International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

Hierarchical CP-ABE Scheme Implementation on Amazon EC2 cloud

D. N. Rewadkar[1], V. S. Dhumal[2]

[1] Associate Professor and Head of Computer Engineering Department, RMD Sinhgad School of Engineering, Warje, Pune. University Of Pune, Maharashtra, India

[2]Student of M.E [Computer Engineering], RMD Sinhgad School of Engineering, Warje, Pune. University Of Pune, Maharashtra, India

Abstract: ***Cloud computing plays vital role in the development of IT industry. It can help a small organization to grow their business. An organization can move from small scale industry to large scale industry. "Cloud" refers internet based data, network, resource storage. So security, integrity, confidentiality requirement need must be fulfill by cloud implementation. Attribute based encryption with ciphertext policy provides efficient encryption of data. Hierarchical implementation implies that an organization can assign different privileges to users according to their role, using a top to bottom approach. Amazon Elastic Compute Cloud (EC2) has made web computing easier for developers. It connects to virtual resources according to user requirement of network resources. This paper describes the implementation of Hierarchical CP-ABE scheme on Amazon EC2 cloud. Also paper include efficiency of encryption and decryption scheme used in implementation***

Keywords: Ciphertext Policy Attribute based encryption **(**CP-ABE), Amazon Elastic Compute Cloud (EC2), Amazon Web Services (AWS) , T2 instance

1. Introduction

Cloud computing enables organizations to move from traditional data storage within organization boundaries. Nowadays IT industry uses cloud infrastructure and provide shared access to network resources, data to users. Cloud implementation has proved rapid growth as it operates at fast speed and require very less maintenance. The cloud service model provides services to users as per their requirement. So Organization can select service according to their need to meet its requirement. Virtualization of hardware reduces dependency and investment on dedicated hardware. Cloud application programming interface (API) allows developers to access cloud services efficiently. Users can connect to cloud services using a web browser so access to services are not dependent on a particular location and device. Sharing of data and resources on cloud computing allows to increase productivity by reducing system response time. As data security is an important aspect of the organization deployment model of cloud computing can be effectively used to increase the complexity level of security.

Implementation of actual cloud starts with the survey of available cloud services to select cloud service. After selection by considering the application area of business, its requirement instances are launched. Here in next sections we are going to describe our application area and its implementation on Amazon Elastic Compute Cloud in detail. The paper is organized as follows, section 2 background describes the literature survey for the implemented scheme, section 3 describes the detail of Amazon EC2 with its features and characteristics, section 4 implementation details describe module information and deployment on actual cloud, section 5 describes the result of implementation, and section 6 we have provided conclusion and future scope.

2. Background

Sahai and Waters recommended ABE (attribute based encryption) in which a set of attributes can be used to match the user's private key and the ciphertext. To decrypt ciphertext by the user's private key set of attributes of both must be matched. But this system was not scalable for big scale organizations [2]. Vipul Goyal et al has initiated the Key policy attribute based encryption (KP-ABE). Here only ciphertext is computed using the set of attributes and private key computed using access structure. But this scheme was limited to small system only [2]. Then Brent Waters et al suggested Ciphertext-Policy Attribute based Encryption (CP-ABE). In CP-ABE access structure used for computation of cipertext and user's private keys deal with a set of the attributes. But this scheme affected by the flexibility issue [3]. Rakesh Bobba et al addressed the flexibility issue of CP-ABE and provided the solution of attribute set recursive structure which is known as (CP-ASBE) [4]. Guojun Wang et al presented a scheme to provide fine grained access control by a combination of ciphertext-policy attribute-based encryption (CP-ABE) and hierarchical identity-based encryption (HIBE) system [5]. Zhiguo Wan et al initiated Hierarchical attributes-set-based encryption (HASBE) by extending the CP-ABE and ASBE with hierarchical implementation. They have provided the scalability and flexibility with their proposed work, but suffers from time overhead of encryption and decryption, complex key structure and deficiency in searching particular document [1].

Our proposed work is influenced by the use of CP-ABE scheme proposed in reference [12] and hierarchical implementation is derived from reference [15,1]. We have provided solutions for the deficiency of reference [1] with

our contribution work which is discussed in section 4. Implementation details.

3. Related work

Amazon Elastic Compute Cloud (EC2) provides a virtual environment in Amazon Web Services (AWS) cloud where developers can deploy and develop their applications. The developer can use virtual server as per the application requirement here. The Instance is a virtual computing environment of Amazon EC2. Instance types specify the configurations of storage capacity, memory, CPU. Key pairs contain private and public key which is used for login securely for launched instance. Here public key is stored in AWS center and private key is stored by the developer. Availibity zones specify the multiple physical locations for instances. The elastic IP address is provision of static IP address for dynamic cloud [7]. Amazon EC2 on windows 2008 server is best suited for deploying application using ASP.NET and Internet Information Server (IIS). So we have selected Amazon EC2 for our web deployment [6].

3.1 Benefits of Amazon EC2

- **Scalability-** It allows to scale applications according to their needs
- **Flexibility-** It allows various configurations while selecting instances which provide flexible access.
- **Reliability-** It provides highly reliable environment with 99.95% availability.
- **Security-** Amazon VPC provides virtual private cloud in which instances are located so it provides highly secure networking.
- **Low cost-** It supports pay as per use by on demand instances, so require less cost for computing capacity [6,7].

3.2 T2 Instance

T2 instance is used for workload which does not use full CPU. So they are best suited for a workload of web server, small scale database. We can use the AWS management console to launch T2 instances. There are 3 instances size of T2 instance,

- T2.micro
- T2.small
- T2.medium

T2.micro is eligible for free tier and balances network, memory and computing resources to build developing environment and web applications of small database [6,7].

4. Implementation details

We have developed web application by considering the structure of one organization which consists of different departments. All departments are monitored by highest centralized authority known as “Admin”. Each department have a head of department called as “General Manager” who control all the employees working at a lower level. This is hierarchical implementation.

4.1 Encryption

We have used RSA and Blowfish algorithm to perform encryption of data. This works as follow

4.1.1 Encryption of Data

Consider AV={ av1, av2, av3,… } is set of attribute values assigned to the user in the system.

1. Encryption algorithm takes every attribute value as input.
   - Input: Attribute value (av1)
2. RSA performs encryption on byte arrays. So a string value of the attribute is converted into a byte.
   - Get Byte [ ](B1) of that av1
3. Using RSA algorithm public key (PU) generated and encryption is performed
   - Generate Public Key (PU) Perform Encryption on B1
   - The byte value will require more space if stored in the database. So again, it is converted into a string as Encrypted attribute (Eattr)
4. Convert B1 into astring (Eattr)

4.1.2 Decryption of Data

Consider these sets of encrypted attribute values

EAV= {eav1, eav2, eav3}

1. Decryption algorithm takes every encrypted attribute value as input
   Input: Encrypted attribute value (eav1)
2. Decryption is also performed on byte arrays. So a string value of the attribute is converted into a byte.
   Convert eav1 into byte [ ](B2)
3. Using public (PU) and private key (PR) decryption is performed
   Generate Private Key
   Perform Decryption on B2
4. The attribute value after decryption is in byte value so again it is converted into a string to view the value of decrypted attribute as Dattr
   Convert B2 into a string (Dattr)

4.1.3 Key size

As we are using CP-ABE scheme so the user’s private key is computed using attributes assigned to the user. We have used sum of the ASCII values of each character of every attribute. So the user’s private key is a number which is easy to remember. So it has overcome the limitation of the complex key size of the existing HASBE system.

4.1.4 Efficient Searching

We have applied the blowfish algorithm to attributes which are used for searching. As this algorithm can be effectively used in the searching applications. So it is best suited for our application to improve searching operation to give the desired result in a single operation as compared to the existing HASBE system.

4.1.5 Deployment on actual cloud

We have created an account in Amazon Web Services. We have selected EC2 service. We launched virtual server by launching an Amazon EC2 instance. It is a 7 step process which starts with selection of an Amazon machine image (AMI). AMI provides various software configurations, including application server, operating system. We have chosen Microsoft Windows Server 2008 R2 with SQL Server Express and IIS as AMI for our web deployment. An Amazon T2 instance of EC2 is selected which is a general purpose free tier eligible instance. The next step is configuration of selected instance, which allows developers to configure according to system requirement. After review and launch, we followed add storage, tag instance and configure security group steps. In the last step we reviewed the selected instance and lunched it. Then new key pair is generated for newly created instance by AWS. We downloaded private key for the login Administrator credential. But the key is in encrypted format. Then status of the instance is as "Now launching". We can check the status of launched instance as initializing after click on Running instance menu. We have used "Get Windows Password" option to decrypt the private key. Then default windows administrator password is retrieved successfully after decryption. And finally Public IP, username and password is displayed on the window which is used to connect remote virtual machine.

To establish a remote desktop connection we have to use the IP address provided by AWS. The "mstsc" command is used to establish connection with the remote computer. After entering IP address we have connected to virtual server by Administrator login and password. We have deployed our web services in wwwroot folder of Inetpub and imported the database in SQL server. And our application was successfully deployed on AWS EC2.

5. Experimental Results

In this section we have presented result graphs of our proposed system Hierarchical CP-ABE system with comparison of the existing HASBE system.

5.1 Time required for Encryption

We have shown the time required for encryption by an existing and proposed system in Figure 1 and 2. A result graph of proposed system indicates reduction in time overhead caused by single algorithm where the use of the two algorithms has achieved encryption in less amount of time.

5.1 Time required for Decryption

We have shown the time required for decryption by an existing and proposed system in Figure 3 and 4. A result graph of proposed system uses a user's private key which is based on the attributed assigned to it. So there is no need to decrypt all attributes so it requires less time wherein existing system whole data is shown to user so there was decryption time overhead.

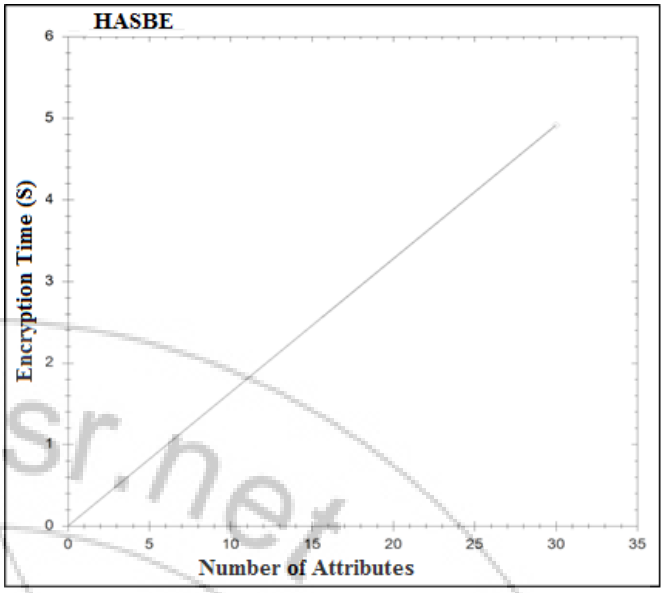

Figure 1: Time required by RSA in Existing HASBE system

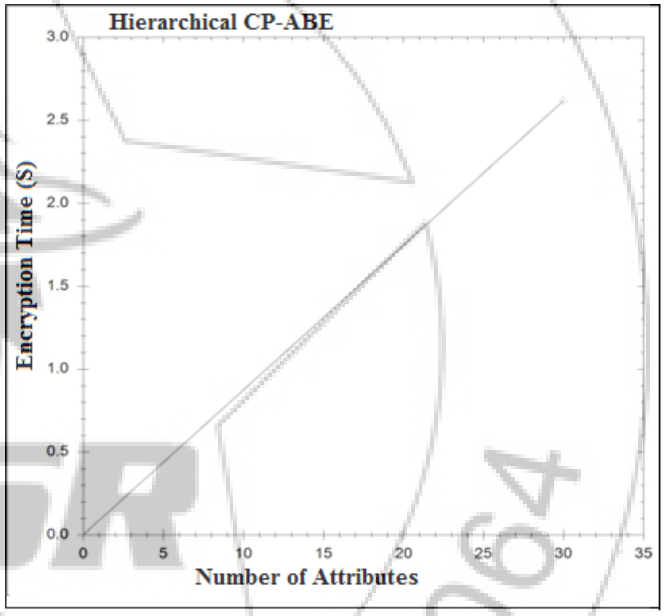

Figure 2: Time required by RSA and Blowfish in the proposed Hierarchical CP-ABE system

6. Conclusion

This paper describes the implantation of web application on actual cloud. We have used Hierarchical CP-ABE scheme and addressed the issues of time overhead for encryption and decryption, complex key structure and searching efficiency. Our proposed work has provided simple key structure and efficient searching of a particular document in single search also we have reduced the time overhead required for encryption and decryption. We have described the actual implementation on cloud in brief, which gives an overall idea of working with actual cloud. As a future scope, we can make use of multiple instances of cloud to scale up the business.

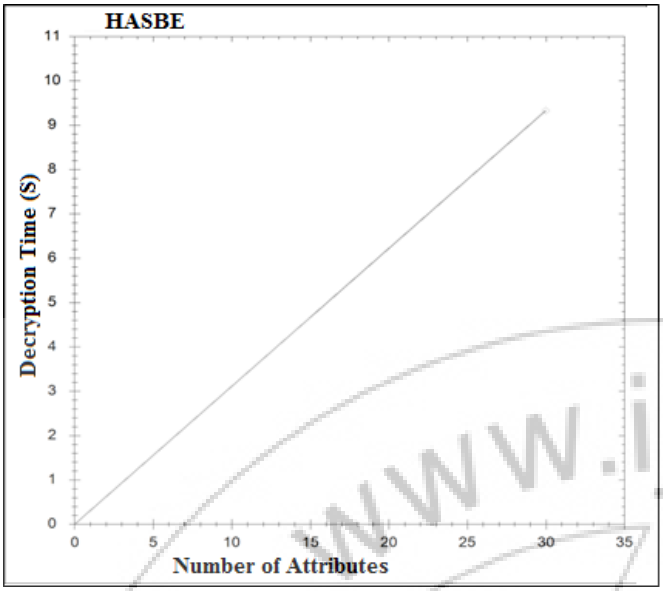

Figure 3: Time required by Existing HASBE system to decrypt all attributes

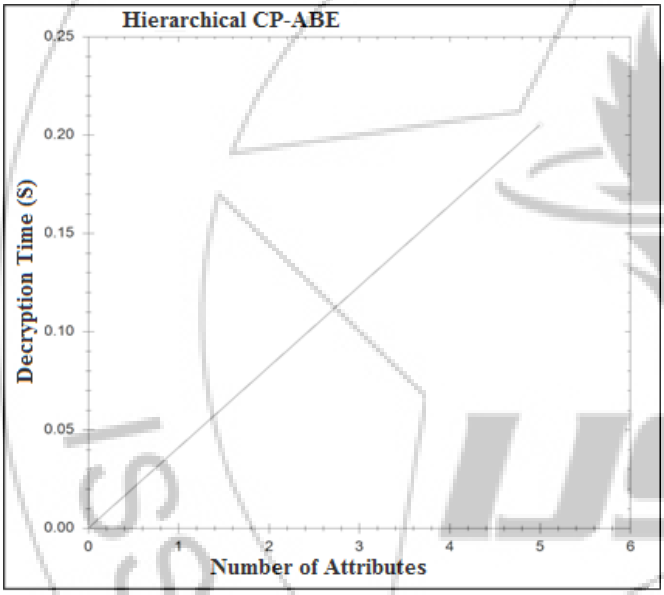

Figure 4: Time required to decrypt some attributes by the proposed Hierarchical CP-ABE system

References

[1] Zhiguo Wan, Jun'e Liu, and Robert H. Deng, "HASBE: A Hierarchical Attribute-Based Solution for Flexible and Scalable Access Control in Cloud Computing", *in IEEE Transactions on information* forensics and security, Vol. 7, No. 2, in April 2012

[2] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attibute-based encryption for fine-grained access control of encrypted data," in Proc. ACM Conf. Computer and Communications Security (ACM CCS), Alexandria, VA , 2006.

[3] J. Bethencourt, A. Sahai, and B. Waters,"Ciphertext-policy at- tribute based encryption," in Proc. IEEE Symp. Security and Privacy, Oakland, CA , 2007.M. Clerc, "The Swarm and the Queen: Towards a Deterministic and Adaptive Particle Swarm Optimization," In Proceedings of the IEEE Congress on Evolutionary Computation (CEC), pp. 1951-1957, 1999. (conference style)

[4] R. Bobba, H. Khurana, and M. Prabhakaran, "Attribute-sets: A practically motivated enhancement to attribute-based encryp- tion," in Proc. ESORICS, Saint Malo, France, 2009.

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

[6] http://aws.amazon.com/ec2/

[7] http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/concepts.html

Author Profile

Prof. D. N. Rewadkar received M.E. Computer Technology, from S.R.T.M. University, Nanded. (2000). Currently he is working as an Associate Professor and Head the Department of Computer Engineering, in RMD Sinhgad School Of Engineering, Warje, Pune. He was a Member of Board of Study (BOS) committee of S.R.T. Marathwada University, Nanded for Computer Science and Engineering. His area of interest is Traffic Engineering and Mobile Communication. He has 20 years of teaching experience.

Vishakha S. Dhumal received the BE degree in Computer Science Engineering from Computer department of K.B.P College of Engineering from Shivaji University, Kolhapur in 2009. Currently she is pursuing ME in Computer Engineering from University of Pune at RMD Sinhgad School of Engineering, Warje, Pune. Her research interests include data security in Cloud computing