RESEARCHERID
THOMSON REUTERS

[ICRTCET-2018] ISSN 2348 – 8034
Impact Factor- 5.070

GLOBAL JOURNAL OF ENGINEERING SCIENCE AND RESEARCHES

MULTILEVEL SECURITY AND DATA PRIVACY IN CLOUD ECOSYSTEM USING COMPOSITE CRYPTOGRAPHIC SYSTEM

Supriya Patil[*1], Priyanka Padki[2], Ramya V[3] & Ramya B J[4]
[*1,2,3&4]Department Of Computer Science, Rajarajeswari College Of Engineering Bangalore, India

ABSTRACT

The development in the field of cloud computing is fast and rapid. This in the context of internet environment opens up a lot of challenging scenarios for security of the data on cloud. This paper proposes a framework for secure ecosystem where we use authentication at many levels, using a combination of encryption techniques and we also propose a new COMPOSITE CRYPTOGRAPHIC SYSTEM (CCS) that combines the benefits of different types of cryptography.

Keywords: *Composite Cryptographic System, secure environment, authentication at many levels, Dropbox.*

I. INTRODUCTION

Cloud computing is causing a major shift in the IT industry. The advancement of technology and the increasing demand of customers have led many associations to use the cloud services and their infrastructure. Though these services are being widely used by several customers but the major concern is with the security and privacy of the cloud services that still continues to be a matter of research [1]. With the advanced technology, Cloud services can be retrieved easily through phones over the internet allowing the customers to send and receive all the important data. In order to attract the customers to make use of the cloud and its services it becomes important for the cloud service providers to provide security for the huge amounts of data. Since in today's world almost everything from browsing to transferring of some important data is through the internet, Security becomes one of the important aspects. With the cloud service providers taking care of huge amounts of customer's data it is necessary to give the customers a trusted service where they can rely on the cloud service providers for the entire security and privacy of their data. When dealing with cloud security there are many features that have to be considered which includes multi factor authentication, data protection and data transparency. Of all, data encryption becomes one of the important means of ensuring data protection, and transparency between users.

Though there are many algorithms that ensure security such as the RSA [10], AES [11] and much more they still have their own drawbacks. Therefore, our focus in this paper is to create a composite cryptographic system wherein we aim at providing a more secure cloud environment by using the full benefits of both a symmetric and an asymmetric encryption technique and create multiple levels of security that includes encrypting the password, generating one time passwords, and transferring of users data to cloud. Also, the paper mainly focuses on encryption schemes where we use advanced encryption standards (AES) for encrypting the user's data and Rivest-Shamir-Adleman (RSA) for the decryption processes. The paper also focuses on the data transmission operations.

The rest of the paper is as follows where Section II focuses on the security issues and Section III deals with the proposed system and Section IV describes the algorithm being used finally Section V elucidates the conclusion and future work.

II. SECURITY CONCERNS IN CLOUD

- **Hijacking:** Hijacking is a process of acquiring illicit access over certain authorized services. Attackers now have the ability to use your login information to access data stored on the cloud. Attackers can alters and manipulate information through hijacked credentials. It accounts for techniques like fraud and exploitation of software. This is one of the top most threat in cloud computing.

- **Integrity, Availability, and Durability:[5]** Customer's data in the cloud is of two types security in storage clouds and security in compute clouds. Basic plans for data integrity are Proof of Retrieval and Provable Data Possession. PDP checks whether the file is retained in server or not where in POR,users can get back the files from the servers. Categories in data integrity guarantees that stored data can also be retrieved at any time. In this case, the customer could simply question the Cloud for every data the customer has stored. Although this would prove possession and unrecoverable, it is very costly in terms of network bandwidth.
- **External Invaders:** The problems or attacks that come from outside is usually referred to as external invaders[12]. Data security plays a crucial role in cloud security. The cloud service providers must ensure that the customer is given the full guarantee and confidence that their data is secure at every point of transmission and no external invaders are given the access to sensitive information and this poses to be one of the main security issues on cloud.[9]
- **Insider threats:** This kind of threats can be unexpected but such threats can exist. An attacker from inside the organization can make use of his/her advantages provided by the organization and can pose a threat to the organization by silently accessing the sensitive or confidential information that is stored in cloud and can pose a major threat and happens to major concern.

III. SYSTEM DESIGN

From past many years, Cloud computing has become an expeditious development in the IT field though there are many issues in it providing security is one of the biggest challenge, so in order to attract more customers to use cloud our focus must be to provide security using cloud security which is the set of policies used to protect data and infrastructure in the cloud.

A) Dataflow design:

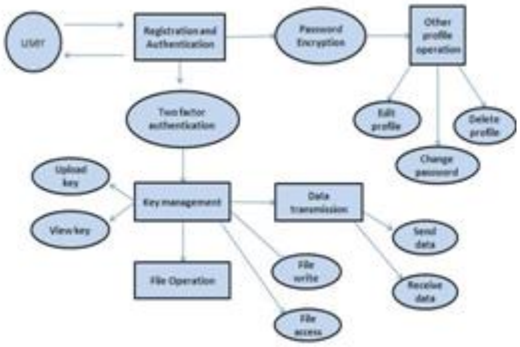


Fig-1: Dataflow of overall system operation

The mentioned fig-1 depicts the overall systems dataflow which include the following aspects:

- **USER ACCOUNT CREATION** : The user creates an account where he provides his personal information and can also perform Other operations from his account like Login, Logout, Edit profile, Delete profile, change password, and retrieve password in case he/she has forgotten it. Only the administrators of the project whom we consider as the owners of the SQLiID portal, will be performing this operation.
- **PASSWORD AND TWO-FACTOR AUTHENTICATION** :The users profile would be **Password encrypted**: Once the account is created he/she would be able to make any changes related to his profile(edit or delete profile, change password)

  Two factor authentication: To avoid hackers to gain access to a person's devices ,User's profile is authenticated by providing One-time password to one complete user session which ensure if he/she is the genuine person and also allocates an extra layer of security.
- **KEY MANAGEMENT**: This helps the users of the portal to superintend their secret keys. The users will be imparted with an interface to upload their secret keys where in the secret key must be in multiples of 128

bits. The users will also be provided with an interface where they can view the list of all the keys uploaded by them and also they can perform other operations like downloading the keys(in order to view the uploaded key) and deleting the keys in case they no longer need it. It is mandatory for the users to upload at least one key before they proceed further for data write operation. However, there is no limit on the number of keys the user is allowed to upload in our portal.

- **DATA TRANSMISSION**: The keys provided would be used for **Data transmission**, where the process of sending and receiving the data occurs.
- **FILE OPERATION**: where the user would be able to perform file write and access operation

B) Architecture Design:

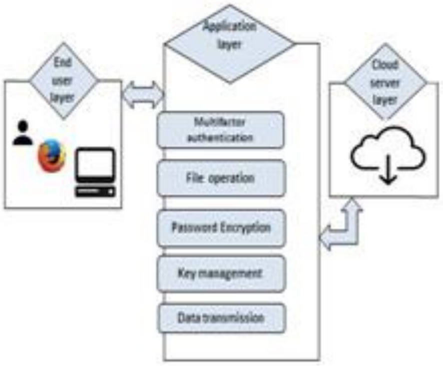


Fig-2: System Architecture

As shown in fig-2 Security measures have been taken care at all levels.

1. **END USER LAYER**: The end user can access Application from any of the web browser from his local machine.

2. **APPLICATION SERVER LAYER**: The information provided by the user forms the base for this layer and therefore he can access the application which includes security at each level that includes

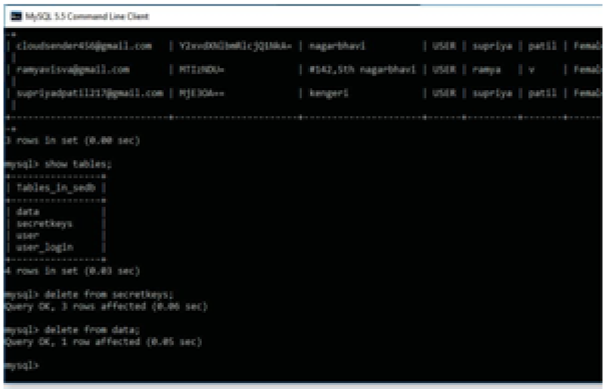
- **MULTIFACTOR AUTHENTICATION** like OTP and password. Two-factor authentication furnish an subsidiary layer of security and makes attackers tough to gain access to a person's devices and online accounts, since speaking the victim's password alone is not enough to pass the authentication check.
- **KEY MANAGEMENT** This module helps the users of the portal to manage their secret keys. The users will be provided with an interface to upload their secret keys**,** where the user has the access to upload, delete or download a key. It is mandatory for the users to upload at least one key before they proceed further for data write operation. However, there is no limit on the number of keys the user is allowed to upload in our portal
- **FILE WRITE OPERATION** This module allows the users to perform the file write operation on the cloud. The user will be provided with an HTML interface where they can browse the file to be uploaded to the cloud. It is mandatory for the users to upload at least one of their secret keys before accessing this module. The users will then be provided with an option to select any of the keys uploaded by them which has to be used for performing the composite cryptography on the file he/she has uploads.
- **FILE READ OPERATIONS:** This module can be used by the end users to download the files they had uploaded into the cloud. This module performs the file read operation from the cloud and performs the decryption operation on the file to be read using the composite cryptographic system (CCS) with the same key used for encryption. The user will be able to see the decrypted file and will be downloaded into the client's system.
- **DATA TRANSMISSION** When the end users send any confidential data from their devices: typically a laptop or desktop, to the cloud application, there are some possibilities that the hacker or the third party can steal the confidential data during the data transmission from the client device to the cloud application. To avoid this, the

confidential data must be encrypted from the client end (laptop/desktop) itself before the data transmission begins.

3. **CLOUD SERVER LAYER**: This layer receives encrypted data from the APPLICATION LAYER which is further being encrypted and stored to provide additional security to data.

C) Database Design:

During the registration phase, the end users are going to select their passwords for their accounts. All the profile information including the password will be stored in the relational database management system like MySQL. However, there are chances that the attacker might compromise the RDBMS and hence getting an illegal access to the user's profile data. In such situations, the attacker will also get an access to the user's password and hence bypassing the security layer of the cloud application. To avoid this, the user's password will not be stored as a plain text on MySQL, instead it will be stored as an encrypted text as shown in the fig-3



```
-+
| cloudsender456@gmail.com    | Y2xvdXNlbmRlcjQ1NkA= | nagarbhavi           | USER | supriya | patil | Femal
 |
| ramyavisva@gmail.com        | MTI1NDU=             | #142,5th nagarbhavi  | USER | ramya   | v     | Femal
 |
| supriyadpatil1217@gmail.com | MjE3OA==             | kengeri              | USER | supriya | patil | Femal
 |
+-----------------------------+----------------------+----------------------+------+---------+-------+------
-+
3 rows in set (0.00 sec)

mysql> show tables;
+----------------+
| Tables_in_sedb |
+----------------+
| data           |
| secretkeys     |
| user           |
| user_login     |
+----------------+
4 rows in set (0.03 sec)

mysql> delete from secretkeys;
Query OK, 3 rows affected (0.06 sec)

mysql> delete from data;
Query OK, 1 row affected (0.05 sec)

mysql>
```

Fig-3. MySQL Database of the System containing users encrypted password and other details.

IV. ALGORITHM

In order to understand the overall working of the system it is better to express it in the form of an algorithm. We in our system introduce **composite cryptographic algorithm.** This would be helpful as it presents the complete working of our system starting from validating the user until storing and extracting the client's data from the cloud. Composite Cryptography has a thin line between slow but safe cryptography and unsafe but fast cryptography. Composite Cryptography combines the benefits of both RSA(symmetric) as well as AES(asymmetric) algorithms and thus considered a highly secure type of encryption.

ENCRYPTION PROCESS:

Step1:User creates an account .
Step2: The user is prompted to enter a password further which he would be receiving a one-time password for verification purposes. This is where we are implementing 2-factor authentication.
Step3:The user must upload a secret key which must be multiples of 128 bits.
Step4: This step involves reading the secret key that is uploaded by the user and uploading a data file that needs to be encrypted by choosing the key that is uploaded already in order to perform the encryption process.
Step5: Generating the key pairs (public and private) using RSA algorithm.
Step6: Encrypting the data file using the key file. AES symmetric encryption is used here in order to encrypt the data file uploaded by the user.
Step7: Further encrypting the key file that was uploaded earlier(step 4) using the public key that was generated(RSA encryption is used).
Step8: Store the encrypted data file on cloud.

Step9: Store the encrypted key file and the generated key pairs locally for future use.

DECRYPTION PROCESS:
Step1: Read the generated private key(step5). Here we use private key for decryption purpose.
Step2: Read the key file that was stored locally earlier during the encryption process.
Step3: Decrypt the key file using the private key (RSA encryption scheme).
Step4: Now read the encrypted data file that was stored earlier from the cloud and decrypt the file using the decrypted key file.

V. IMPLEMENTATION

This section focuses on the implementation of composite cryptographic algorithm. The technical aspects of implementation of the system are realized as explained: we are implementing algorithm using Eclipse IDE using Apache Tomcat which is an open source web server and servlet container. To run this server we first need to download eclipse IDE and install it after installing successfully server gets activated. We also make use of Database MYSQL the world's most widely used open source relational database management system (RDBMS) that runs as a server providing multi-user access to a number of databases. Talking of our proposed work we have our Dropbox account where an Application is created by generating a code and thus linked with eclipse. The implementation here also includes data transmission operations where we will be able to encrypt the user’s data and store it in the cloud and retrieve the decrypted data whenever the user needs it. The following implementation exhibits the working of the proposed algorithm.

A) IMPLEMENTATION OF USER PROFILE OPERATIONS: In this step, the user is actually requested to create an account that includes his/her personal information.

Account operations module provides the following functionalities to the end users of our project.

- Register a new seller/ buyer account
- Login to an existing account
- Logout from the session
- Edit the existing Profile
- Change Password for security issues
- Forgot Password and receive the current password over an email
- Delete an existing Account

Fig-4 shows the flowchart of the user profile operations.

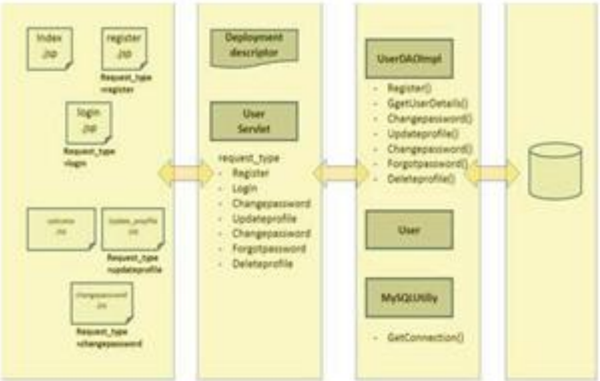


Fig-4. The flowchart of the user profile operations.

Account operations module will be re-using the DAO layer to provide the above functionalities.

The DAO layer is the service layer which provides database CRUD (create, update, read, and delete) services to the other layers. It will contain the POJO classes to map the database tables into java object. It also contains the Util classes to maintain the database connections.

B)IMPLEMENTATION OF TWO FACTOR AUTHENTICATION: The 2 factor authentication includes an encrypted password that is given by the user while creating an account and also a one-time password that would be sent to his email or personal number provided by the user to make sure that he/she is the genuine person. 2FA can be divergence with single-factor authentication (SFA), a security process in which the user provides only one factor -- typically a password. Two-factor authentication provides an extra layer of security and makes it harder for hackers to gain access to a person's devices and online accounts, because knowing the victim's password alone is not enough to pass the authentication check.

User can access the application by creating a new account, after creating the account the user can now login where he/she is prompted to enter his password. Further process is represented in Fig-5.

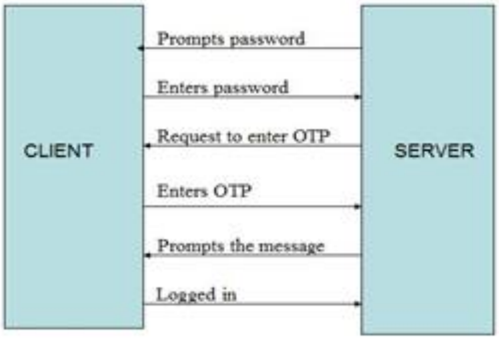


Fig-5.Two factor authentication process.

IMPLEMENTATION OF KEY MANAGEMENT: This Module allows the user to upload the keys as shown in fig-6 and also allows the user to view the uploaded keys as shown in fig-7. The users will be provided with an interface to upload their secret keys. The secret key must be in multiples of 128 bits.

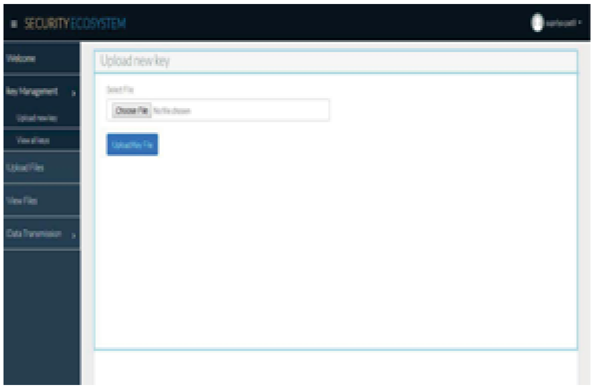
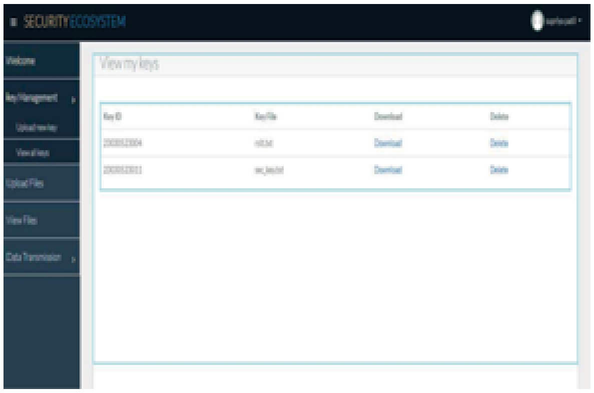


Fig-6. The snapshot of the upload key of the key management.



View my keys

Key ID	Key File	Download	Delete
2003052004	rsit.txt	Download	Delete
2003052011	sec_key.txt	Download	Delete

Fig-7. The snapshot of the view key of the key management

E) IMPLEMENTATION OF FILE WRITE OPERATIONS: In this module all the encrypted data that is provided by the user would be transmitted to the cloud from the application layer which in turn would be encrypted to provide additional level of security. Fig-8 shows the flowchart of the file write operations.

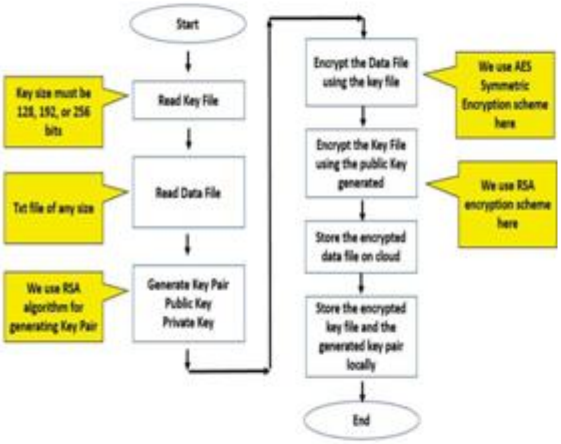

Start
Key size must be 128, 192, or 256 bits
Read Key File
Txt file of any size
Read Data File
We use RSA algorithm for generating Key Pair
Generate Key Pair Public Key Private Key
Encrypt the Data File using the key file
We use AES Symmetric Encryption scheme here
Encrypt the Key File using the public Key generated
We use RSA encryption scheme here
Store the encrypted data file on cloud
Store the encrypted key file and the generated key pair locally
End

Fig-8. The flowchart of the file writes operations.

F) *IMPLEMENTATION OF FILE ACCESS OPERATIONS*: This module includes implementation of file view and delete operations.Also performs the decryption operation using the composite cryptographic system with the same key used for encryption. The user will be able to see the decrypted file and will be downloaded into the clients system.

Fig-9 shows the flowchart of the file access operations

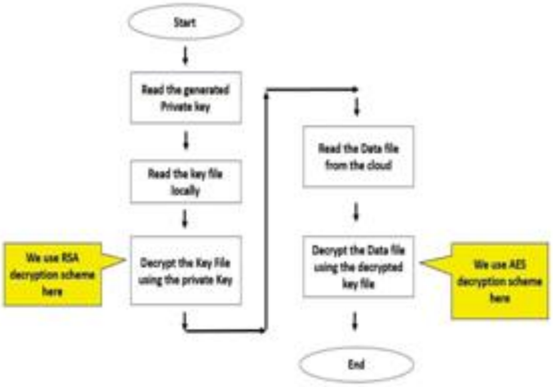
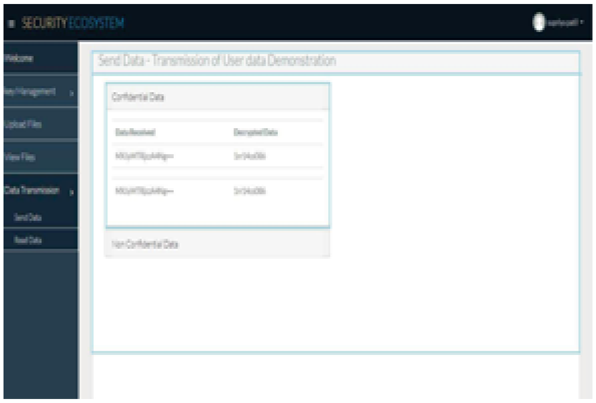

Start
Read the generated Private key
Read the key file locally
Decrypt the Key File using the private Key
We use RSA decryption scheme here
Read the Data file from the cloud
Decrypt the Data file using the decrypted key file
We use AES decryption scheme here
End

Fig-9.The flowchart of the file write operations.

IMPLEMENTATION OF DATA TRANSMISSION OPERATIONS: This includes the process of implementing the send and receives operations that users send any confidential data from their devices: typically a laptop would help in the transmission of data. When the end or desktop, to the cloud application, there are some possibilities that the hacker or the third party can steal the confidential data during the data transmission from the client device to the cloud application. To avoid this, the confidential data must be encrypted from the client end (laptop/desktop) itself before the data transmission begins. This module allows the users of our portal to experience how this kind of security has been implemented. Fig-10 shows how confidential data's are encrypted



Send Data - Transmission of User data Demonstration

Confidential Data

Data Received	Decrypted Data
[illegible]	[illegible]
[illegible]	[illegible]

Non Confidential Data

Fig-10. The snapshot of how confidential data are encrypted in data transmission.

LIVE CLOUD DEPLOYMENT: Finally after the implementation of all the modules the entire application is deployed on live cloud so that it is available to everyone across the globe and can be accessed by anyone. In our system

we use Dropbox.
Fig-11. Shows the snapshot of the Dropbox

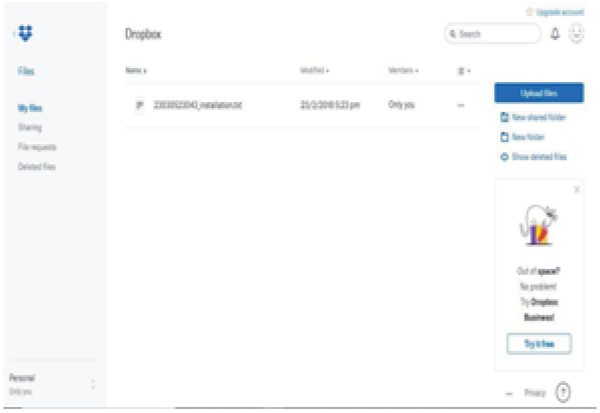
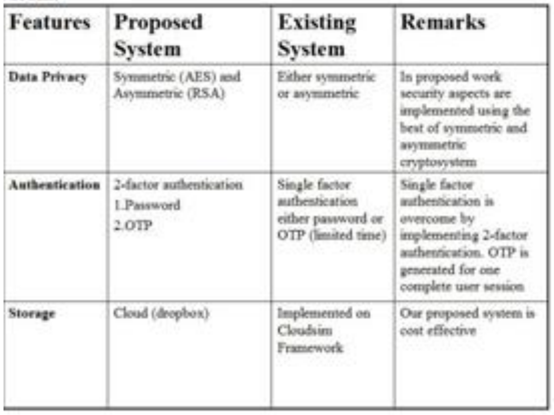


Fig-11. The snapshot of the Dropbox.

VI. COMPARATIVE ANALYSIS OF EXISISTING VERSUS PROPOSED WORK

The comparative analysis basically gives us a brief description about the advances prior to the existing systems and the current system. Though the Existing systems implemented security the issues were not taken care at all the levels which is overcome in our proposed system. Also, the single factor authentication in prior system have been replaced with the strongest form of authentication which happens to be multi factor authentication. [13], [14].

Table-1 Comparative analysis of proposed and existing system



Features	Proposed System	Existing System	Remarks
Data Privacy	Symmetric (AES) and Asymmetric (RSA)	Either symmetric or asymmetric	In proposed work security aspects are implemented using the best of symmetric and asymmetric cryptosystem
Authentication	2-factor authentication 1.Password 2.OTP	Single factor authentication either password or OTP (limited time)	Single factor authentication is overcome by implementing 2-factor authentication. OTP is generated for one complete user session
Storage	Cloud (dropbox)	Implemented on Cloudsim Framework	Our proposed system is cost effective

VII. CONCLUSION AND FUTURE WORK

This paper mainly focuses on Composite Cryptographic System that incooperates the benefits of different types of encryption schemes. The cloud environment developed here ensures that the user data is secure and trusted and also takes care of the security issues at various levels so that the user data is not leaked or misused at any cost thereby preventing huge data loss. In the design process we also make use of 2 factor authentication method in order to check the genuinity of a person. The future work basically can include methods or system and also implement data transmission operations for huge files. And it might also provide multilevel security based on password, OTP and biometrics. This is achieved by either making the system run in a multi cloud ecosystem or use some different techniques that would prevent hacking and data loss and also take care of the backup or recovery

[ICRTCET-2018] ISSN 2348 – 8034
Impact Factor- 5.070

REFERENCES

1. *Kandukuri BR, Paturi VR, Rakshit A. Cloud security issues. In: IEEE international conference on services computing, 2009.*
2. *Cheikh Brahim Ould Mohamed El Moctar; Karim Konaté " A survey of security challenges in cloud computing" 2017 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET).*
3. *Jun Huang; Jinyun Zou; Cong-Cong Xing "Competitions among Service Providers in Cloud Computing: A New Economic Model" IEEE Transactions on Network and Service Management 2018*
4. *R. Barona; E. A. Mary Anita" A survey on data breach challenges in cloud computing security: Issues and threats" 2017 International Conference on Circuit ,Power and Computing Technologies (ICCPCT)*
5. *Descher M, Masser P, Feilhauer T, Tjoa AM, Huemer D. Retaining data control to the client in infrastructure clouds. In: International conference on availability,reliability and security, ARES '09, 2009, p. 9–16.*
6. *Huang, Wei, et al. "The State of Public Infrastructure-as-a-Service Cloud Security." ACM Computing Surveys (CSUR) 47.4 (2015): 68.*
7. *Aich, Asish, Alo Sen, and Satya Ranjan Dash. "A Survey on Cloud Environment Security Risk and Remedy." Computational Intelligence and Networks (CINE), 2015 International Conference on. IEEE, 2015.*
8. *Singh, Aarti, and Manisha Malhotra. "Security Concerns at Various Levels of Cloud Computing Paradigm: A Review." International Journal of Computer Networks and Applications 2.2 (2015): 41-45.*
9. *Naresh vurukonda1 , B.Thirumala Rao "A Study on Data Storage Security Issues in Cloud Computing" 2nd International Conference on Intelligent Computing, Communication & Convergence (ICCC-2016).*
10. *Harshitha Y,Seema S,Apoorva p "comparative study on rsa algorithm of multikeyword search scheme over encrypted cloud data" 2017 international Conference on Intelligent Computing and Control (I2C2)*
11. *Shady Mohamed Soliman*, Baher Magdy*and Mohamed A. Ab ElGhany " Efficient Implementation of the AES Algorithm for Security Applications" 2016 IEEE.*
12. *Srikanta Patnaik, Editor in Chief Conference Organized by Interscience Institute of Management and Technology Bhubaneswar, Odisha, India.. 2nd International Conference on" Intelligent Computing, Communication & Convergence" (ICCC-2016)*
13. *Ali Gholami ,ErwinLaure "security and privacy of sensitive data in cloud computing: a survey of recent developments " (2015)*
14. *Eman Meslhy,Sherif El-etriby,Hatem Ahemed Abd elkader "Data Security Model for Cloud Computing" Article • August 2013.*

.