Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IMPACT FACTOR: 5.258

IJCSMC, Vol. 5, Issue. 4, April 2016, pg.22 – 32

iLoon: Data Encryption with Data Auto-Deletion Scheme in Cloud Database

Ashwini Zanzad[1], Anjali Selokar[2], Nandini Jain[3], Sneha Godbole[4], Kalyani Gajbhiye[5]

[12345]CSE & DBACER, INDIA

[1] ashwini.zanzad31@gmail.com; [2] aselokar77@gmail.com; [3] nandinijain117@gmail.com;
[4] snehagodbole13@gmail.com; [5] kalyanigajbhiye1988@gmail.com

Abstract— ***iLoon is an application for a group of people or an organization where user can send their confidential data to other user. Using this application user can share and access data. The data can be shared with multiple authorized users at same instance of time. The data encrypts before sending to other users. The unused and secure data gets deleted after user specific time. The user can specify the TTL for any document, text or image. TTL for document will provide the expiration time for any document. This project focuses on maintenance of cloud database as it will delete data after user specified TTL and it will refresh the cloud database storage. The application uses a combination of symmetric key (AES) and asymmetric key (MCP- ABE) scheme with time specific attribute. It is a secure encryption technique with data auto-deletion. In this scheme the cipher text contains the time interval generated from the time server. The cipher text can only decrypted if it is in the allowed time interval. If the time expires then cipher text gets automatically deleted from the cloud database. This scheme reduces manual deletion of data from the cloud database.***

A SQL cloud database is used for storing the data. Admin can access the database anywhere over internet. This document is a template. An electronic copy can be downloaded from the conference website. For questions on paper guidelines, please contact the conference publications committee as indicated on the conference website. Information about final paper submission is available from the conference website.

Keywords— ***TTL, AES, MCP-ABE, Integrity, Confidentiality***

I. Introduction

The cloud is a growing technology which uses network and servers to maintain data and applications. Securing cloud is most threatening issue of cloud computing services. Specially, where user wants to share their private data to other users using cloud. The cloud security is an important aspect to share data over cloud. It is not possible to maintain full lifetime privacy security for data over cloud. The growing hacking and cracking industry will create a problem for private data which is kept over the cloud. Suppose a user want to sends his ATM pin to other user. The data is sent using only encryption technique. The sender reads that data but not delete it after viewing .then after some days if someone hacks his account then all private data including ATM pin would be known by the hacker. So to avoid such situation the encryption method with TTL for document is used.

This application is limited for small group of users, organization, or institution. It is not the social networking site. After the user registration, User can not directly access the application. First the registration goes to the admin. Admin will verify that user is actually belongs to that organization or group .user can only use this application, after he is verified by admin. Admin has right to grant the access or deny the access. With this application, user can share text, pdf and images to different users. The art of protecting information by transforming it (encrypting it) into an unreadable format, called cipher text. Only those who possess a secret key can decipher (or decrypt) the message into plain text. Encrypted messages can sometimes be broken by cryptanalysis, also called code breaking, although modern cryptography techniques are virtually unbreakable. As the Internet and other forms of electronic communication become more prevalent, electronic security is becoming increasingly important. Cryptography is used to protect e- mail messages, credit card information, and corporate data. Cryptography systems can be broadly classified into symmetric-key systems that use a single key that both the sender and recipient have, and public-key systems that use two keys, a public key known to everyone and a private key that only the recipient of messages uses. The project uses a combination of symmetric and asymmetric key encryption based technique. Symmetric key is private key encryption technique which uses single private key for encryption as well as decryption. Asymmetric key encryption technique uses pub- lic attributes for encryption, which takes the public data attributes of the user for encryp- tion. The data is encrypted from the different combination of public attributes. After the encryption process is performed, the data is sent to that user whose attributes are used. The data is sent only to those users whose attributes are used for encryption. Other users belonging to this group receives only cipher text. This attributes based encryption technique combines with the auto deletion scheme. In this technique, the cipher text is assigned with an time interval. The time instance is generated from the time server which is present at the host computer. The cipher text is present in the cloud database only till the Time-to-live for the document is valid. This encryption technique with TTL solves the problem of security by providing authorized time interval to the document. After the time expires, the data gets self deleted, which maintains the memory. it reduces human efforts to delete the data. This project will aim at combining private and public key encryption methods.

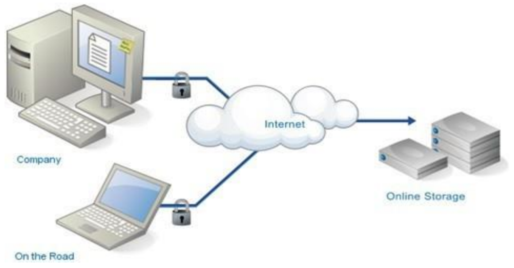


Figure 1.1: Online Cloud Database

The application uses a cloud database for storing data. Admin can access the data from the cloud database anywhere from the internet. This cloud database is SQL database. It has capacity of 1 GB. A cloud database is a database that typically runs on a cloud computing platform. There are two common deployment models: users can run databases on the cloud independently, using a virtual machine image, or they can purchase access to a database service, maintained by a cloud database provider. Of the databases available on the cloud, some are SQL-based and some use a NoSQL data model. Some cloud platforms offer options for using a database as a service, without physically launching a virtual machine instance for the database.In such a configuration, application owners do not have to install and maintain the database themselves. Instead, the database service provider takes responsibility for in- stalling and maintaining the database, and application owners pay according to their age. For example, Amazon Web Services provides three database services as part of its cloud offering: SimpleDB, a NoSQL key-value store; Amazon Relational Database Ser- vice, a SQL-based database service with a MySQL interface; and DynamoDB. Similarly, Microsoft offers the Azure SQL Database service as part of its cloud offering.

II. LITERATURE REVIEW

As there is need to share data with other user through cloud. So the cloud should consider security which is main issue in cloud computing. In this paper the confidential data which uploaded in the cloud use key-policy attribute-based encryption with time-specified attributes (KP-TSABE) scheme. In this scheme cipher text is labeled with time interval proposed by data owner and only decrypt if it is within time interval. The data can be access, store, downloaded within time instant but after time interval expired the data is securely self deleted and it will refresh the memory. Timed-specific encryption (TSE) provides an interesting encryption service where an encryption key is associated with a predefined release time, and a receiver can only construct the corresponding decryption key in this time instance applying the ABE to the shared data will intro- duce several problems with regard to time-specific constraint and self-destruction. [1]

In this paper they present attribute based access scheme for scalable media. The data which user wants to deliver on that data they apply attribute like age, gender, or nationality. The combination of both data and attribute can send to other user. Without using list of user names it uses attribute which provide data privacy by attribute based encryption. For this purpose they introduced multi message cipher text policy attribute based encryption technique. By using this it efficiently use attribute on that data so user whose attribute get match then only that user can decrypt that data so these attribute scheme [2]

The data can be shared in cloud so there is requirement to handle that data with security. This security is provided through encryption process. In this paper they describe AES encryption algorithm to implement security. AES is symmetric encryption algorithm. It is based on substitution and permutation network. AES perform all its computation on bytes rather than bits. So it uses 10 rounds for 128 bit key, 12 rounds for 192 bit key, and 14 rounds for 256 bit key. [3]

The confidential data when uploading in cloud then there is need of security. For maintaining that security we apply encryption. In this paper it uses mediated certificate less public key encryption (MCL-PKE) scheme without pairing operation which uses to give practical solution of shearing sensitive data. In this paper data owner encrypt that data using cloud generated public key then that data get uploaded into cloud .After successful authorization the data get partially decrypted and then user uses private key to fully de- crypt that data . Here cloud is work as storage and key generation center. [4]

III. PROBLEM STATEMENT

In today's computing environment there is a great need of security data need of security, data integrity and confidentiality for securing data over the internet .Data transmission need secured way to protected.

It is not possible to maintain full lifecycle, privacy security of any data. No user can protect their data for longer time. Growing hacking and cracking industry will crack account. So there should be any mechanism for self destructing the data .once the user receives the private data, it should get automatically self destroyed. There is limited database memory and when the data in database increases then load in the database also increases, which results in the slow process. so automatically deletion of data will result in memory management. The existing database needs platform, so better to use cloud database for storage, Admin can anytime use the database for the internet.

IV. PROPOSED SYSTEM

The proposed application is used to share the confidential data over the network. The application has user friendly graphical user interface. This application is for the group of people, organization, small scale company or institution. User can only use the application after the verification from the admin. Admin can grant the access or deny the access. The combination of public key and private key algorithm is used here. For encryption AES is used. AES is symmetric key encryption algorithm which uses single key for encryption and decryption. The cipher text is then transmitted using key MCP-ABE algorithm which uses public attribute for the transmission. The cipher text goes to the user whose attribute are selected. User can specify TTL for data before sending. As TTL expire data automatically get deleted. Thus TTL we are using time specified attribute scheme. Proposed application is using cloud database, online database make the database plat- form independent and location independent. Admin can anytime access the data.

Modules

These are the various modules of project. The first module is registration form in which the user will register him. The second module is admin verification form to verify the user. The third module is login form to get access to homepage. The fourth module is Homepage.

Registration Form

The first step in the system is to register the user. It is only after registration process the user can login into the system and can use it.

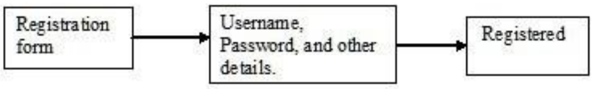


Figure 4.1: Registration process

In the registration module first a user needs to register him/her by providing necessary information such as name, username, email address and password etc. username is the field in which user can insert any name what he want to insert as his/her username. Whereas in password he should insert 6 character not less than that otherwise it shows exception same in case of phone number, where their is need of only 10 digit if it is less then same then the message will pop up. So remaining field should be insert by user which is very common like city, address, email id. The project name is the name of project on which they are working. And then click on register so after that user will register for this we are using SQL INSERT query to insert the information into the table SharedDataRegister into online database. After successful registration, the data first goes to the admin for verification. If the above processes are successfully carried out the user will get access to his/her personal home page where he/she will be able to perform various operations such as sharing and downloading of files.

Admin Approval Form

After the user has registered him successfully, this page is of Approval of account where user who registered is shown in this page. In this page there are four column. First column contain user-id which is the id of user. In second column there is full-name where full name of user is shown. In next column there is project name which consist of the name of project which is given by user at the time of registration. And final column contain the phone number.

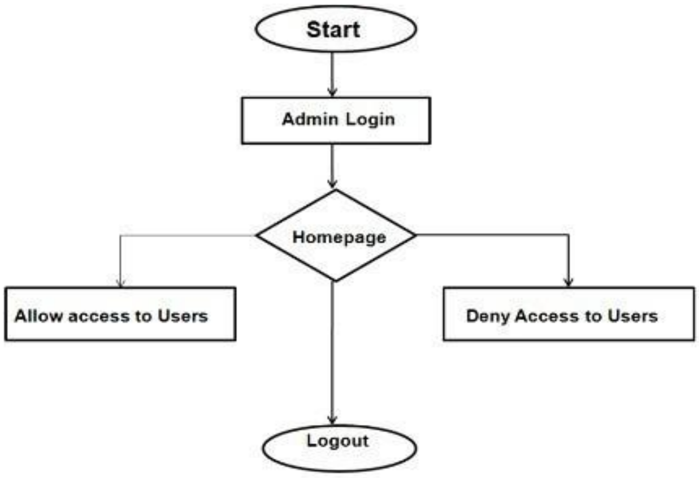


Figure 4.2: Admin verification

if he want to provide authorization to this user then he click on that user-id and select after that click on grant so this user will become authorized and can share data whereas if admin want to remove authorization then he click on deny button after that user can not send data or anything.

Login Form

In the login module a screen appears which contains two specific fields namely USER NAME and PASSWORD. Here using SqlConnection Class we have created a database named TeamV. Using SELECT query we are verifying the user-id and password entered by the user with the data stored in SharedDataRgistered table. If the user-id and password are matched and the the admin has granted access, the user will be logged in. Otherwise the pop up box will show credential invalid. If the user is not registered then user can click on register button to register.

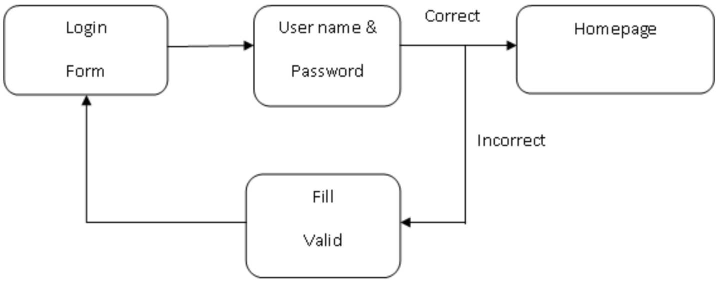


Figure 4.3: Login form

Homepage

After the successful registration and passing the verification module the specific user will get access to his personal home page where he/she can perform various operations like sharing and downloading of text, PDF files, mp3 files and images. This is the page which come after login. Here user first click on refresh button then the list of user come on left hand side where username and fullname is given of various user who are authorized. Then user can select the names to whom user want to send data that user name will be added in add recipient column. User can also use project name to send the data. By selecting project name .user can send the data to multiple user. if user want to send data in text format then he click on text and type text. Same with image and Pdf , he click on image radio and then click on browse.

Then he add key which user want to insert . This key is symmetric key which is use for encryption of the message then click on sent so the message box will pop up that message sent successfully. After that user add TTL (time to live)in hrs:min format like 00:22 it means for 2 min . Up to that 2 min the data will present in this system after this if time will expire, then the data will self destructed. The inbox shows the list of files received by the user.

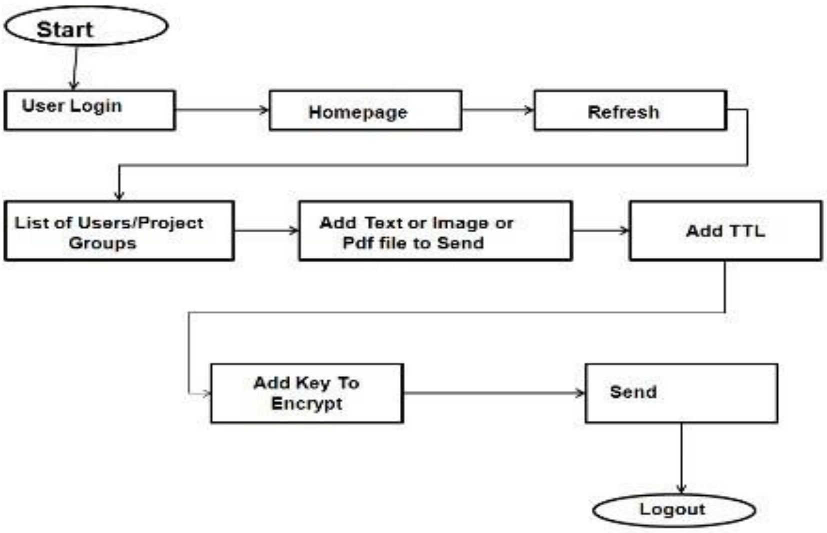

Start
User Login
Homepage
Refresh
List of Users/Project Groups
Add Text or Image or Pdf file to Send
Add TTL
Add Key To Encrypt
Send
Logout

Figure 4.4: Homepage

Inbox

This page will come after clicking on check inbox. This page consist of the username from whom the data received. It consist of type field as second column where it shows whether the data is in text format or in image format. And in third column there is data field which consist of data in encrypted form. This encrypted form data is the combination of cipher text and the key. Last column contain time to live which consist of time up to which the data will remain in system. After that time expired the data will self destructed. Then in this page at lower side there is block for key where user insert key which is symmetric key and click on decrypt and view so then next page come which is for output.

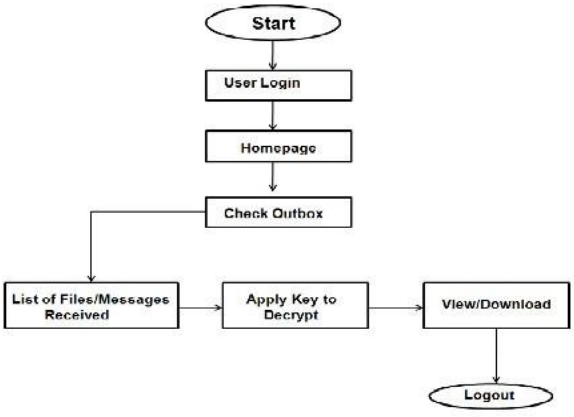


Figure 4.5: Inbox

Auto-deletion scheme

The ciphertext generated from the AES algorithm is provided with the TTL.TTL de- scribes the expiration time of the data. In this scheme, user enter the time in HH:MM format. This time provided by the user then added with current time of the system. The time of the data increases. when the time from the server matches with this data time ,then SQL query is fired and the ciphertext gets deleted.

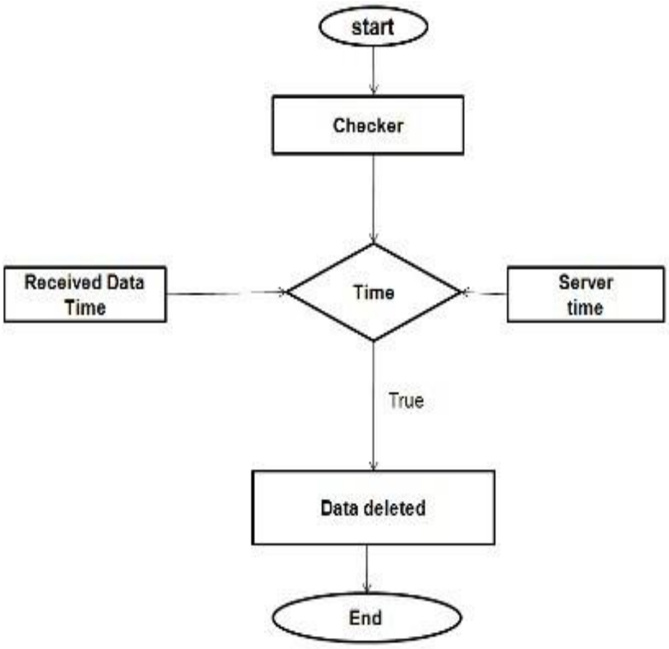


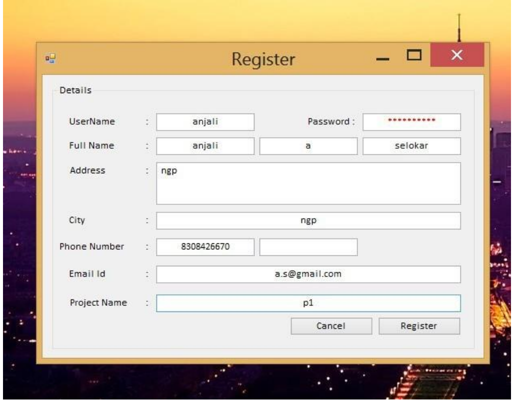
Figure 4.6: Auto-deletion scheme

V. Results

The snapshots generated by this project are as follows. This includes registration, verification, login, homepage, inbox and outbox.

Registration Page

Registration page is the first module of our application in which the user will provide his name, email address and password and other necessary details about him/her



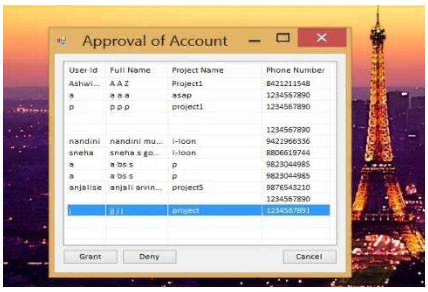
Details

UserName	:	anjali	Password :	***********	
Full Name	:	anjali	a	selokar	
Address	:	ngp			
City	:	ngp			
Phone Number	:	8308426670			
Email Id	:	a.s@gmail.com			
Project Name	:	p1			

Figure 5.1: Registration Page

Admin Approval Page.

This is the Admin approval page, where admin will approve access of every registered users. In this admin will check users details that the registered user is actually a part of that organization or not. Then admin will grant the permission to user to access application, if user is valid. Otherwise admin will deny the access to application to that particular user.



User Id	Full Name	Project Name	Phone Number
Ashwi...	A A Z	Project1	8421211548
a	a a a	asap	1234567890
p	p p p	project1	1234567890
			1234567890
nandini	nandini mu...	i-loon	9421966336
sneha	sneha s go...	i-loon	8806619744
a	a bs s	p	9823044985
a	a bs s	p	9823044985
anjalise	anjali arvin...	project5	9876543210
			1234567890
j	jj j j	project	1234567891

Figure 5.2: Admin Approval Page

Login Page

In the login page module the user has to enter his/her user name and password to get log in.His email id will be used as User name if the user provides correct data for the mentioned fields the user will be successfully logged in.

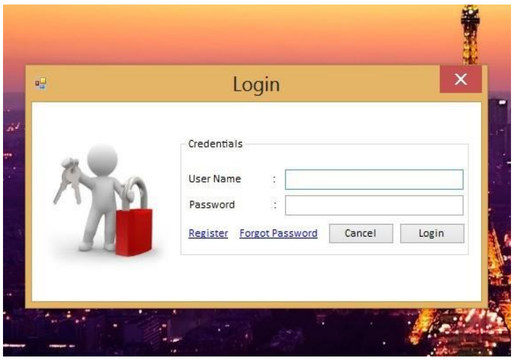


Figure 5.3:Login page

Homepage

This is personal home page of user where he/she can perform various operations like sending and downloading of text or PDF files or images. In homepage the list of Users and project groups shown whom user can send data. At a time user can send data to many user and a project group. After selection of type of data the TTL (Time to Leave) is applied on the data with the encryption.

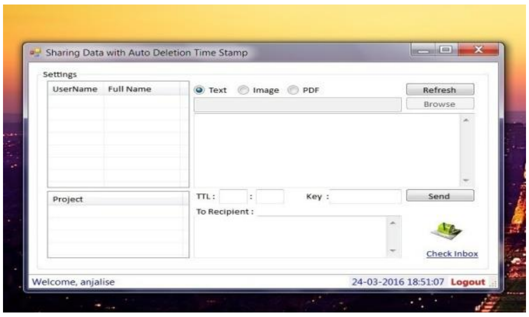
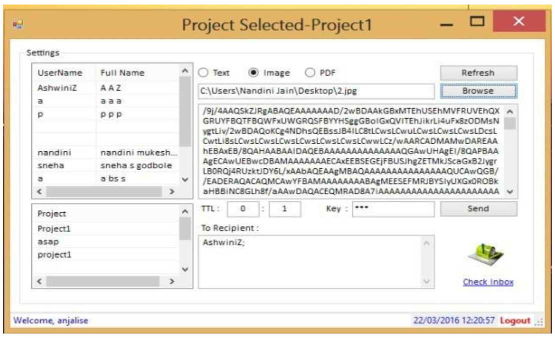


Figure 5.4: Homepage

SEND DATA

In this figure 4.5 ,user can send image to selected users. By encrypting the cipher text text with the TTL. And providing a key to receivers for decryption applies for PDF and text.


Project Selected-Project1

Settings

UserName	Full Name
AshwiniZ	A A Z
a	a a a
p	p p p
nandini	nandini mukesh...
sneha	sneha s godbole
a	a bs s

○ Text ● Image ○ PDF

C:\Users\Nandini Jain\Desktop\2.jpg

/9j/4AAQSkZJRgABAQEAAAAAAAD/2wBDAAkGBxMTEhUSEhMVFRUVEhQX
GRUYFBQTFBQWFxUWGRQSFBYYHSggGBoIGxQVITEhJikrLi4uFx8zODMsN
ygtLiv/2wBDAQoKCg4NDhsQEBssJB4ILC8tLCwsLCwuLCwsLCwsLCwsLDcsL
CwtLi8sLCwsLCwsLCwsLCwsLCwsLCwwLCz/wAARCADMAMwDAREAA
hEBAxEB/8QAHAABAAIDAQEBAAAAAAAAAAAAAAAQGAwUHAgEI/8QAPBAA
AgECAwUEBwcDBAMAAAAAAAAECAxEEBSEGEjFBUSJhgZETMkJScaGxB2Jygr
LB0RQj4RUzktJDY6L/xAAbAQEAAgMBAQAAAAAAAAAAAAAAQUCAwQGB/
/EADERAQACAQMCAwYFBAMAAAAAAAAABAgMEESEFMRJBYSIyUXGx0ROBk
aHBBiNC8GLh8f/aAAwDAQACEQMRAD8A7iAAAAAAAAAAAAAAAAAAAAAAAAA

TTL : 0 : 1 Key : ***

To Recipient :

AshwiniZ;

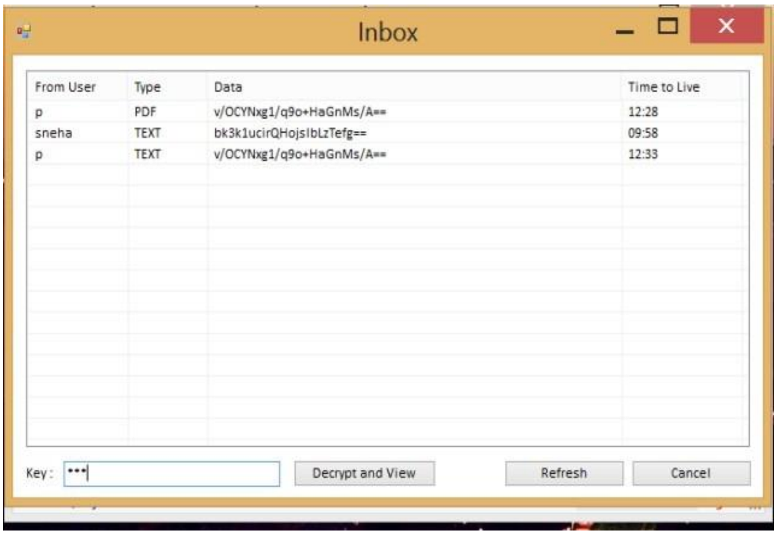
Project
Project1
asap
project1

Welcome, anjalise

22/03/2016 12:20:57

Inbox

In this page the received files by the user are displayed with fetch data from SharedData database. User can only view the data only by applying key of decryption, but the data only visible for the given time.In this page authorized user can view and download whatever he/she received.


Inbox

From User	Type	Data	Time to Live
p	PDF	v/OCYNxg1/q9o+HaGnMs/A==	12:28
sneha	TEXT	bk3k1ucirQHojsIbLzTefg==	09:58
p	TEXT	v/OCYNxg1/q9o+HaGnMs/A==	12:33

Key : ***

Figure 5.6: Send Data

View data(output box)

In this page user can also view and download images, and they are stored on the database for the provided time only, after that time get expired the data will automatically get deleted.

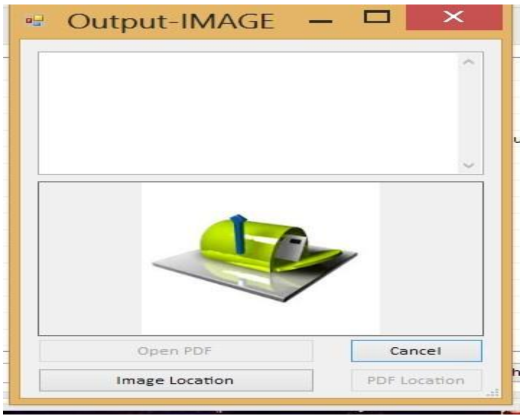


Figure 5.7: view data

Time To Leave

In this Page the work of auto-deletion is performed. For this the time which is add with current of the system with the message sent by the sender. After receiving the message the timer starts automatically and it match the time which is stored in the database with the message, if it will matches the will get deleted

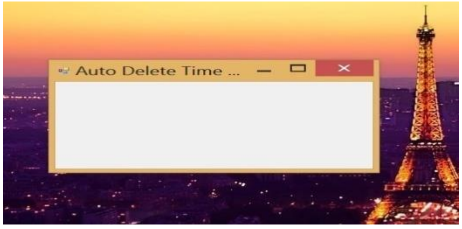


Figure 5.8: TTL application

VI. Conclusions

In this project, we proposed the novel AES encryption algorithm with TSA scheme which is able to achieve the time specific ciphertext. In order to solve these problems by implementing the authorization period and time controllable self data deletion after expectations of time. This project is able to share confidential data with multiple user or a project group. The PDF, image and text are encrypted uses AES which uses public attributes. The sending process uses MSP-ABE scheme, which takes the user public attributes (name and project name), thus the ciphertext is only secured by those user whose attributes are involves in the encryption process. The combination of AES with MSP-ABE with data auto-deletion scheme is successfully implemented in the project.

Acknowledgement

We have great pleasure to express our most sincere regards and deep of gratitude to our project guide **Ms. Kalyani Gajbhiye**, Asst. Prof., Department of Computer Science & En- gineering, DBACER, Nagpur for her valuable guidance for completing final year project **"iLoon: Data Encryption with Data Auto-deletion Scheme in Cloud Database"**. We are very much thankful to our Head of Department **Mr. R. S. Thakur**, Principal **Dr. V.H. Tatwawadi** and other staff member of the Department of Computer Science and Engi- neering for their valuable support and helping attitude. Finally, we would like to extend our thanks to all those who have contributed, directly or indirectly to make this project successful.

References

[1] Zhiqiang Yao Jianfeng Ma Qi Li Kui Geng Jinbo Xiong, Ximeng Liu and Patrick S. Chen. A secure data self-destructing scheme in cloud computing. *IEEE TRANSAC- TIONS ON CLOUD COMPUTING*, VOL. 2, NO. 4,, OCTOBER-DECEMBER 2014.

[2] Zhuo Wei Yongdong Wu and Robert H. Deng. *Attribute-Based Access to Scalable Media in Cloud-Assisted Content Sharing Networks*, volume VOL. 15, NO. 4. IEEE TRANSACTIONS ON MULTIMEDIA, June 2013.

[3] Xiaoyu Ding Seung-Hyun Seo, Mohamed Nabeel and Elisa Bertino. *”An Efficient Certificateless Encryption for Secure Data Sharing in Public Clouds*. 2nd Interna- tional Workshop on Cloud Servive Brokerage, 2009.

[4] Prof.R.R. Tuteja Shakeeba S. Khan. Security in cloud computing using cryptographic algorithms. *(International Journal of Innovative Research in Computerand Commu- nication Engineering(An ISO 3297: 2007 Certified Organization),* Vol. 3, Issue 1, January 2015.

[5] William Stallings.*Cryptography and Network Security Principles and Practice*, vol- ume FIFTH EDITION. Pearson Education, 2008.