International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2019 IJSRCSEIT | Volume 5 | Issue 3 | ISSN : 2456-3307
DOI : 10.32628/CSEIT195359

Efficient and Enhanced Data Encryption In Cloud Computing

Mahalingam. R[1], S. Jeevanandham [2], Dr. N. Suguna[3]
[1]PG Scholar, [2]Assistant Professor, [3]Professor
Akshaya College of Engineering and Technology, Kinathukadavu, Coimbatore, Tamilnadu, India

ABSTRACT

Cloud computing transforms the way information technology (IT) is consumed and managed, promising improved cost efficiencies, accelerated innovation, faster time-to-market, and the ability to scale applications on demand. However, as the shape of the cloud computing is emerging and developing rapidly both conceptually and in reality, the legal/contractual, economic, service quality, interoperability, security and privacy issues still pose significant challenges. In this project, we describe various service and deployment models of cloud computing and identify major challenges. In particular, we discuss three critical challenges: security and privacy issues in cloud computing. Some solutions to mitigate these challenges are also proposed along with a brief presentation on the future trends in cloud computing deployment. The use of cloud computing has increased rapidly in many organizations. Cloud computing provides many benefits in terms of low cost and accessibility of data. Ensuring the security of cloud computing is a major factor in the cloud computing environment, as users often store sensitive information with cloud storage providers but these providers may not be trusted.
Keywords : Cloud Computing, Cloud Platform, Data Privacy, Data Security, Models of Cloud Computing.

I. INTRODUCTION

Big data is a concept which is used to describe a huge amount of both structured and unstructured data that is so large. It becomes very difficult to process such data using traditional database models like (DBMS, RDMS) and software methodologies. A most important concern is that, if the volume of data is too big or it moves too fast or it exceeds current processing capacity, then it becomes a risky one.

Big data has the ability to provide, improve operations and it makes process faster, and take more intelligent decisions for the organizations. It gets origin from Web search companies who had the problem of querying very large distributed aggregations of loosely-structured data. But, the challenge of keeping those huge amounts of structured and unstructured data leads to the change, as a result of increase in number of data sharing devices. When big data is effectively captured and analyzed efficiently, it can lead to efficiency improvements, increased sales, lower costs, better customer service, and improved products service. Companies are able to gain a more complete understanding of their business, and their customers.

Cloud computing is a technology to access the resources available in the servers through Internet. Cloud computing technology becomes popular in the recent years due to its several advantages over traditional methods, like flexibility, scalability, agility, elasticity, energy efficiency, transparency, and cost saving. Cloud resources are shared resources which can be accessed by any one, anytime and anywhere. It is accessible through any devices like mobile, desktops,

laptops, tablets etc… The resources and information are provided for the users based on demand services. It allows the users to pay only for the resources and workloads they use.

II. LITERATURE SURVEY

Cloud is nothing but a server and a number of servers interconnected through it. Cloud providers are the one who own large data centres with massive computation and storage capacities. They sell these capacities on-demand to the cloud users who can be software, service, or content providers for the users over the internet. In the recent years the major cloud providers are Google, Microsoft, and Amazon etc.

Traditional Cryptography encryption techniques such as identity based encryption, public key encryption etc, are used to provide security to the data from third party hackers. By employing traditional mechanisms it is not possible to protect some confidential sensitive information being leaked to the public and also to the cloud server. This is because traditional mechanisms do not consider the anonymity of a cipher text sender or receiver. Accordingly anyone with the knowledge of obtaining a cipher text can obtain the public key of the text, which means hacker will know the owner of the text.

Public key encryption (PKE) is the more frequently used encryption mechanism which allows a data sender to encrypt data by using the public key of the receiver such that, only the valid recipient can access gain to those data. Public key type of encryption does not support anonymity, update of cipher text receiver which is required to maintain consistency and efficiency.

There are some traditional mechanisms such as anonymous IBE which consider anonymity of cipher text sender and receiver, but it does not support the update of cipher text recipients. Traditional encryption mechanisms are applicable only for small amount of data. If the encrypted data is large, encryption and de-encryption process might be a time consuming and a costlier one.

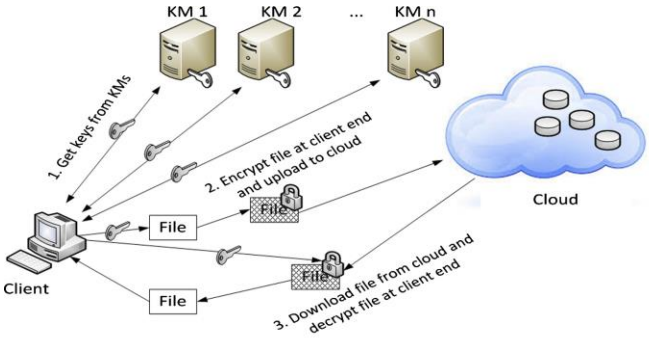
III. PROBLEM DEFINITION

The need of secure big data storage service is more desirable than ever to date. The basic requirement of the service is to guarantee the confidentiality of the data. However, the anonymity of the service clients, one of the most essential aspects of privacy, should be considered simultaneously. Moreover, the service also should provide practical and fine-grained encrypted data sharing such that a data owner is allowed to share a cipher text of data among others under some specified conditions. This paper, for the first time, proposes a privacy-preserving cipher text multi-sharing mechanism to achieve the above properties. It combines the merits of proxy re-encryption with anonymous technique in which a cipher text can be securely and conditionally shared multiple times without leaking both the knowledge of underlying message and the identity information of cipher text senders/recipients. Furthermore, this paper shows that the new primitive is secure against chosen-cipher text attacks in the standard model.

As increase in number of individual users and public and private organizations choose to upload their data in cloud force us to keep the data more securable from being hacked. The data of an individual user should be kept confidential and it should be accessed only by the authenticated users. While providing security, the most important aspect to be considered before storing the data is that, the anonymity of the service providers. The services which are used for data storage should provide a high quality encrypted data sharing. These services provides the way that, only the cipher text of the data is shared to the authorized individuals by the data owners under some restricted and specified conditions.

The features mentioned above are commonly required to maintain secure processing, and these features are achieved by employing a new technique called cipher text multi sharing mechanism. In this mechanism a proxy re-encryption technique are employed in which only the cipher text to be shared securely and conditionally over multiple times. It also ensures that, original message and information identity of cipher text senders and receivers is not leaked and it also ensures it is not vulnerable to cipher text attacks.

Architecture Diagram



Existing System:

In contrast to traditional solutions, where the IT services are under proper physical, logical and personnel controls, Cloud Computing moves the application software and databases to the large data centers, where the management of the data and services may not be fully trustworthy. This unique attribute, however, poses many new security challenges which have not been well understood.

Disadvantages of Existing System

1. No user data privacy
2. Security risks towards the correctness of the data in cloud

IV. PROPOSED SYSTEM

We focus on cloud data storage security, which has always been an important aspect of quality of service. To ensure the correctness of users' data in the cloud, we propose an effective and flexible distributed scheme with two salient features, opposing to its predecessors. By utilizing the encryption keys our scheme achieves the integration of storage correctness insurance. Unlike most prior works, the new scheme further supports secure and efficient dynamic operations on data blocks, including: data update, delete and append.

Advantages of Proposed System:

1. In this paper, we propose an effective and flexible distributed scheme with explicit dynamic data support to ensure the correctness of users' data in the cloud.
2. Cloud Computing is not just a third party data warehouse. The data stored in the cloud may be frequently updated by the users, including insertion, deletion, modification, appending, etc. To ensure storage correctness under dynamic data update is hence of paramount importance. However, this dynamic feature also makes traditional integrity insurance techniques futile and entails new solutions.

Module:

User Module

1. User Registration:

Before logging to the cloud, user has to register their details like user id, password. This registration will used to avoid anonymous users. By this user will get a user name and password for their account. Every user must be register then only they can log in the cloud.

2. Log in:

In this module user enter their user name and password what they registered. After log in to cloud user can manage their cloud data.

3. Upload File:

In this module user can upload the file to cloud, for each files uploaded, random private key is generated and these private keys will encrypt the uploaded file and gets stored in cloud. User can view the encrypted file that is stored in cloud. User can select the available Cloud Service Provider and store the data in cloud.

4. View Uploaded File

In this module user can view the original uploaded file by specifying public key given for specific uploaded file by Cloud Service Provider. Once again user has to enter Private Key given for specific uploaded file. Here double decryption is done to get the original data. If a hacker gets the access to uploaded file, only encrypted data will be shown to him, instead of original data.

Cloud Service Provider Module

1. Log in:

In this module Cloud Service Provider enter their user name and password. After log in to cloud, for each user files uploaded, random public key is generated and these public keys will encrypt the uploaded file and gets stored in cloud.

2. View Encrypted File

Cloud Service Provider can view the encrypted file that is stored in cloud. Cloud Service Provider can view the available user files that are allotted to them. He can't view other Cloud Service Provider files.

V. Conclusion and Future Work

Cloud computing is changing the way IT, departments buy IT Businesses have a range of paths to the cloud, including infrastructure, platforms and applications that are available from cloud providers as online services. Many people may be confused by the range of offerings and the terminology used to describe them and will be unsure of the risk and benefits. Security is a major requirement in cloud computing when we talk about data storage. Information needs protection, there are many Security Threats, and different types of security risks need to be discussed. In order to improving the security and protection and building the Secure Cloud, There are number of existing techniques used to implement security.

In this paper, we put forward an efficient record storage security in cloud service. The encryption of record permits storing of the record in straightforward and efficient way. Dynamic operations are a further important concept where, encoding and decoding process secures records. It also provides method for flexible access and retrieval. Cost is reduced in data storage. The time and space is also reduced through storage. Also the remote data integrity checking identifies the threats and unruly server while storing the records in cloud guaranteeing data security. Future effort is designed to offer advanced level of protection and probing mechanisms for outsourced evaluations in cloud services.

VI. REFERENCES

[1]. G. Ateniese, K. Benson, and S. Hohenberger, 2009 ,"Key-private proxy Re-encryption," in Topics in Cryptology–CT-RSA (Lecture Notesin Computer Science), vol. 5473. Berlin, Germany: Springer-Verlag, pp. 279-294.

[2]. Sun Microsystems, 2009, "Introduction to Cloud Computing Architecture", Sun Microsystems Inc., white paper, pp. 1-17

[3]. MELL, P. and GRANCE, T, 2009. "Definition of Cloud Computing", Draft NIST working, vol.5, pp. 7-19.

[4]. 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.

[5]. Bellare, Mihir; Rogaway, Phillip (21 September 2005), "Introduction to Modern Cryptography, by random grids, vol.1, pp.10-21.

Cite this article as :

Mahalingam. R, S. Jeevanandham, Dr. N. Suguna, "Efficient and Enhanced Data Encryption In Cloud Computing", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 5 Issue 3, pp. 153-157, May-June 2019.
Journal URL : http://ijsrcseit.com/CSEIT195359