JES
Journal of Engineering Sciences

Vol 10, Issue 9, Sept /2019
ISSN NO:0377-9254

A TIME INTERVAL BASED FINE GRAINED ACCESS CONTROL SCHEME IN CLOUD COMPUTING

[#1]M.VANI, M.Tech Student
[#2]Dr.Y.Rama Mohan, Associate Professor
DEPT OF CSE
G.PULLAREDDY ENGINEERING COLLEGE, KURNOOL

ABSTRACT:

Cloud computing is an emerging technology for the different organization for sharing and storing the information. Fine-grained access control schemes used in cloud computing. In this type of schemes, each data item has given its access control policy. If a user wants to access the data item needs to provide its authorizations and verified by the data owner attribute-based access control policy. Though data might be accessed by intruders when the data is an available extensive period in cloud servers, to protect the data, we proposed a time interval based fine grained access control scheme in cloud computing in cloud computing. Our proposed model develop the cloud framework in a secure manner which allows to the user to access the data only in specified time interval defined by the data owner along with the match the fine-grained access policy attributes, which can protect the data from the intruders and cloud service providers. Compared with the existing schemes, the proposed scheme provides higher-level of privacy.

I. INTRODUCTION

During the last few years, cloud computing has become a buzzword on the internet. In simple terms, it is the process of delivering services hosted on remote data centers connected through the internet. According to analysts, this market segment has a compound annual growth rate (CAGR) of around 10%, and is expected to reach USD 205.48 billion by 2018. The cloud computing services market can be segmented broadly into three categories based on service types: SaaS (Software as a Service), IaaS (Infrastructure as a Service), and PaaS (Platform as a Service). Adoption of this new IT infrastructure is widely accepted worldwide, and has become a common way of running businesses in the last ten years.

1.1 Types of Cloud:

Public cloud: It is the one of the cloud in where the cloud services are being available to users via a service provider over the Internet. It provides a control mechanism to the users.

Private Cloud: It provides many advantages over public cloud , but the main difference between public and private cloud is that the data is managed properly within the organization only, without the limits of network bandwidth.

Community Cloud: It is basically managed by a group of originations that have a common objective to achieve. The members can share and access the data in the cloud.

Hybrid Cloud: This is the combination of both public and private cloud. It is defined as multiple cloud systems, where they are connected in a way that allows programs and data to be moved easily from one system to another.

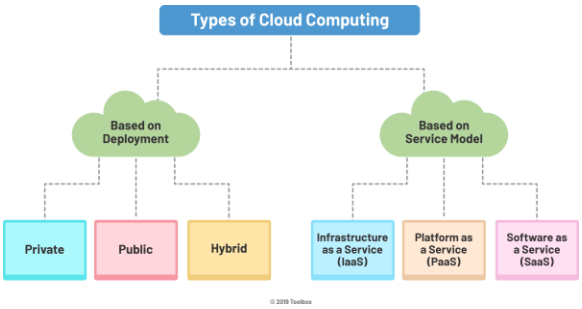


Figure 1. Types of Cloud Computing

CLOUD technology is the next big leap forward in the field of Information Technology, which is derived with Service architecture and Virtual environment. It's in common use to share data with help of cloud offering services with other users, friends etc. E.g. Such as Google Drive, Drop box etc. Shared data might consist of sensitive or personal information of the user sharing the data or vice versa (e.g. Profile information, health or property records, etc.). It's always the users responsibility to safeguard own data and avoid misuse of it. It becomes a challenge for user to protect self-data on cloud network, to overcome this scenario it is important to design and allocate time interval based data availability assigned by the user and access control to

the data until the expiry period. The shared data should be auto flash after the user-defined expiration time. Basic can be to store the data in encrypted format but disadvantage with classic encryption is the owner should know what information the users wants to share and with whom this makes the process to sharing the data to many a bit hectic.

To overcome this disadvantage we have ABE (Attribute based encryption) which enables one to many encryptions. ABE has the ability to provide data security as well as access control to the minimum level. We also have data encryption with time and attributed based access tree which provides encryption service based on Time as variable, where an encryption key is associated with a predefined lease time, and an authorized receiver can construct the corresponding decryption key in this time instance. On this basis, **Paterson et al.**[1] designed a time specific encryption (TSE) scheme, which is able to specify a suitable time interval such that the cipher text can only be decrypted in this interval (decryption time interval, DTI). ABE has issues with Time Constrains whereas TSE has problems with Access Control both these issues can be addressed with the help of KPABE (Key-policy ABE) and where we can apply time interval to each attribute in the form of decryption attributes.

Access Control Models

As cloud computing provides on-demand access to resources and services, we need to have proper security arrangement in terms of authentication and authorization. Access control model does exactly the same work to monitor, control and limit the access to cloud users on the set of resources and services [2]. Access control increases security of a system and gives predefined access to the resource. Access control is a policy or procedure that allows, denies or restricts access to a system [3]. Access Control in Cloud depends on the cloud storage and its data security and the access option becomes very necessary option in cloud. Access control is very important part in the data center of government and business.

Defining Attribute-Based Access Control

ABAC can control access based on three different attribute types: user attributes, attributes associated with the application or system to be accessed, and current environmental conditions.

An example of ABAC would be allowing only users who are type=employees and have department=HR to access the HR/Payroll system and only during business hours within the same timezone as the company.

ABAC is not only the most flexible and powerful of the four access control models, but is also the most complex. In fact, technically ABAC is capable of enforcing DAC, MAC, and RBAC.

At its core, ABAC enables fine-grained access control, which allows for more input variables into an access control decision. Any available attribute in the directory can be used by itself or in combination with another to define the right filter for controlling access to a resource.

Attribute based Access Control (ABAC)

ABAC works with identification, authentication, authorization and accountability. RBAC had a problem of assigning privileges to the user, which is solved by ABAC. It considers attributes of user request. In attribute based access control the attributes are considered based on the user's request and the type of access user wish to access and the needed resources of user. ABAC is more secure and flexible and scalable and it provides hierarchical structure.

Attribute based Encryption (ABE)

ABE model was proposed by Sahai and Waters[4] in 2005. ABE allows users to encrypt and decrypt data based on user attributes. The secret key of a user and the ciphertext are dependent upon attributes. The decryption of a ciphertext is possible only if the set of attributes of the user key matches the attributes of the ciphertext. ABE enforces access control through public key cryptography. The main goal for these models is to provide security and access control. The main aspects are to provide flexibility, scalability and fine grained access control. In classical model, and this can be achieved only when user and server are in a trusted domain [5]. Another problem with attribute based encryption (ABE) scheme is that data owner needs to use every authorized user's public key to encrypt data. So various ABE based access control schemes have been proposed to overcome this problem.

II.LITERATURE SURVEY

The literature survey contains study of different access control mechanism for cloud computing. Mainly we have focused on Attribute based access control, role based access control, Identity based

encryption, Attribute based encryption and Role based encryption.

The characteristics of an Ideal Access control and Encryption Schema:

Data confidentiality: Data is get encrypted before uploading to the cloud, so unauthorized user of the cloud cannot know the information about data stored on cloud. Only authorized users, those who are having decryption key can access the data.

Fine-grained access control: A different user from the same group gets the different access right. So users belongs to the same group can access the different data according to his access rights.

Scalability: When the number of users of the system increases it may effect on the system performance. So the performance of the system is not get affected by increased numbers of authorized users.

Flexibility: Flexibility of the cloud allows companies to adjust to any problems that may occur during day-to-day operations. It also allows using extra resources at peak times, to satisfy consumer demands.

Security: While updating login credentials for example password or for requesting extra attributes. We must ensure that only valid user is performing those operations. As well as system must provide security from different attacks like session hijacking, session fixation etc.

A. A View of Cloud Computing

In this paper [11] author had defined cloud computing as application which provide service over an internet and the datacenters hardware and software which provide those services. In this paper cloud is datacenters made of hardware and software. When cloud is available in pay-as-you go bases then it is made available to public and it is called public cloud, whereas we refer private cloud as internal datacenters of some organization or a business, this is not available to general public. Cloud computing is the sum of SaaS i.e software as a service and utility computing. Cloud computing can offer services below the cost medium-size datacenters. In cloud computing people can be users or providers like utility computing. In this paper they given there more focus in application software which needs to scale up and down more rapidly to match needs of cloud computing. Also, infrastructure software needs to be aware that it will no longer run on bare metal but can be run on VMs. And lastly hardware machine should be designed in such a way that its purchasing cost is low.

B. Cryptographic Cloud Storage

In this paper [12] author had considered a problem of building a secure cloud storage service on top of public cloud infrastructure where the service provider does not trust the customer. In order to achieve our goal they had describe several architecture that combine non-cryptographic primitives. Two encryption scheme has been described in this paper i.e searchable encryption scheme and attribute based encryption scheme. Searchable encryption scheme is a method to encrypt a search index so that its data is hidden from the adversary and is known only to the party who has token. Search index is generated with the help of collection of files. In attribute-based encryption scheme each user is having a decryption key along with the set of attributes. Decryption is performed only if the attributes associated with the decryption key will match the encrypted message.

C. Achieving Secure, Scalable, and Fine-Grained Data Access Control in Cloud Computing

In the paper [13] author had used key-policy attribute based encryption technique. This technique is combined with proxy re-encryption and lazy encryption technique. With the help of KP-ABE technique we can access fine-grained data access control and can do the efficient operation such as file creation/deletion and can also grant new user. When proxy re-encryption technique is combined with KP-ABE we can resolve the issue of user revocation. With the help of this data owner can delegate their computational task to cloud servers. Cloud server keep a partial copy of each user having a secret key. When there is a need of user revocation the data owner re-defines a certain set of attributes along with proxy re-encryption keys and sends them to cloud servers. When these proxy re –encryption keys is received to cloud server it update user secret key components and again reencrypt the data files without knowing the plaintext of data files. This improvement releases the data owner from the huge computational overhead on user revocation. To degrade the computational overhead from cloud server on user revocation, we use technique of lazy re-encryption. Using lazy re-encryption, cloud server will aggregate multiple successive secret key and then update file reencryption operations into one, and thus statistically save the computational overhead. Thus, confidentiality of user access privilege and user secret key accountability can be achieved.

JES
Journal of Engineering Sciences
Vol 10, Issue 9, Sept /2019
ISSN NO:0377-9254

III. PROJECT SCOPE AND OBJECTIVES

3.1 Contributions

In this project, we propose a novel secure time interval based data flashing scheme for data sharing in cloud computing. We first introduce the notion of fine grained access control policy to, formalize the model and provide the security model of it. Data protection towards privacy and security is the prime concerns from the intruders. When data is availability for longer period of time , it may create problem to make data leakage or hack , in order to protect the data from the intruders, time interval based self-flashing scheme is proposed. This scheme makes data availability only in specified time period, once time has been expired automatically data has been flashed from the cloud data storage. Finally, we prove that our proposed scheme is secure. Especially, our proposed model has the following advantages with regard to security and fine-grained access control compared to other secure self-destructing schemes.

3.2 Our Proposed Scheme

A key-policy attribute-based encryption with time interval attributes (KP-TIABE), a novel secure data model in cloud computing is proposed here. Every ciphertext is labeled with a time interval while private key is associated with a time instant in the KP-TIABE scheme. if both the time instant is in the allowed time interval and the attributes associated with the ciphertext satisfy the key's access structure the ciphertext can only be decrypted. Secure Data Sharing in Clouds (SeDaSC) methodology that provides is proposed here:

1) Data Confidentiality and Integrity

2) Access Control

3) Data Sharing

4) Insider Threat Security

5) forward and backward access control

6) Share Time Expire

7) Secret Key Management.

Research Objective:

Design a Secure A key-policy attribute-based encryption with time interval attributes (KP-TIABE) for privacy preserving and access controlling in cloud framework .

IV.BLOCK DIAGRAM

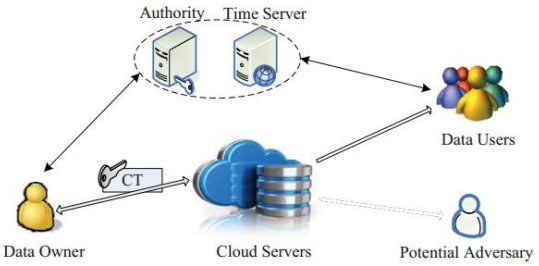


Figure 2: Proposed Architecture

Figure 4.1 Represents the proposed model architecture , which comprise with five modules such as Data Owner,Authority,Time Server, Data Users ,Cloud servers and Potential adversary.

DATAFLOW

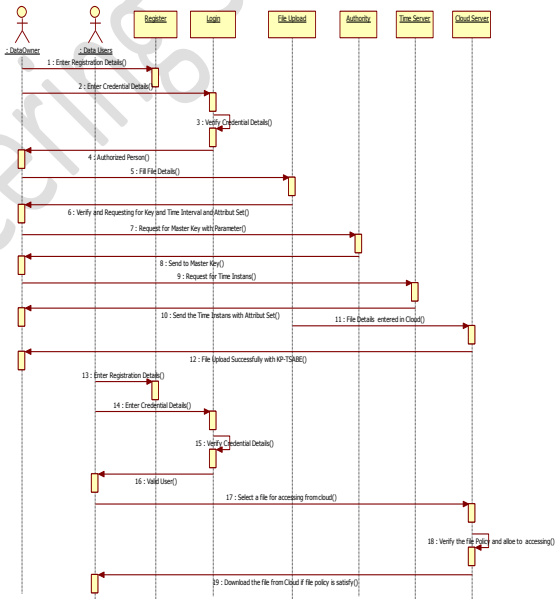


Figure 3: Dataflow Diagram

4.1 Module:

Data owner

Data owner can provide data or files that contain some sensitive information, which are used for sharing with his/her friends (data users). All these shared data are outsourced to the cloud servers to store.

Authority

It is an indispensable entity which is responsible for generating, distributing and managing all the private

keys, and is trusted by all the other entities involved in the system.

Time server

It is a time reference server without any interaction with other entities involved in the system. It is responsible for a precise release time specification.

Data users

Data users are some people who passed the identity authentication and access to the data outsourced by the data owner. Notice that the shared data can only be accessed by the authorized users during its authorization period.

Cloud servers

It contains almost unlimited storage space which is able to store and manage all the data or files in the system. Other entities with limited storage space can store their data to the cloud servers.

Potential adversary

It contains the security and validation of the data in the cloud server.

4.2 Advantages of KP-TIABE System:

- Attribute based encryption (ABE) has significant advantages based on the tradition public key encryption instead of one-to-one encryption because it achieves flexible advantages
- With regard to security and fine-grained access control compared to other secure self-destructing schemes.
- Supporting user-defined time-specific authorization, fine-grained access control and data secure self-destruction. The algorithm level of the KP-TIABE scheme includes four algorithms: Setup, Encrypt, Keygen, and Decrypt. The details of the algorithm specified in Table.3.1

Algorithm	Specification
Setup	This algorithm is run by the Authority and takes as input the security parameter
Encrypt	This algorithm generates the ciphertext which is associated with the fuzzy attribute.
KeyGen	This algorithm takes as input the master key, associated with a time instant and outputs a private key.
Decrypt	This algorithm takes as input the ciphertext and the private key When a set of time specific attributes satisfies, it is able to decrypt the ciphertext and return the plaintext.

4.3 System Descriptions of the KP-TIABE

System setup

In the system initialization phase, a data owner chooses a large security parameter k and attribute universe U, and invokes the algorithm Setup(1k , U) belonging to the algorithm level to generate system parameters params and master key MSK.

Encryption with time constraint

The data owner chooses an attribute set S for the shared message M and defines a time interval set TS for S. Then, the data owner invokes the algorithm Encrypt(M, params, S, TS) to encrypt M to its ciphertext CT, which is associated with the set S and TS. Finally, CT is sent to cloud servers.

Fine-grained access control during the authorization period

When a user wants to access the shared data M during its authorization period, he must pass the identity authentication and should perform the following processes: Firstly, the current time instant tx is provided by the time server with tx € Tt , which is associated with each attribute x. If Tt ε TS and the attribute set of the user matches the access tree ε. Then, the Authority runs the algorithm KeyGen MSK Tt to generate the private key SK and sends it to the user. Once the user received the SK, he will get the CT from the cloud servers and invokes the algorithm Decrypt CT to obtain the shared data M. Because each attribute x is associated with a current time instant tx, if and only if tx ε TS and attribute set matches ε, the user can obtain the correct private key SK to decrypt CT. Therefore, the KP-TIABE scheme allows for extremely flexible implementation of fine-grained access control through combining different attributes with corresponding time intervals.

Data Self-Destruction After Expiration

Once the current time instant t_x lags behind after the threshold value (expiration time) of the valid time interval R the user cannot obtain the true private key SK. Therefore, the cypher text CT is not able to be decrypted in polynomial time, facilitating the self-destruction of the shared data after expiration. Although the computational cost seems to be expensive, optimizations are made to alleviate the computational cost. After the optimization, the final computational cost is located in a reasonable range. The proposed KPTSABE scheme provides a big advantage by supporting user-defined time-specific authorization, fine-grained access control and data secure self-destruction, which are not well satisfied by the existing schemes

V. ALGORITHM

HASH

A hashing algorithm is a mathematical function that condenses data to a fixed size. So, for example, if we took the sentence…

"The Quick Brown Fox Jumps Over The Lazy Dog" …and ran it through a specific hashing algorithm known as CRC32 we would get: **"07606bb6"** This result is known as a hash or a hash value. Sometimes hashing is referred to as one-way encryption. Hashes are convenient for situations where computers may want to identify, compare, or otherwise run calculations against files and strings of data. It is easier for the computer to first compute a hash and then compare the values than it would be to compare the original files.

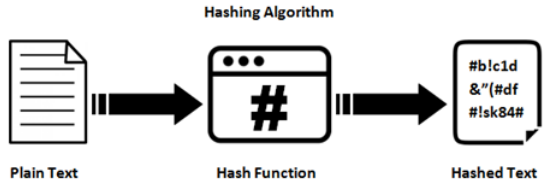
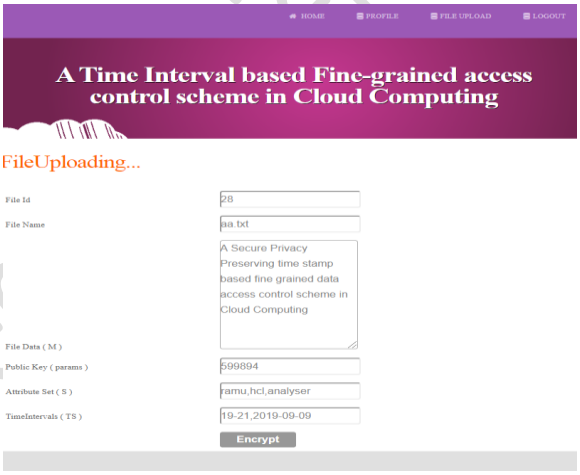


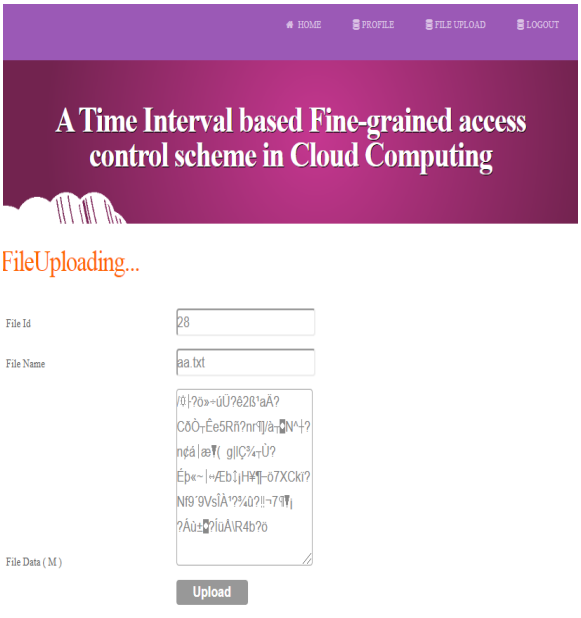
Figure : 4 Hashing Algorithm Flow.

1. Hash-based message authentication codes (HMAC)

- Hash-based message authentication codes (or HMACs) are a tool for calculating message authentication codes using a cryptographic hash function coupled with a secret key. You can use an HMAC to verify both the integrity and authenticity of a message.
- Data integrity checks are vital to secure communications. They enable communicating parties to verify the integrity and authenticity of the messages they receive. In secure file transfer protocols like FTPS, SFTP, and HTTPS, data integrity/message authentication is usually achieved through a mechanism known as HMAC.

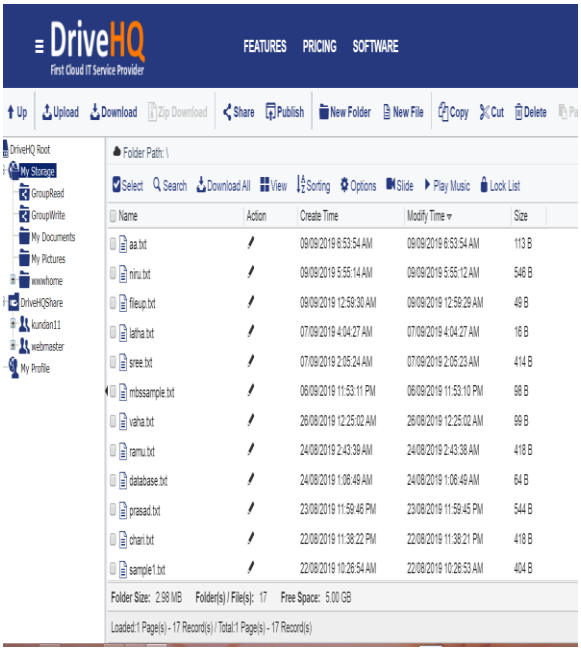
VI.RESULT

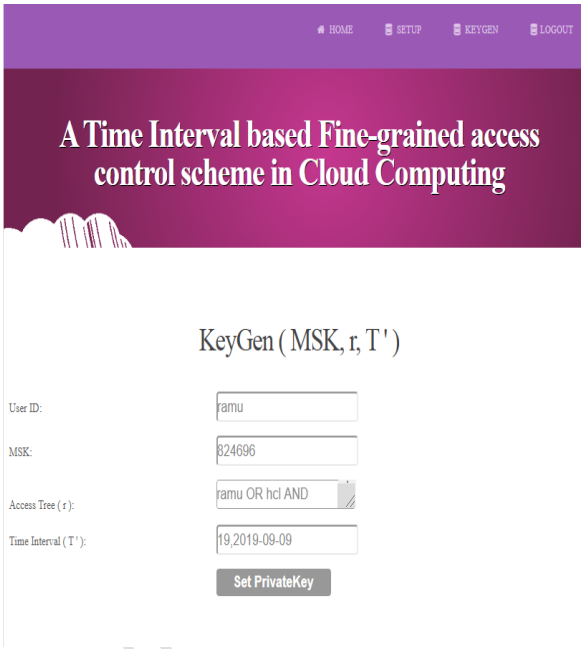


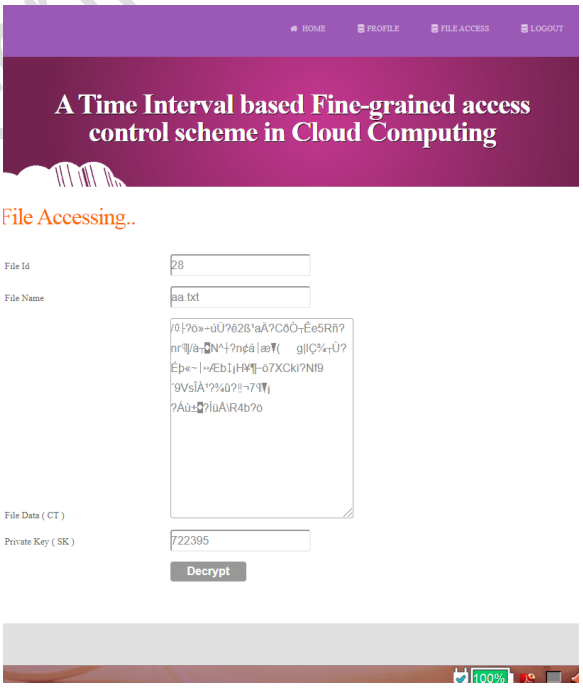


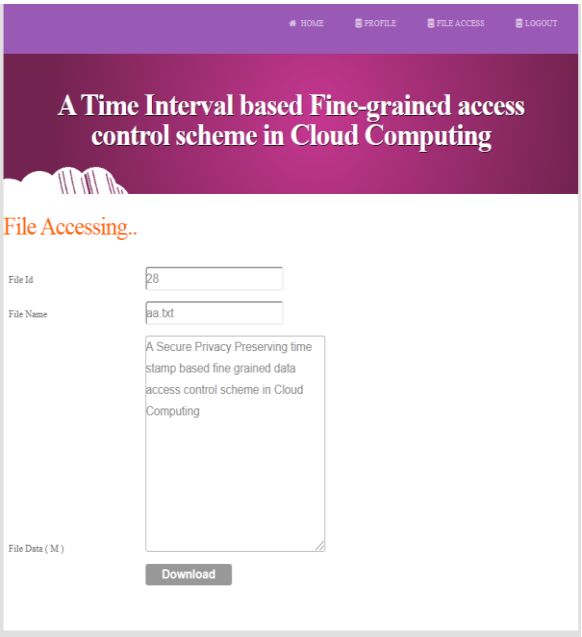
Journal of Engineering Sciences

Vol 10, Issue 9, Sept /2019
ISSN NO:0377-9254









VII.CONCLUSION

In this project, we conclude that our proposed model entitled A time interval based fine grained access control scheme in cloud computing. This model secures the owners' data from the unauthorized users, and it allows the users only in a specified time interval to access the data with the satisfaction of a fine-grained access policy scheme. When a user attempts to access the stored data at a definite time Even though fine-grained access policy matched with the user attributes, data will be self-destructed and not available.

References

[1] K. Yang, Q. Han, H. Li, K. Zheng, Z. Su and X. Shen, "An Efficient and Fine-Grained Big Data Access Control Scheme With Privacy-Preserving Policy," in IEEE Internet of Things Journal, vol. 4, no. 2, pp. 563-571, April 2017.doi: 10.1109/JIOT.2016.2571718

[2] Rajanikanth aluvalu, lakshmi Muddana "A Survey on Access Control Models in Cloud Computing" Springer International Publishing, Advances in Intelligent Systems and Computing 337, DOI: 10.1007/978-3-319- 13728-5_7.

[3] Punithasurya K, Jeba Priya S "Analysis of Different Access Control Mechanism in Cloud", International journal of Applied Information Systems, Vol. 4, September 2012.

[4] A. Sahai and B. Waters, "Fuzzy identity-based encryption," inProc.EUROCRYPT, 2005, pp. 457473

[5] N.krishna, L.Bhavani "HASBE: A Hierarchical Attribute Set Based Encryption For Flexible, Scalable And Fine Grained Access Control In Cloud Computing" International Journal of Computer & Organization Trends –Volume 3 Issue 9 – Oct 2013

[6] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in Proc. IEEE Symp. Security and Privacy,Oak-land, CA, 2007.

[7] Keith Frikken,Mikhail Atallah, Fellowand Jiangtao "Attribute based access control" in IEEE TRANSACTIONS ON COMPUTERS, VOL. 55, NO. 10, OCTOBER 2006.

[8] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in Proceedings of the 13th ACM conference on Computer and communications security, pp. 89-98, 2006.

[9] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in Proceedings of IEEE Symposium on Security and Privacy, pp. 321-334, 2007.

[10] G. Wang, Q. Liu, and J.Wu, "Hierarchical attribute-based encryption for fine-grained access control in cloud storage services," in Proceedings of the 17th ACM conference on Computer and communications security, pp. 735-737, 2010.

[11] Xuefeng Liu, Yuqing Zhang, Boyang Wang, and Jingbo Yan. "Mona:Secure Multi-Owner Data Sharing for Dynamic Groups in the cloud" IEEE transaction on parallel and distributed systems, vol. 24, no.6, june 2013.