Future Generation Computer Systems 73 (2017) 90–105

Contents lists available at ScienceDirect

Future Generation Computer Systems

journal homepage: www.elsevier.com/locate/fgcs

Time efficient secure DNA based access control model for cloud computing environment

Suyel Namasudra [a,*], Pinki Roy [a], Pandi Vijayakumar [b], Sivaraman Audithan [c], Balamurugan Balusamy [d]

[a] *Department of Computer Science and Engineering, National Institute of Technology Silchar, Silchar, Assam, 788010, India*
[b] *Department of Computer Science and Engineering, University College of Engineering Tindivanam, Tamilnadu, 604001, India*
[c] *Department of Electronics and Communication Engineering, P. R. Engineering College, Thanjavur, 613007, India*
[d] *School of Information Technology and Engineering, VIT University Vellore, Tamilnadu, 632014, India*

HIGHLIGHTS

- The proposed scheme uses data sizes for efficient and secure data accessing.
- To improve the data security, a long 512-bit key has been used in the proposed scheme.
- Key generation and key retrieval time at the data owner's side and user's side are respectively less.
- Experimental results and theoretical discussions prove the efficiency of the proposed scheme.

ARTICLE INFO

Article history:
Received 14 November 2016
Received in revised form
3 January 2017
Accepted 12 January 2017
Available online 16 January 2017

Keywords:
Cloud computing
DNA sequence
Big data
Primer
CloudSim

ABSTRACT

The uses of Big Data (BD) are gradually increasing in many new emerging applications, such as Facebook, eBay, Snapdeal, etc. BD is a term, which is used for describing a large volume of data. The data security is always a big concern of BD. Besides the data security, other issues of BD are data storage, high data accessing time, high data searching time, high system overhead, server demand, etc. In this paper, a new access control model has been proposed for BD to solve all these issues, where fast accessing of the large volume of data are provided based on the data size Here, a long 512-bit Deoxyribonucleic Acid (DNA) based key sequence has been used for improving the data security, and it is secured against the collision attack, man-in-the-middle attack, internal attack, etc. The proposed scheme is evaluated in terms of both theoretical and experimental results, which show the proficiency of the proposed scheme over the existing schemes.

1. Introduction

BD is one of the advanced areas of research, which carry the capability of great impact in the information science field. BD is a large volume of data, comprised of both structured and unstructured forms. BD basically implies large size data, which requires advanced technology and analytics methods for data transformation and information extraction. The outcome is smart and efficient sharing and communication of data or information for physical, social and economical benefits. For handling the BD, cloud computing is the backend technology, in which the Cloud Service Provider (CSP) provides many services and data storage facilities to the globally distributed clients [1]. It has recently achieved much interest from both IT companies and academia. Cloud services can be described as "X as a service (XaaS)", where X can be software, platform, etc. Many business-oriented models have been already developed by cloud computing technique [2].

In cloud computing, there are mainly three parties, namely CSP, Data Owners (DO) and users. The CSP manages the services. The DO stores any size of data on the cloud server, and the user sends a request for accessing data or any kind of services from the cloud server. From the user's side, a computer or laptop or any electronic device is needed with web browsing facility. This simple requirement for users brings a high demand for cloud computing. Nowadays, many companies are providing cloud services, such as Google, Apple's iCloud, Amazon's EC2, etc. [3].

[*] Corresponding author.
E-mail address: suyelnamasudra@gmail.com (S. Namasudra).

http://dx.doi.org/10.1016/j.future.2017.01.017
0167-739X/© 2017 Elsevier B.V. All rights reserved.

It is very difficult to choose between cloud based data storage and non-cloud based data storage at the time of storing large volume of data [4]. With the gradual development of cloud computing, it also arises many problems. Data security is one of the main requirements of any size of data in cloud computing because of its internet-based services [5,6]. Users face many consequences if their confidential or sensitive large volumes of data are disclosed to the unauthorized users. Besides data confidentiality, other strong requirements of cloud computing are fine-grained access control and privacy preserving. Location label based approach is a significant process for maintaining privacy of users [7]. At the time of accessing a large volume data, data contents should be secured with respect to the CSP. Traditional access control models usually assumed that the DO and CSP are in the same trusted domain [8]. Nowadays, this assumption is wrong because of the heterogeneous domains in the cloud environment. DOs store their own large volume of data in encrypted form, so that it can also be shared in some external domain [9]. The process of cloud computing is an internet-based activity, which attracts by many hackers. Thus, cloud computing again faces lots of security issues because of those hackers. Out of all these issues, access control can be considered as a major issue of cloud computing. Access control model can be defined as a procedure by which a user can access data from the cloud servers [10]. Many secure and efficient access control schemes have been developed to solve many problems, such as high access time, data confidentiality, low performance, security, etc. [11–30,55].

In Key Policy Based Attribute Based Encryption (KPABE) [31], the ciphertext is associated with a set of attributes, and user's private key is associated with an access structure. A user is able to decrypt a ciphertext if his/her access tree satisfies the attributes in the ciphertext. Since the access policy is assigned in the private keys, the DO does not have control over the encryption policies, rather s/he has to rely on the key generator. In Cipher Policy Based Attribute Based Encryption (CPABE) [32], every ciphertext is assigned to an access policy, and the private key of the user is created based on the user's attributes. A user is able to decrypt the ciphertext if user's attributes satisfy the access policy assigned in the ciphertext. In CPABE, DO is the main authority of the encryption policy, and the private key of the user cannot be modified unless and until the whole system reboots. Zhu et al. [33] proposed Towards Temporal Access Control (TTAC) model for restricting user's access rights. In TTAC, the CSP records the current time that means when users make data request. Novel Data Access Control (NDAC) scheme was proposed by Gao et al. [34] for secure data accessing and data confidentiality. Here, the DO must be always online throughout the entire data communication. Danwei et al. [35] proposed a model, namely Usage Control Based Access Control Model (UCON). In this model, there are a number of modules, and it takes a large amount of time to provide a file. Role Based Access Control Model (RBAC) was introduced by Ferraiolo and Kuhn [36], in which user's access request is granted on the basis of the job role. In RBAC, user's sensitive or confidential file may face security problems because of many hackers. For a collaborative cloud environment, Wu et al. [37] suggested Gateway Based Access Control (GBAC) scheme. Yu et al. [38] proposed Attribute Based Access Control (ABAC) scheme based on the attributes of users. In UCON, GBAC and ABAC, the CSP may require searching the entire database to grant one data, and maintenance of the database is very difficult because of the scatter manner of the data storage. Therefore, searching time of data as well as accessing time of large volume of data may be very high.

DNA based encryption techniques are the most interesting area for security because of the complex structure of DNA. Basically, there is no direct connection between DNA and information security. But, the complex structure of DNA brings a lot of interest for researchers in the field of information security. In [39], a data hiding process has been proposed by using DNA. There are three sub-phases in this scheme to encrypt a message. Khalifa and Atito [40] proposed a steganography scheme for secure data exchanging process. In this scheme, data may face security issues because if any attacker gets reference key, s/he can easily access user's sensitive data. All these schemes may have many problems in practical implementation, such as high data accessing time, high data searching time, and user's confidential data may face many security issues Besides, these schemes have high system overhead.

To solve the aforementioned problems of the existing schemes, a novel access control scheme has been proposed in this paper for secure and efficient data accessing in a cloud computing environment. The proposed scheme is based on the data size. In the proposed scheme, the CSP maintains a table that facilitates efficient and fast data accessing. In the table, large volumes of data are stored based on the size. When the CSP receives a request for a large volume of data, s/he initiates a query based on the requested size of the data from the table, and provides the data. The CSP needs not to search the entire database for one data. So, the proposed model can minimize high data searching time. Since data searching time can be decreased, data accessing time can be automatically decreased. Moreover, a 512-bit long DNA sequence is used to generate the key for data encryption. The use of the DNA sequence defines more randomness in the proposed scheme, thus improving the data security. This key is randomly generated through phases of several circles. DNA primers are also used in the proposed encryption scheme to improve the security. The major contributions of this paper are listed below:

(i) A new data access control model has been proposed in this paper for a large volume of data. The proposed scheme can minimize many problems like high data accessing time, high searching time for providing the public key of the DO and high overhead of the system.

(ii) To improve the data security, a long 512-bit key has been used, which is based on the DNA sequence.

(iii) In the proposed scheme, the DNA based secret key generation time at the DO's side and the key retrieval time at the user's side are less.

(iv) Theoretical performance analyses as well as experimental results are also presented in this paper. Both of them prove that the proposed scheme is more efficient and secured than the existing schemes.

The rest of the paper is organized as follows: Section 2 reviews the related works. Background studies have been presented in Section 3. Section 4 highlights the problem statements. The proposed scheme has been discussed in Section 5. In Section 6, security analysis of the proposed scheme has been presented. The cloud simulation environment has been presented in Section 7. Results and discussions are given in Section 8. Advantages of the proposed scheme are presented in Section 9. Finally, conclusions and future works of the paper are presented in Section 10.

2. Related works

In a cloud computing environment, access control model ensures that only valid users access data from the cloud server. Since there are many hackers or malicious users in the cloud server, the security of a data may be at risk. Therefore, the CSP should provide security to the sensitive or confidential data against the unauthorized users including malicious DOs or any potential competitors.