JCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Volume-5, Issue-5 E-ISSN: 2347-2693

Ttpse- Trusted Third Party With Symmetric Encryption Towards Secured Cloud Storage

Shreeraghav Kulkarni[1*], Sujata Terdal[2]

[1]Department of Computer Science, PDA College of Engineering (VTU University), Karnataka, India
[2]Department of Computer Science, PDA College of Engineering (VTU University), Karnataka, India

[*]*Corresponding Author: kulkarni.shreeraghav@gmail.com, Tel.: +91-8861152777*

Online Available at: www.ijcseonline.org

Received: 20/Apr/2017, Revised: 28/Apr/2017, Accepted: 21/May/2017, Published: 30/May/2017

***Abstract*—** Mutual trust in computer security is known as accepting on the same security architecture by two participating parties. Today, most of the users prefer to keep their data in the cloud with Cloud Storage Providers (CSP), some of the popular cloud storage providers are Drop Box, SkyDrive, and Google Drive and so on. Most of the cloud storage providers operate on secured http layer, therefore they provide underneath security for any data transmission. However, users often do not know in what ways the cloud service providers uses his data. Security of the critical data (for ex. Critical health record) is extremely difficult for the user to trust the service provider completely, and keep the record as it is. Beside this, once the storage link of the cloud is shared user has very little control on the link sharing. In the past several techniques have been proposed to provide security to the data in the cloud, however, not significant work has been carried out, towards offering a solution to address the problem of lack of mutual trust. In this work we develop a unique third party solution for providing mutual trust between the user and the cloud service provider. Our application takes a user key, encrypts every contents that need to be stored in a cloud space and then stores the data. While accessing the same data user needs to provide his key, then the encrypted data is downloaded from the cloud and is decrypted locally. We use symmetric key encryption as middle layer security for the mutual trust. We also analyze the performance of three very popular symmetric key encryption techniques such as AES, 3DES, RC2 and evaluate the performance of the same. The performance of the different algorithms varies according to data loads.

***Keywords*—** Cloud Storage Provider(CSP), Mutual Trust, Trusted Third Party, Access Control, AES, 3DES, RC2.

I. INTRODUCTION

In the present time of computerized world, different associations deliver a lot of sensitive information including individual data, electronic health records, and money related information. The nearby administration of such enormous measure of information is tricky and expensive because of the necessities of high storage capacity and qualified personnel [1]. Hence, Storage-as-a-Service offered by Cloud Storage Provider (CSP) developed as an answer for relieve the weight of vast nearby information storage, and lessen the burden of maintenance cost, by means of outsourcing information storage [2], [3]. There are some concerns regarding confidentiality, integrity and access control of the data in the cloud [4]. In Cryptography, a Trusted Third Party (TTP) is an element which encourages connections between two parties who both trust the outsider; The Third Party audits all critical exchange correspondence between the parties, in view of the simplicity of making false computerized content. Cryptography is typically referred to as “the investigation of mystery” [5], [6], while these days is most connected to the meaning of encryption [7]. Encryption is the way toward changing over plain content “unhidden” into cipher text “covered up” by methods, for reasonable calculation to secure it against information assaults [8]. Unscrambling is the way toward changing over meaningless cipher content into plain content using key generated by encryption algorithm. If same key is used by both sender and recipient to scramble and decode the contents, than such method is termed as symmetric key cryptography. For key exchange secure channel is required between sender and beneficiary. Two cipher modes adopted by symmetric algorithm are: Stream cipher and block ciphers.

Asymmetric encryption is the other type of encryption where two keys are utilized. One of which is secret and one of which is public. The public key is used to scramble plaintext, whereas private key is used to unscramble the cipher text.

Encryption
Decryption
Plain Text
Cipher Text
Plain Text

Figure 1. Encryption Decryption Flow

Brief definition of common symmetric key encryption techniques [9], [10] are given below.

- Advanced Encryption Standard (AES)/Rijndael: Advanced Encryption Standard, is a symmetric square figure that can scramble information piece of 128 bits utilizing symmetric keys 128,192, or 256. AES scramble the information square of 128 bits in 10, 12 and 14 rounds depending on the key size. Brute force attack is the only effective attack known against this algorithm.
- Triple DES:Triple DES essentially develops the key size of DES by applying the algorithm three times in succession with three distinctive keys. The consolidated key size is therefore 168 bits, past the range of DES.
- RC2:RC2 is a symmetric square figure that operates on 64 bit quantities. It utilizes variable size key, but 128 bit key would normally be considered good. The algorithm expands a single message by up to 8 bytes.

Rest of the paper is organized as follows, section I contains the introduction of cloud computing security, section II contains related work, section III contains existing system, section IV contains proposed system, section V contains system design, section VI contains discussion and results, section VII contains conclusion and future work.

II. Related Work

Distributed computing is an arrangement of IT administrations that are given to a client over a system on a rented premise and with the capacity to scale up or down their administration prerequisites. Handing over imperative information to another organization is troubling. Author introduces a detailed analysis of the cloud computing security issues and challenges [1] focusing on the cloud computing types and the service delivery types. The clear and simple treatment of cryptography in [2], [3] had the impact of empowering the implementation and embedding of cryptography into systems with objective to realize security goals. Storage service by Cloud Service Provider is a answer to soften the weight of most extreme neighbourhood information storage and minimize the maintenance cost by means of outsourcing data storage [4], [5] that allow data owner to encrypt the delicate information before outsourcing to the public cloud. Through this resolution data is encrypted below a certain key, which is communal only with authoritative users. The un-definitive clients, including the Cloud Service Provider (CSP), are not capable to access the data ever since they do not have the decryption key. This common solution has been broadly incorporated into existing schemes [6], [7].

Asymmetric encryption strategies are very nearly 1000 times slower than symmetric procedures, since they require more computational processing power [8].

There are various algorithms are available to perform encryption, it's been difficult for user to determine which is most suitable. Author proposed study of symmetric encryption algorithms [9], [10], provides the evaluation of the most common symmetric algorithms namely: AES, DES, 3DES, RC2 and RC6. Comparison has been conducted for each algorithm such as extraordinary size of information pieces, battery control utilization, distinctive key size, and encryption/unscrambling time. From the result several points are concluded. First; in the case of change in packet size, it was concluded that RC6 has preferable execution than other algorithm. Second; on the account of changing key size, it can be seen that higher key size leads to clear change in battery and time consumption.

III. Existing System

Most of the third party based mutual trust software adopts symmetric key encryption technique such as AES. One of the major problems with AES technique is that it is the block cipher technique and therefore it is extremely difficult to use such block cipher technique for media data.

Disadvantages of Existing System:

- User files are thus encrypted in the user authorization with Drop Box or SkyDrive cloud storage service providers and data is stored as it is.
- Data transmission is secured however data storage is in-secure.

IV. Proposed System

We propose new third party solution, for offering security to every type of file that is been stored and retrieved from cloud storage provider. Whenever user selects a directory to be stored in the cloud all the files in the directory (word, ppt, audio, video, image, data etc.) are encrypted with a key given by the user and these files remain encrypted. By downloading files in other pc and demonstrating that file is unusable without the key.

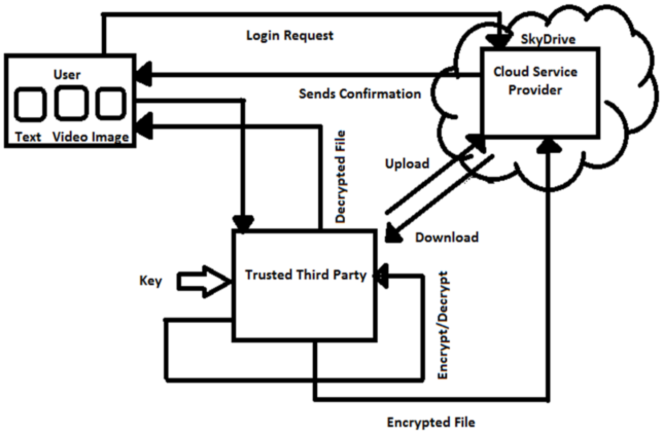


Figure.2: Block Diagram of proposed system

As shown in above figure 2, whenever user needs to access his files again the files corresponding to specific directory are decrypted in the background. After downloading from the SkyDrive user is able to work with those files. Once user prefers to update data in SkyDrive the modified file re-encrypted and replaces the alternate one.

V. System Design

Our system consists of three modules, User, App (Trusted Third Party), SkyDrive as shown in the figure.3. As the data owner wants to stores the data in cloud it's been difficult for user to trust Cloud Service Provider (CSP), for storage of data. So we introduce the trusted third party, here the user stores the data, it could be text or image files, into the SkyDrive through trusted third party. To get access the user needs to authenticate by the SkyDrive, by providing user credentials, SkyDrive sends the access token to trusted third party for user authentication. Whenever user wants store any files, it may be text or image files or audio etc. those files need to be encrypted. So the trusted third party asks user for the local password and the encrypted files are stored in SkyDrive. The user when stores files in cloud, because it is a cloud it gives URL to every file it gives to the user. When user request for the file, the trusted the party will download the encrypted files itself from the SkyDrive, and asks the local password to user than it decrypts the file and return the requested file to user.

Our Frame work Comprises of three main modules:

A. User Module
B. SkyDrive API Module
C. Trusted Third Party Module

A. User Module

In this module, we build up the information proprietor module. Proprietor produces the delicate information and stores it in cloud that is SkyDrive. In order to store the data in cloud first the information proprietor needs to enrol with cloud service provider (SkyDrive). After registering the proprietor gets credential login access using their username and password. The data owner then can upload their files in it the details of uploaded files are also listed in separated menu all the uploaded files are encrypted securely.

B. SkyDrive API Module

In this module, we develop the cloud service provider which provides the storage space to store the owner's files and images and to make them available for authorized users. We also consider the cloud is untrusted and thus the confidentiality and integrity of data in the cloud may be at risk so we introduce the Trusted Third Party entity.

C. Trusted Third Party (TTP) Module

In this module, we develop the TTP an entity who is trusted by all other framework segments and has abilities to recognize deceptive gatherings. In this module the TTP gets the access token from cloud to encrypt the files which the user wants to store and it gives the local password to authorized user that password is taken by TTP for encryption of files and store it into cloud. When the user wants to access the stored files the user needs to be authorized by cloud service and the user should get local password from TTP to decrypt the files.

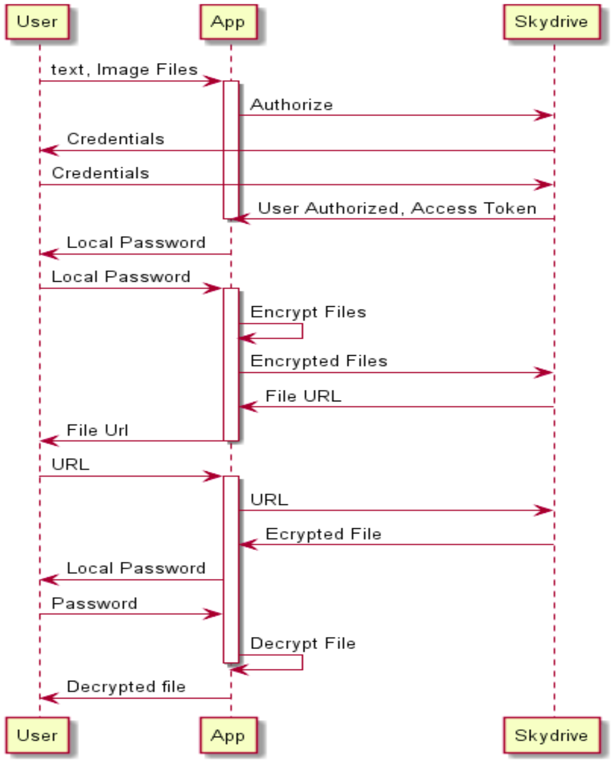
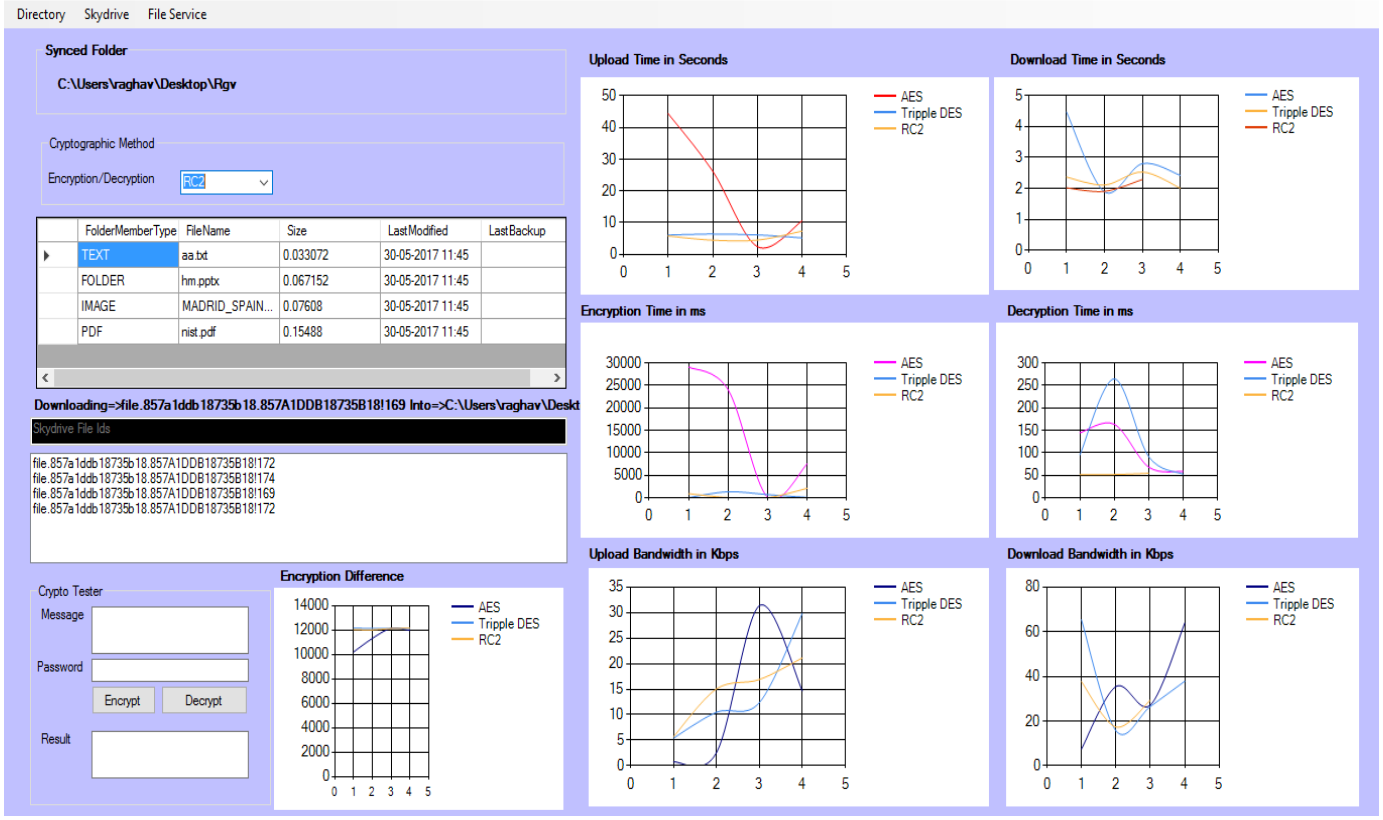


Figure.3: Sequence diagram of proposed system

VI. Discussion And Results

In this paper .NET implementation is used to perform evaluation of different symmetric encryption techniques. The implementation uses managed wrappers for Rijndeal, 3DES and RC2 accessible in System.Security.Cryptography that wraps unmanaged implementations accessible in CryptoAPI. These are RijndaelManaged, 3DESCryptoServiceProvider, RC2CryptoServiceProvider. Here we are giving provision for client to select AES, 3DES, or RC2 symmetric key encryption methods, in order to scramble/decode the contents that need to be stored in cloud.



Synced Folder

C:\Users\raghav\Desktop\Rgv

Cryptographic Method

Encryption/Decryption RC2

	FolderMemberType	FileName	Size	LastModified	LastBackup
▸	TEXT	aa.txt	0.033072	30-05-2017 11:45	
	FOLDER	hm.pptx	0.067152	30-05-2017 11:45	
	IMAGE	MADRID_SPAIN...	0.07608	30-05-2017 11:45	
	PDF	nist.pdf	0.15488	30-05-2017 11:45	

Downloading=>file.857a1ddb18735b18.857A1DDB18735B18!169 Into=>C:\Users\raghav\Deskt

Skydrive File Ids

```
file.857a1ddb18735b18.857A1DDB18735B18!172
file.857a1ddb18735b18.857A1DDB18735B18!174
file.857a1ddb18735b18.857A1DDB18735B18!169
file.857a1ddb18735b18.857A1DDB18735B18!172
```

Crypto Tester

Message

Password

Result

Figure.3: TTPSE Snapshot depicts the comparative results of Different encryption methods

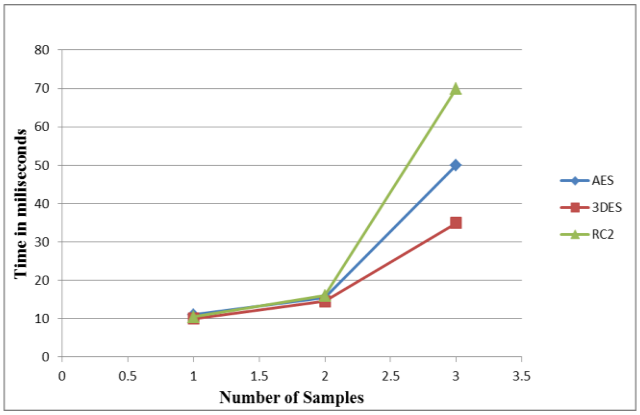


Figure.4: Encryption Response Time

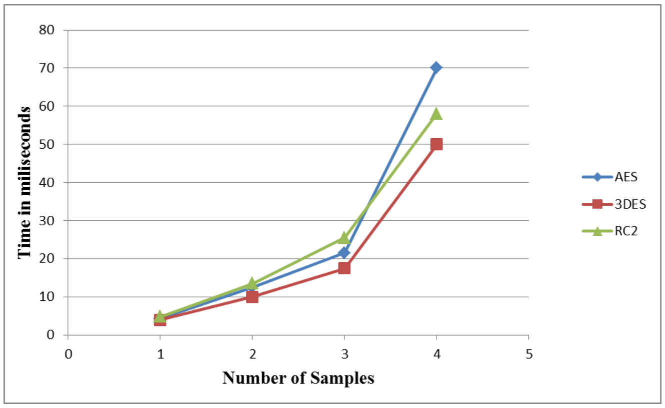


Figure.5: Decryption Response Time

Encryption time is used to calculate the throughput of an encryption scheme. It indicates the speed of encryption. Results are given in Figure 5 and Figure 6 for the selected three symmetric encryption algorithms at different packet sizes. Figure 5 gives the encryption response time and Figure 6 gives decryption response time. We can notice that there is no significant difference between both encryption and decryption methods.

Table 1. Comparison of Various Packet Size for AES, 3DES and RC2

Sl No.	Algorithm	Pack Size(kb)	Encrypt Time(ms)	Decrypt Time(ms)
1	AES	12	1.3	4.3
	3DES		1.2	3.9
	RC2		1.4	4.8
2	AES	55	11	12.5
	3DES		10	10
	RC2		15.5	13.5

3	AES	80	14.5	21.5
	3DES		16	17.5
	RC2		13.5	25.5
4	AES	452	50	70
	3DES		35	50
	RC2		70	58

VII. Conclusion And Future Work

7.1 Conclusion

With the growing usage of the cloud storage for data storage, it is become paramount important to offer scalable security solution for data storage. Even though the data transmission to the cloud and from the cloud is secured through 128 bit key, and over secured socket layer, the stored data in the cloud remain unencrypted. We have offered secured mutual trust solution as a third party between the user and cloud service provider. Our solution takes care of encrypting the file before uploading to the cloud and decrypting them before saving them in local storage while downloading. In this work we have demonstrated the use of our third party with real time OneDrive cloud. From Table 1, it was observed that encryption time (1.2, 10, 16, 35 ms) and decryption time (3.9, 10, 17.5, 50 ms) is lesser for 3DES algorithm compared to AES and RC2 algorithms for different pack sizes (12, 55, 80, 452 kb) considered. It is also observed that RC2 consumes longest encryption time.

7.2 Future Work

System can also be improved by incorporating some kind of hashing mechanism by means of which searching of encrypted data in the cloud becomes easier. Once the data is encrypted it is not been indexed by any cloud searching technique. Hashing before the encryption and storing such hashing in the cloud could make it easier to search encrypted files stored in the cloud.

References

[1] Mithilesh Mittal, Pradeep Sharma, PK. Gehlot, “*A Comparative Study of Security Issues& Challenges of Cloud Computing*”, International Journal of Scientific Research in Computer Science and Engineering, Vol.1, Issue.5, pp.9-15, 2013.

[2] Ayad Barsoum, Anwar Hassan “*Enabling Dynamic data and Indirect Mutual Trust for Cloud Computing Storage System*”, IEEE Transactions on Parallel and Distributed Systems,Vol.24, Issue.(12, pp.2375-2385, 2013.

[3] Cong Wang, Kui Ren, “*Towards Publicly Auditable Secure Cloud Data Storage Services*”, IEEE Network, Vol.24, Issue.4, pp.19-84, 2010.

[4] S.D.C. Vimercati, S. Foresti, S. Jajodia, S. Paraboschi, P. Samarati, “*Over-encryption: Management of access control evolution on outsourced data*”, in Proceedings of the 33rd International Conference on Very Large Data Bases, Austria, pp.123-134, 2007.

[5] Schneier Bruce,”*Applied cryptography: Protocols Algorithms and Source code in C (*2nd edition*)*”, *John Wiley & Sons*, United States, pp.1-784,1996.

[6] AJ. Menezes, VOorschot, PCV. Anstone, A. Scott , *“Handbook of Applied Cryptography*” , Jaypee publisher, India, pp.34-58, 1996.

[7] A. Sharma, RS Thakur, S. Jaloree, “*Investigation of Efficient Cryptic Algorithm for image files Encryption in Cloud*”, International Journal of Scientific Research in Computer Science and Engineering, Vol.4, Issue.5, pp.5-11, 2016.

[8] Dong, Russello,Dulay, “*Shared and Searchable Encrypted data for Untrusted Servers*”, International Journal of Computer Security, Vol.19, Issue.3, pp.367-397, 2011.

[9] SL. Mewada, P. Sharma, SS. Gautam, “*Classification of Efficient Symmetric Key Cryptography Algorithms*”, International Journal of Computer Science and Information Security (IJCSIS), Vol. 14, No. 2, pp.105-11, 2016

[10] Md.A. Mushtaque, “*Comparative Analysis on Different parameters of Encryption Algorithms for Information Security*”, International Journal of Computer Sciences and Engineering, Vol.2, Issue.4, pp.76-82, 2014.