ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 4, April 2017

A Data Security Self-Attribute System in Cloud Computing

Dhanesh Lokhande, Prof. Kumaresan P

Final Year M.Tech Student, Dept. of Computer and Communication Engineering], SITE, VIT University, Vellore, India

Assistant Professor, SITE, VIT University, Vellore, India

ABSTRACT: With the fast improvement of flexible cloud services it becomes progressively powerless to utilize cloud services to share information in a friend circle in the cloud computing condition. Since it is not practical to implement full lifecycle protection security, access control turns into a testing task, particularly when we share sensitive information on the cloud serverss. In the KP-TSABE plot, each ciphertext is set apart with a period interval while private key is connected with a period minute. The ciphertext must be decoded if both the time minute is in the permitted time interval and the properties related with the ciphertext satisfy the key's get the chance to structure. The sensitive information should be securely self-destructed after a client determined close period.

KEYWORDS: privacy-preserving, cloud computing. Sensitive information, secure self-destructing, fine-grained access control system,

I. INTRODUCTION

Concerning accessibility of records there are a progression of cryptographic frameworks which go the extent that allowing an without examiner to guarantee the openness of documents for the information holder without dribbling anything about the information proprietor's lack of clarity “ABE(Attributebased encryption)” method gives an effective technique to achieve both information security and fine-grained get to control. In the “key-strategy ABE (KP-ABE)” plan to be explained in this paper, the ciphertext is named with set of distinct traits. Just when the arrangement of clear characteristics fulfills the get to structure in the key, the client can get the plaintext all in all, the proprietor has the privilege to indicate that specific delicate data is legitimate for a restricted timeframe, or ought not be discharged before a specific time. “Timed-release encryption (TRE)” gives a fascinating encryption benefit where an encryption key is related with a predefined discharge time, and a beneficiary can just build the comparing decoding key in this time occurrence. On this premise, Paterson et al. proposed a period particular.. A computing Cloud is an arrangement of network empowered services, giving versatile, QoS ensured, typically personalized, inexpensive computing infrastructures on request, which could be gotten to in a simple and pervasive way. Each individual is producing colossal amount of information than any time in recent memory, and this rate is just going to build step by step. Likewise more importantly the organizations have significantly higher rate of producing information which is in certainty more sensitive as well. Henceforth, organizations are regularly more worried about the security of their information to store it on cloud storage, the majority of this prompts to the expanded authentication request. As a way to deal with holding control of information on cloud is to make utilization of the encryption of all cloud information. The issue is that encryption limits information. The encoded information gets to be distinctly dangerous in looking and ordering. Information put away in clear-text can be efficiently searched by specifying a keyword. This is not possible to do with conventional encryption plans. Upgraded and more sophisticated cryptography may offer new devices to make the information searchable scrambled. Encryption plans like searchable encryption otherwise called predicate encryption that permit operation and calculation on the ciphertext, permits the information proprietor to figure an ability from his mystery key. A capacity encodes an search query, and the cloud can utilize this ability to choose which archives coordinate the search query, without the necessity of any extra data. Other cryptographic systems, for example, Homomorphic encryption and Private Information Recovery.

II. LITERATURE SURVEY

In this paper, they propose a model which permits clients to validate to the administration safely and control the exposure of their traits. The proposed display offers clients' an adaptability to produce moment personality alongside accreditation required to validate specialist organization. The moment personality for each specialist co-op makes extreme for them to track client's get to atterns. Because of quick change in personality, specialist organization will most likely be unable to find user(s). The proposed show plans to helps the clients to safeguard protection of their information. [1]

This paper demonstrates the, and methodically look at existing examination on cloud relocation. Technique—they drove an exact written work review (SLR) of 23 picked ponders, dispersed from 2010 to 2013. They requested and broke down the picked amasses in light of a depiction structure that we in like manner present in this paper. Comes to fruition—The investigation mix achieves a learning base of current responses for legacy-to-cloud movement. This review also perceives investigate gaps and course for impending research. It recognizes the prerequisites for a development framework to help improving the advancement level and in this manner trust into cloud migration. This review exhibits a nonattendance of equipment support to automate development errands. This survey furthermore recognizes prerequisites for building alteration and self-flexible cloud-engaged structures. [2]

In this paper, they proposed a various leveled characteristic based get to control conspire by broadening ciphertext-arrangement property based encryption with a progressive structure of multiauthorities and abusing quality based mark (ABS). The proposed plot not just an accomplishes adaptability because of progressive structure, additionally acquires fine-grained get to control with validation in supporting compose benefit on outsourced information in cloud computing. [3]

This paper addresses the testing open issue by, on one hand, describing and approving access techniques in light of data properties, and, of course, allowing the data Our proposed plot moreover has striking properties of customer get the opportunity to profit security and customer puzzle key duty. Expansive examination exhibits that our proposed plan is exceptionally capable and provably secures under existing security models. [4]

The least complex approach to ensure the security of delicate client information is to scramble the information ahead of time, and afterward reveal the information unscrambling key just to those approved clients. Be that as it may, the touchy client information will be spilled while the decoding key is presented to unapproved clients. In this paper, they propose a protected self-destructing plan for electronic information (SSDD for short). By security investigation, we demonstrate that our SSDD plan can oppose against not just the customary cryptanalysis and the savage drive assaults, additionally the assaults in the DHT system, for example, the store sniffing assault, the query sniffing assault, and the standard DHT attack. [5]

III. EXISTING SYSTEM APPROACH

With the quick change of adaptable cloud services, it turns out to be continuously powerless to use cloud services to share data in a friend area, since it is not useful to execute full lifecycle assurance security, get to control transforms into a testing undertaking, especially when we share delicate data on cloud servers. Keeping in attention end goal to handle this issue.

IV. PROPOSED SYSTEM APPROACH

In the KP-TSABE strategy, each ciphertext is set apart with a period interval though private key is connected with a period minute. The ciphertext must be decrypted if both the time minute is in the permitted time interval and the attributes related with the ciphertext fulfil the key's get the chance to structure. The KP-TSABE can tackle some imperative security issues by supporting user defined approval period and by giving fine-grained get to control in the period.

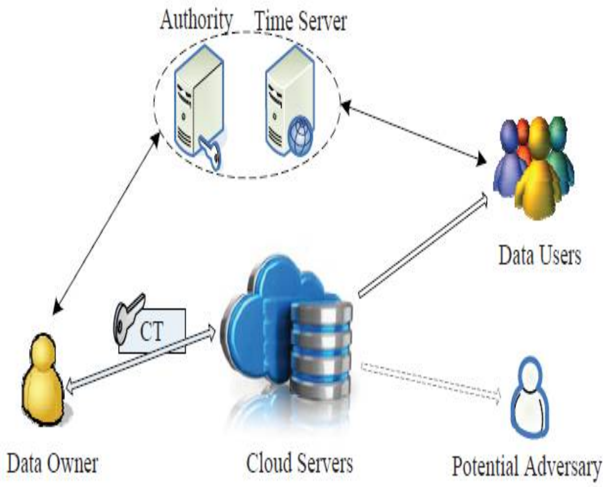


FIG 1: SYSTEM ARCHITECTURE

Advantages of proposed system:

1. Attribute based encryption (ABE) has significant advantages based on the public key encryption instead of the one-to-one encryption method because it acquires flexible advantages
2. Regard to security and fine-grained accesscontrol compared to other
3. supporting user-defined time-specific authorization, fine-grained get to control and information secure self destruction

V. PROPOSED SYSTEM ALGORITHM

1. Encryption:

The encryption algorithm are utilized to calculate the initial allocation information. Every input information is encrypted

2. KP-TSABE:

The KP-TSABE plan can be defined as an collection of the accompanying four algorithms: Setup, Encrypt, KeyGen, and Decrypt, This algorithms is controlled by the Authority and takings as input the security parameters 1 and attribute universe U, creates framework public parameters params and the ace key MSK

VI. PROPOSED SYSTEM MODULES

The proposed system has the following modules along with the particular functional requirements.

1. Sensitive Data,
2. secure self-destructing,
3. fine-grained access control,
4. privacy-preserving
5. cloud computing

DOI: 10.15680/IJIRCCE.2017. 0504109

Registration:

The Registration Modules show the new User Register, The Information of new user In The Order Of The List For Client Propose

Login

The Login Module shows the User Can Login Using His/ Her Name and unique Key

Sensitive information

To start with, SSDD does not consider the issue of the desired release time of the sensitive information the close time of both SSDD and FullPP Second, SSDD and many different plans are dependent on the perfect presumption of "No attacks on VDO (vanishing data object) before it terminates" . Third, it is exhibited that the Vanish plan is vulnerable against the Sybil attacks from the DHT network, the SSDD scheme and different plans are comparable. Therefore, indicating that the encoded information thing must be decrypted between The information owner encrypts his/her information to share to clients in the framework, in which each client’s key is related with a get to tree and each leaf node is related with a time moment.

Secure self-destructing

Wang et al. enhanced the Vanish framework and proposed an protected “self-destructing arrangement for electronic data (SSDD)”. In the SSDD conspire, a data is scrambled into a ciphertext, self-destructing arrangement for data sharing in distributed computing. At that point, we give a particular construction technique about the plan. At long last, we verify that the KP-TSABE plan is secure

Fine-grained accessed control

In order to implement fine-grained get to control, we relate each attribute in the attribute set with a period interval (approval period). The attribute is valid if and just if the present time moment is in this time interval. Just if the substantial quality in the ciphertext satisfies the get to tree in the key, the algorithm can decode the message effectively. The algorithm level of the KP-TSABE conspire incorporates four algorithm: Setup, Encrypt, KeyGen, and Decrypt.

Privacy-preserving

Because of the absence of time constraints, the previously mentioned ABE plans don't support client defined authorization period and secure self-devastation after termination for privacy-preserving of the information lifecycle in cloud computing. Along these lines, it turns into a major challenge to protect the privacy of those shared information in cloud, particularly in cross-cloud and huge information condition. To meet this challenge, it is important to design a comprehensive answer for bolster client defined approval period and to give fine-grained get to control during this period. The shared information ought to act naturally obliterated after the client defined termination time.

Cloud computing

Tysowski et al. adjusted the ABE and utilized re-encryption algorithm to recommend a novel plan to protect mobile client's information in cloud computing condition. Because of the absence of time requirements, the previously mentioned ABE plans don't support client defined approval period and secure self- destruction after expiration for protection saving of the information lifecycle in cloud computing. It is a period interval from the formation of the shared information, approval period to expiration time. This paper gives full lifecycle security assurance to shared information in cloud computing

Upload

If user want to upload every file here this module convert to your file into the ciper text format, again your process is completed

Download

If user want to download your file, then its before that must want to key of the data file name and the key submitted, then your original file is download

V. RESULT

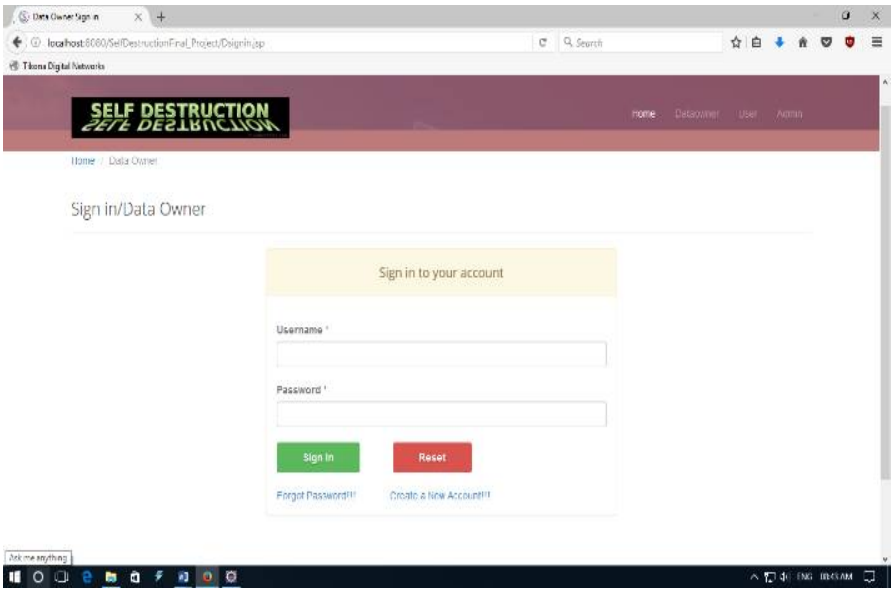
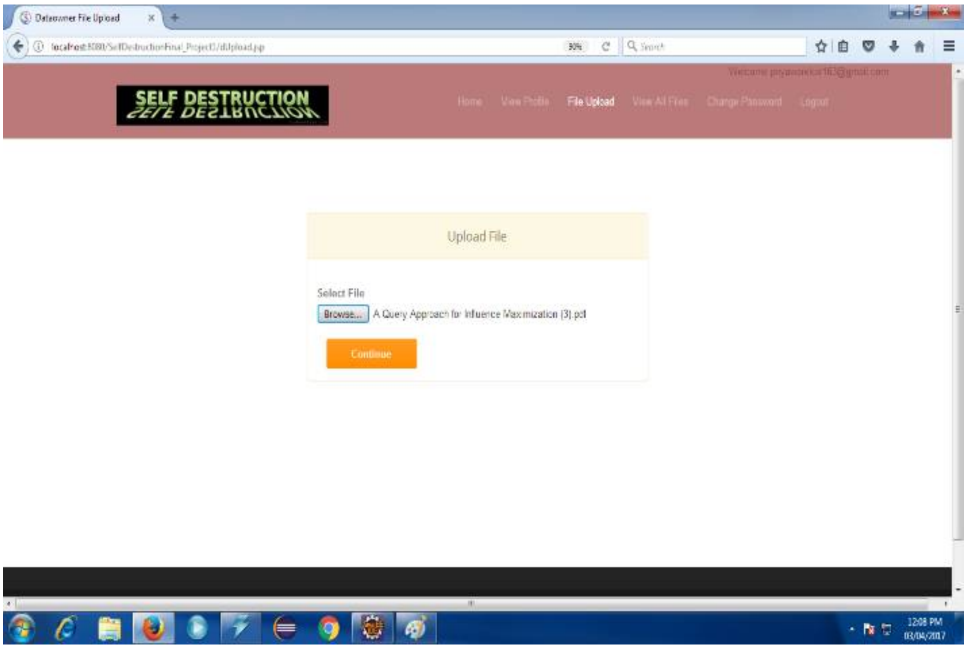
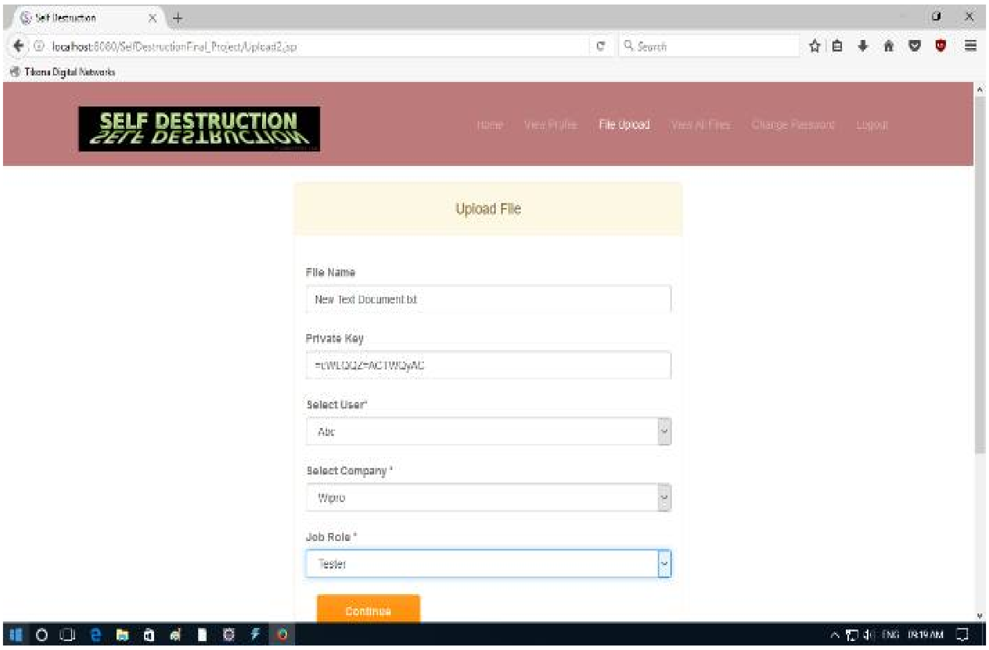


Figure 2. Data_Owner/ User Login



A Query Approach for Influence Maximization (3).pdf

Figure 3. Upload the file



Upload File

File Name: New Text Document.txt

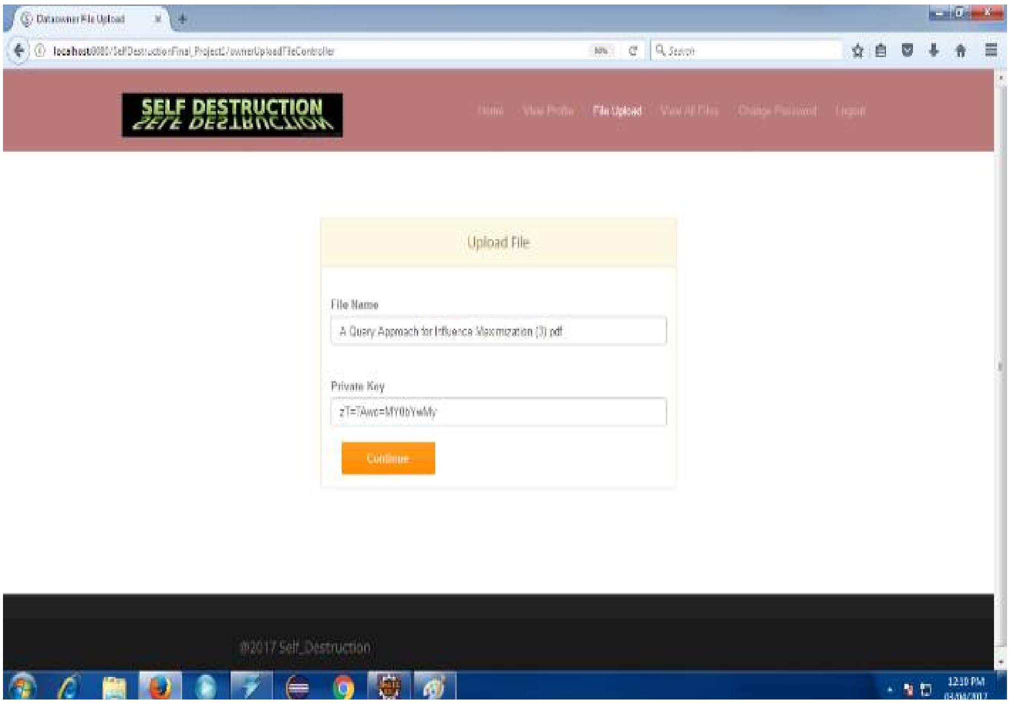
Private Key: =tWLQGZ=ACTWQyAC

Select User*: Abc

Select Company *: Wipro

Job Role *: Tester

Figure 7. Set Attribution

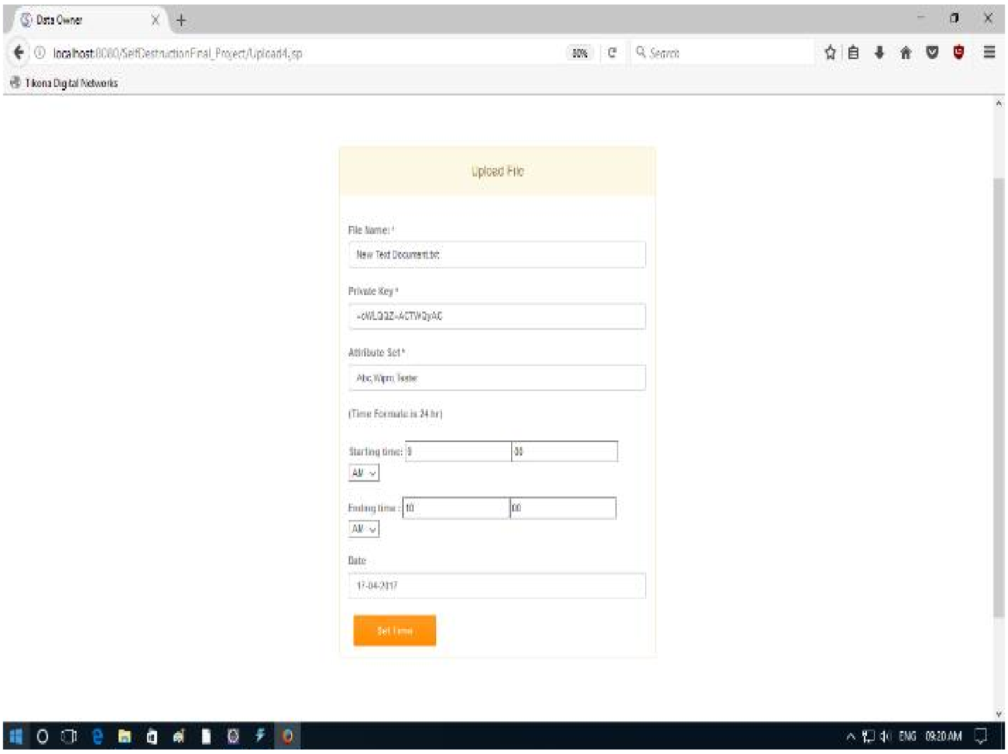


Upload File

File Name: A Query Approach for Influence Maximization (3).pdf

Private Key: zT=TAwc=MY0bYwMy

Figure 8. Set Private key



Upload File

File Name: *
New Text Document.txt

Private Key *
+cWLQ3Z+ACTV#2yAC

Attribute Set *
Abc,Wipro,Tester

(Time Format is 24 hr)

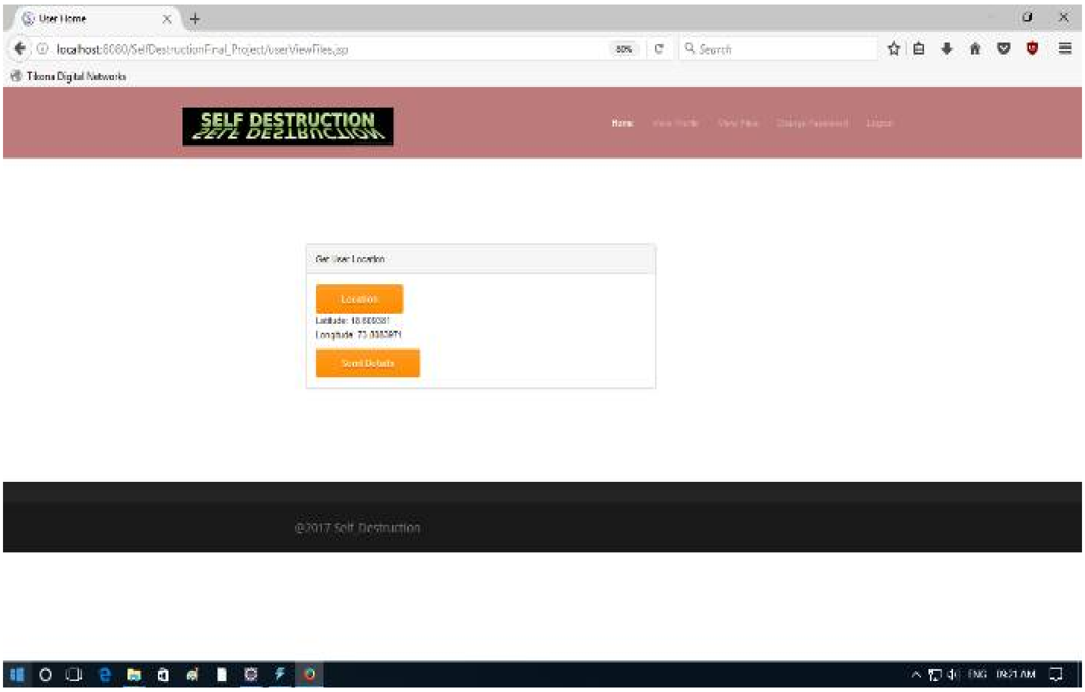
Starting time: 9 30
AM

Ending time : 10 00
AM

Date
17-04-2017

Set Time

Figure 9. Set Time/date and location



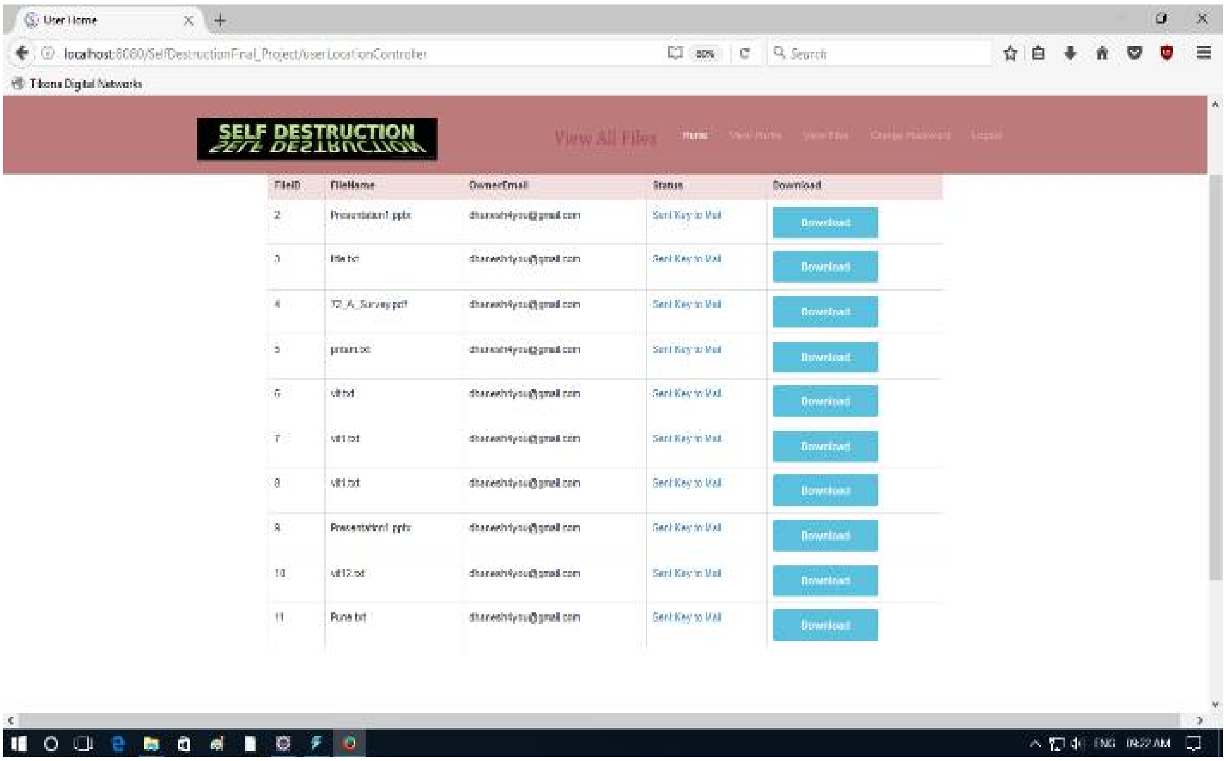
Get User Location

Location

Latitude: 18.609381
Longitude: 73.8882971

Send Details

Figure 10. User Location Trace



FileID	FileName	OwnerEmail	Status	Download
2	Presentation1.pptx	dhanesh4you@gmail.com	Sent Key to Mail	Download
3	file.txt	dhanesh4you@gmail.com	Sent Key to Mail	Download
4	72_A_Survey.pdf	dhanesh4you@gmail.com	Sent Key to Mail	Download
5	pntars.txt	dhanesh4you@gmail.com	Sent Key to Mail	Download
6	vit.txt	dhanesh4you@gmail.com	Sent Key to Mail	Download
7	vit1.txt	dhanesh4you@gmail.com	Sent Key to Mail	Download
8	vit1.txt	dhanesh4you@gmail.com	Sent Key to Mail	Download
9	Presentation1.pptx	dhanesh4you@gmail.com	Sent Key to Mail	Download
10	vit12.txt	dhanesh4you@gmail.com	Sent Key to Mail	Download
11	Pune.txt	dhanesh4you@gmail.com	Sent Key to Mail	Download

Figure 11. User Download file

VI. CONCLUSION

With the quick development of flexible cloud services, a lot of new difficulties have emerged. One of the most essential issues is the way to safely erase the outsourced information stored in the cloud severs. In this paper, we proposed a unique KP-TSABE scheme which can complete the time- definite ciphertext in order to tackle these issues by implementing adaptable fine-grained get to control during the approval time frame and time-controllable self-destruction after expiration to the shared and outsourced information in cloud computing. We also provided system model and a security model for the KPTSABE conspires. Besides, we proved that KPTSABE is secure in the standard model. The far reaching examination shows that the proposed KP-TSABE plan is better than other existing plans.

ACKNOWLEDGMENT

I would like to express my special gratitude to my guide Prof. Kumaresan P, School of Information Technology and Engineering, VIT University whose esteemed guidance and immense support encouraged to complete the project successfully.

REFERENCES

1. Dishant Soni, “Privacy preservation using novel identity management scheme in cloud computing”, 2015 Fifth International Conference on Communication Systems and Network Technologies.
2. Pooyn Jamshiddi, Aakash Ahmad, and Claus Pahl, “Cloud Migration Research: A Systematic Review”, IEEE TRANSACTIONS ON CLOUD COMPUTING, VOL. 1
3. Xuejiao Liu1, Yingjie Xia1, Shasha Jiang1, Fubiao Xia2, Yanbo Wang3, “Hierarchical Attribute-based Access Control with Authentication for Outsourced Data in Cloud Computing”
4. Shuchenguu Yu, Conge Wang, Kui Reen , and Wenjing Lou, “ To Achieving Secure, and Scalable, and Fine-grained information Access Control system in Cloud Computing” , IEEE INFOCOM 2010

5. Fengshun Yue, Guojun Wang, and Qin Liu," The Secure Self-Destructing method for Electronic information", 2010 IEEE

6. Rongxing Lu, Hui Zhu, Ximeng Liu, Joseph K. Liu, and Jun Shao, "Toward Efficient and Privacy-Preserving Computing in Big Data Era", IEEE Network, July/August 2014

7. B. Wang, B. Li, and H. Li, "Oruta: Privacy-preserving public auditing for shared data in the cloud," Cloud Computing, IEEE Transactions on, vol. 2, no. 1, pp. 43–56, 2014

8. J. Xiong, Z. Yao, J. Ma, X. Liu, Q. Li, and J. Ma, "Priam: Privacy preserving identity and access management scheme in cloud," KSII Transactions on Internet and Information Systems (TIIS), vol. 8, no. 1, pp. 282–304, 2014.

9. J. Xiong, F. Li, J. Ma, X. Liu, Z. Yao, and P. S. Chen, "A full lifecycle privacy protection scheme for sensitive data in cloud computing," Peer-to-Peer Networking and Applications. [Online]. Available: http://dx.doi.org/10.1007/s12083-014-0295-x

10. P. Jamshidi, A. Ahmad, and C. Pahl, "Cloud migration research: A systematic review," Cloud Computing, IEEE Transactions on, vol. 1, no. 2, pp. 142–157, 2013.

11. R. Lu, H. Zhu, X. Liu, J. K. Liu, and J. Shao, "Toward efficient and privacy-preserving computing in big data era," Network, IEEE, vol. 28, no. 4, pp. 46–50, 2014.

12. K. Kasamatsu, T. Matsuda, K. Emura, N. Attrapadung, G. Hanaoka, and H. Imai, "Time-specific encryption from forward-secure encryption," in Security and Cryptography forNetworks. Springer, 2012, pp. 184–204.

BIOGRAPHY

Dhanesh Lokhandeis a M.tech student in the Digital Communication Department, School of Information and Technology(SITE), VIT University,Vellore(TN), India. His area of interests is Digital Communication, Wireless Communication and Cloud Computing etc.