TWO-WAY CLOUD SHARE

[1]G. Ajay, [2]Jakeer Hussain, [3]B. Lokesh, [4]K. Nikhil Sai, [5]K Sathiya Priya

[1,2,3,4]Students, [5]Assistant Professor
Department of Computer Science and Engineering,
Bharath Institute of Science & Technology affiliated to
Bharath Institute of Higher Education and Research, Chennai, Tamilnadu, India

Abstract- **The widespread use of cloud storage in the recent years can be attributed to the existence of compelling applications such as file backup, data storage and file sharing. Data privacy is the primary concern in information technology. At the moment two-factor authentication is widely used in online environments. The goal of this project is to use the cloud storage, cloud sharing and other issues in a unique way which helps us to reduce time and money .This paper focuses on the implementation of cloud sharing and cloud storage with two-factor authentication and data privacy as the primary concern.**

INTRODUCTION:

Data is acknowledged as the most vital asset of an organization because it defines the uniqueness of every enterprise. It is the main foundation of information, knowledge, and ultimately the wisdom for correct decisions and actions. It might be helping to cure a disease, boost a company’s revenue, make a building more efficient or be responsible for achieving the targets, and improving the performance [1].Furthermore, storage, analysis, and sharing of data are the essential services required by any organization to upgrade its performance [2]. However, with the explosive evolution of data, enormous pressure emerges on the enterprises for storing the voluminous data locally [3]. Also, it has become difficult to explore the data due to limited resources [4]. Most businesses have shifted to the cloud for these services due to its several advantages such as on-demand service, scalability, reliability, elasticity, measured services, disaster recovery, accessibility, and many others [5]. Cloud computing is a paradigm that enables huge memory space and massive computation capacity at a low cost. It allows users to obtain the intended services across multiple platforms irrespective of location and time and consequently conveys an extensive convenience to the cloud users [6]. By migrating the local data management system into cloud storage and using cloud-based services, users can accomplish cost savings and productivity enhancements to manage projects and establish collaborations [7]. Therefore, individuals and organizations are shifting increasingly to the cloud for their multiple services [8]. With the growing expansion of cloud computing technologies, it is not difficult to imagine that almost all the businesses will be switched to the cloud in the foreseeable future [9]. Despite the multiple features offered by cloud computing, it encounters several impediments that may obstruct its fast growth, if not tackled appropriately [10]. Consider a real implementation, where an enterprise permits its staff or departments to store and share the data through the cloud. By exploiting the cloud, the enterprise can be completely released from the burden of maintaining and storing the data locally [11], [12]. Nevertheless, it also endures various security threats, which are the leading concerns of cloud users [13]. Firstly, outsourcing the data to the cloud servers signifies that the data is out of the users’ control resulting in discomfort to the users because the outsourced data may comprehend sensitive and valuable information. Secondly, data sharing is frequently put into operation in a hostile and open environment, and the cloud server turned out to be a target of attacks. In the worst condition, users’ data may be revealed by the cloud server itself for illegal profit [14], [15]. Furthermore, the data need to be shared among distinct relevant stakeholders, for instance, business partners, employees, customers, etc., interior or exterior of the organization’s premises for upgrading the performance of the business. However, the recipient party can maltreat this data and disclose it purposefully or inattentively to some unauthorized third party [16], [17].
Fig. 1 represents a sharing environment where the data owners need to share the organization’s valuable data to the cloud platform due to the limited storage and computational capacity of the enterprises and the multiple benefits of clouds. Furthermore, the cloud data is shared with multiple users as per different requirements for its utility purpose. However, the recipient party may leak the data after obtaining it. The data can be leaked by the involved parties or may steal by the unauthorized party through illegal access. Data leakage or loss may induce a severe threat to the organization’s confidentiality. It can diminish the value of shareholders, decline the firm’s rank and status, and destruct the enterprise’s goodwill and reputation [18]. As the data is an important asset of an organization, thus it is essential to keep this asset secure. There arises a necessity for solutions that can protect the data efficiently in the sharing environment.

A number of models for data protection in the cloud environment have been explored and developed for many applications. Typically, data protection is achieved through leakage prevention and leaker detection and this article concentrates on achieving efficient protection by preventing leakage and detecting the malicious entity responsible for leakage as depicted in Fig. 2. The major approaches for preventing data leakage are tailored by utilizing cryptography, access control mechanisms, and differential privacy with machine learning techniques while leaker detection is mainly achieved through watermarking and probabilistic techniques.

LITERATURE SURVEY:

[1] RushikeshNikam, and Manish Potey. Some online data services often come with security issues such as confidentiality and integrity. The problem scenario ranges multi-fold: to secure organizational data from peer organizations, to provide sharing of data files between users keep the identity anonymous, to handle recovery of vital data modules, etc. This paper proposes a solution to eliminating the above-mentioned problems. The solution aims at achieving Confidentiality using CP-ABE (Ciphertext Policy- Attribute Based

Encryption) and user authentication with Multifactor Authentication (MFA). Security is achieved at various levels such as providing a static username-password as the entry-level authentication, followed by OTP based on the token generator technique. These tokens are generated using QR code technology and act as credentials for each user. The provision of default tokens is also available for genuine users that fail to use the QR code generator at some point. This allows availability to authorized users. Encryption is done using CP-ABE.

CP-ABE(Algorithm)In CP-ABE, it is not the set of attributes that do the working but the policies defined over a set of attributes carry the encryption process. In this scheme, the User's private key is based on a group of attributes whereas the ciphertext is based on the access structure defined over system-specific attributes. A user can decrypt a text if his attributes satisfy the policy specified in the cipher text. Policies are defined over attributes using conjunctions, disjunctions, and {n, m}-threshold gates, i.e. n out of m attributes have to be present. In CP-ABE there is no separate access control or authorization mechanism. It is incorporated into the encryption mechanism itself. Users can even obtain their secret keys after data encryption using the access structure is an important add-on. Hence, data can be encrypted even with not knowing the genuine user groups which can decrypt, and only specifying the policy is quite enough. Future users are given a key based on the attributes that the policy satisfy and such users are only genuine decrypters of the system.

[2]Mousa, Allam.In This Paper Some of the important parameters of the Blowfish encryption algorithm are analyzed and examined to see how these parameters may affect the performance of the algorithm. The peflonnance indices here are the security and speed of the algorithm. For each case, the eng.ptioddecryptionkq length has been changed and its effect on the performance p is noticed. Moreover, the file size is changed and its effect on the performance of the algorithm was noticed. This has shown that changing the key length does not affect the encryption or decryption time whereas changing the plaintext file size is directly rejected on the processing time.

Encryption is hiding data while being transmitted or stored. That is transforming the information from one form (plain text) into another one (cipher text) by using certain algorithms depending on some keys. On the other hand, decryption is transforming the cipher text back to its plain text using the same algorithm and key. This algorithm consists of some mathematical functions and operations that perform the encryption process in many ways. and the key is a specific number (usually a Large one) that is usually used by the algorithm and its calculations. Key management is the set of procedures supporting the establishment and maintenance of keying relationships between authorized parties. Thus the risk is transferred from the problem of securing the data to the problem of securing and managing keys. An important issue here is choosing the encryption key, this depends on many things such as how long does the data need to be kept secure? What kind of encryption is being used (symmetric or asymmetric)? How valuable is the data being secured? For information that needs to be secure for only minutes, hours, or perhaps weeks, a 64-bit symmetric key will suffice. For data that needs to be secure for years or decades, a 128-bit key should be used. For data that needs to remain secure for the foreseeable future, one may want to go with as much as a 160-bit key.

Blow Fish(algorithm) Some of the Blowfish algorithm specifications can be summarized as [3], [4];

1. Symmetric block cipher.
2. 64-bit Block.
3. Variable-length key, from 32-bit (4 Bytes) to 448
4. Run at an acceptable clock speed.
5. Suitable and efficient for hardware implementation
6. Unpatented and no license is required.

The algorithm consists mainly of two parts; the key-expansion part and the data-encryption part (51. Key expansion converts a key of at most 448 bits into 4168 bytes. There is a P-array and four 32-bitS-boxes. The P-array contains 18, 32-bit subkeys, while each S-box contains 256 entries. Data encryption occurs via a 16-round Feistel network. Each round consists of a key-dependent permutation, and a key- and data-dependent substitution. All operations are XORs and additions on 32-bit words. The only additional operations are four indexed array data lookups per round [4].

[3]Rizvi, S. A. M.In this Paper The two main characteristics of a good encryption algorithm are Security and Speed. Usually, security algorithms have to be embedded in a variety of applications like e-banking, online shopping, mail, etc. So they should be fast as well as secure in different environments. In this paper, we do a security v/s performance analysis of two algorithms Twofish and AES. First, we will discuss the security issues of both algorithms by considering their safety factor. Then we study the encryption speed of both algorithms by encrypting different types of data (text, image, audio) and analyze their performance in terms of throughput of every algorithm on different sizes of RAMs. The results show the relationship between the performance of algorithms and size of RAM and the type of data.

From mail to money when everything is getting digital, the Internet becomes the one and main medium of communication in all aspects of our life.

TwoFish and AES(Algorithm)Twofish is an algorithm from Counterpane Internet Security, it is highly suited for large microprocessors and also for smart card microprocessors. A brief overview of the concepts and considerations relevant to the Twofish design procedure is given in [2]. Currently, the best attacks on Twofish use different versions of differential cryptanalysis, None of them succeeds on the full number of rounds with the present computational power. B. AES has a Non-Feistel structure, based on a sophisticated mathematical design. Its simple structure attracts cryptographers and cryptanalysts. It encrypts 128-bit block size with 128/192/256 bit key for 10/12/14 rounds. AES has a safety factor of less than 2, which implies that it is somewhat more delicate for the advancements of cryptanalysis. Making the safety factor of AES equivalent to Two-fish would require 24 rounds of AES. An increase in the number of rounds may reduceits performance.

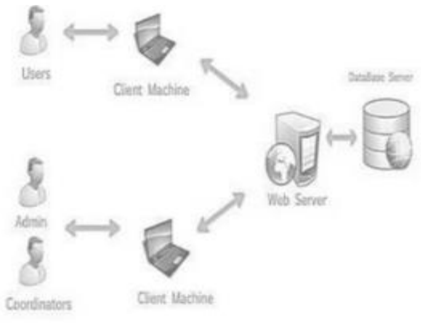
[4] Zhou, Xin, and Xiaofei Tang.In this Paper Cryptographic technique is one of the principal means to protect information security. Not only has it ensure the information is confidential but also provides a digital signature, authentication, secret sub-storage, system security, and other functions. Therefore, the encryption and decryption solution can ensure the confidentiality of the information, as well as the integrity of information and certainty, to prevent information from tampering, forgery, and counterfeiting. The encryption

and decryption algorithm's security depends on the algorithm while the internal structure of the rigor of mathematics, also depends on the key confidentiality. Key in the encryption algorithm has a pivotal position, once the key was leaked, it means that anyone can be in the encryption system to encrypt and decrypt information, it means the encryption algorithm is useless. Therefore, what kind of data you choose to be a key, how to distribute the private key, and how to save both data transmission keys are very important issues in the encryption and decryption algorithm. This paper proposed an implementation of a complete and practical RSA encrypt/decrypt solution based on the study of the RSA public key algorithm. In addition, the encrypt procedure and code implementation are provided in detail.

PROPOSED SYSTEM:

In this system we proposed a unique way in which user can share the part of his cloud to the other user which may resolve the issues of Google Cloud and IBM Cloud.
Here, we used the
Two-Fish Algorithm. It is a symmetric key block cipher. It will provide another level of assurance and be a bit more secure.
It uses a block size of 128 bits, having a key length of 256 bits. It takes 16 rounds of encryption.

SYSTEM ARCHITECTURE:



MODULE DESCRIPTION:

- Congregation and Endorsement of cloud storage.
- Generation of Authentication Keys - Random Class function.
- Processing and protecting of data using the two-fish algorithm
- Performance analysis

Congregation and Endorsement of Cloud Storage:

In today's world cloud storage is the primary asset to any organization and sector. Cloud storing platform should ensure the security by permitting only authenticated users or processes to gain access to their protected resources. Organization should provide end to end encryption to the uploaded data. In the initial stage of this step, we are splitting the storage through the user's generated splitting form process. We treated as input for our application. we are enabling users to use the application for uploading and downloading their files securely.

Generation of Authentication Keys - Random Class function:

In this module, we are providing the user authentication in one more layer by providing a key known to be secret in addition to the username and password. True Random Number generation is surprisingly difficult to do right. One of the results is that even now, there is no 'approved' or 'standardized' method for generating truly random numbers. By using the random function, we are creating the secret key and the private key for the user. When the user is allowed to upload a file, here we are creating a specific key to access the file. Whenever the user uploads a file, it moves to the next module in processing

Processing and protecting of data using the two-fish algorithm

- Encryption helps in protecting private information, and sensitive data, and can enhance the security of communication between user and client.
- In this module by using the **TWO–FISH** Algorithm, we are encrypting the user's data.
- Two – Fish Algorithm undergoes 16 rounds of encryption, involving a block – size of 128 bits.
- It generates a key of length 256 bits.
- It is a Symmetric-key algorithm, involving only one key at the time of encryption and decryption.
- It converts the normal text/format into cipher text. It is a Feistel network structure.

Performance analysis

File Name	File Size	Time(s)	
		Encrypt	Decrypt
ABCD.txt	100Kb	0,093	0,031
John.jpg	200Kb	0,234	0,047
Word.docx	300Kb	0,312	0,078
Presentation.ppt	400Kb	0,421	0,125
Project.pdf	500Kb	0,765	0,187

After the implementation of the Two-Fish algorithm program during the simulation of five (5) different datasets for encryption and decryption processes, here we detailed their time of encryption and decryption respectively

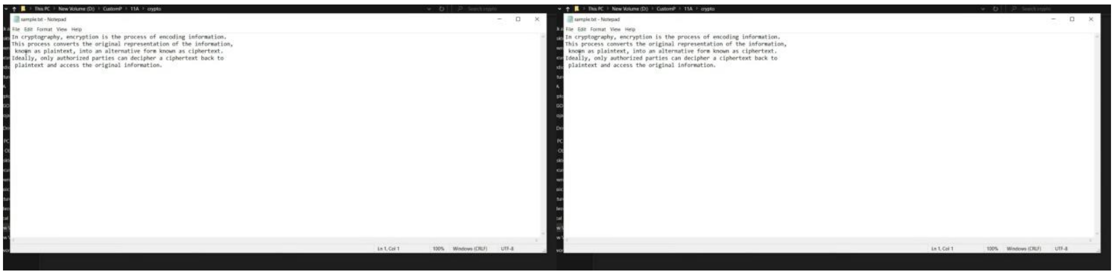
CONCLUSION:

We feel that Two-way cloud share for sharing the cloud is a better option for advanced security and low price for he user's.. Some of the challenges can be anticipated, such as advances in computation that are making it progressively easier to share cloud and advance security.

FUTURE WORK:

In the future, sharing cloud and two-factor data authentication may be used to efficiently secure files online. The encryptions made using two-fish algorithms are most welcoming as they are the future technologies. Hereafter the cloud sharing in various platform would be better and more accurate with advance technology and the encryption and decryption techniques would be better and more accurate when they are made using machine learning techniques and models.

SCREENSHOTS (Encryption and Decryption file):

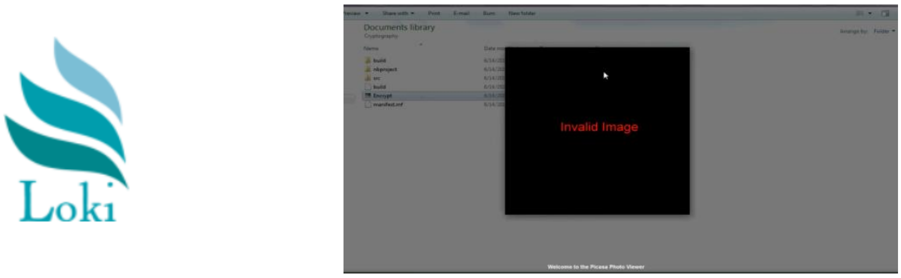


This PC > New Volume (D:) > CustomP > 11A > crypto
sample.txt - Notepad
File Edit Format View Help
Ln 1, Col 1
100%
Windows (CRLF)
UTF-8

```
In cryptography, encryption is the process of encoding information.
This process converts the original representation of the information,
 known as plaintext, into an alternative form known as ciphertext.
Ideally, only authorized parties can decipher a ciphertext back to
 plaintext and access the original information.
```

```
In cryptography, encryption is the process of encoding information.
This process converts the original representation of the information,
 known as plaintext, into an alternative form known as ciphertext.
Ideally, only authorized parties can decipher a ciphertext back to
 plaintext and access the original information.
```

SCREENSHOT (Encryption Img):



REFERENCES:

[1] RushikeshNikam, and Manish Potey. "Cloud storage security using multi-factor authentication." 2016 International Conference on Recent Advances and Innovations in Engineering (ICRAIE). IEEE, 2016.

[2] Mousa, Allam. "Data encryption performance based on Blowfish." 47th International Symposium ELMAR, 2005. IEEE, 2005.

[3] Rizvi, S. A. M., Syed ZeeshanHussain, and Neeta Wadhwa. "Performance analysis of AES and TwoFish encryption schemes." 2011 International Conference on Communication Systems and Network Technologies. IEEE, 2011.

[4] Zhou, Xin, and Xiaofei Tang. "Research and implementation of RSA algorithm for encryption and decryption." Proceedings of 2011 6th international forum on strategic technology. Vol. 2. IEEE, 2011.

[5] A. Nadeem and M. Y. Javed, "A performance comparison of data encryption algorithms", Information and Communication Technologies, ICICT 2005, pp.84-89, 2005.

[6] Li, Yibin, et al. "Privacy protection for preventing data overcollection in a smart city." IEEE Transactions on Computers 65.5 (2015): 1339-1350.

[7] Krikor, Lala, et al. "Image encryption using DCT and stream cipher." European Journal of Scientific Research 32.1 (2009): 47-57.

[8] Shubhi Mittal, Shivika Arora and Rachna Jain "PData Security using RSA Encryption Combined with Image Steganography",2016.

[9] A. K. Singh and I. Gupta, ‘‘Online information leaker identification scheme for secure data sharing,’’ Multimedia Tools Appl., vol. 79, no. 41, pp. 31165–31182, Nov. 2020.

[10] E. Zaghloul, K. Zhou, and J. Ren, ‘‘P-MOD: Secure privilege-based multilevel organizational data-sharing in cloud computing,’’ IEEE Trans. Big Data, vol. 6, no. 4, pp. 804–815, Dec. 2020