ISSN:0975-9646

Encryption Algorithm for Cloud Computing

Ankita Nandgaonkar[1], Prof. Pallavi Kulkarni[2]

[1,2]*Computer Engineering,*
Mumbai University, India

Abstract— **Cloud computing is the next big thing after internet in the field of Information technology. It is an Internet-based computing technology, in which software, Shared recourses and information are provided to consumers and devices on-demand, and as per user's requirement on a pay per use model. Even though the cloud continues to grow in popularity, Usability and respectability, Problems with data protection and data privacy and other Security issues play a major setback in the field of Cloud Computing. Privacy and security are the key issue for cloud storage. Encryption is a well known technology for protecting sensitive data .This paper proposes a combined approach of Identity based and attribute based access policy for encryption technique of cloud storage which can be implementable on cloud platform. The report analyses the feasibility of the applying encryption algorithm for data security and privacy in cloud Storage with other existing algorithms.**

Keywords— **Cloud Storage, Cipher text, encryption, access control, attribute-based encryption, constant ciphertext length,decryption, Cryptography.**

I. INTRODUCTION

A. Cloud computing

Cloud Computing is the ability to access a pool of computing resources owned and maintained by a other trusted party via the Internet. It is a way of delivering computing resources based on existing technologies such as server virtualization. The "cloud" is composed of hardware, storage, networks, interfaces, and services which provide the way through which users can access the infrastructures, computing power, applications, and services on demand which are independent of locations. Cloud computing involves the transfer, storage, and processing of information on the „providers‟ infrastructure, which is not included in the „customers‟ control policy.

Cloud computing has attracted widespread attention and support in many fields. In the cloud computing environment, many services such as resource renting, application hosting, and service outsourcing are the on-demand service in the IT field. .e.g. Amazon‟sEC2, Amazon‟s S3, Google App Engine and Microsoft‟s Azure etc. Cloud computing can provide flexible computing capabilities, reduce costs and capital expenditures and charge according to usage.The concept Cloud Computing is linked closely with those of Information as a Service (IaaS), Platform as a Service (PaaS), Software as a Service (SaaS)[1]. Here comes the first benefit of the Cloud Computing i.e. it reduces the cost of hardware that could have been used at user end. As there is no need to store data at user‟s end because it is already at some other location. So instead of buying the infrastructure required to run the processes and Save bulk of data which. You are just renting the assets according to your requirements.

The similar idea is for all cloud networks [2]. It uses remote services through a network using various resources. It is basically meant to give maximum with the minimum resources i.e. the user is having the minimum hardware requirement but can use the maximum capability of computing. This is possible only through this technology which requires and utilizes its resources.

In cloud computing, users store their data files in cloud servers. Thus, it is crucial to prevent unauthorized access to these resources and realize secure resource sharing. In traditional access control methods, we generally assume data owners and the storage server are in the same secure domain and the server is fully trusted. However, in the cloud computing environment, cloud service providers can be attacked by malicious attackers. These attacks may leak the confidential information of users for commercial interests as the data owners commonly store decrypted data in cloud servers. How to realize access control to the encrypted data and ensure the confidentiality of data files of users in an untrusted cloud environment are the major problems. Moreover, since the number of users is large in a cloud computing environment, how to realize scalable, flexible and fine-grained access control is strongly desired in the service-oriented cloud computing model.

B.Data storage in cloud computing

Cloud storage means "*the storage of data online on the cloud*" wherein a company's data is stored in and accessible from multiple distributed and connected resources that comprise a cloud.

Cloud storage can provide the benefits of greater accessibility and reliability; rapid deployment; strong protection for backup, archival and disaster, recovery purposes; and lower overall storage costs as a result of not having to purchase, manage and maintain expensive hardware. But, cloud storage does have the security and compliance concerns [2].

II. LITERATURE SURVEY

***A. Attribute-based Access Control with Constant-size Ciphertext in Cloud Computing**:*

This approach proposes CP-ABE with constant cipher text size and maintains the size of cipher text and the computation of bilinear pairing at a constant value, that improves the efficiency of the system, reduce the extra overhead of space storage, data transmission and computation. A hierarchical access control system supports inheritance of authorization which reduces the burden and risk in the case of single authority.

Approach:
CP-ABE consists of four polynomial time algorithms:
The data owner first encrypts the data file using asymmetric key DEK and then encrypts DEK by using the proposed scheme with a specific access control policy. The data owner uploads the final ciphertext and stores it in the cloud servers. Whether a user can access and de-crypt the data file depends on how to obtain the symmetric key, which is decided by the user"s set of access attributes.

This algorithm contains 4 sub algorithms.

1. Setup : This algorithm takes as input the initial information such as security parameter and attribute universe description, and outputs a public key *PK* and master secret key *MK*.
2. Encrypt : This algorithm takes as input a public key *PK* , a message *M* and an access structure , , and outputs a ciphertext *CT* .
3. KeyGen : This takes as input *MK* and, and outputs a secret key *SK*, with An attribute set for a user.
4. Decrypt : This algorithm takes as input *PK*, a secret key *SK* and *CT* , and outputs a message *M* if and only if the set of attributes satisfies an access structure *t* , is associated with the ciphertext.

How they achieved constant size cipher text policy

In order to ensure the confidentiality and integrity of the data, owners of data will store the encrypted data files in the cloud and realize access control to the files bacon trolling the decryption ability of users. The complexity of the CP-ABE algorithm means it is not suitable to encrypt large data files. Therefore, we first encrypt the data file using a symmetric data encryption key DEK and get the same ciphertext of data files as [10]. Then we encrypt DEK using the CP-ABE algorithm with constant-size ciphertext and obtain the ciphertext of DEK. Therefore, users can access the data file by decrypting the ciphertext of DEK and the ciphertext of the data file in turn [6].

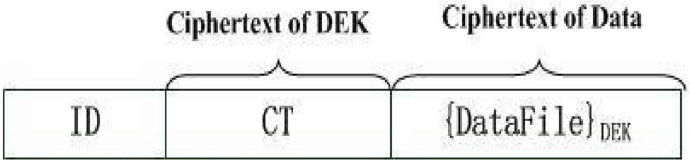


Fig. 1 :Structure of File storage

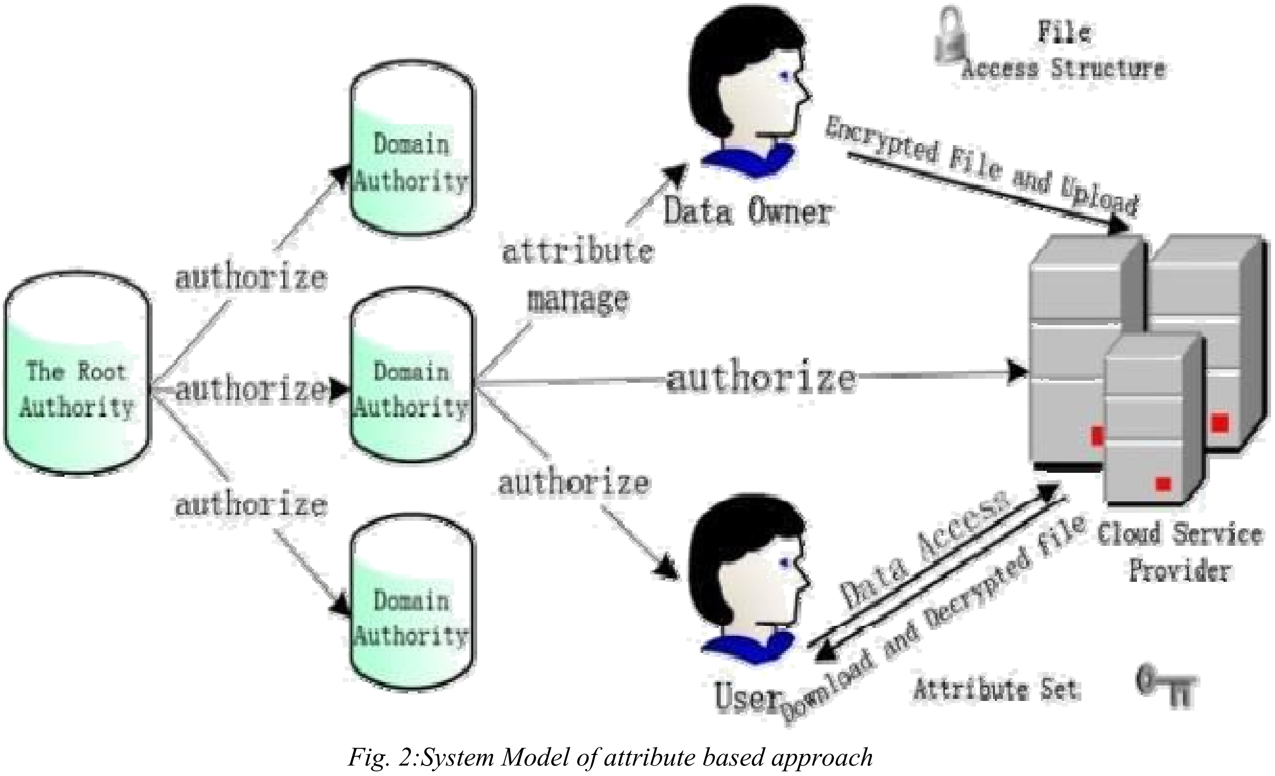


Fig. 2:System Model of attribute based approach

.Pros and cons of this approach:
Pros:

1. Hierarchical attribute based system
2. Risk factor minimized
3. Attribute based access control
4. Efficient
5. Less Cost
6. Less burden on single authority

Cons:

1. High complexity because of bilinear pairing evaluation
2. Constant size cipher text so more burden
3. Not practical because of constant size cipher text policy.
4. Exponential operation required for constant size cipher text operation.

B. *Two-Factor Data Security Protection Mechanism For Cloud Storage System*

This algorithm allows a sender to send an encrypted message to a receiver through a cloud storage server. The sender only needs to know the identity of the receiver but no other information (such as its public key or its certificate). The receiver needs to possess two things in order to decrypt the cipher text. The first thing is his/her secret key stored in the computer. The second thing is a unique personal security device which connects to the computer. It is impossible to decrypt the cipher text without either piece.

Approach:

The encryption process is executed twice. First encrypt the plaintext corresponding to the public key or identity of the user. Then encrypt it again corresponding to the public key or serial number of the security device. For the decryption stage, the security device first decrypts once. The partially decrypted ciphertext is then passed to the computer which uses the user secret key to further decrypt it. Without either part (user secret key or security device) one cannot decrypt the ciphertext. If the user has lost his security device, then his/her corresponding ciphertext in the cloud cannot be decrypted forever! That is, the approach cannot support security device update/ revocability.

Real world implemented example: At AT&T labs, in a druva system, a message is first encrypted under a user key k1, and next uploaded to a cloud server. The user key k1 is further encrypted by another user key k2, and stored in the server as well. The key k2 is held by the user. When retrieving the message, the user needs to use k2 to recover k1 which is further used to recover m. It is undeniable that this message-key encrypt mechanism is much better than the mode only using a single key to encrypt an outsourced data, and storing the ciphertext along with the key in the server. Nevertheless, this mechanism suffers from a potential risk in practice. Once the user loses the key k2, all data of the user stored in the cloud cannot be retrieved. The lack of revocability for encryption factor limits the flexibility of the system [7].

Pros and cons
Pros:

1. High level Security
2. Double encryption Cons:

Cons:

1. Revocability difficult
2. Cost more

C. Shared authority based privacy preserving authentication protocol

The proposed system has a shared authority based privacy-preserving authentication protocol (SAPA) to address above privacy issue

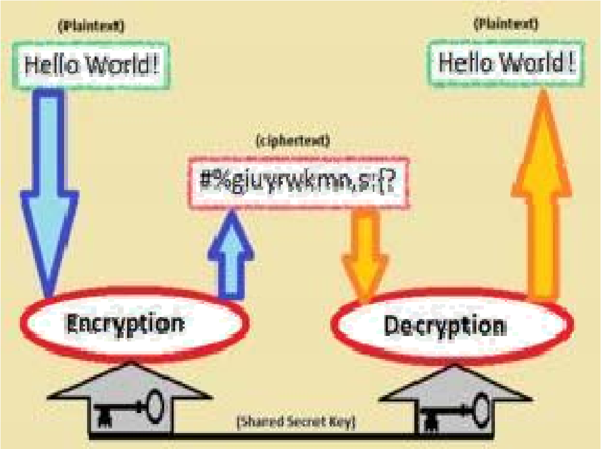


Fig 3: Encryption Process

The main goals are as follows.
1) Identify a new privacy challenge in cloud storage, and address a subtle privacy issue during a user challenging the cloud server for data sharing, in which the challenged request itself cannot reveal the user‟s privacy no matter whether or not it can obtain the access authority.
2) Authentication protocol to enhance a user‟s access request related privacy, and the shared access authority is achieved by anonymous access request matching mechanism.
3) Apply cipher text-policy attribute based access control to realize that a user can reliably access its own data fields, and adopt the proxy re-encryption to provide temp authorized data sharing among multiple users.

Approach:
A shared authority based privacy preserving authentication protocol (SAPA) for the cloud data storage, which realizes authentication and authorization without compromising a user‟s private information.
{Ua, *Ub}* respectively generate the session identifiers *{sidUa* , *sidUb }*, extract the identity tokens *{TUa* , *TUb}*, and transmits
{sidUa // *TUa* , *sidUb* // *TUa }* to *S* as an access query to initiate a new session. Accordingly, we take the interactions of *Ua* and
S as an example to introduce the following authentication phase. Upon receiving *Ua*‟s challenge, *S* first generates a session identifier *sidSa* , and establishes the master public key *mpk* = (*gi; h; hi;*BG*; e*(*g; h*)*;H*) and master privacy key

msk = (*_; g*). Thereinto, S randomly chooses _ ∈ Zq, and computes gi = gαi and hi = hαi−1 (i = {1; :::; n} ∈ Z∗). S randomly chooses _ ∈ {0; 1}∗ , and extracts Ua‟s access authority policy PUa = [pij]n×m (pij ∈ {0; 1}), and Ua are assigned with the access authority on its own data fields DUa within PUa ‟s permission. S further defines a polynomial FSa (x; PUa) according to PUa and TUa . S computes a set of values {MSa0, MSa1, {MSa2i},

MSa3, MSa4} to establish the ciphertext CSa = {MSa1; {MSa2i};MSa3;MSa4}, and transmits sidSa

Authentication*:* The ciphertext-policy attribute based access control and bilinear pairings are introduced for identification between *Uθ* and *S*, and only the legal user can derive the ciphertexts. Additionally, *Uθ* checks the re-computed ciphertexts according to the proxy re-encryption, which realizes flexible data sharing instead of publishing the interactive users‟ secret keys.

- Data Anonymity: The pseudonym PIDU are hidden with hash function so that other entities cannot derives the real values by inverse operations. Hence, an adversary cannot recognize the data, even if the adversary intercepts the transmitted data, it will not decode the full-fledged cryptographic algorithms.
- *User Privacy:* The access request pointer (e.g., *RUx U_*) is wrapped along with H(sidS|| PIDU_) for privately informing *S* about *Uθ*‟s access desires. Only if both users are interested to communicate with each other, *S* will establish the re-encryption key *kU_* to realize authority sharing between *Ua* and *Ub*. Otherwise, *S* will temporarily reserve the desired access requests for a certain period of time, and cannot accurately determine which user is actively interested in the other user‟s data fields.
- Forward Security*:* The dual session identifiers *{sidS , sidU}* and pseudorandom numbers are introduced.

Pros and cons of this approach:

Pros:

1. More security
2. Works fine with untrusted cloud server
3. Attribute based access request
4. flexible

Cons:

1. More space overhead
2. High complexity

III. PROPOSED SYSTEM

- I am combining various approaches of encryption algorithm so that we can achieve security with flexibility.
- Access control policy will be based on number of attributes but the size of cipher text will be varying.
- By using public key which is Role based encryption and master key generation is used for attribute based access control. So while encryption, using random attributes of files some unique master key will be generated.
- I have tried to combine Identity based encryption and attribute based encryption to generate secret key which will act as a private key for a user.
- I am using 16 bit key format so it will be difficult to crack for stranger.
- Encrypted file will be saved at specified path , as well original file will also get save so we can achieve safe and backup kind of thing .

Limitations of proposed system:

- It can work fine with text , pdf file ,word file .
- This encryption method is not applicable for image or media file.
- User has to remember key which is of 16 bit.
- Space overhead because of original and encrypted copy will be saved in desktop before sending it to server.
- Because of attribute based encryption, time linearly depends on number of attributes selected for generation of master key.

IV. IMPLEMENTATION

Modules:

1. Owner
2. User
3. Access Control
4. Cloud Service Provider
5. Encryption & Decryption
6. File Download
7. Trusted Third Party

*A. System Configuration***:-**

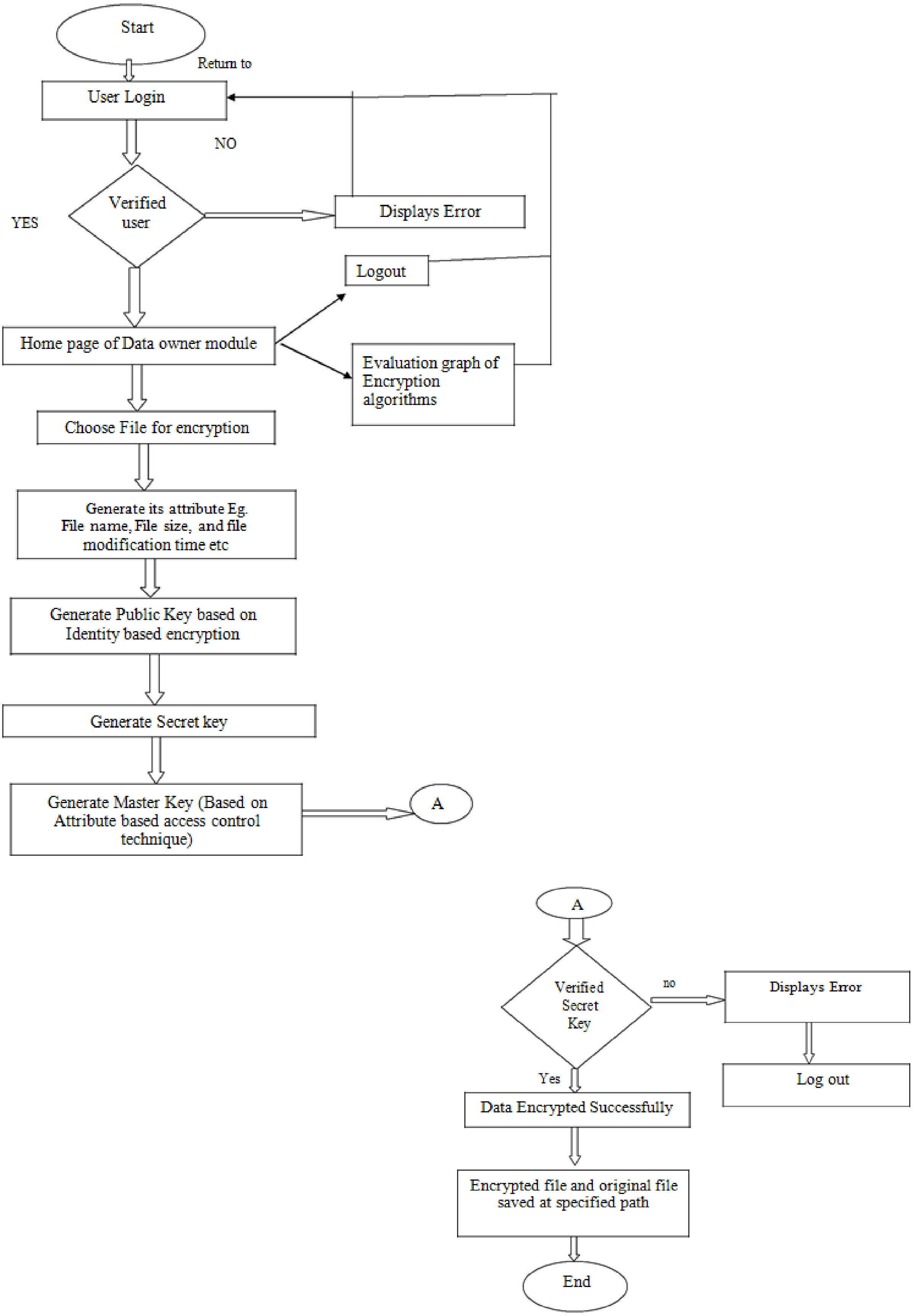
H/W System Configuration:-

Processor	-Pentium 3rd generation
Speed	**-1.1 GHz**
RAM	-256 MB (min)
Hard Disk	-20 GB
Floppy Drive	-1.44 MB
Key Board	-Standard Windows Keyboard
Mouse	- Two or Three Button Mouse
Monitor	-SVGA

S/W System Configuration:-

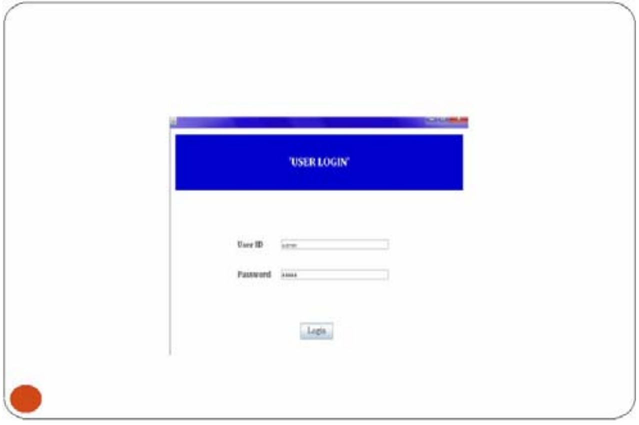
Operating System	:Windows95/98/2000/XP
Application Server	: Tomcat5.0/6.X
Front End	: HTML, Java, JSP
Scripts	: JavaScript.
Server side Script	: Java Server Pages.
Database	:My sql
Database Connectivity	: JDBC.

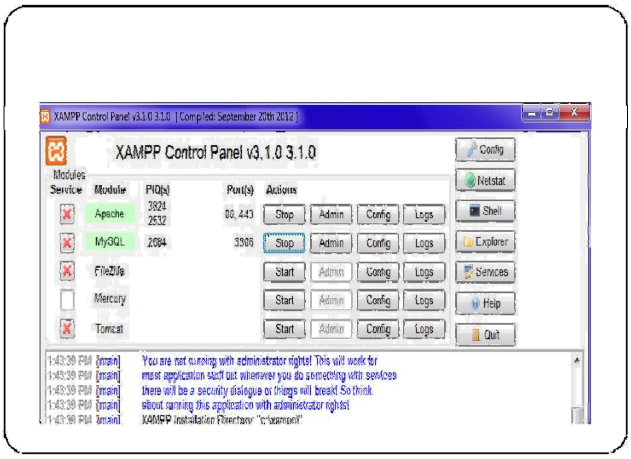
Fig. 4 *Data Flow Diagram for Proposed System*


Start
Return to
User Login
NO
YES
Verified user
Displays Error
Logout
Home page of Data owner module
Evaluation graph of Encryption algorithms
Choose File for encryption
Generate its attribute Eg. File name, File size, and file modification time etc
Generate Public Key based on Identity based encryption
Generate Secret key
Generate Master Key (Based on Attribute based access control technique)
A
A
Verified Secret Key
no
Displays Error
Log out
Yes
Data Encrypted Successfully
Encrypted file and original file saved at specified path
End

Some snapshots of implementations

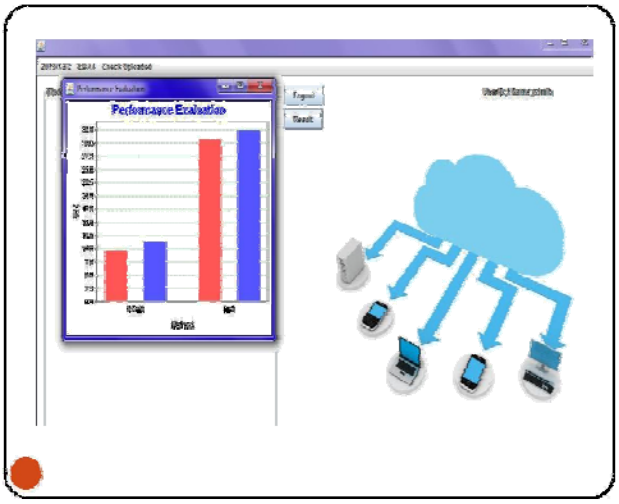
□ User Login Form

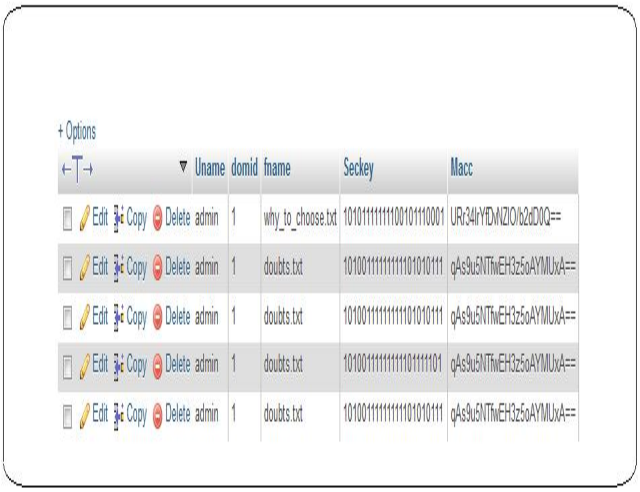




```
1:43:39 PM  [main]   You are not running with administrator rights! This will work for
1:43:39 PM  [main]   most application stuff but whenever you do something with services
1:43:39 PM  [main]   there will be a security dialogue or things will break! So think
1:43:39 PM  [main]   about running this application with administrator rights!
1:43:39 PM  [main]   XAMPP Installation Directory: "c:\xampp\"
```

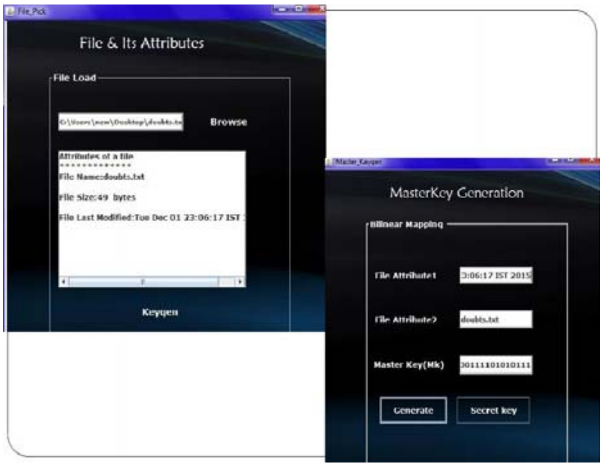
XAMPP for Database creation





	Uname	domid	fname	Seckey	Macc
□ Edit Copy Delete	admin	1	why_to_choose.txt	1010111111100101110001	URr34IrYfDvNZIO/b2dD0Q==
□ Edit Copy Delete	admin	1	doubts.txt	1010011111111101010111	qAs9u5NTfwEH3z5oAYMUxA==
□ Edit Copy Delete	admin	1	doubts.txt	1010011111111101010111	qAs9u5NTfwEH3z5oAYMUxA==
□ Edit Copy Delete	admin	1	doubts.txt	1010011111111101111101	qAs9u5NTfwEH3z5oAYMUxA==
□ Edit Copy Delete	admin	1	doubts.txt	1010011111111101010111	qAs9u5NTfwEH3z5oAYMUxA==

Table for Secret key



C:\Users\new\Desktop\doubts.tx

Attributes of a file
****
File Name:doubts.txt
File Size:49 bytes
File Last Modified:Tue Dec 01 23:06:17 IST

File Attribute1: 3:06:17 IST 2015
File Attribute2: doubts.txt
Master Key(Mk): 0111101010111

V. Conclusions and Future work

Cloud computing is an emerging trend of IT delivery that intends to make the Internet the ultimate home of all computing resources like storage, computations, and accessibility. It is a technology that will be adopted if the areas of concerns like security of the data will be covered with strong mechanism. The strength of cloud computing is the ability to manage risks in some particular security issues. My suggested algorithm for data security shows its need. Security algorithms mentioned for encryption and decryption can be implemented in future to enhance security framework over the network. In the future, I will try to develop algorithm to make advancement to my research by providing algorithm for encryption, decryption and batch auditing to provide authenticatication.

Below Matrix presents Performance Comparison of different approaches based on various parameters which that approach fulfils.

Parameter	**Attribute based access control with constant cipher text**	**Two factor data security protection mechanism**	**Shared authority based privacy preserving protocol**	**Proposed System**
Platform	Cloud computing	Cloud computing	Cloud computing	Cloud computing
Key Size	Constant(16 bit)	Variable	Variable	Constant
Scalability	Scalable	Scalable	Scalable	scalable
Security Level	Secured	Very high	High	high
Access Control Policy	Hierarchical based(Inheritance of authorization)	Distributed	Third party authorization scheme	Hierarchical
Scheme of working	Constant Bilinear Pairing for constant size cipher Text	Identity based double encryption mechanism is used.	Data authorization, Preservation, Proxy re encryption is achieved .	Re encryption Technique used.
Overhead	Reduced space storage	Extra running time for security device recognition	More	Space overhead
Revocation Method	Not used.	Allows revocability of device	Not used	Not used
Cost	Less	Moderate	More	Less
Computational complexity	Polynomial	Less	More	Less

REFERENCES

[1] H. Takabi, J.B.D. Joshi, and G-J. Ahn, “Security and Privacy Challenges in Cloud Computing Environments,” IEEE Security & Privacy, vol. 8, no. 6, 2010.

[2] R. Buyya, C. S. Yeo, and S. Venugopal, Market oriented cloud computing: vision, hype, and reality, for delivering IT services as computing utilities, Proc. 10th IEEE International Conference on High Performance Computing and Communications.

[3] Rohit Bhadauria and Sugata Sanyal, A Survey on Security Issues in Cloud Computing and Associated Mitigation Techniques. International Journal of Computer Applications, Volume 47- Number 18, June 2012, On page(s): 47-66.

[4] Zhidong Shen, Li Li , Fei Yan, Xiaoping Wu , Cloud Computing System Based on Trusted Computing Platform, International Conference on Intelligent Computation Technology and Automation, Volume 1, May 2010, On page(s): 942-945.

[5] Wei Teng,Geng Yang,Member, IEEE,Yang Xiang,SeniorMember, IEEE, Ting Zhang and Dongyang Wang “Attribute-based Access Control with Constant-size Ciphertext in Cloud Computing”, IEEE TRANSACTIONS ONCOMPUTERS, VOL. 6, NO. 1, JANUARY 2014

[6] Kan Yang, Student Member, IEEE, and Xiaohua Jia, Fellow, IEEE “Expressive, Efficient, and Revocable Data Access Control for Multi-Authority Cloud Storage”, IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 25, NO. 7, JULY 2014

[7] Joseph K. Liu, Kaitai Liang_, Willy Susilo, Jianghua Liu, Yang Xiang “Two-Factor Data Security Protection Mechanism for Cloud Storage System” IEEE Transactions on Computers ,2015.

[8] Hong Liu, Student Member, IEEE, Huansheng Ning, Senior Member, IEEE, Qingxu Xiong, Member, IEEE, and Laurence T. Yang, Member, IEEE “Shared Authority Based Privacy-preserving Authentication Protocol in Cloud Computing “IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS VOL:PP NO:99 YEAR 2014.