DNA Based Access Control Method in Cloud Environment

L.S. Swasthimathi, Dr. S. Sivagurunathan

Abstract— Cloud Computing is a thriving technology due to its scalability, flexibility and cost-effective and pay-per-use model. Because of the advantages of the cloud technology most of the organizations are moving the data to the cloud. But many of the new problems are introduced by moving data to the cloud in addition to the existing problems. One of the major problems faced in the cloud environment is access control and security of data. Many of the access control mechanisms are followed in the cloud. In this paper, we are proposing an efficient access control method based on Deoxyribonucleic Acid (DNA) cryptography. By taking the advantages of unique features of DNA sequences, the secure and efficient access control mechanism is developed.

Keywords—Access Control, Cloud Computing, DNA, Security.

I. INTRODUCTION

Cloud computing is the renowned technology for storing and processing large volumes of data. Most of the organizations are moving their data in the cloud to make them available whenever and from wherever it is required. Cloud service providers (CSP) provide many services and facilities to the clients in different forms like infrastructure as a service (IaaS), Platform as a service (PaaS), Software as a Service, Data as a service (DaaS)[1]. The advantages of moving data to the cloud are many like scalability, accessibility, availability, increased user mobility, green technology etc[2]. Besides the advantages of cloud, it also faces many challenges like loss of control of data, vendor lock in and security of data[2]. One of the major challenges faced by cloud computing is the security of the data stored in the cloud. The major concern of security and privacy issues in the cloud exists because of the user has no control over the data which is stored in the cloud. In the CSA (Computer Security Alliance) report of top threat in 2013[3], data security is listed as one of the top threats in the cloud. It has three important dimensions namely confidentiality, integrity and availability. Access control is an important method of giving access rights only to the authorized users for achieving data confidentiality.

In the cloud environment, the key components are data owner (DO), Cloud service provider (CSP) and data user (DU). The CSP stores the data in its location or in the data owner's location based on whether public or private cloud is used. It provides services requested by the data user. The data user would be able to access the data from anywhere based on the access policy assigned to the user.

Revised Version Manuscript Received on March 10, 2019.

L.S. Swasthimathi, Research Scholar, Gandhigram Rural Institute (Deemed to be University), India. (Email: swasthimathi@gmail.com)

Dr. S. Sivagurunathan Research Supervisor and Assistant Professor, Gandhigram Rural Institute (Deemed to be University), India.(Email: svgrnth@gmail.com)

II. RELATED WORKS

A. Access Control Methods

In a cloud computing environment, the security of data is at risk due to the mischievous users and hackers. So, the access control model allows only valid and genuine users to access data from the cloud server.

Many access control schemes have been developed to solve the problems faced by the cloud. Attribute based encryption (ABE) is one of the commonly used access scheme over the conventional cryptographic techniques. It was first introduced by shamir [4] in which sender of a message can specify an identity such that only the intended receiver can decrypt the data. In ABE, the attributes are viewed as an identity to access the data. There are two types of ABE such as Key Policy based ABE (KP-ABE) and Cipher Policy based ABE (CP-ABE). In KP-ABE[5], the ciphertext is associated with the set of attributes, and private key is associated with an access structure. Decryption is possible if and only if the access tree satisfies the attributes in the ciphertext. In CP-ABE[6], ciphertext is assigned to an access policy, and private key is based on the user's attributes. If user's attributes satisfy the access policy, then only a user will be able to decrypt the ciphertext.

In Role Based Access Control Model (RBAC)[7], the access is granted based on the role of the user. The access rights are based on the role and roles are not transferrable. In Gateway Based Access Conrol (GBAC) [8], each user's data is converted into Security Assertion Markup Language (SAML) format and then it is sent to the user. The entire access control is in the hands of the gateway of the CSP which does the translation. This access method takes more time for searching the data in the server and accessing the data. In Purpose Based Access Control Model (PBAC)[9], the purpose tree is maintained for access control. The access of data will be granted if the reason of access matched with the intended purpose of the data.

B. DNA cryptography

DNA or Deoxyribonucleic Acid is a long molecule, which contains genetic information. All of our body cells contain the same DNA. It can be used to store and transmit data. Strands of DNA are long polymers of millions of linked nucleotides. These nucleotides consist of one of four nitrogen bases, a five carbon sugar and a phosphate group. The nucleotides that make up these polymers are named after the nitrogen base that

it consists of: Adenine (A), Cytosine (C), Guanine (G) and Thymine (T)[10]. We can utilize these four letters to encode information. For encoding the information, we can make use of any 24 combinations from four letters.

DNA Cryptography can be defined as a technique of hiding data in terms of DNA sequence. In the cryptographic technique, each letter of the alphabet is converted into a different combination of the four bases which make up the human deoxyribonucleic acid (DNA).

The DNA concept for securing and hiding data is used by many researchers today. Gehani et al. [11] first introduced the DNA concept in the field of cryptography. Phangal et al.[12] used DNA sequencing and substitution method to improve the traditional symmetric key encryption. Abbasy and Shanmugan [13] proposed DNA sequences to hide data for improving confidentiality in cloud. In [14] Hitaswi et.al., proposed encryption and decryption algorithm based on DNA bases. Neha et al.[15] proposed a data hiding through DNA complementary rule. Wang et al. [16] proposed a novel technique of DNA computing with RSA algorithm for secure transmission of data. They have combined DNA computing with asymmetric encryption. In [17], Zhang and Gao proposed a technique for data hiding using DNA codon. Gupta and Singh [18] proposed an encryption scheme based on DNA and Ribonucleic Acid (RNA) sequences.

III. RESULTS & PROPOSED SYSTEM

Our proposed system consists of three entities CSP, Data Owner and Data User. The CSP provides cloud services and infrastructure for storing data for both DO and DU.

In the first phase, CSP generates the public and private key pair for all data users and owners. In the user registration phase, the private key of the user is communicated over the secure channel. Once the user registration is over, the user can login into the system. Whenever the user requests the file from the CSP, it provides the public key of the owner to the user to get the DNA key. Using the public key of the owner it requests the DNA key from the data owner. After checking the authenticity of the user from the CSP, owner creates a DNA key for the user using user's attributes. In the data access phase, the user shows the certificate to the CSP and request the file from the CSP. The CSP provides the encrypted file to the user where the file is decrypted by the user using the DNA key and secret key for decryption which is provided by the owner.

A.DNA Based Key Generation

The attributes of the user are considered as a full string and each letter of the string is assigned some decimal value. This decimal sequence is generated by the data owner using their own sequence using Table 1. These decimal values are converted into binary string in the next step. This binary string is used as key for the encryption of data which is stored in the cloud. Here we are using 256 bits DNA key for simplicity. In the next step, the binary string is divided into four parts of 64 bits each. Each 64 bit part is assigned a four letter sequence using any one out of 24 combinations of letters A, T, C and G randomly using the Table 2. Then the complementary rules are applied in the sequence which is obtained from the previous step. Here, we are using the complimentary rules as A->C, T->G, G->A,C->T. The complimentary rules are used to complicate the intruder to guess the DNA sequences. The complimented sequence is rotated twice to the left to form the DNA based key.

Table 1. Decimal Encoding Table

Character	Decimal Value	Character	Decimal Value
A	1	a	37
B	2	b	38
C	3	--	--
D	4	$	98
---	---	#	97
--	--	@	96
--	---	--	---
---	---	[	104
0	27	]	102
1	28	&	101

Table 2. DNA Base Assignment Table

Sr. No	DNA Base	Sr. No	DNA Base
1	ACGT	13	GATC
2	ACTG	14	GACT
3	ATCG	15	GTAC
4	ATGC	16	GTCA
5	AGTC	17	GCTA
6	AGCT	18	GCAT
7	CAGT	19	TCGA
8	CATG	20	TCAG
9	CGAT	21	TACG
10	CGTA	22	TAGC
11	CTGA	23	TGAC
12	CTAG	24	TGCA

IV. IMPLEMENTATION

To experiment the proposed scheme, a cloud simulation platform has been set up using cloud sim 3.0. CloudSim[19] toolkit was developed by a group of researchers at the University of Melbourne. CloudSim toolkit has four layers, namely cloud services, cloud resources, user interface structures and virtual machine services. There are several entities in the CloudSim toolkit, namely Cloud Information Service (CIS), host, data center, Virtual Machine (VM), cloudlet, broker and VM Manager (VMM). CloudSim toolkit is installed on laptop with 3.40 GHz Intel corei3 processor, 4 GB RAM and 500 TB storage capacity with Windows 10 Operating System. Java version 8 with Netbeans 8.1 as IDE is used for execution purpose.

V.PERFORMANCE OF THE PROPOSED SYSTEM

Our proposed scheme is secure against the collision attack, man-in-the-middle attack and password guessing attack.

It does not reveal any sensitive information about the user

to the CSP. The DNA sequence is generated using the user's personal information like aadhar card no, email id and date of birth etc. The attributes of two users cannot be same. Even any malicious user, who wants to access data illegitimately from the cloud, would not be getting all the attribute information of an authorized user. The decimal encoding table is provided by the owner only to the authorized user.

DNA based secret key will not be provided to the user unless and otherwise it is authenticated from the CSP. No middle man can request the key from the data owner. So, our proposed system is secure against the man-in-the-middle attack.

Our proposed system is also secure against the password guessing attack. DNA key is generated based on the user's attributes. DNA key is generated based on the data owner's decimal encoding and ATCG combinations. The final key is generated by using complimentary rules and rotation. We use the complementary rules and rotation for confusing the attacker.

The key generation time is less when compared to other access control schemes. In the cloud environment the number of users varies from time to time. From the Fig.1, it clearly shows that even if there are ups and downs in the key generation time, it is less compared to other access control methods.

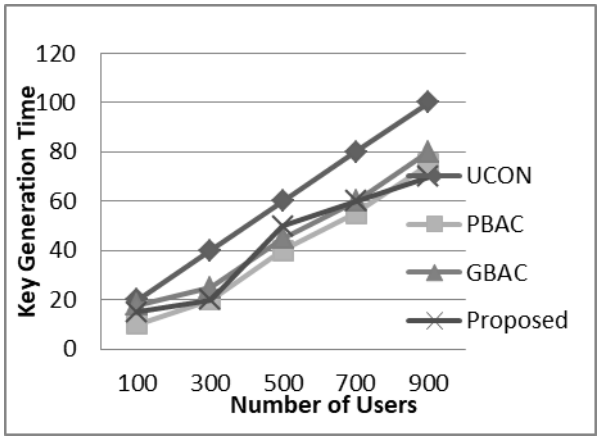

Figure 1. Number of Users Vs Key Generation Time

REFERENCES

1. V. Chang, Y.H. Huo, M. Ramachandran, "Cloud computing adoption framework: a security framework for Business clouds", Future Generation Computer Systems, 57 (2016) 24-41.
2. Velte, T., & Robert, C. (2010). "Cloud Computing: A practical Approach". McGraw Hill Professional.
3. "The notorious nine: Cloud Computing Top Threats in 2013", February, 2013, Cloud Security Alliance.
4. ShamirA, "Identity-based cryptosystem and signature schemes", in advances in cryptology, Berlin, Germany: springer-verlag, 1985, pp.47-53.
5. V. Goyal, O. Pandey, A. Sahai, B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data", Proceedings of the 13th ACM Conference on Computer and Communications Security, New York, USA, 2006, pp. 89-98.
6. J. Bethencourt, A. Sahai, B. Waters, "Ciphertext-policy attribute based encryption", Proceedings of the IEEE Symposium on Security and Privacy, Berkeley, CA, 2007, pp. 321-334.
7. D.F. Ferraiolo, D.R. Kuhn, "Role-based access controls", Proceedings of the 15th National Computer Security Conference, Baltimore, USA, 1992, pp. 554-563.
8. Y. Wu, V. Suhendra, H. Guo, "A gateway-based access control scheme for collaborative clouds", Proceedings of the 7th International Conference on Internet Monitoring and Protection, Stuttgart, Germany, 2012, pp. 54-60.
9. L. Sun, H. Wang, "A purpose based usage access control model", International Journal of Computer and Information Engineering 4 (1) (2010) 44-51.
10. https://en.wikipedia.org/wiki/DNA accessed on 12th November 2016
11. Gehani, A., LaBean, T., and Reif, J, "Dna-based cryptography". Aspects of Molecular Computing, pages 167188, Springer, 2003.
12. Phangal, S. and Kumar, M, "A dual security scheme using dna key based dna cryptography", Proceedings of the 2014 International Conference on Information and Communication Technology for Competitive Strategies, page 37. ACM, 2014.
13. Abbasy, M. R. and Shanmugam, B, "Enabling data hiding for resource sharing in cloud computing environments based on dna sequences", IEEE World Congress on Services, IEEE,2011.
14. N. Hitaswi and K. Chandrasekaran, "A Bio-Inspired Model to Provide Data Security in Cloud Storage", 2016 International conference on information technology, the next generation IT summit.
15. Neha Pallavi, Archana Singh and Surya Prakash Dwivedi, "A DNA Based Secure Data Hiding Technique for Cloud Computing", Internaltional Journal of Current Engineering and Technology, Vol. 6, No. 4 (Aug 2016).
16. X. Wang, Q. Zhang, "DNA computing-based cryptography", Proceedings of the 4th IEEE International Conference on Bio-Inspired Computing, Beijing, China, 2009, pp. 1-3.
17. S. Zhang, T. Gao, "A novel data hiding scheme based on DNA coding and module-N operation", International Journal of Multimedia and Ubiquitous Engineering 10 (4) (2015) 337-344.
18. R. Gupta, R.K. Singh, "An improved substitution method for data encryption using DNA sequence and CDMB", Proceedings of the 3rd International Symposium, SSCC 2015, Kochi, India, 2015, pp. 197-206.
19. Rodrigo N. Calheiros, Rajiv Ranjan, Anton Beloglazov, Cesar A. F. De Rose, Rajkumar Buyya,"CloudSim: a toolkit for modeling and simulation of cloudcomputing environments and evaluation of resource provisioning algorithms", Software Practice and Experience, 2011; 41:23–50.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication