Indian Journal of Science and Technology, *Vol 8(S9), 318–325, May 2015*

ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645
DOI: 10.17485/ijst/2015/v8iS9/65600

Secure Data Storage and Data Retrieval in Cloud Storage using Cipher Policy Attribute based Encryption

R. Saikeerthana* and A. Umamakeswari

School of Computing, SASTRA University, Thanjavur - 613401, Tamil Nadu, India; keerthanainspirative@gmail.com, aum@cse.sastra.edu

Abstract

Cloud is an arising and a massive technical development of this modern era which offers variety of services to satisfy the needs of multiple users. Cloud technology has various advantages such as high availability, storage, fast data retrieval, it still has a limitation to overcome which is known as security. Ciphertext Policy Attribute Based Encryption is a proficient technique for addressing this security issue, in which the owner of the data will create a control structure for encrypting the information. Decryption is possible when the peculiar attributes of the users satisfies that access control tree. Private keys for the users will be generated based on the attributes of the users. Another aspect to be considered in this technique is key escrow problem where single third party authority has the ability to decrypt the ciphertext which might contain sensitive information. In order to overcome this problem multiple authority CP-ABE is introduced. In the proposed scheme key generation for the users will issued by separate key generation authority and attributes of the users will be managed by attribute management authority. So none of the authority can decrypt data holder's secret information. Authorities cannot pool data so the collision attack is not possible. Illustration of the proposed technique follows in the later sections of the paper.

Keywords: Cloud Computing, Encryption Techniques, Key Escrow, Multiple Authority CPABE, Security

1. Introduction

Cloud computing is an emanate paradigm tailored to meet business and research needs. The cloud storage offers various advantages such as large amount of storage in the Pay-Per-Use policy, data availability, and fast access for the retrieval of data. Cloud computing layers are responsible for different types of services we acquire. SaaS layer provides access to various software which can be used as per our need instead of downloading and installing in the system. Iaas manages virtual machines, networks etc. PaaS provides facility ford employing a number of applications or services by reducing the high cost and difficulty of buying and governing the primary capabilities of present software and hardware. Cloud service providers are intended to provide various storage services[10]. Users will be benefited as they can store large amount of data in third party storage saving their own system space. The most important and prominent issue to be addressed is security. Cloud service providers[11] offer various security mechanisms, but if an adversary gets access to the user's data, then it affects the privacy of the user. Security should be provided for sensitive data of the user through various authentication and authorization mechanisms. Generally user data are secured by encryption and decryption techniques[13]. Data can be encrypted by converting plain text into a cipher text using the sender's public key and decrypted by converting cipher text into plain text by the private key. Various cryptographic algorithms

*Author for correspondence

are used for implementing the above said mechanism. Profuse techniques for eradicating these security issues are Attributed Based Encryption[1], Time based Proxy re-encryption[2], Token based encryption and Ciphertext policy based encryption. In Attribute Based Encryption, the user data will be divided into various attribute sets. Key Generation Center will generate keys for these attribute sets. All these attributes are described by creating an access control tree structure using different access policy built on the encrypted data. If the end user needs to retrieve data from storage of cloud, their attribute set should match the values of the access tree which is embedded into an access policy. Initially user data will be separated into various attributes and encryption will be done by binding them into an access tree structure. In order to decrypt the data from the cloud storage, the attribute set has to satisfy the conditions specified in the access policy. Token based encryption uses a mechanism of issuing tokens to the users for a predetermined period of time. User and cloud service provider should have advance communication regarding time based tokens so that even if the data owner is offline, the user can retrieve the data for specified amount of time. Proxy re-encryption also includes another technique called searchable encryption which implements a key word search instead of searching the whole database of the cloud storage. This is an efficient mechanism that saves time. Data security is achieved because data can be retrieved only when the index value matches the attribute set value.

2. Related Works

In[3] proposed an idea of two authorities. Ciphertext Policy Attributed Based Encryption mainly concentrates on rectifying key escrow problem by separating legal authorities for issuing end user private keys in to two facets: key authority: Generates personalized key component to every user mainly for preventing collusion attack and it is not responsible for attributes. Attribute management authority. This attribute management authority is mainly responsible for managing attributes and issuing attribute keys to data consumers. A protective communication takes places using two party computation protocol takes place between attribute management authority and key generation authority which prevents them acquiring any secret data of some other user therefore no one can acquire the private keys of other users. In[4] proposed an idea of hierarchical attribute based encryption. Cipher Policy Hierarchical Attribute Based Encryption scheme, attributes of the user are arranged in a matrix format where users with high level attributes can grant the access rights to the lower level users. This scheme includes multiple users from various organizations. In[5] proposed an idea of searchable encryption. Searchable encryption is a well-organized technique for data retrieval which uses attribute-based encryption. Various facets include Privacy of information: High level privacy is assured. None of them can access communication information about data content such as response, query and also regarding the ciphertext. Data holder's Privacy: True Identification of the data owner cannot be found from the encrypted data. End user's Privacy: Original Identities of the receivers cannot be acquired from the encrypted content. In[2] proposed an idea of time based encryption. This scheme will permits an end user's data access control capability to lapse axiomatically after a certain period of specified time that can be done even if the owner of the data is not online while performing user revocations mechanism. The owner of the data and storage service provider should share root private key which contains secret information in a predefined time with a storage service provider which can axiomatically update the specified time for accessing the data. In[6] proposed a technique which elaborates transformation of key policy attribute based encryption to searchable encryption. This encryption facilitates multiple data consumers to acquire a flexible search on remote encrypted data. This can be done by key word search on different attribute sets of the user.

3. System Architecture

The detailed explanation of how Cipher Policy technique works is shown in the Figure 1.

4. Contribution of Work

This paper contributes a detailed explanation and working phenomenon of Attribute Based Encryption which contains two main facets, Key Policy Attribute Based Encryption and Ciphertext Policy Attribute Based Encryption. Attribute Based Encryption in cloud storage is mainly for secure retrieval of user data which can be done by using Searchable

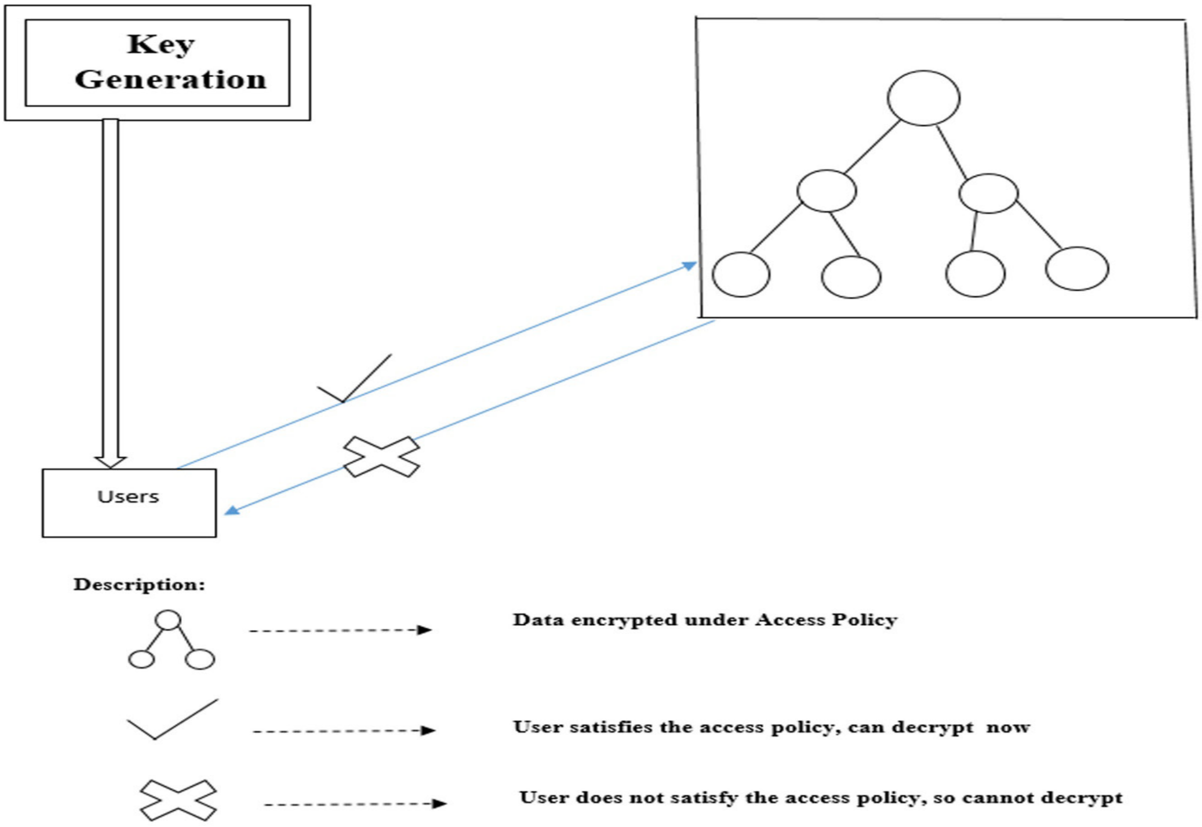

Key Generation
Users
Description:
Data encrypted under Access Policy
User satisfies the access policy, can decrypt now
User does not satisfy the access policy, so cannot decrypt

Figure 1. Ciphertext Policy Attribute Based Encryption.

Encryption as well as Hierarchical Attribute Based Encryption. Implementation below describes the working methodology of Cipher Policy Attribute Based Encryption.

4.1 Attribute based Encryption

An Attribute Based Encryption scheme mainly permits data access control over data that was encrypted which can be achieved by access policy and by attributes. In this scheme data encryption and decryption is hinge on the attributes of end user where the secret key is generated for the attributes of the data. Attributes include user data such as user location, subscription plan of the user and occupation of the user. ABE is developed based on the stimulus of IBE[7](Identity Based Encryption) which is otherwise called as Fuzzy IBE. ABE is mainly framed based on two important facets namely Key Policy Attribute Based Encryption and Cipher Policy Attribute Based Encryption.

4.1.1 Key Policy Attribute based Encryption

Key Policy Attribute Based Encryption[8] uses attributes for describing encrypted data and it will form an access tree structure for those attributes. This policy will generate user keys for the data that was encrypted and certain access control tree policies are embedded into the private key of the users. The encryptor is only allowed to know the decryptor's public attributes. If the legitimate user needs to ingress the data from storage cloud, then end user attribute sets should match with the access control policy in order to get access for successful data retrieval. This scheme is mainly designed for a single person to multiple group communications. This algorithm deals with the four step process as shown below:

4.1.1.1 Setup

In this algorithm, K1is the parameter designed for security that can generate two keys system public key Pu K1 and System master secret key Ma K1. Pu K1 is used for encrypting the messages of the sender. Ma K1 mainly prompts end user private keys that contain secret information that can be accessed by the particular authority.

4.1.1.2 Encryption

Input to the algorithm is delineated in the form of message M1, public key Pu K1 and attribute set. It generates output in the form of cipher text CT1.

4.1.1.3 Key Generation

Algorithm accepts two inputs, the access control tree structure A1 and master secret key Ma K1. It generates output in the form of a secret key Se K1. So using this key end user can decrypt the encrypted message when the attribute set match A1.

4.1.1.4 Decryption

Input for this algorithm is a user's secret key Se K1, access control tree structure A1 and ciphertext CT. Output will be the message M1 when the user attributes set satisfy the data owner's access control tree structure A1. The Key Policy-Attribute Based Encryption technique can attain fine-grained access control.

4.1.2 Cipher Policy Attribute based Encryption

Cipher Policy Attribute Based Encryption (CP-ABE)[9] scheme, every ciphertext is correlated with access control policy tree and user's secret key is cognate with attribute sets of the end user. Decryption of the ciphertext is possible when the user gratifies the control tree created the data owner. KP-ABE is the reverse format of CP-ABE. This algorithm inherits the same scheme as KP-ABE for originating the access structure in the encrypted data. This access tree structure allows the encrypted data to specify what are the attributes must present to decrypt the encrypted data. This implies, if the end user's key with attribute set that gratify the access control tree structure, the data can be recovered. This technique contains four algorithms:

4.1.2.1 Setup

In this algorithm we define input K1 as a security parameter that will generate two keys Public key Pu K1 and System Master secret key Ma K1. Pu K1 is used for encrypting the messages of the sender. Ma K1 is mainly to prompt user secret keys which can be acquired by the particular authority only.

4.1.2.2 Encrypt

Input to the algorithm delineated in the form of message M1, public key Pu K1, and an access control tree structure A1. It will generate output in the form of cipher text CT.

4.1.2.3 Key-Gen

Algorithm accepts two inputs attribute sets and the master secret key Ma K1. It will generate output in the form of a secret key Se K1 which allows the user to decrypt the encrypted message under an access control tree structure A1.

4.1.2.4 Decrypt

Input for this algorithm will be user's secret key Se K1 mainly for an attributes set and the cipher text CT. Output for this algorithm will be the message M1 only if it gratify the user's access control tree structure A1 cognate with the CT. It can overcome the limitation of KP-ABE wherein the encrypted data could not choose which user could decrypt. This scheme will reinforce the data access control in the real time environment. End user's secret key in this techniques the collaboration of attribute sets that will be correlated with the access control structure in the encrypted data.

4.2 Hierarchical Attribute-based Encryption

Hierarchical attribute-based encryption as shown in Figure 2, encryption scheme has a master node which will be the root master node that correlates with third party trust, multiple domain authority master nodes which correlate with multiple consortium users. The property of hierarchical key generation is used in hierarchical identity based encryption mainly for generating keys. In a Cipher text policy hierarchical attribute based encryption scheme, the attributes are arranged in a matrix form and the users with higher-level attributes can delegate their access rights to the users at a lower level. This specific feature empowers cipher text policy hierarchical attribute based encryption system to include large number of users from various organizations by delegating keys, e.g., Validating efficient data sharing between hierarchically arranged groups. For this technique Cipher text policy hierarchical attribute based encryption scheme is constructed with short cipher texts.

5. Implementation

Cipher Policy Attribute Based Encryption involves four algorithms. Initially the setup algorithm does not take any input other than system parameters to generate two important keys, system public key and system master key as shown in Figure 3. For generating private keys, inputs required are attributes of the user, master key and public key.

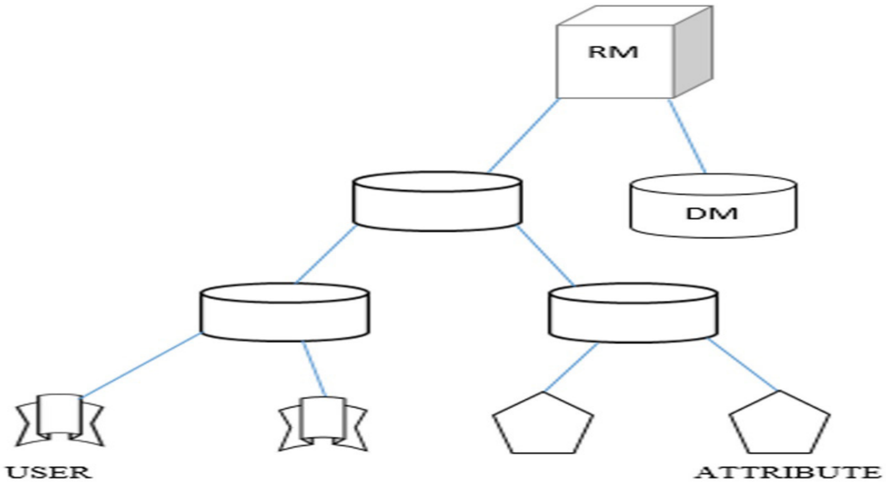
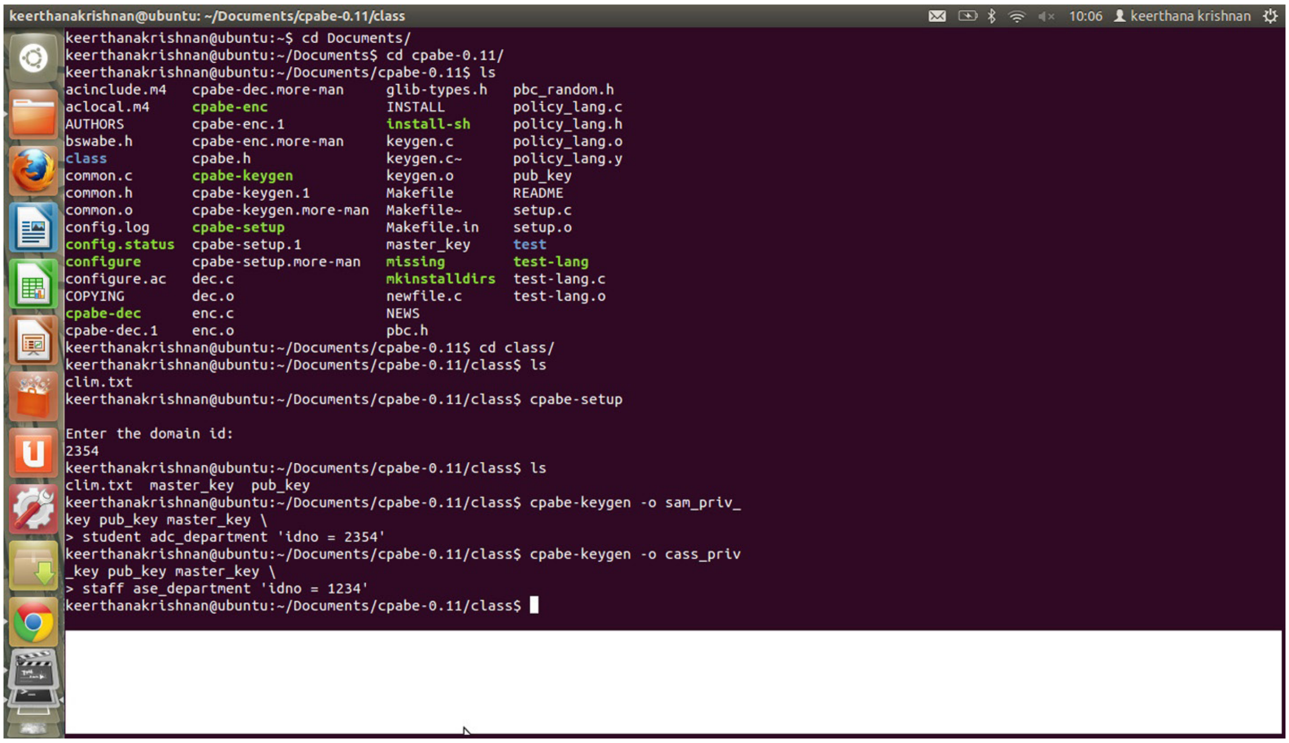


Figure 2. Hierarchical Attribute Based Encryption.

Next step is encryption. Encryption of the plain data will be converted into ciphertext by embedding the access control tree over the plain data. This access control tree structure is created by the owner of the data specifying certain peculiar attributes which contains logical gates as shown in Figure 5. Decryption by the data user is possible when the user satisfies the access control tree created by the data owner. This system is very efficient when the data owner wants to give access to a large group of people. The advantage of this technique is that it can give access to adequate data, for example log data. This ciphertext policy attribute based encryption requires cryptographic library called Pairing Based Cryptography (Pbc). Figure 4 shows access control tress embedded over the data such as student from Computer Science Department and staff or dean of Mechanical Department. Decryption is done with the private key the user holds. User's private key is embedded with various attributes, so when a user holds the private key with attribute created by the data owner's access control tree, then the user can decrypt the data. Encrypted document will be in an encrypted form which no one can access unless they hold the corresponding private key for the encrypted data as shown in Figure 6. Finally decryption algorithm will be executed by specifying inputs such as a private key and encrypted data document. Output for this algorithm would be decrypted data i.e. plain data. Computation time can also be generated for calculating efficiency.

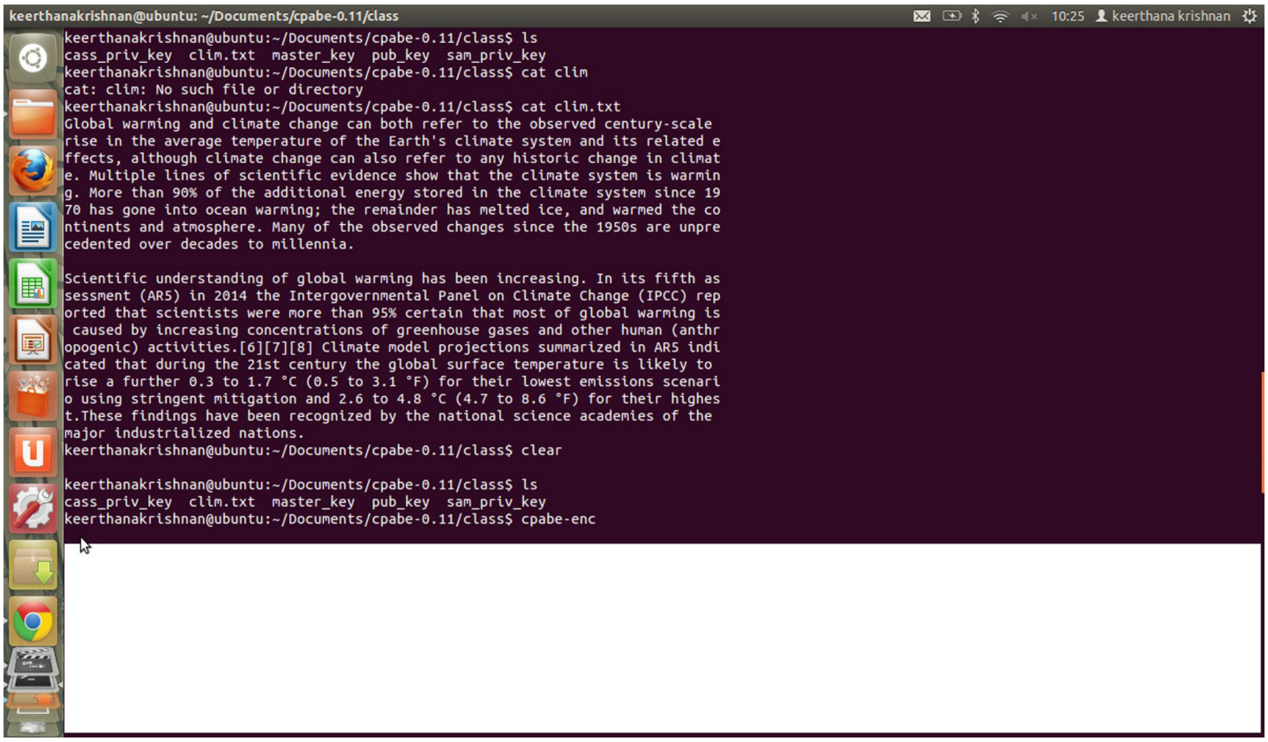
6. Conclusion

This paper presents the implementation of cipher text policy attribute based encryption. This technique is mainly built for maintaining Personal Health Records, Data of social networks, cloud data storage. All these databases contain important user personal data which needs a high level of privacy for securing these sensitive data. So ABE can be very much adopted in this case. Hierarchical Attribute Based Encryption framed based on the facet cipher policy. This scheme is needed when data sharing takes between hierarchically arranged groups of people. In this technique user data are arranged in a matrix form where high level users can give access to low level users. Real Environment application example for this scheme is communication between various teams of software development project. Based on these schemes data can be stored and retrieved in a secure manner from the cloud storage. Various proposed methods such as searchable encryption, hierarchical method are the notable aspects of this attribute based encryption. This paper also addresses various key challenges of the traditional encryption algorithm. The main intention for adopting attribute based encryption techniques is for increasing the security level. In future, these security schemes can be enhanced for providing high level security in data storage and data sharing.



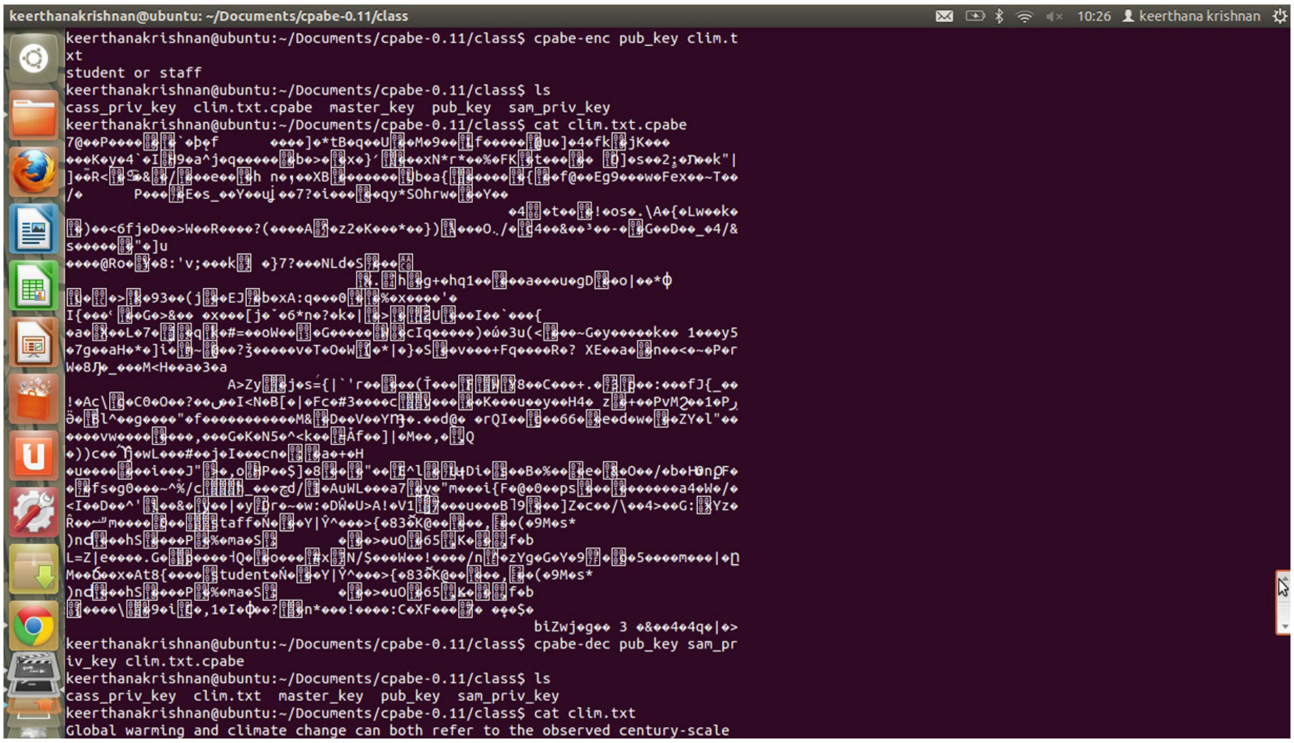
```
keerthanakrishnan@ubuntu:~$ cd Documents/
keerthanakrishnan@ubuntu:~/Documents$ cd cpabe-0.11/
keerthanakrishnan@ubuntu:~/Documents/cpabe-0.11$ ls
acinclude.m4   cpabe-dec.more-man     glib-types.h   pbc_random.h
aclocal.m4     cpabe-enc              INSTALL        policy_lang.c
AUTHORS        cpabe-enc.1            install-sh     policy_lang.h
bswabe.h       cpabe-enc.more-man     keygen.c       policy_lang.o
class          cpabe.h                keygen.c~      policy_lang.y
common.c       cpabe-keygen           keygen.o       pub_key
common.h       cpabe-keygen.1         Makefile       README
common.o       cpabe-keygen.more-man  Makefile~      setup.c
config.log     cpabe-setup            Makefile.in    setup.o
config.status  cpabe-setup.1          master_key     test
configure      cpabe-setup.more-man   missing        test-lang
configure.ac   dec.c                  mkinstalldirs  test-lang.c
COPYING        dec.o                  newfile.c      test-lang.o
cpabe-dec      enc.c                  NEWS
cpabe-dec.1    enc.o                  pbc.h
keerthanakrishnan@ubuntu:~/Documents/cpabe-0.11$ cd class/
keerthanakrishnan@ubuntu:~/Documents/cpabe-0.11/class$ ls
clim.txt
keerthanakrishnan@ubuntu:~/Documents/cpabe-0.11/class$ cpabe-setup

Enter the domain id:
2354
keerthanakrishnan@ubuntu:~/Documents/cpabe-0.11/class$ ls
clim.txt  master_key  pub_key
keerthanakrishnan@ubuntu:~/Documents/cpabe-0.11/class$ cpabe-keygen -o sam_priv_
key pub_key master_key \
> student adc_department 'idno = 2354'
keerthanakrishnan@ubuntu:~/Documents/cpabe-0.11/class$ cpabe-keygen -o cass_priv
_key pub_key master_key \
> staff ase_department 'idno = 1234'
keerthanakrishnan@ubuntu:~/Documents/cpabe-0.11/class$ 
```

Figure 3. Generation of public key and master key.



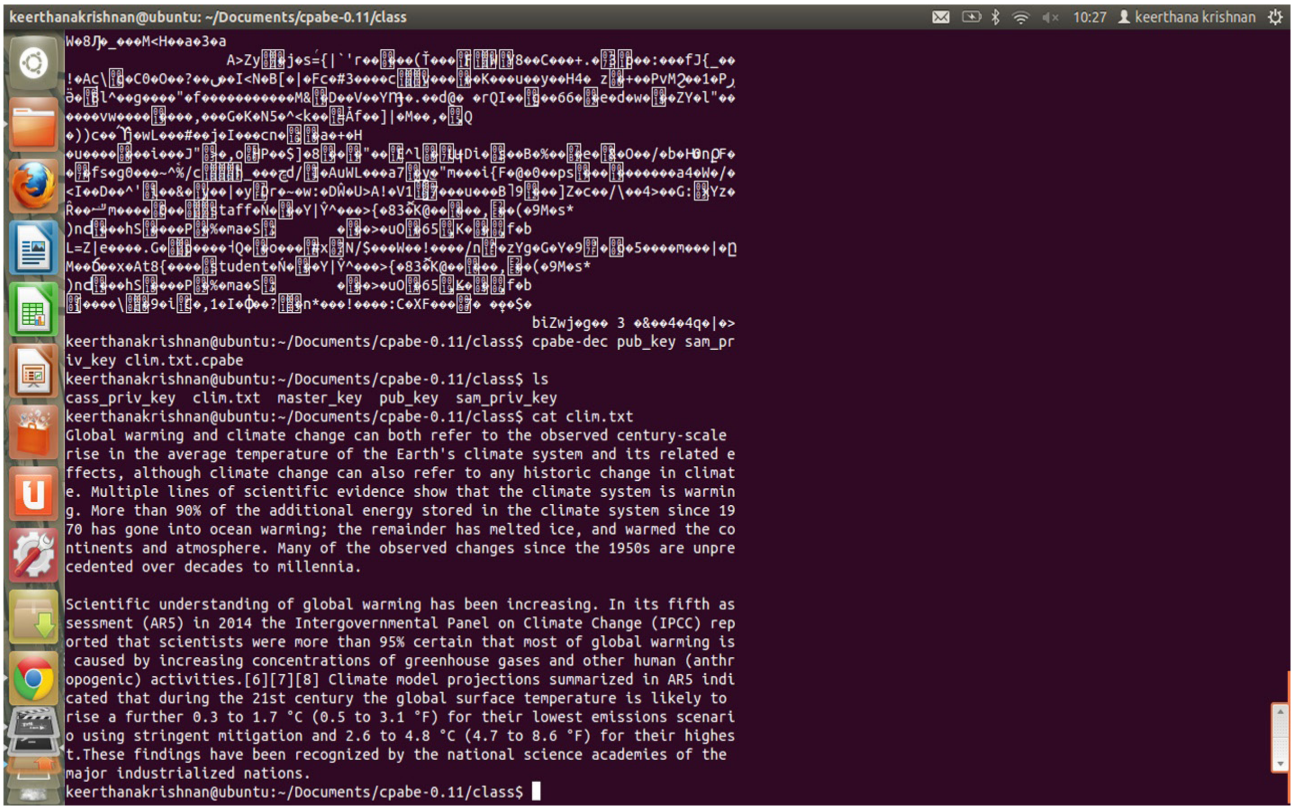
```
keerthanakrishnan@ubuntu:~/Documents/cpabe-0.11/class$ ls
cass_priv_key  clim.txt  master_key  pub_key  sam_priv_key
keerthanakrishnan@ubuntu:~/Documents/cpabe-0.11/class$ cat clim
cat: clim: No such file or directory
keerthanakrishnan@ubuntu:~/Documents/cpabe-0.11/class$ cat clim.txt
Global warming and climate change can both refer to the observed century-scale
rise in the average temperature of the Earth's climate system and its related e
ffects, although climate change can also refer to any historic change in climat
e. Multiple lines of scientific evidence show that the climate system is warmin
g. More than 90% of the additional energy stored in the climate system since 19
70 has gone into ocean warming; the remainder has melted ice, and warmed the co
ntinents and atmosphere. Many of the observed changes since the 1950s are unpre
cedented over decades to millennia.

Scientific understanding of global warming has been increasing. In its fifth as
sessment (AR5) in 2014 the Intergovernmental Panel on Climate Change (IPCC) rep
orted that scientists were more than 95% certain that most of global warming is
 caused by increasing concentrations of greenhouse gases and other human (anthr
opogenic) activities.[6][7][8] Climate model projections summarized in AR5 indi
cated that during the 21st century the global surface temperature is likely to
rise a further 0.3 to 1.7 °C (0.5 to 3.1 °F) for their lowest emissions scenari
o using stringent mitigation and 2.6 to 4.8 °C (4.7 to 8.6 °F) for their highes
t.These findings have been recognized by the national science academies of the
major industrialized nations.
keerthanakrishnan@ubuntu:~/Documents/cpabe-0.11/class$ clear

keerthanakrishnan@ubuntu:~/Documents/cpabe-0.11/class$ ls
cass_priv_key  clim.txt  master_key  pub_key  sam_priv_key
keerthanakrishnan@ubuntu:~/Documents/cpabe-0.11/class$ cpabe-enc
```

Figure 4. Generation of private key for the users.



```
keerthanakrishnan@ubuntu:~/Documents/cpabe-0.11/class$ cpabe-enc pub_key clim.t
xt
student or staff
keerthanakrishnan@ubuntu:~/Documents/cpabe-0.11/class$ ls
cass_priv_key  clim.txt.cpabe  master_key  pub_key  sam_priv_key
keerthanakrishnan@ubuntu:~/Documents/cpabe-0.11/class$ cat clim.txt.cpabe
7@◆◆P◆◆◆◆□□`◆þ◆f      ◆◆◆◆]◆*tB◆q◆◆U□◆M◆9◆◆□f◆◆◆◆◆□u◆]◆4◆fk□jK◆◆◆
◆◆◆K◆y◆4`◆I□9◆a^j◆q◆◆◆◆◆□b◆>◆□x◆}´□◆◆xN*r*◆◆%◆FK□t◆◆◆□◆ □]◆s◆◆2;◆Ɲ◆◆k"|
]◆◆R<□◆&□/□◆◆◆e◆◆□h n◆,◆◆XB□◆◆◆◆◆◆□b◆a{□◆◆◆◆□{□◆f@◆◆Eg9◆◆◆w◆Fex◆◆~T◆◆
/◆      P◆◆◆□E◆s_◆◆Y◆◆uj◆◆7?◆i◆◆◆□◆qy*SOhrw◆□◆Y◆◆
                                                ◆4□◆t◆◆□!◆os◆.\A◆{◆Lw◆◆k◆
□)◆◆<6fj◆D◆◆>W◆◆R◆◆◆◆?(◆◆◆◆A□◆z2◆K◆◆◆*◆◆})□◆◆◆O./◆□4◆◆&◆◆³◆◆-◆□G◆◆D◆◆_◆4/&
s◆◆◆◆◆□"◆]u
◆◆◆◆@Ro◆□◆8:'v;◆◆◆k□ ◆}7?◆◆◆NLd◆S□◆◆□
                                  □.□h□g+◆hq1◆◆□◆◆a◆◆◆u◆gD□◆o|◆◆*ф
□◆□◆>□◆93◆◆(j□◆EJ□b◆xA:q◆◆◆0□□%◆x◆◆◆◆'◆
I{◆◆◆‘□◆G◆>&◆◆ ◆x◆◆◆[j◆˘◆6*n◆?◆k◆|□>□□U□◆◆I◆◆`◆◆◆{
◆a◆□◆◆L◆7◆□□q□◆#=◆◆◆W◆◆□◆G◆◆◆◆◆□□cIq◆◆◆◆◆)◆ώ◆3u(<□◆◆~G◆y◆◆◆◆◆k◆◆ 1◆◆◆y5
◆7g◆◆aH◆*◆]i◆□~□◆◆?ǯ◆◆◆◆◆v◆T◆O◆W□◆*|◆}◆S□◆v◆◆◆+Fq◆◆◆◆R◆? XE◆◆a◆□n◆◆<◆~◆P◆r
W◆8Ꭻ◆_◆◆◆M<H◆◆a◆3◆a
                    A>Zy□j◆s={|`'r◆◆□◆◆(Ť◆◆◆□□□8◆◆C◆◆◆+.◆□□◆◆:◆◆◆fJ{_◆◆
!◆Ac\□◆C0◆O◆◆?◆◆ں◆◆I<N◆B[◆|◆Fc◆#3◆◆◆◆c□◆◆◆□◆K◆◆◆u◆◆y◆◆H4◆ z□+◆◆PvM Ձ◆◆1◆P,
ə◆□l^◆◆g◆◆◆◆"◆f◆◆◆◆◆◆◆◆◆◆◆M&□D◆◆V◆◆Yɱ◆.◆◆d@◆ ◆rQI◆◆□◆◆66◆□e◆dw◆□◆ZY◆l"◆◆
◆◆◆◆vW◆◆◆◆□◆◆◆,◆◆◆G◆K◆N5◆^<k◆◆□Ăf◆◆]|◆M◆◆,◆□Q
◆))c◆◆Ἧ◆wL◆◆◆#◆◆j◆I◆◆◆cn◆□□a◆+◆H
◆u◆◆◆◆□◆◆i◆◆◆J"□◆,o□P◆◆$]◆8□◆□"◆◆□^l□□Di◆□◆◆B◆%◆◆□e◆□◆O◆◆/◆b◆H0nϱF◆
◆□fs◆g0◆◆◆~^%/c□□_◆◆◆ꝣd/□◆AuWL◆◆◆a7□y◆"m◆◆◆i{F◆@◆0◆◆ps□◆◆□◆◆◆◆◆◆a4◆W◆/◆
<I◆◆D◆◆^'□◆◆&◆□◆◆|◆y□r◆~◆w:◆DŴ◆U>A!◆V1□◆◆◆u◆◆◆B19□◆◆]Z◆c◆◆/\◆◆4>◆◆G:□Yz◆
Ȓ◆◆ـــmo◆◆◆◆□◆◆□staff◆Ń◆□◆Y|Ŷ^◆◆◆>{◆83◆K@◆◆□◆◆,□◆(◆9M◆s*
)nd□◆◆hS□◆◆◆P□%◆ma◆S□        ◆□◆>◆uO□65□K◆□□f◆b
L=Z|e◆◆◆◆.G◆□◆◆◆◆ɟQ◆□o◆◆◆◆□x□N/$◆◆◆W◆◆!◆◆◆◆/n□◆zYg◆G◆Y◆9□◆□◆5◆◆◆◆m◆◆◆|◆Ω
M◆◆ɗ◆◆x◆At8{◆◆◆◆□student◆Ń◆□◆Y|Ŷ^◆◆◆>{◆83◆K@◆◆□◆◆,□◆(◆9M◆s*
)nd□◆◆hS□◆◆◆P□%◆ma◆S□        ◆□◆>◆uO□65□K◆□□f◆b
□◆◆◆◆\□9◆i□◆,1◆I◆ф◆◆?□n*◆◆◆!◆◆◆◆:C◆XF◆◆◆□◆ ◆◆◆$◆
                                                biZwj◆g◆◆ 3 ◆&◆◆4◆4q◆|◆>
keerthanakrishnan@ubuntu:~/Documents/cpabe-0.11/class$ cpabe-dec pub_key sam_pr
iv_key clim.txt.cpabe
keerthanakrishnan@ubuntu:~/Documents/cpabe-0.11/class$ ls
cass_priv_key  clim.txt  master_key  pub_key  sam_priv_key
keerthanakrishnan@ubuntu:~/Documents/cpabe-0.11/class$ cat clim.txt
Global warming and climate change can both refer to the observed century-scale
```

Figure 5. Encryption of the data.



```
W◆8Ꭻ◆_◆◆◆M<H◆◆a◆3◆a
                    A>Zy□j◆s={|`'r◆◆□◆◆(Ť◆◆◆□□□8◆◆C◆◆◆+.◆□□◆◆:◆◆◆fJ{_◆◆
!◆Ac\□◆C0◆O◆◆?◆◆ں◆◆I<N◆B[◆|◆Fc◆#3◆◆◆◆c□◆◆◆□◆K◆◆◆u◆◆y◆◆H4◆ z□+◆◆PvM Ձ◆◆1◆P,
ə◆□l^◆◆g◆◆◆◆"◆f◆◆◆◆◆◆◆◆◆◆◆M&□D◆◆V◆◆Yɱ◆.◆◆d@◆ ◆rQI◆◆□◆◆66◆□e◆dw◆□◆ZY◆l"◆◆
◆◆◆◆vW◆◆◆◆□◆◆◆,◆◆◆G◆K◆N5◆^<k◆◆□Ăf◆◆]|◆M◆◆,◆□Q
◆))c◆◆Ἧ◆wL◆◆◆#◆◆j◆I◆◆◆cn◆□□a◆+◆H
◆u◆◆◆◆□◆◆i◆◆◆J"□◆,o□P◆◆$]◆8□◆□"◆◆□^l□□Di◆□◆◆B◆%◆◆□e◆□◆O◆◆/◆b◆H0nϱF◆
◆□fs◆g0◆◆◆~^%/c□□_◆◆◆ꝣd/□◆AuWL◆◆◆a7□y◆"m◆◆◆i{F◆@◆0◆◆ps□◆◆□◆◆◆◆◆◆a4◆W◆/◆
<I◆◆D◆◆^'□◆◆&◆□◆◆|◆y□r◆~◆w:◆DŴ◆U>A!◆V1□◆◆◆u◆◆◆B19□◆◆]Z◆c◆◆/\◆◆4>◆◆G:□Yz◆
Ȓ◆◆ـــmo◆◆◆◆□◆◆□staff◆Ń◆□◆Y|Ŷ^◆◆◆>{◆83◆K@◆◆□◆◆,□◆(◆9M◆s*
)nd□◆◆hS□◆◆◆P□%◆ma◆S□        ◆□◆>◆uO□65□K◆□□f◆b
L=Z|e◆◆◆◆.G◆□◆◆◆◆ɟQ◆□o◆◆◆◆□x□N/$◆◆◆W◆◆!◆◆◆◆/n□◆zYg◆G◆Y◆9□◆□◆5◆◆◆◆m◆◆◆|◆Ω
M◆◆ɗ◆◆x◆At8{◆◆◆◆□student◆Ń◆□◆Y|Ŷ^◆◆◆>{◆83◆K@◆◆□◆◆,□◆(◆9M◆s*
)nd□◆◆hS□◆◆◆P□%◆ma◆S□        ◆□◆>◆uO□65□K◆□□f◆b
□◆◆◆◆\□9◆i□◆,1◆I◆ф◆◆?□n*◆◆◆!◆◆◆◆:C◆XF◆◆◆□◆ ◆◆◆$◆
                                                biZwj◆g◆◆ 3 ◆&◆◆4◆4q◆|◆>
keerthanakrishnan@ubuntu:~/Documents/cpabe-0.11/class$ cpabe-dec pub_key sam_pr
iv_key clim.txt.cpabe
keerthanakrishnan@ubuntu:~/Documents/cpabe-0.11/class$ ls
cass_priv_key  clim.txt  master_key  pub_key  sam_priv_key
keerthanakrishnan@ubuntu:~/Documents/cpabe-0.11/class$ cat clim.txt
Global warming and climate change can both refer to the observed century-scale
rise in the average temperature of the Earth's climate system and its related e
ffects, although climate change can also refer to any historic change in climat
e. Multiple lines of scientific evidence show that the climate system is warmin
g. More than 90% of the additional energy stored in the climate system since 19
70 has gone into ocean warming; the remainder has melted ice, and warmed the co
ntinents and atmosphere. Many of the observed changes since the 1950s are unpre
cedented over decades to millennia.

Scientific understanding of global warming has been increasing. In its fifth as
sessment (AR5) in 2014 the Intergovernmental Panel on Climate Change (IPCC) rep
orted that scientists were more than 95% certain that most of global warming is
 caused by increasing concentrations of greenhouse gases and other human (anthr
opogenic) activities.[6][7][8] Climate model projections summarized in AR5 indi
cated that during the 21st century the global surface temperature is likely to
rise a further 0.3 to 1.7 °C (0.5 to 3.1 °F) for their lowest emissions scenari
o using stringent mitigation and 2.6 to 4.8 °C (4.7 to 8.6 °F) for their highes
t.These findings have been recognized by the national science academies of the
major industrialized nations.
keerthanakrishnan@ubuntu:~/Documents/cpabe-0.11/class$ █
```

Figure 6. Decryption of the encryption.

7. References

1. Bethencourt J, Sahai A, Waters B. Ciphertext-policy attribute-based encryption. IEEE Symposium on Security and Privacy, 2007 SP'07. 2007; IEEE.
2. Liu Q, Wang G, Wu J. Time-based proxy re-encryption scheme for secure data sharing in a cloud environment. Information Sciences. 2014; 258:355–70.
3. Hur J, Koo D, Hwang SO, Kang K. Removing escrow from ciphertext policy attribute-based encryption. Computers and Mathematics with Applications. 2013; 65(9):1310–7.
4. Deng H, Wu Q, Qin B, Domingo-Ferrer J, Zhang L, Liu J, et al. Ciphertext-policy hierarchical attribute-based encryption with short ciphertexts. Information Sciences. 2014; 275:370–84.
5. Koo D, Hur J, Yoon H. Secure and efficient data retrieval over encrypted data using attribute-based encryption in cloud storage. Computers and Electrical Engineering. 2013; 39(1):34–46.
6. Han F, Qin J, Zhao H, Hu J. A general transformation from KP-ABE to searchable encryption. Future Generation Computer Systems. 2014; 30:107–15.
7. Sahai A, Waters B. Fuzzy identity-based encryption. Advances in Cryptology-EUROCRYPT 2005. Springer; 2005. p. 457–73.
8. Boneh D, Franklin M. Identity-based encryption from the Weil pairing. Advances in Cryptology-CRYPTO 2001. Springer; 2001.
9. Ibraimi L, Petkovic M, Nikova S, Hartel P, Jonker W. Mediated ciphertext-policy attribute-based encryption and its application. Information security applications: Springer; 2009. p. 309–23.
10. Rajathi A, Saravanan N. A survey on secure storage in cloud computing. Indian Journal of Science and Technology. 2013; 6(4):4396–401.
11. Neela TJ, Saravanan N. Privacy preserving approaches in cloud: A survey. Indian Journal of Science and Technology. 2013; 6(5):4531–5.
12. Sharifi AM, Amirgholipour SK, Alirezanejad M, Aski BS, Ghiami M. Availability challenge of cloud system under DDOS attack. Indian Journal of Science and Technology. 2012; 5(6):2933–7.
13. Pairing-based cryptography library. Available from: http://crypto.stanford.edu/pbc/
14. Available from: https://gmplib.org/