IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 7, May 2023

Hybrid Cryptography: Secure File Storage on Cloud using AES, RC6 and Blowfish Algorithm

Trupti Mankar[1], Nirmala Sagar[2], Pooja Bhusari[3], Snehal Gulbhamwar[4], Prof. Dhananjay Dumbere[5]
Students, Department of Information Technology[1,2,3,4]
Professor, Department of Information Technology[5]
Rajiv Gandhi College of Research and Technology, Chandrapur, Maharashtra, India

Abstract: *In this era, cloud computing is used in various fields like industry, military, college, etc. for various services and storage of huge amount of data. Data stored in this cloud can be accessed or retrieved on the users request without direct access to the server computer. But the major concern regarding storage of data online that is on the cloud is the Security. This Security concern can be solved using various ways, the most commonly used techniques are cryptography and steganography. But sometimes a single technique or algorithm alone cannot provide high-level security. So we have introduces a new security mechanism that uses a combination of multiple cryptographic algorithms of symmetric key and steganography. In this proposed system, RC6 (Rivest Cipher 6), AES (Advanced Encryption Standard) and Blowfish algorithms are used to provide security to data. All the algorithms use 128-bit keys. LSB steganography technique is used to securely store the key information. Key information will contain the information regarding the encrypted part of the file, the algorithm and the key for the algorithm. File during encryption is split into three parts. These individual parts of the file will be encrypted using different encryption algorithm simultaneously with the help of multithreading technique. The key information is inserted into an image using the LSB technique. Our methodology guarantees better security and protection of customer data by storing encrypted data on a single cloud server, using AES, RC6 and Blowfish algorithm..*

Keywords: Cryptography, Encryption, Decryption, Cloud Storage, Cloud Security

I. INTRODUCTION

Technological advancements are resulting in trends and movements that improve the quality of life. In this fast life where every person uses a smartphone and has access to the internet, the major concern that the people face is regarding the security of their information present online. This security concern is also about the file that is stored online on a cloud. This can be solved with the help of cryptography.

Cryptography techniques convert original data into Cipher text. So only legitimate users with the right key can access data from the cloud storage server. The main aim of cryptography is to keep the security of the data from hackers, online/software crackers, and any third-party users. Non-legitimate user access to information results in loss of confidentiality. Security has the characteristics to block or stop this kind of unauthorized access or any other kind of malicious attacks on the data here by securing the users' trust.

In the cloud computing environment, security is deemed to be a crucial aspect due to the significance of information stored on the cloud and the different services provided to the users. This data can be confidential and extremely sensitive. Hence, the data management and security should be completely reliable. It is necessary that the data in the cloud is protected from malicious attacks.

So, for the security of the data, we introduced a new mechanism in which we are using a combination of multiple symmetric key cryptography algorithm and steganography. In this proposed system Advanced Encryption Standard (AES), Rivest Cipher 6 (RC6) and Blowfish algorithms are used to provide security to data.

LSB algorithm is used for image steganography. Sensitive data of the user is hidden into a cover image for security purposes.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 7, May 2023

AES, RC6, and Blowfish algorithms are combined to form a hybrid algorithm to accomplish better security. The Steganography part assists in storing the key information safely. It makes it difficult for the attacker to recover the secret file of the user.

II. LITERATURE REVIEW

Security is an important factor in this digital age. So, a huge amount of research is conducted in this domain to protect client's information from any security breach and leaks.

[1]K.Shahade and V. S. Mahale in their research introduced a Hybrid encryption algorithm which was a combination of RSA algorithm and AES algorithm. In their system, the user creates and stores the RSA private key with himself and also create an RSA public key while uploading the data. In the cloud, the server calls the RSA and AES algorithm for encryption of the file and then properly store the file on the server.

[2]P. Uddin researched an efficient way for information hiding using Text Steganography along with Cryptography. In this study, steganography of pure text was proposed, including private key cryptography that provides a high level of security. According to the algorithm after embedding the cipher text in the cover text, the text seems like ordinary text.

[3]S. D. Patil suggested a system for the hiding text in cover images using the LSB algorithm and for decoding using the same method. The use of the data of this algorithm can be stored in the Least Significant Bit of the title image. Even then, the human eye cannot notice the hidden text in the image.

[4]S. Hesham in her research proposed an algorithm that increases the efficiency of the Advanced Encryption Algorithm. The proposed method reduces the critical path delay of the original algorithm. Compared to the original AES encryption/decryption algorithm the proposed algorithm provides an efficiency improvement of 61% and 29% respectively.

[5]To make the centralised cloud storage secure ECC(Elliptic Curve Cryptography) algorithm is implemented. This approach uses single key for encryption and decryption and complete process takes place at the client side. This methodology performs steps such as: a.Authentication, b.Key generation operation, c.Encryption, d.Decryption.

[6]In this proposed system three step procedure is used. Firstly, Diffie Hellman is used for exchanging keys. Thereafter authentication is performed using digital signature scheme. Finally, data is encrypted using AES and then uploaded to the required cloud system. For decryption reverse procedure is implemented.

[7]Combination of RSA algorithm and MD5 to assure various security measures such as confidentiality, data integrity, non-repudiation etc. It uses RSA key generation algorithm for generation of encrypted key for encryption and decryption process. MD5 digest is used for accepting an input of length up to 128 bit and processing it and generating an output of padded length for encryption and decryption process.

[8]Implementation of Trusted Storage System using Encrypted File System (EFS) and NTFS file system drive with help of cache manager for securing data files. EFS encrypts stored files by automatically using cryptographic systems. The process takes place as follows, firstly application writes files to NTFS which in turn places in cache and return backs to NTFS. After this NTFS asks EFS to encrypt files and heads them towards the disk.

[9]Cloud Storage Security Service is provided by using separate servers viz. User Input, Data Storage and User Output. Three different servers are used to ensure that failure of any of the servers doesn't harm the data. User Input server is used for storing user files and input data by providing user authentication and making sure the data is not accessed by any of the unauthorized means. Data storage server is the place where the encryption using AES is performed to secure user input and then the encrypted files are transferred to User Output server. User Output Server is the place from where user gets the output file or the decrypted file and use it for further time.

[10] Author - Punam V. Maitri, Aruna Verma, Year – 2016

Description – The paper focuses on how files are securely stored on a cloud platform. Also, it discusses the problem of using only a single algorithm to encrypt the file and how ineffective it will be on the cloud. This paper splits the file into blocks and each block is encrypted using AES, blowfish, RC6algorithm. The key information about which file uses which algorithm is sent to the receiver using steganography modern approach to file system integrity checking.

[11]Author – M. Malarvizhi, J. Angela JennifaSujana, T. Revathi, Year – 2014

Description - The main focus of the paper is on the integrity of files and restoring the files if integrity is violated. The proposed system uses a pattern of each protected file to determine its modification. The method used for pattern

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 7, May 2023

generation is cryptographic hash functions. The system also uses a database that stores the files that need to be protected and their hash codes. To check the integrity of the file the hash code of the file is produced and checked with one in the database. If the file is successfully tested positively then access is granted otherwise the administrator gets alerted and if it is saved copy is available of the same file then the file is restored. New approach to user authentication using digital signature.

[12] Author - Jerzy Kaczmarek, MichałWróbel, Year -2008

Description – This paper describes an approach to the integrity of files and restoring the files if any problem is arising in the future. This proposed course uses a pattern of each protected file to determine its modification. Methods used for pattern generation are cryptographic hash functions. This system uses a database that stores the names of all files that are to be protected and their hash codes. To check the integrity of the file the hash code of the file is produced and checked with one in the database. After the file is verified then only access is granted else the administrator is been alerted about the problems and a saved copy of the same file is restored safely. Secure file sharing using cryptographic techniques in the cloud.

[13] Author - RashiDhagat, Purvi Joshi, Year– 2016 Description – The paper focuses on providing the facility to securely store and share the data in a group using cloud technology for storage. The method discussed in the paper uses group signature and encryption techniques. The advantage of this proposed method is that data owners can store the file without showing their true identity to others in the cloud. Public key exchange known as (PKA).

[14] Author - Bilal Habib, Bertrand Cambou, DuaneBooher, Christopher Philabaum, Year – 2017

Description – This paper provides a new method to implement the public key infrastructure. The PKI has the disadvantage that the mathematical relation between public and private between the public and the private key is maintained. Paper proposes a new PKI scheme with addressable elements (PKA). The approach proposed removes the mathematical relation between public and private keys using addressable cryptographic tables. Secure data sharing in cloud storage using key aggregation cryptography.

[15] Author - Tulip Dutta, Amarjyoti Pathak, Year – 2016

Description – This paper discusses how a secret key can be shared with other users to whom access needs to be given. It discusses the problem with using a single key to encrypt all data and using different keys for different files. The solution described in the paper tries to address both the problem using key aggregation. In key aggregation, different data files are encrypted with different keys and then for decryption, a single aggregated key is used. The encryption algorithm used is AES and the system is being implemented in java using the key store data structure. Achieving cloud security using third party auditor, MD5, and identity- based encryption.

[16] Author -Bhale Pradeep Kumar Gajendra, Vinay Kumar Singh, More Sujeet, Year – 2016

Description – This paper overcomes the security tradeoff and improves the performance of data transmission and increases security. Also, MD5 hashes are no longer considered cryptography secure. An approach to hybrid cryptography on cloud environment.

[17] Author -Mr. Rohit Barvekar, Mr. ShrajalBehere, Mr. Yash Pounikar, Ms. Anushka Gulhane, Year -2018

Description - The proposed security mechanisms will prevent confidential data from being misused making the system more reliable. High speed: The proposed method will make encryption and decryption with proper keys much faster than usual. Security in Cloud Computing using Cryptographic Algorithms.

[18] Author - Shakeeba S. Khan, Prof. R. R. Tuteja, Year – 2015

Description -The proposed algorithm is a Multilevel Encryption and Decryption algorithm. Only the authorized user can access the data. Even if some intruder gets the data, he must have to decrypt the data at each level which is a very difficult task without a valid key. It is time-consuming as multiple encryption and decryption take place. Secure data sharing using cryptography in a cloud environment.

[19] Author - Anjali Patil, Nimisha Patel, Dr. Hiren Patel, Year – 2016

Description - In this paper, The system satisfies confidentiality, integrity, and authentication. Provides access control. The confidentiality of data is dependent on a trusted crypt server.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 7, May 2023

III. PROPOSED SYSYEM

In the proposed system, a method for securely storing files in the cloud using a hybrid cryptography algorithm is presented. In this system, the user can store the file safely in online cloud storage as these files will be stored in encrypted form in the cloud and only the authorized user has access to their files.

1. User Registration

For accessing the services the user must first register yourselves. During the registration process various data like Name, username, password, email id, the phone number will be requested to enter. Using this data the server will produce unique user-specific keys that will be used for the encryption and decryption purpose. But this key will not be stored in the database instead it will be stored using the steganography algorithm in an image that will be used as the user's profile picture.

2. Uploading a File on Cloud

When the user uploads a file on the cloud first it will be uploaded in a temporary folder.
Then user's file will be split into N parts.
These all parts of file will be encrypted using cryptographic algorithms. Every part will use a different encryption algorithm.
These all parts of file will be encrypted using different algorithms that are AES, 3DES, RC6. The key to these algorithms will be retrieved from the steganographic image created during the registration.
After the split encryption, the file reassembled and stored in the user`s specific folder. The original file is removed from the temporary folder.
Then Combining all Encrypted Parts of file.

3. Download a File from the Cloud

When the user requests a file to be downloaded first the file is split into N parts.
Then these parts of file will be decrypted using the same algorithms with which they were encrypted. The key to thealgorithms for the decryption process will be retrieved from the steganographic image created during the registration.
Then these parts will be re-combined to form a fully decrypted file.
Then file will be sent to the user for download.

IV. PROBLEM FORMULATION AND DESIGN:

The many advantages of using cloud storage include:
1. It eliminates the need for carrying physical storage devices.
2. Data in any format can be stored using cloud storage.
3. Cloud storage provides safe backup, as opposed to physical storage devices where loss of device, data corruption by a computer virus, natural disasters, amongst other causes, can lead to loss of data.
4. Cloud storage is more cost-effective as it eliminates the need to invest in hardware,
5. Cloud storage also helps developers collaborate and share their work in a more efficient and speedy manner.

Another advantage of cloud storage could be additional security. The proposed system aims to make the cloud storage system secure using data encryption. Thus, the aim of the proposed system is to increase security of data uploaded onto the cloud by using encryption algorithms to make the system more secure.
The system is designed such that it works in the following way:
1. The user signs in if already registered, or signs up to register themselves by providing their details such as name, email id, phone number, password for account et cetera.
2. The user then selects the file that is to be uploaded by browsing from local storage.
3. The user then selects the encryption algorithm that they want to use. The proposed system provides the choice between using a combination of AES and RC6 or AES and Blowfish.
4. The selected file gets uploaded after getting encrypted using the selected encryption algorithm combination.
5. The user also has the option of viewing the files that they have uploaded or have access to and downloading them.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 7, May 2023

6. On selecting a file to download it, the user is sent the decryption key on their email id that was entered on registration or sign-up.
7. Using this key, the user can download the decrypted or original file.
8. The system also provides a comparison with respect to security between the two hybrid encryption algorithm combinations i.e., AES and RC6 hybrid combination and AES and Blowfish combination.

The system is thus secure, as it provides a double layer of security. Confidential user login credentials are the first layer of security. The second layer is the encrypted file. Since the file is encrypted and then stored on the cloud, even if an attacker gains access to the cloud, they would only have access to the encrypted files. The file can be decrypted using only the decryption key, which is only sent to the user's email id which was entered during registration/sign-up time.

Therefore, the proposed system is designed to provide cloud storage features to users of the portal such as uploading and downloading files to the cloud, wherein the selected files are first encrypted and then uploaded to the file, and can be downloaded using only secret decryption key.

An additional feature is the comparative study between the two hybrid algorithm approaches, namely AES and RC6 combination and AES and Blowfish combination.

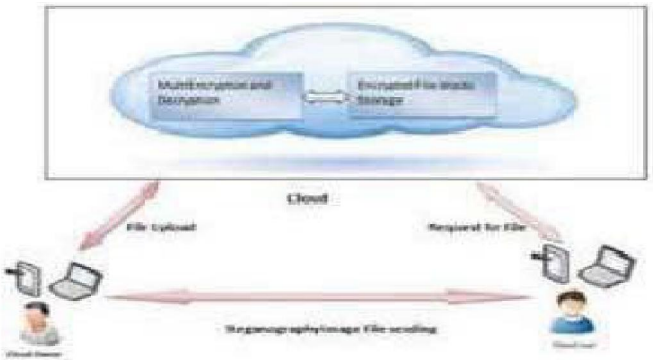


Fig:- Existing System Architecture

Fig:- High Level System

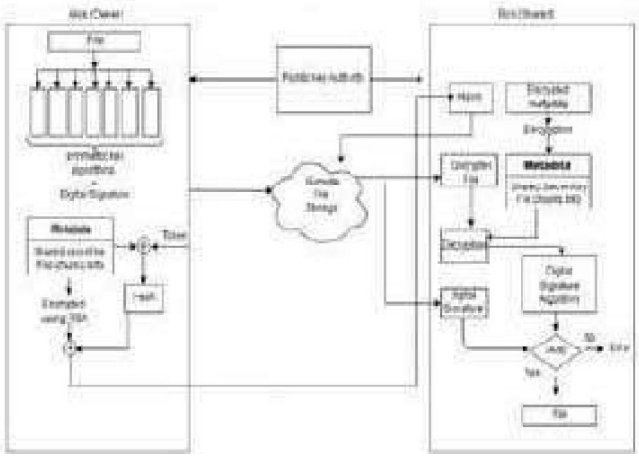


Fig:- Proposed System Architecture

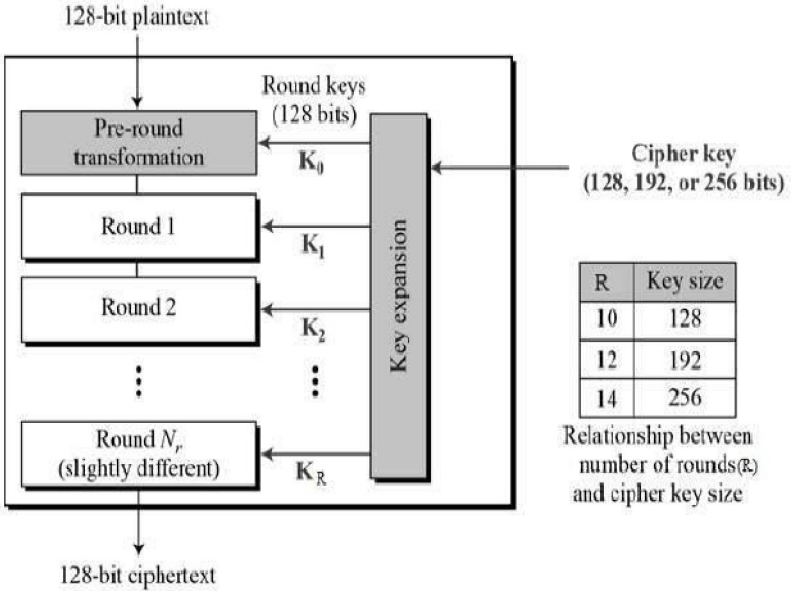
IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 7, May 2023

In our proposed system there are four blocks each having different functionality.
The file is divided into chunks and then every chunk is encrypted using the AES algorithm and a digital signature for the file is generated. A metadata file is created consisting of secret keys and information about file chunks.
On the server, files are stored and a table is maintained to map hash codes with file names.
A different server is maintained as a trusted center for the distribution of the public key.
Lastly, there is a block for downloading the file. The file downloaded is decrypted then it's digital signature is verified before showing the file to the user.

V. LEARNING METHODOLOGY:

AES Algorithm:

The Advanced Encryption Standard (AES) also known as 'Rijndael' is a symmetric-key block cipher algorithm having three fixed 128-bit block ciphers with cryptographic key sizes of 128, 192 and 256 bits respectively.
The AES algorithm has maximum block size of 256 bits whereas Key size is unlimited. The AES design is based on a substitution-permutation network (SPN) and does not use the Data Encryption Standard (DES) Feistel network, thus making it stronger and faster than Triple-DES.
Step-wise description of the algorithm:
Key Expansions:
Round keys are derived from the cipher key using AES key schedule, it also requires a separate 128-bit round key block for each round plus one more.
Initial Round:
Add Round Key - using bitwise xor each byte of the state is combined with a block of the round key.
Rounds:
(a) Sub Bytes - according to a lookup table each byte is replaced with another in a non-linear substitution step.
(b) Shift Rows - a transposition step where the last 3 rows of the state are shifted cyclically a certain number of steps.
(c) Mix Columns - a mixing operation which operates on the columns of the state, combining the 4 bytes in each column.
(d) Add Round Key
Final Round (no Mix Columns).
(a) Sub Bytes
(b) Shift Rows
(c) Add Round Key



R	Key size
10	128
12	192
14	256

Relationship between number of rounds(R) and cipher key size

Fig.: - Working of AES algorithm

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 7, May 2023

Rivest Cipher 6 (RC6)

RC6 is a symmetric key block cipher. RC6 (Rivest Cipher 6) is an enhanced version of the old RC5 algorithm. RC6 – w/r/b means that four w-bit-word plaintexts are encrypted with r-rounds by b-bytes keys. It is a proprietary algorithm patented by RSA Security.

RC6 operators as a unit of a w-bit word using five basic operations such as an addition, a subtraction, a bit-wise exclusive-or, a multiplication, and a data-dependent shifting. The RC6 algorithm has a block size of 128 bits and also works with key sizes of 128-bit, 192-bit, and 256 bits and up to 2040 bits. The New features of RC6 include the use of four working registers instead of two and the inclusion of integer multiplication as an additional primitive operation. The use of multiplication significantly increases the diffusion per round, which allow more security, fewer laps and greater performance. Furthermore, like RC5, it can also support various word-lengths, key sizes and number of rounds. RC6 algorithm is very similar in structure to the RC5 algorithm. In fact, RC6 could be considered as two parallel RC5 encryption processes, although RC6 uses an additional multiplication operation that is not used in RC5 algorithm to make the rotation of each bit in a word dependent, not just the least significant bits.

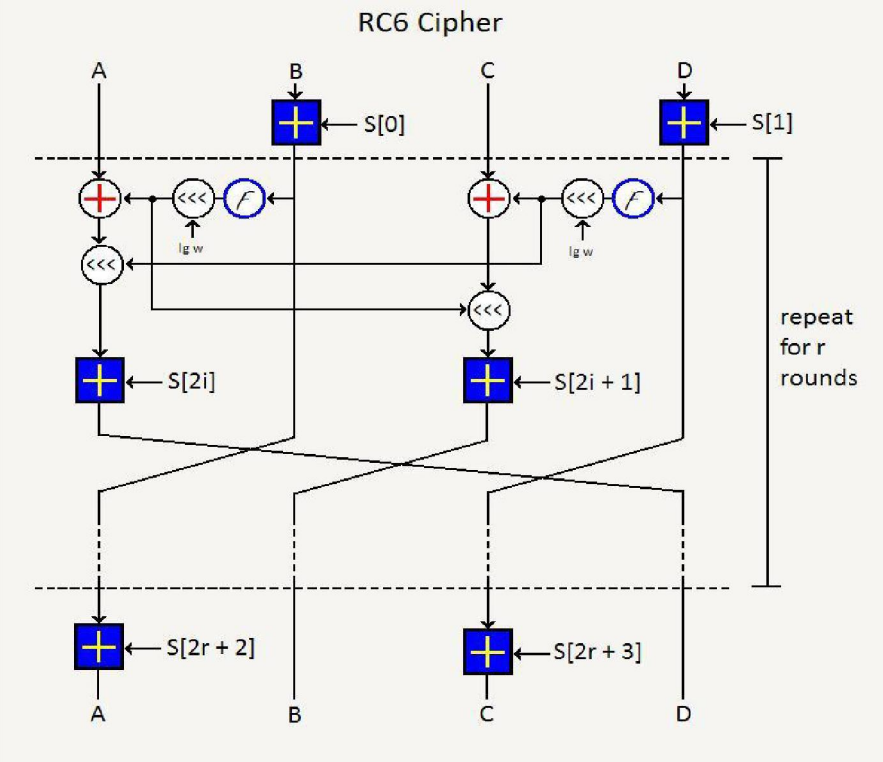


Fig:- Working of RC6 Algorithm

Blowfish Algorithm

Blowfish is a symmetric block encryption algorithm designed which is fast, compact, simple and secure to use as:

It encrypts data on large 32-bit microprocessors at a rate of 26 clock cycles per byte and can run in less than 5K of memory. It uses addition, XOR, lookup table with 32-bit operands. Also the key length is variable, it can be in the range of 32-448 bits: default 128 bits key length. It is suitable for applications where the key does not change often, like communication link or an automatic file encryptor. It is unpatented and royalty-free.

Description of Algorithm:

Blowfish symmetric block cipher algorithm encrypts block data of 64-bits at a time. It will follow the 16 rounds Feistel network and this algorithm is divided into two parts.

1. Key-expansion
2. Data Encryption

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 7, May 2023

Key-expansion:

It will convert a key into several sub key arrays totalling 4168 bytes consisting at most 448 bits. Blowfish uses five subkey-arrays:

One 18-entry P-array consisting of 32-bit sub keys:

P1,P2,. . . . . .,P18 and four 256-entry S-boxes of 32-bit each:

S1,0, S1,1,. S1,255

S2,0, S2,1,. S2,255

S3,0, S3,1,. S3,255

S4,0, S4,1,.....S4,255

These keys are generated earlier to any data encryption or decryption.

Data Encryption:

It is having a function to iterate 16 times of network. Each round consists of 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 lookup tables for each round.

Algorithm: Blowfish Encryption

Divide x into two 32-bit halves: xL, xR

For i = 1 to 16:

xL = XL XOR Pi

xR = F(XL) XOR xR

Swap XL and xR

Swap XL and xR (Undo the last swap.)

xR = xR XOR P17

xL = xL XOR P18

Recombine xL and xR

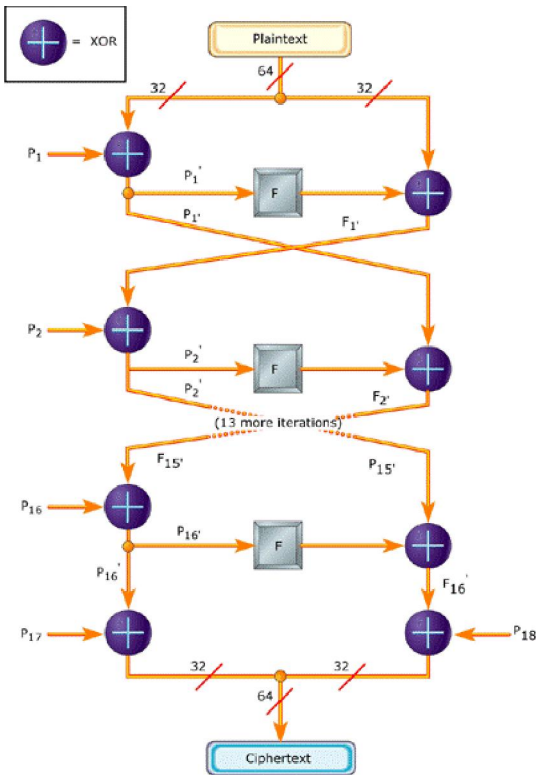


Fig:- Working of Blowfish Algorithm

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 7, May 2023

DATAFLOW DIAGRAM:

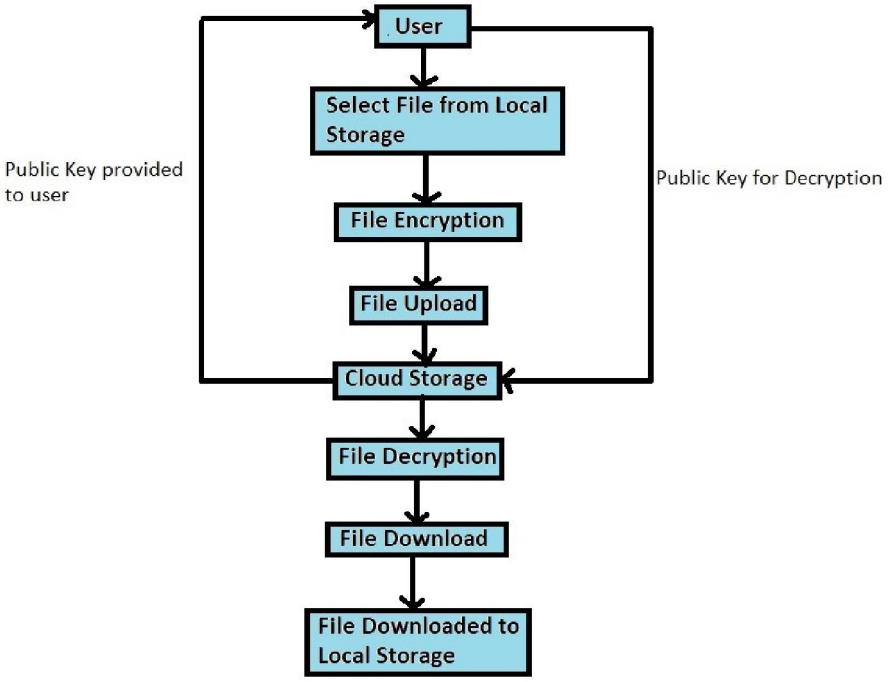
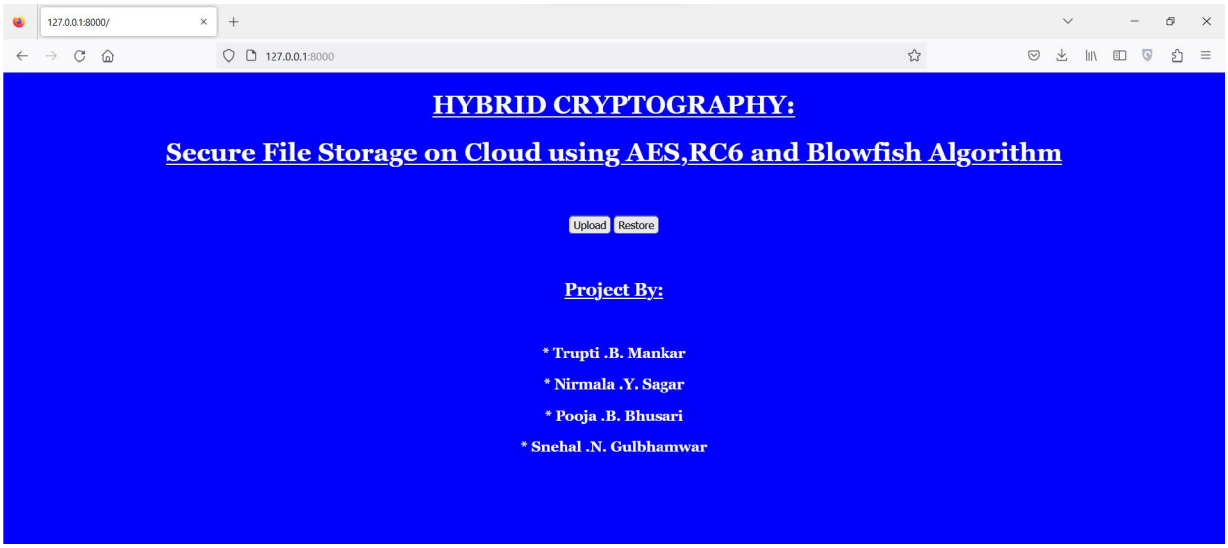
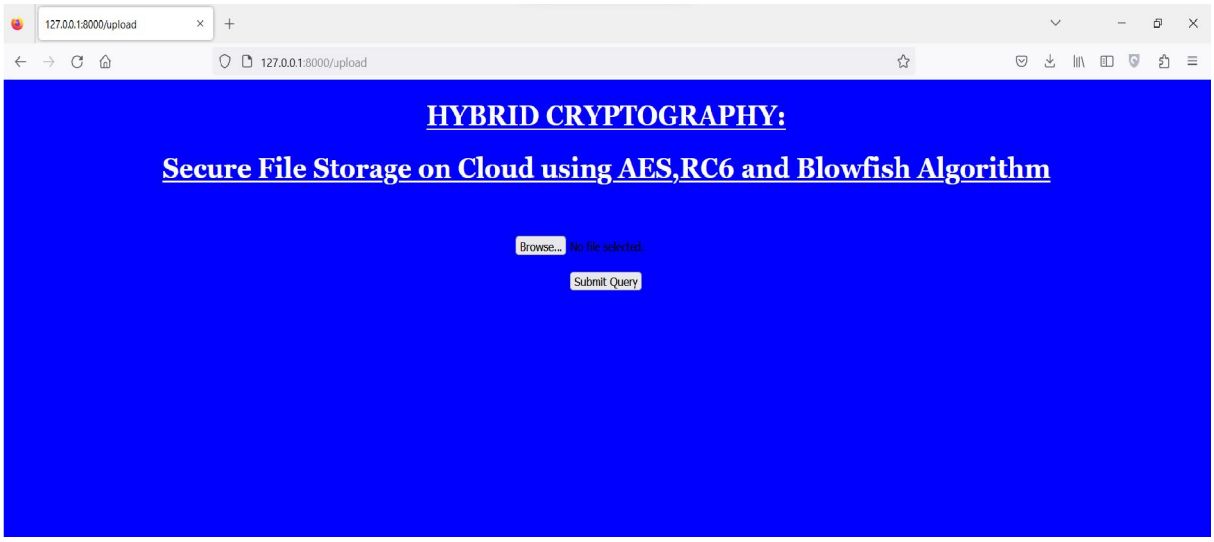


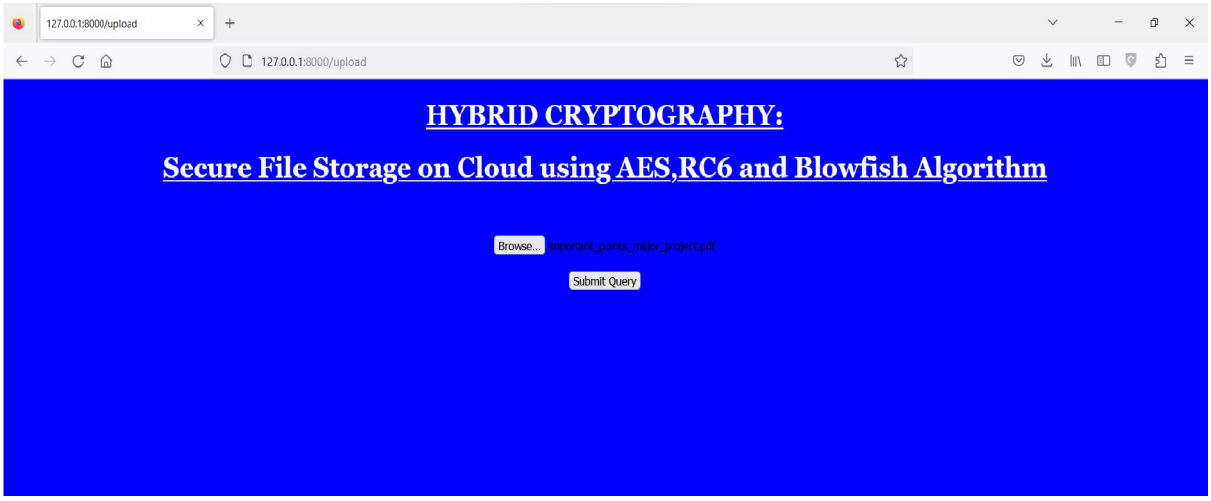
Fig:- Dataflow of the Project

OUTPUTS:

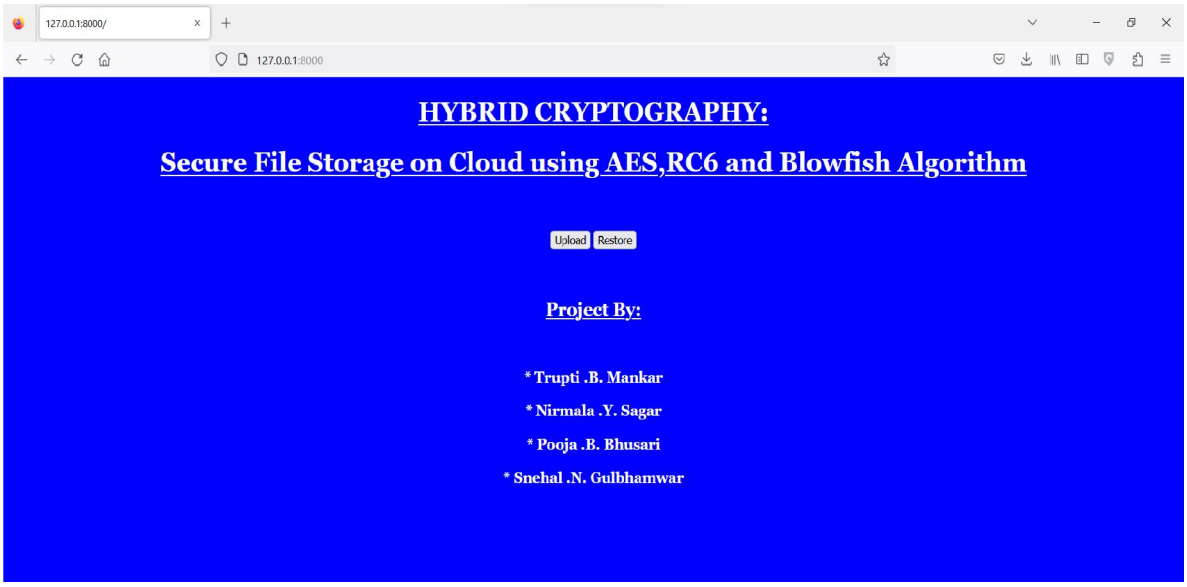


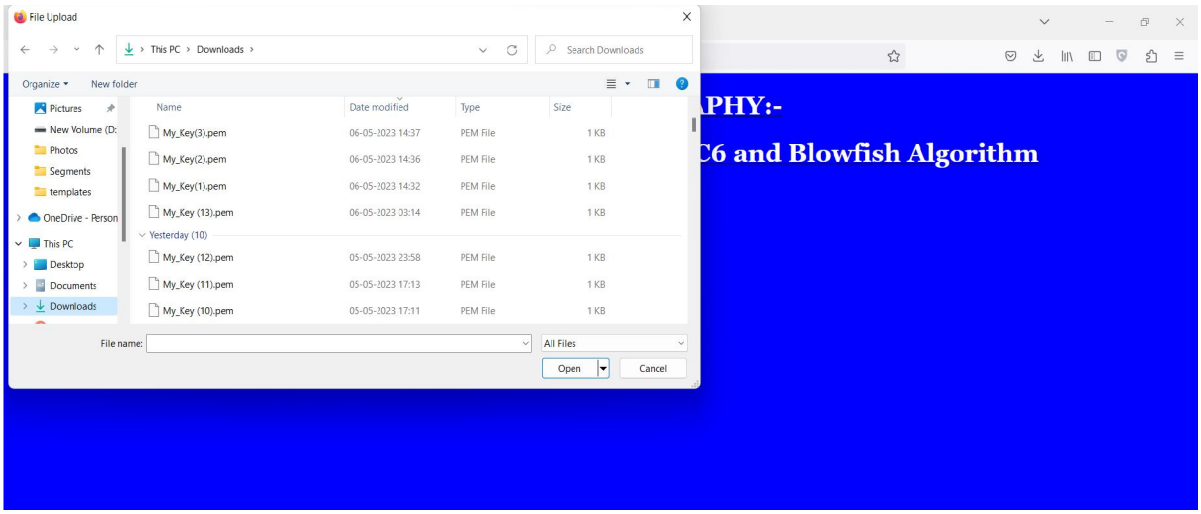
IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 7, May 2023





IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 7, May 2023





IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 7, May 2023

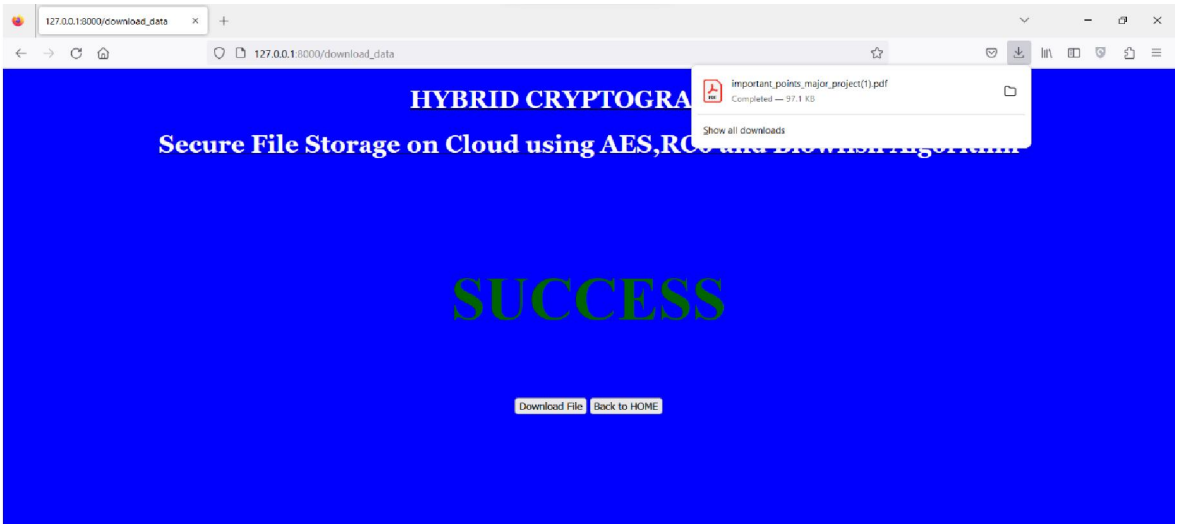


Fig:- Outputs of the Project

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 7, May 2023

VI. CONCLUSION

This project implements a double stage encryption algorithm that provides high security, scalability, confidentiality and the easy accessibility of multimedia content in the cloud. The proposed algorithm is crucial in the second stage, the randomly generated key provides more security than the conventional encryption system. The ciphertext is stored in the cloud instead of original multimedia content. The cipher text is undoubtedly hard to recover the original content for random asymmetric key. Wide application of the proposed algorithm protects the information from the side channel attacker to grab the multimedia data from the cloud. Thus, the multimedia content is safe in the cloud.

REFERENCES

[1] A. K. Shahade, V.S. Mahalle, "Enhancing the Data Security in Cloud by Implementing Hybrid (Rsa&Aes) Encryption Algorithm", IEEE, INPAC, pp 146-149, Oct .2014.
[2] Palash Uddin, Abu Marjan, "Developing Efficient Solution to Information Hiding through text steganography along with cryptography", IEEE, IFOST, pages 14-17, October 2014.
[3] R. T. Patil and P. S. Bhendwade , "Steganographic Secure Data Communication",IEEE, International Conference on Communication and Signal Processing, pages 953-956,April 2014.
[4] Klaus Hofmann and S. Hesham, "High Throughput Architecture for the Advanced Encryption Standard Algorithm" IEEE, International Symposium on Design and Diagnostics of Electronic Circuits & Systems, pages 167- 170, April 2014.
[5]Kumar, A., Lee, B. G., Lee, H., & Kumari, A. (2012). Secure storage and access of data in cloud computing. 2012 International Conference on ICT Convergence (ICTC).
[6] Rewagad, P., & Pawar, Y. (2013). Use of Digital Signature with Diffie Hellman Key Exchange and AES Encryption Algorithm to Enhance Data Security in Cloud Computing. 2013 International Conference on Communication Systems and Network Technologies.
[7] Ping, Z. L., Liang, S. Q., & Liang, L. X. (2011). RSA Encryption and Digital Signature. 2011 International Conference on Computational and Information Sciences.
[8] Sunita Sharma,AmitChugh:'Suvey Paper on Cloud Storage Security'.
[9] Rawal, B. S., & Vivek, S. S. (2017). Secure Cloud Storage and File Sharing. 2017 IEEE International Conference on Smart Cloud (SmartCloud).
[10] Maitri, P. V., & Verma, A. (2016). Secure file storage in cloud computing using a hybrid cryptography algorithm. 2016 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET), 1635–1638. https://doi.org/10.1109/wispnet.2016.7566416
[11]. Shaikh, S., & Vora, D. (2016). Secure cloud auditing over encrypted data. 2016 International Conference on Communication and Electronics Systems (ICCES). doi:10.1109/cesys.2016.7889842
[12]. Gajendra, B. P., Singh, V. K., & Sujeet, M. (2016). Achieving cloud security using third party auditor, MD5, and identity-based encryption. 2016 International Conference on Computing, Communication, and Automation (ICCCA), 1304–1309. https://doi.org/10.1109/ccaa.2016.7813920
[13]. Bhandari, A., Gupta, A., & Das, D. (2016). Secure algorithm for cloud computing and its applications. 2016 6th International Conference - Cloud System and Big Data Engineering (Confluence), 188–192. https://doi.org/10.1109/confluence.2016.7508111
[14]. Taha, A. A., Elminaam, D. S. A., &Hosny, K. M. (2018). AN IMPROVED SECURITY SCHEMA FOR MOBILE CLOUD COMPUTING USING HYBRID CRYPTOGRAPHIC ALGORITHMS. Far East Journal of Electronics and Communications, 18(4), 521–546. https://doi.org/10.17654/ec018040521
[15]. Kranthi Kumar K, Devi T,(2018). Secured Data Transmission in Cloud Using Hybrid Cryptography. International Journal of Pure and Applied Mathematics, 119(16), 3257-3262.
[16]. Shimbre, N., & Deshpande, P. (2015). Enhancing Distributed Data Storage Security for Cloud Computing Using TPA and AES Algorithm. 2015 International Conference on Computing Communication Control and Automation. doi:10.1109/iccubea.2015.16

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 7, May 2023

[17]. Ronak Karani ,TejasChoudhari , Anindita Bhajan , Madhu Nashipudimath 2020). Secure File Storage Using Hybrid Cryptography.2020 INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN TECHNOLOGY, 6(9).
[18]. Shakeeba S. Khan, Prof.R.R. Tuteja, "Security in Cloud Computing using Cryptographic Algorithms", 2015
[19]. Anjali Patil, Nimisha Patel, Dr. Hiren Patel "Secure data sharing using cryptography in cloudenvironment", 2016
[20]. Fortine Mata, Michael Kimwele, George Okeyo, "Enhanced Secure Data Storage in Cloud Computing Using Hybrid Cryptographic Techniques (AES and Blowfish