ijiarec.com

ISSN: 2348-2079 FEB-2015

International Journal of Intellectual Advancements and Research in Engineering Computations

USER BASED ENCRYPTOR TO PROVIDE HIGH DATA PRIVACY IN CLOUD

Sathish kumar.A[1], Sathyapriya.G[1], Vasanthkumar.U[1], Kavitha.M[2]

ABSTRACT

Data privacy in cloud has become a more complicated task with the increasing number of cloud users. Privacy can be attained in cloud through many ways but they come with the sacrifice of accessibility or performance. Encryption may be said to one of the most significant process to maintain data privacy. The main problem with the encryption and various methods that uses encryption to provide data privacy is that they are time consuming. Several encryptions provide a high level privacy with cost of time. In current circumstances performance is as important as security. This paper focuses on this to provide a high level privacy along with the performance. In this paper a new method of carrying out this encryption process is focused. According to this paper a single encryption can not be as efficient as a proper combination of some algorithms. Clustering of data is also carried out to increase the efficiency and privacy of confidential data. Several algorithms like Modified Blowfish, AES and RSA are used in this methodology. The main objective focused is to provide a user based encryption which gives a fair range of Security and Speed.

Keywords: Data privacy, Cloud, Encryption, Security, Speed, Clustering, Blowfish, AES, RSA.

INTRODUCTION:

Cloud computing is becoming one of the most widely used technology. Mostly all the enterprises have shifted to the cloud but many of the cloud users fear to move their private data to the cloud; this is because of the data security issues. Ownership of the data moved to cloud gets lost when a user moves his data into cloud. It is not possible for all the enterprise to have their own private cloud environment they should rely only on third party cloud environment. The data in cloud can not be under the control of user and so the access over data can't be restricted from other users. The encryption mechanism is used to provide security to these data moved into cloud.

There are several methods, in which the privacy is provided through encryption some of them are,

PRIVACY MANAGER

A privacy manager for cloud computing reduces the risk in cloud computing. Private data of user can be prevented from being accessed by the unauthorized person. Cloud computing services are becoming fashionable in business model. In general data are directly uploaded by the user into the cloud, so that the user data is in unencrypted form. Even if the data are encrypted the encryption is done by a third party and a third party can't be trusted every time. This results in the lack of data privacy. The solution to this problem is provided by the privacy manager using *obfuscation.* This idea says that instead of sending data to the cloud directly, the data is sent to the cloud in the encrypted form and the processing of data is done in the encrypted form. The original data is retrieved by the *de-obfuscation.* The obfuscation method

Author for Correspondence:
[1]B.E., Final year (CSE), SNS College Of Technology, TN, India.
[2]Kavitha.M, AP/ Department of (CSE), SNS College Of Technology, TN, India, E-Mail: tameezh05@gmail.com

uses a key which is chosen by user. This method provides a high level of user based privacy. The main drawback of this mechanism is that the data in cloud can't be used by any applications.

ADVANTAGES

1. High data privacy
2. User based encryption

DRAWBACKS

1. Data can't be used in applications
2. Attribute Based Encryption (ABE)

An attribute based encryption was introduced by Sahai and Waters in 2005 and the goal was to provide security and access control. Attribute based encryption provides the fine grained sharing of encrypted data. In this method the set of attributes are selected and the cipher text and the private key is generated for the set of attributes .The receiver can decrypt the cipher text only when the private key is known to the user. Attribute-based encryption (ABE) is a public-key based one to many encryptions that allows users to encrypt and decrypt data based on user attributes. In which the private key of a user and the cipher text are dependent upon attributes (e.g. the country he lives, or the assets he has). In such a system, the decryption of a cipher text is possible only if the set of attributes of the user key matches the attributes of the cipher text. Decryption is only possible when the number of matching is at least a threshold value. There are several types in Attribute based encryption:

a. Key Policy Attribute Based Encryption(KP-ABE)
b. Cipher Text Policy Attribute Based Encryption
c. Attribute-based Encryption Scheme with Non- Monotonic Access Structures
d. Hierarchical attribute-based Encryption
e. Multi-Authority Attribute Based Encryption

ADVANTAGES

1. Fine grained sharing of encrypted data
2. Enables to have different keys for different attributes

DRAWBACK

- Each attribute is encrypted separately which is time consuming
- Separate keys are generated and so key handling is complex
- Key generation may become a complex task

PROPOSED METHOD

Each encryption algorithms has its own advantage. The idea behind our method is to utilize the advantage of using several algorithms. This project provides a user level encryption which enables a high level privacy in cloud for user's data. It is based on the idea of having a tool to encrypt user data in the user environment before sending into the cloud. Processing of data before sending to cloud involves several steps

1. Cluster Formation
2. Cluster Based Encryption
3. Key Encryption
4. Special Key Generation
5. Decryption

CLUSTER FORMATION

The user data is divided into clusters by the user. Cluster formation is just like separating the attributes in data. A cluster may be of several attributes or just a separate attribute as per user preference. The encryptor provides an UI which enables the user to form his own desired clusters of data.

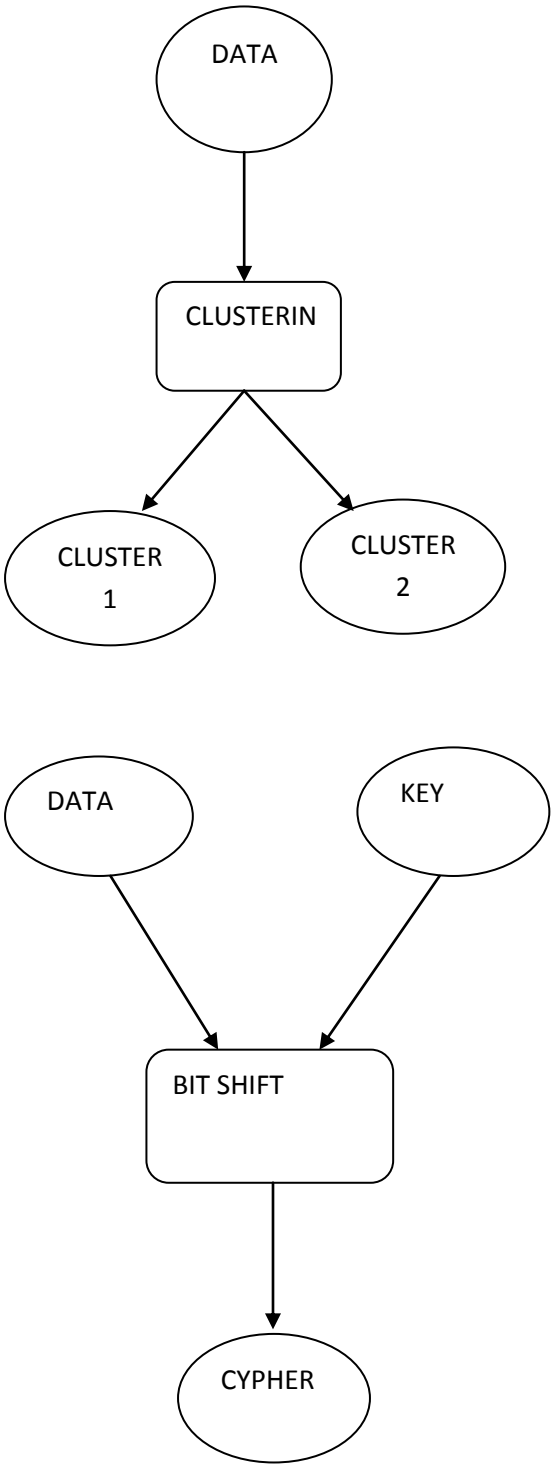
Clustering enhances fine grained access over encrypted data. Attribute based encryption has a difficulty of maintaining a huge number of keys. But in clustering mechanism the number of keys to be maintained is lowered.

CLUSTER BASED ENCRYPTION

Each clusters formed by the user are encrypted by the encryptor using a modified Blowfish algorithm. Each cluster gets its own key of variable length. A cluster can be decrypted only with its own key.

MODIFIED BLOWFISH ALGORITHM

Blowfish algorithm is the most time efficient algorithm available. The main drawback is that it lacks security. Generally blowfish uses ex-or operation to produce cipher text. In this method we use a modified blowfish algorithm that uses bit shifting instead of ex – or operation.



KEY ENCRYPTION

The cluster keys generated by using modified blowfish algorithm are again encrypted using AES algorithm. This key encryption provides a high level of security to the keys and this process is not even visible to the user. So even if the key is stolen by any third party the data can't be decrypted as the original key is not available. The encryptor (both user side and application side) can only get the original key from this encrypted key and a special key generated by the user's encryptor.

SPECIAL KEY GENERATION

Special key generation is not based on the cluster of data but based on the data set the encryptor is handling. This key is used by the application decryptor to obtain the original key from the encrypted key.

This key makes the process more protective allowing only another encryptor tool to decrypt the data.

DECRYPTION

The application using the data are given specific access over clusters by the data owners. The encrypted key is provided to the application decryptor by the data owner. The decryptor attains the special key from the encryptor without user knowledge. An encryptor can communicate only with another trusted decryptor in application side, with the special key the original key is obtained by processing the encrypted key. The data corresponding to the specific cluster can alone be decrypted with the key obtained.

CONCLUSION

Cloud Computing is still a new and evolving paradigm where computing is regarded as on-demand service. Once the organization takes the decision to move to the cloud, it loses control over the data. Thus, the amount of protection needed to secure data is directly proportional to the value of the data. Security of the Cloud relies on trusted computing and cryptography.

In our proposed work, data privacy is provided by designing efficient privacy handler. This method provides high security and efficient blowfish algorithm is designed to manage the time so that this method consumes only less time. This method provides high level of security.

REFERENCES

[1]. Siani Pearson, Yun Shen and Miranda Mowbray.A Privacy Manager for Cloud Computing**,** 2009

[2]. Vipul Goyal,Omkant Pandeyy, Amit Sahaiz, Brent Waters.Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data**,**2013

[3]. Faraz Fatemi Moghaddam, Omidreza Karimi , Dr. Ma'en T. Alrashdan.A Comparative Study of Applying Real-Time Encryption in Cloud Computing Environments, 2013

[4]. U. Somani, K. Lakhani, and M. Mundra. Implementing Digital Signature with RSA Encryption Algorithm to Enhance the Data Security of Cloud in Cloud Computing, 2010, pp. 211-216

[5]. S.Alshehri, S. P. Radziszowski, and R. K. Raj. Secure Access for Healthcare Data in the Cloud Using Ciphertext-Policy Attribute-Based Encryption, 2012, pp. 143-146

[6]. S. J. Aboud, M. A. Alfayoumi, M. Alfayoumi, and H. Jabbar. An Efficient RSA Public Key Encryption Scheme, 2008, pp. 127-130.

[7]. Jungwoo Ryoo, Syed Rizvi, William Aiken and John Kissell. Cloud Security Auditing: Challenges and Emerging Approaches, 2014

[8]. Lu´ıs S. Ribeiro, Carlos Viana-Ferreira, Jos´e Lu ıs Oliveira, and Carlos Costa. Ensuring Confidentiality While Preserving Interoperability, 2013

[9]. Wenhai Sun, Shucheng Yu, Wenjing Lou, Y. Thomas Hou , Hui Li. Verifiable Attribute-based Keyword Search with Fine-grained Owner-enforced Search Authorization in the Cloud, 2013