© 2019 IJSRSET | Volume 6 | Issue 3 | Print ISSN: 2395-1990 | Online ISSN : 2394-4099
Themed Section : Engineering and Technology

# Secure and Efficient Cloud Computing Framework Using Time and Attribute Combining Access Control Method

**Paurnima Prakash Kawale[1], Prof. Roshani Talmale[2]**

[1]MTech Scholor, Department of Computer Science and Engineering Tulsiramji Gaikwad-Patil College of Engg and Technology Nahpur, Maharashtra, India

[2]Dept. of Computer Science and Engineering Tulsiramji Gaikwad-Patil College of Engg and Technology Nahpur, Maharashtra, India

## ABSTRACT

In various organizations the demand for the cloud computing going on increasing day by day. That growing acceptance is only due the various services provided by the cloud computing. As the cloud computing provides basic services like allowing for infrastructure sharing , large storage, multi-tenancy which would ultimately leads to increase computational efficiency, flexibility, decrease complexity, and also reduces the data processing cost. But with this, security plays very important role in the success of cloud computing. Most common issues with cloud computing includes data ownership, data privacy and its proper storage for efficient manipulation and updating. Protecting the data of the data owners from an unauthorized users would requires to perform the encryption operation on the entire data and this mechanism increases cost as well as the processing time. Proposed system has some solutions to overcome such problems by using the concept of data classification according to its importance and combined access control with Time and attribute factors for time sensitive data in public cloud. Data get classified according its importance in three categories and the choice of the encryption algorithm will depends on the data importance. That will make the computing efficient. Time and Attribute factors when collectively considered for providing the access control that will provide the data confidentiality, privacy as well as security requirement for time-sensitive data that stored in public cloud. Enhanced security and analysis of system performance proved that proposed system is efficient as well as provides the security requirement for any organization and indivuals.

**Keywords :** Access Control Method, Cloud Computing Framework, Cloud Computing, Encryption

## I. INTRODUCTION

Present scenario of the development in the provision of IT service, various efficient and cost-effective techniques going on its successful deployment with implementation. One of the efficient and mostly preferred computing techniques is Cloud Computing. For understanding the need of proposed system we first go through the analysis of working mechanism that followed in the cloud computing currently. Any organization or an individual who wants to share the data on the cloud first needs to provide data to any trustable cloud service provider. But before uploading the data on cloud data owner thinks twice about proper mentainance and security for their important the private data. Since after delivering the data for outsourcing only service provider would have all access control on it, all the operations including mentainance and manipulation will only done by the service provider. So in such scenario data owner needs the guarantee about strong data privacy and security from any of the cloud service provider so that feel relax and will not worried about data privacy and security. Many of the service providers assures the security to the data owners, but the cases of the cloud data hacking noticed recently. To provide the solution over this problem proposed system is evolved having some advance concept of mechanism which will provide strong security as well as an efficient processing which will helps in reducing the computing cost.

Proposed system mainly develop a reliable framework which provides

- Strong Security, confidentiality and integrity of data while the transaction as well as storage of the data on the cloud.
- Reduces the processing time for encryption by applying the method of data classification based on its importance instead of applying the same encryption algorithm on entire data.
- Concept of combining the attributes and time for both user as well as data owners results in strong access control for time-sensitive data in public cloud.
- Support to both fine-grained access control and time sensitive data publishing.

Security based cloud-storage framework is used to encrypt the data based on degree of the confidentiality through three levels: NORMAL, SECURE, HIGHLY SECURE.

Whenever the data owner wants to outsource the data on the cloud must specify the level of security and according to selected security level data will get encrypted.

## II. FRAMEWORK DETAILS

There are three levels of security as depicted below:
Level 1: NORMAL
This level is used to specify data do not requires high level security that data can be encrypted using HTTPS and TLS to guarantees the privacy among users.
Level2: SECURE
This level is used to specify the data having medium level confidentiality like personal data or bills which needs to use an encryption algorithm like AES 128.
Level3: HIGHLY SECURE
At this level of security the critical data that needs to protect using strongest encryption algorithm such as AES-256 so that top-secret data can be encrypted and protected from unauthorized access. Also SHA-2 will use for maintaining the integrity of data.
Security-based framework working diagram

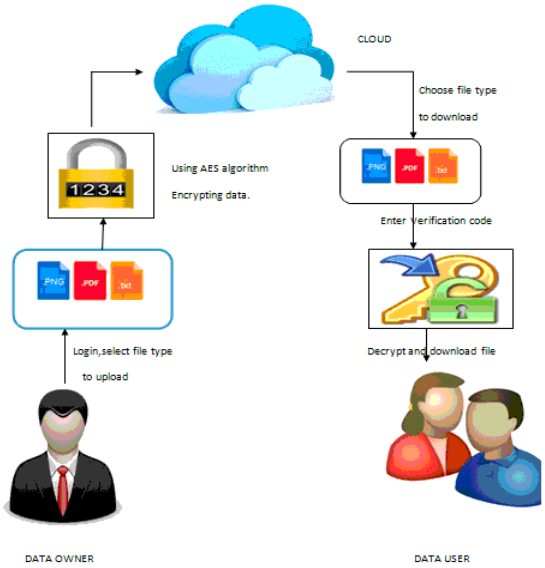

Fig1: Security-based framework working

Algorithm 1 Proposed Algorithm

```
procedure Proposed Function
    Check Files
    Set X[]= User File
    Repeat
        Length=File length
        Switch File Type
            Case File in Level 1
                Start=Time Now
                Copy(file, Location)
                End=Time Now
            End Case
            Case File in Level 2
                Start=Time Now
```

```
AES128(file, Location)
End=Time Now
End Case
Case File in Level 3
Start= Time Now
AES256(file, Location)
End= Time Now
End Case
End Switch
Deff= End-start
Write Results(File, Size, Start, End, Deff)
until File in X[]= NULL
```

System Security Model using Time and Attribute Combining access Method

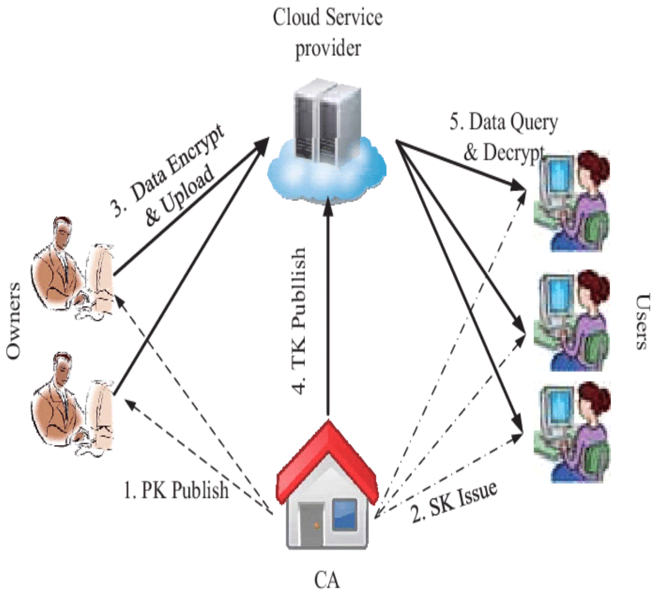

Fig 2: Flow Diagram of System by Access Combining attribute And Time

As shown in the above fig System module contains four modules which are depicted as follows

- Central Authority (CA): Responsibility of managing security protection of entire system is taken by CA. It publishes system parameters and distributes security key to each users. In addition with it acts as a time agent to maintain the timed release function.
- The Data Owner (Owner): decides the access policy based on some specific attribute set and one or more releasing points for each file, and then encrypts the file under the decided policy before uploading it.
- The Data Consumer(User):is assigned a security key from CA. user can query any cipher text stored in the cloud but can decrypt it only if both of the conditions like: attribute set satisfies the access policy and the current access time is later than the specific releasing time.
- Cloud Service Provider (Cloud): includes the administrator of cloud and cloud servers. It undertakes the storage task for other entities, and executes access privilege releasing algorithm under the control of CA.

As depicted in Fig2 the cipher texts are transmitted from owners to cloud, and users can query any cipher texts. CA controls the system with the following two operations 1) It issues security key to each user, according to user's attribute set; 2) at each time point, it publishes a time token, which is used to release access privilege of data to users.

## III. Literature Survey

Cloud storage has many benefits and can enhance team-work and collaborative efforts by allowing the members to access shared data. Though all the services user get from the cloud still it has some limitations. On the public cloud data can be manipulated, changes or deleted without taking the permission of owner.

Based on the various cryptographic primitives, there have been numerous works on data sharing in cloud storage. Among these schemes, some aimed at protecting the integrity of shared data, e.g. [1-3] and some aimed at protecting the confidentiality and access control of the data e.g.[3].

Some researchers have also tried to combine the mechanisms of TRE (Time Releasing Encryption) and CP-ABE (Cipher text-policy Attribute based Encryption), such as [4] to provide a flexible and fine-grained access control for time sensitive data.

In [4] the authors proposed a time-domain access control system, in which access control takes both users' attribute set and the access time into consideration. This work archives data access privilege automatically releasing for users without data owner's online participation. However, it introduces heavy extra overhead: The authority needs to generate update keys for all potential attributes each time to implement time-related function, and computational complexity increases with amount of involved attributes.

A smarter scheme is needed to realize fine-grained access control for time-sensitive data in cloud storage.

## IV. Objective and Benefits

- Provides Confidentiality and integrity of data in both transmission and storage: Proposed system provides the confidentiality and integrity of data through implementation of an encryption algorithm based importance of the data. Also provides the Time and Attribute combine Access control for time sensitive data.
- Reduces the processing time in encrypting data: The new concept of data classification according to its importance and applying the various encryption algorithms according degree of security and privacy instead of applying same encryption on entire data that leads to reduce the time required for encryption.

## V. Conclusion

Proposed system is efficient and provides efficient security based cloud storage framework that enhances the processing time and assures confidentiality and integrity through data classification and applying TLS, AES and SHA based on the type of classified data. Also provides better access control for time sensitive data on public cloud without affecting the privacy, and most important integrity and security. I plan to enhance my framework by considering new aspects like fast automatic data classification and implementation of various cryptographic algorithms that will provide higher degree of confidentiality and security.

## VI. REFERENCES

[1]. Flexible, Secure and Reliable Data Sharing Service Based on Collaboration in Multi-cloud Environment, Qing Wei, Huaibin Shao and Gongxuan Zhang, 30 April 2018.

[2]. Baishuang Hu, Qin Liu, Xuhui Liu, Tao Peng, Guojum Wang & Jie wu, "DABKS: Dynamic Attributes based Keyword search in cloud computing ," IEEE communication and information system security symposium. 2017.

[3]. K. Yang, Z. Liu, X. Jia, and X. Shen, "Time-domain attribute-based access control for cloud-based video content sharing: A cryptographic approach," IEEE Transaction on Multimedia, vol.18, no, pp. 940-950, 2016.

[4]. Sheren A. El-Booz, Gamal Attiya, Nawal El-Fishawy,"A Secure Cloud Storage System Combining time-based One Time Password & Automatic blocker Protocol," International Computer Engineering Conference, December 2015.

[5]. Dr. R. Sugumar, K. Arul Marie Jaycee, " Data Security in Cloud Using Enhanced Symmetric Encryption Algorithm," International Journal of Engineering Research and Technology, Vol. 6 Issue 10, Oct. 2017.

[6]. V Gokula Krishnam, J Gowtham Kumar, I Kalyyanasundar, R Sanjay,"A Secure Multi-ware Dynamic Group Data Sharing in Cloud, " IJARIIE, Vol.-4 Issue 2018

[7]. Lo'ai Tawalbeh, Raad S. Al-Qassas, Nour S. Darwazeh, Yaser Jararweh, fahd Al-Dosari"Security attack & Cryptography Solutions for Data Sharing in Public Cloud Storage," International Conference on cloud and Autonomic Computing, 2015.

[8]. S. Arul Oli, Dr. L. Arockiam,"Ensure & Secure Data Confidentiality in Cloud Computing Environment Using Data Obfuscation Technique," International Journal of Advanced Research in Electronics and Communication Engineering, Vol. 5, Issue 1, Jan. 2016.

[9]. Cong Wang, Sherman S. M. Chow, Qian Wang, Kui Ren, Wenjing Lou, "Privacy-Preserving Public Auditing for Secure Cloud Computing," IEEE Transaction on Service Computing.

[10]. Min Chen, Yongfeng Qian, Jing Chen, Kai Hwang , Shiwen Mao, Long Hu," Privacy Protection & Intrusion Detection for Cloudlet-based Medical Data Sharing." IEEE Transaction on Cloud Computing, Vol.XX, No. YY, MONTH 20XX.

[11]. F. J. M. Pasquier, Jitender Singh, Jean Bacon, Olivier Hermant, "An Information Flow Control Model for Cloud Computing."

[12]. Priyanka S. Mane, Yogesh B. Gurav, "Secure Cloud Computing Using Decentralized Information Flow Control." IARJSET Vol. 3, Issue 6, June 2016.

[13]. M. Quwaider and Y. Jararweh, "Cloudlet-based efficient data collection in wireless body area networks," Simulation Modelling Practice and Theory, vol. 50, pp. 57-71. 2015.

[14]. H. Tian, Y. Chen, C.-C. Chang H. Jiang, Y. Huang, Y. Chen, and J. Liu, "Dynamic-hash-table based public auditing for secure cloud storage," IEEE Transaction on Service Computing, Available online, 2016.

[15]. Vishal R Pancholi, Dr. Bhadresh P Patel, "Enhancement of cloud computing with secure data storage using AES," International journal for Innovative Research in science and Technology, Vol. 2, Issue 9, Feb. 2016

[16]. Ibrahim M. Al-Jabri, Mustafa I. Eid, M. Sadiq Sohail, "A Group Decision-Making Method for Selecting Cloud Computing Service Model," International Journal of Advanced Computer Science and Applications, Vol.9, No.1,2018.

[17]. Dr. Ramalingam Sugumar, K. Raja, "Study on Enhancing Data Security in Cloud Computing Environment," International Journal of Computer Science and Mobile Applications, Vol.6 Issue.3, March-2018, pg.44-49.

[18]. J. Li, W. Yao, Y. Zhang, and H. Qian, "Flexible and fine-grained attribute-based data storage in cloud computing," IEEE Transactions on Service Computing, Available online, 2016.

[19]. H. Wang, "Identity-based distributed provable data possession in multi cloud storage," IEEE Transactions on Services computing, vol. 8, no.2, pp. 328-340, 2015.

[20]. Varsha Alangar, "Cloud computing Secuirity and Encryption," International Journal of Advance Research in Computer Science and Management Studies, Vol. 1, Issue 5, Oct. 2013.

[21]. Bhairavi Kesalkar, Deepali Bagde, Manjusha Barsagade, Namita Jakulwar, Prof. Shrikant Zade, "Implementation of Data De-Duplication using Cloud Computing," IJARIIT 2018.

**Cite this article as :**

Paurnima Prakash Kawale, Prof. Roshani Talmale, "Access Control Method, Cloud Computing Framework, Cloud Computing, Encryption", International Journal of Scientific Research in Science, Engineering and Technology (IJSRSET), Online ISSN : 2394-4099, Print ISSN : 2395-1990, Volume 6 Issue 3, pp. 183-187, May-June 2019.
Journal URL : http://ijsrset.com/IJSRSET196347