
   λ is size of the group
   U is universal description
2. It first run g(λ) to obtain (p,G,Gt,e)
3. Where G and Gt are the cyclic group of prime order p.
4. It choose g,u,v,d ϵ G
   a.α,α ϵ Zp* uniformly at Raandom
5. For each attribute i ϵ U it choose a random value si ϵ Zp*
6. Pk = (G,Gt,e,g,u,v,d, g^{α} ,e(g,g),Ti=$g^{s(i)}$)

Msk= α

B Key Generation unit:

The key generation algorithm is randomely picks the value of t ϵ zp* the secret key sks = (S,k,K0,K1,Kt) is computed as the k= g^{α} $g^{\alpha t}$ K0= g^{1} ,Kt= T^{i} for all ϵ S.

In these algorithm user has to calculate the private key for decrypt the data with the help of the key generation it takes input as a message that contains the data int the form of binary digit formate using ABE

encryption it convert the cipher text.

C Encryption & Storage Unit:

The mysql is used to store the data in the form table that contain the rows and columns formate that act the back end of the project .these mysql is connected to the any programming language with of the syntax as

well as the commands.

MySQL databases consist of a(ny) number of tables. Tables hold the data. Tables are made up of columns and rows. A user that has been given CREATE and DROP permissions on a database can create and remove tables of that database. The CREATE TABLE command simultaneously creates the table and defines its structure (although the structure of the table can later be changed using the ALTER TABLE command).

How it works for encryption :

1. List of users U = {u1; u2,….. un)
2. List of Attributes A = {a1; a2; , , , , ak)
3. Each user will be assigned a subset of attributes
4. D = {d1; d2,,,,, dx0 Where D ϵ A
5. Each encrypted _le will be assigned an access tree T in which:
6. Leaf Nodes are attributes in A.
7. Each none leaf node is a gate Node with assigned
8. Threshold.
9. The threshold kx ,0 < kx < numx where numx is the number of children for node x.
10. If the Node is an AND kx = numx.
11. If the Node is an OR kx = 1

How it works with Example:

a. Attributes: { Doctor ; Nurse ; A ;B ; C }.
b. Users:

1. User1: { Doctor ; A }
2. User2: { Doctor ; C }:
3. User3: { Nurse ; B }

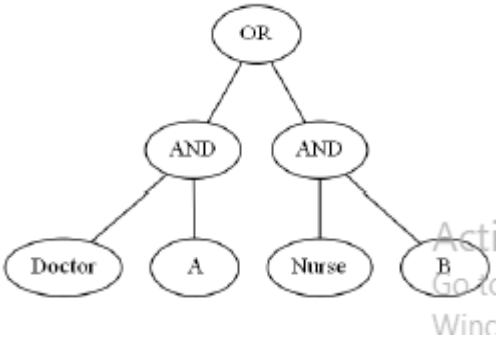


Figure 5: Searching Technique

The encryption algorithm take the input public key parameters pk and a message M is used to encrypted the data with the help of the LSSS structure A=(a,p) where A is L*N matrix and p is the row of the each attribute

it choose a random vector of the two values provided by the access structure and finally the original plain text is converted in to the cipher text it can be achieve the security of the data.

D Decryption Unit:

The decryption algorithm takes the input parameters of the public key parameters Pk , and private Sks=(S,K0,K1,Kt) for a set of attribute S and a cipher text CT=((A,P),C,C1,C1,C1… D1,C2,C2,C2..D2 i) for an access structure A=(A,P) if S does not satisfied the structure of the A it output is does not satisfied . suppose that S is satisified the access structure of the L=(1,2,3…….l) be defined as l={I; p(i) ϵ S }.

$$\frac{\prod_{i\epsilon I}(e(C1,i,K0).e(Kp(i),D1,i)^{\omega i})}{e(C'1,K)}$$

$$C1 . \quad \frac{(\prod_{i\epsilon I} e(g,g)^{\alpha t Ai.v.\omega i}}{(e(g,g)^{\alpha s}\, e(g,g)^{\alpha t s}}$$

$$= M.\ e(g,g)^{\alpha s}. \qquad = M,$$

$$\frac{\prod_{i\epsilon I}(e(C2,i,K0).e(Kp(i),D2,i)^{\omega i})}{e(C'2,K)}$$

$$C2 . \quad \frac{(\prod_{i\epsilon I} e(g,g)^{\alpha t Ai.v.\omega i}}{(e(g,g)^{\alpha s'}\, e(g,g)^{\alpha t s}}$$

$$= M.\ e(g,g)^{\alpha s'}. \qquad =$$

Obviously, the above CP-ABE scheme satisfies correctness. Observe that, in our construction, a cipher text includes three parts: (C1,C1,C1,D1) (c2,c2,c2, d2) and . The first and second parts are encryptions of message and a random message respectively, using the encryption algorithm of Waters' CP-ABE scheme . In fact, the second and third parts are redundant. However, the redundant parts are the point that we can construct a CP-ABE with verifiable outsourced decryption from the above CP-ABE scheme.

E Proxy Server Unit:

In computer networks a proxy server is a server (a computer system or an application) that acts as an intermediary for requests from clients seeking resources from other servers. A client connects to the proxy server, requesting some service, such as a file, connection, web page, or other resource available from a different server and the proxy server evaluates the request as a way to simplify and control its complexity. Proxies were invented to add structure and encapsulation to distributed systems Today, most proxies are web proxies, facilitating access to content on the World Wide Web.

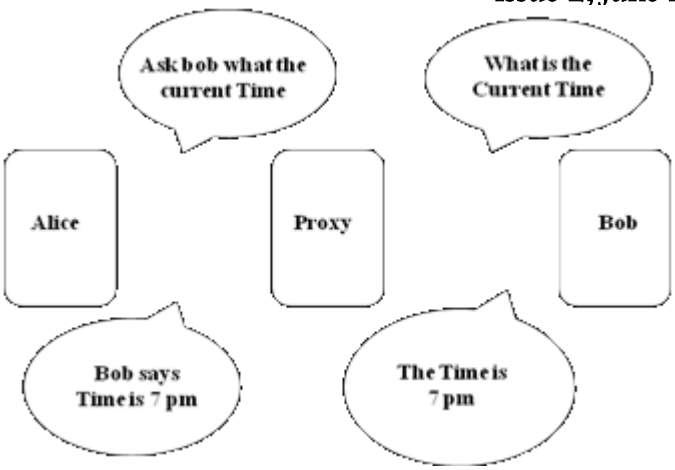


Figure 6: Model Data Retrive Technique

In the above example there are two user ane user is define as the alice and another user is defined as bod. Suppose alice send the information is encrypted with the bob public key and send to the proxy server it is an intermediate server transfer of data to the bob . bob can decrypt the data with the help of the private key of the allice Transferring of data between two computer devices.

V. CONCLUSION

In this paper, we considered a new requirement of ABE with outsourced decryption: verifiability. We modified the original model of ABE with outsourced decryption proposed by Green *et al.*to include verifiability. We also proposed a concrete ABE scheme with verifiable outsourced decryption and proved that it is secure and verifiable. Our scheme does not rely on random oracles. To assess the practicability of our scheme, we implemented it and conducted experiments in a simulated outsourcing environment. As expected, the scheme substantially reduced the computation time required for resource-limited devices to recover plaintexts

VI. WORK DONE AND DISCUSSION:

This paper presents a security of the data stored in the cloud and it is easily can decrypt the data based on the user attributes. The data is decrypted by the proxy server which is operated by the cloud.

REFERENCES:

[1]. Sahai and B. Waters, "Fuzzy identity-based encryption," inProc. EUROCRYPT, 2005, pp. 457–473.

[2]. V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryp-tion for fine-grained access control of encrypted

[3]. data," inProc. ACM Conf. Computer and Communications Security, 2006, pp. 89–98.

[4]. R.Ostrovsky,A.Sahai,and B.Waters,"Attribute-basedencryption with non-monotonic access structures," inProc. ACM

[5]. Conf. Computer and Communications Security, 2007, pp. 195–203.

[6]. B. Waters, "Ciphertext-policy attribute-based encryption: An expres-sive, efficient, and provably secure realization," inProc. Public Key Cryptography, 2011, pp. 53–70.

[7]. A. B. Lewko, T. Okamoto, A. Sahai, K. Takashima, and B. Waters, "Fully secure functional encryption: Attribute-based encryption and (hierarchical) inner product encryption," inProc. EUROCRYPT, 2010, pp. 62–91.

[8]. T. Okamoto and K. Takashima, "Fully secure functional encryption with general relations from the decisional linear assumption," inProc. CRYPTO, 2010, pp. 191–208.

[9]. A. B. Lewko and B. Waters, "Unbounded HIBE and attribute-based encryption," inProc. EUROCRYPT, 2011, pp. 547–567.

[10]. J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," inProc. IEEE Symp. Security and Privacy, 2007, pp. 321–334.

[11]. L. Cheung and C. C. Newport, "Provably secure ciphertext policy ABE," inProc. ACM Conf. Computer and Communications Security, 2007, pp. 456–465.

[12]. N. Attrapadung, J. Herranz, F. Laguillaumie, B. Libert, E. de Panafieu, and C. Ràfols, "Attribute-based encryption schemes with constant-size ciphertexts,"Theor. Comput. Sci., vol. 422, pp. 15–38, 2012.

[13]. S. Hohenberger and B. Waters, "Attribute-based encryption with fast decryption," inProc. Public Key Cryptography, 2013, pp. 162–179.

[14]. M. Green, S. Hohenberger, and B. Waters, "Outsourcing the decryption of ABE ciphertexts," inProc. USENIX Security Symp., San Francisco, CA,USA,2011.

[15]. M. Bellare and P. Rogaway, "Random oracles are practical: A para-digm for designing efficient protocols," inProc. ACM Conf. Computer and Communications Security, 1993, pp. 62–73.

[16]. R. Canetti, O. Goldreich, and S. Halevi, "The random oracle method-ology, revisited (preliminary version)," in Proc. STOC, 1998, pp. 209–218.

[17]. J. B. Nielsen, "Separating randomoracle proofs from complexity theo-retic proofs: The non committing encryption case," inProc. CRYPTO, 2002, pp. 111–126.

