BEST: International Journal of Management Information Technology and Engineering (BEST: IJMITE)
ISSN (P): 2348–0513, ISSN (E): 2454–471X
Vol. 7, Issue 8, Aug 2019, 9–12
© BEST Journals

A CIPHER TEXT MULTI-SHARING CONTROL ON BIG DATA STORAGE

S. SATHIYA PRIYA[1] & P. SAKILA[2]

[1]Department of Computer Science, Prist University, Thanjavur, Tamil Nadu, India

[2]Assistant Professor, Department of Computer Science, Prist University, Thanjavur, Tamil Nadu, India

ABSTRACT

Nowadays, users those who are accessing social media or health care applications are becoming more day by day. To store large volume data used by a software application, we had implemented secure storage service. “Big-Data” will have the capacity to store huge volume data and very fast data retrieval via services. Simultaneously, we consider privacy, data which gets stored via big-data application. Moreover, the application services share fine grained encrypted information. Data-owners will allow the end-user for sharing cipher-text data among some other third party service providers. In this paper, we had proposed cipher-text multi-sharing mechanism to attain privacy preserving data sharing big-data. The advantages of proxy-re-encryption and anonymous technique are listed below. 1, a cipher-text can be securely and conditionally shared between ‘n’ number of times. 2, without leaking knowledge of underlying message & identity of cipher-text sender or receiver.

KEYWORDS: Big Data Secure Storage, Secure Storage Services, Sharing Encrypted Data & Cryptographic Re-Encryption Techniques

1. INTRODUCTION

Security data exchanged between service-provider and data-owner via third-party application are most important concern in today’s world. Cloud computing playing major role in empowering and promoting “Big-Data”, due to its efficient data processing capability. Only trusted third-party service providers able to modify or update data which is stored in cloud servers, others can only view data through remote access. There might be possibility for some common issues like privacy, security, data integrity, dynamic updates etc., while remote access of big-data storage. Each & every time it’s not possible to check consistency of data, because lots of user’s are accessing data via application over internet.

In order providing fast accessing data & ensuring security of consumer’s data. We force each individual, public & private organizations to store data in cloud either public or private cloud storage. Data which get stored in cloud by any individual user should be kept confidential. It can be accessed only by authorized users. Anonymity of service provider should be considered before storing data in storage. Application services which used for cloud storage provided with high quality encrypted data sharing process. Data owner can provide cipher text data gets stored in cloud storage of third party service providers. Under certain situations, data owner set restrictions & specific conditions to some third party service providers. These features are achieved by employing a new technique called cipher text multi sharing mechanism.

2. BIG DATA

“Big-Data” process large volume both “labelled” & “UN-labelled” data. Multiple columns/fields stored in database table, even for all rows called as “Labelled Data”. If table columns or field data are not even called as “UN- Labelled Data”.

UN-labelled data is very difficult to process using age old database models like DBMS, RDMS. In case, the amount of data too huge/ grows faster/ exceeds actual processing capacity become risky one. Overcome bad situation, “Big-Data” has the ability to provide improved operations, makes its processes faster, takes more intelligent decision for the organization, etc.

A). Big Data Importance

When Big-Data used more effectively software applications then bulk retrieval, searching, parsing & filtering data is much faster than some other applications. Companies using big-data in their own software products will not compromise performance and provide better customer satisfaction. Nowadays Big-Data widely used in call centre, social-media and financial industries in order improving customer-interaction and customer-satisfaction.

B). Big Data Evaluation

Databases differentiated into 2 different types; they listed below.

- Column Oriented Database
- Schema-Less Database.

In Row Oriented databases, either amount of data volume increases or more number of un-structured data available. Therefore, query processing efficiency becomes very slow. Later Column Oriented database came into existence which store data by focusing on column instead storing as rows like earlier. These kinds of databases are more efficient for customer relationship management, data ware housing etc. In Big-Data, there are ‘n’ numbers of database types available, such as document storage, key-value pair storage which is used for storing and retrieving huge amount of both structured and unstructured data.

C). Map Reduce

“Map-Reduce” consists 2 different tasks, listed below.

- "Map" Task
- "Reduce" Task.

“Map-Reduce” defined as programming models or data-processing technique for distributed computing. “Map-Reduce” main advantage, it can scale data-processing over ‘n’ number of nodes at same time. Input data-set converted to different key/value pair sets is called as “Map Task". Several outputs of map task are combined to form a reduced set of tuples.

3. PUBLIC-KEY-ENCRYPTION

From age olden days cryptographic and hashing technique are used to secure data which is being stored in cloud or big-data storage. Later hackers used a technique to communicate by hiding text in images, which is called as stenography. Like our traditional methods public-key-encryption techniques is used to generate public and private key for both sender and receiver. The main advantage of the current technique is that the receiver has to share the public key to the sender, before sharing any sort of file or data to the receiver. With the help of receiver’s public key the data or file which is to be shared to the receiver has been encrypted before sharing. So that only valid receiver can decrypt the data and view it. Key generation for sender and receiver will happen only once in a time. So that throughout the time period of the application the receiver and sender can able to view the shared data.

4. RESULTS AND DISCUSSIONS

A). Proxy Re-Encryption VS. Identity-Based Cryptography Approaches

In order to decrease the work load of the data owner, proxy re-encryption technique is proposed in this paper. It allows the semi-trusted third party service provider called as proxy to convert the encrypted cipher-text of particular key into an encryption of the same message with the help of another key. (i.e.) we call it as double encryption. Identity-Based Cryptography is derived from public-key cryptography in which the receiver's identity can be evaluated based on their personal details such as receiver's unique id, e-mail address, name, contact number, etc. We had conducted experiment to compare the performance of our proposed public-key cryptography and identity-based cryptography approaches.

B). Comparison With Existing Work

It has been proved that the proposed two different cryptographic methods are much better than the existing ones, when comparing with the aspects of security, very less anonymity, etc. Attackers will have very less options to crack the encrypted cipher-text and view the plain text or data.

5. CONCLUSIONS

In this paper, we had proposed two different encryption mechanisms to store and share the data in a secure manner. The first one is public-key encryption and the second one is identity-based encryption. In future the proposed encryption mechanisms can be converted from unidirectional approach to bi-direction one, in order to safeguard the information of both the sender and receiver. The results obtained show the efficiency and effectiveness of our proposed mechanisms.

REFERENCES

1. Bellare, Mihir; Rogaway, Phillip (21 September 2005), "Introduction to Modern Cryptography, by random grids, vol.1, pp.10-21.
2. J. Shao, 2012, "Anonymous ID-based proxy re-encryption," in Information Security and Privacy (Lecture Notes in Computer Science), vol. 7372. Berlin, Germany: Springer-Verlag, pp. 364–375.
3. D. Boneh and X. Boyen, 2007, "Introduction". "ID secures identity-based encryption", Berlin, Germany: Springer-Verlag, 2007, vol.3027, pp. 223–238.
4. C.K. Chu and W.G. Tzeng (August 2006), "Identity-based proxy re-encryption", (Lecture Notes in Computer Science), Berlin, Germany: Springer-Verlag, 2006, vol. 4779, pp. 189–202.