Mathematical Statistician and Engineering Applications
ISSN: 2094-0343
2326-9865

Hybrid Cryptographic solution using RSA, Blowfish and MD5 for Information Security in Cloud Computing

Anjana[1], Dr. Ajit Singh[2]
saroha.anjana@gmail.com, ghanghas_ajit@rediffmail.com
Department of CSE & IT, Bhagat Phool Singh Mahila Vishwavidyalaya, Khanpur Kalan, Sonipat, Haryana, India

Article Info
Page Number: 1250-1268
Publication Issue:
Vol. 71 No. 3s (2022)

Article History
Article Received: 22 April 2022
Revised: 10 May 2022
Accepted: 15 June 2022
Publication: 19 July 2022

Abstract:
Cloud computing is a cutting-edge computing model in which computational resources are made available through the Internet as services. Cloud storage services must come equipped with privacy and security features. And they have become an issue in cloud computing as a result of the data owner's lack of control and reliance on the cloud computing provider. Simultaneously, as cloud services transmit large amounts of data, the likelihood of thieves obtaining data increases. The current approach is being offered to address the challenges associated with delivering a secure cloud storage service. It enables users to securely transport data within a cloud system by using RSA, MD5 and Blowfish encryption techniques. Cloud computing is a well-established, scalable, and profitable technique of providing commercial services. The basic purpose of cloud applications is to provide organisations with flexible access to the computer systems in order to improve their performance. Cloud data security, a performance research to determine how to improve the encryption technology's security, and an assessment of cloud computing and its potential repercussions Data is encrypted with RSA Partial before being transmitted to the cloud server. Following upload, the hash value is determined using the MD5 hashing algorithm. All of these approaches are subjected to the following processes. Encryption/Decryption, Uploading data to the cloud, Hashing.

Keywords: Cloud security, AES, DES, Blowfish, MD5 Hash algorithm.

I. INTRODUCTION

Cloud computing is a term that refers to a technique for gaining remote access to a variety of resources via the internet. Cloud computing services can be purchased on a per-resource and on-demand basis. Cloud computing is an umbrella word for a technology that facilitates the delivery of hosting services via the internet. It is continually evolving, and other large cloud providers, including Amazon, Google, Microsoft, and Yahoo, have emerged. Cloud computing is typically separated into three segments: "Application," "Storage," and "connectivity," with each component providing a distinct service for a distinct purpose to be used in a distinct business.

The rise of cloud computing is being felt by users, who are uploading sensitive and non-sensitive data to the cloud in order to share it or save money. Despite these benefits, cloud computing confronts a number of data security and privacy concerns, which are hindering its growth. Data is outsourced in cloud computing, and users want to protect their data so that it

is only accessible to authorised individuals. It is vital that data owners who use cloud computing make judgments concerning data access restrictions.

Cloud computing is used to give resources, services, and information to those that request them. For instance, cloud customers can assert that they use the services to perform their tasks under a pay-as-you-go approach that shields them from the huge capital investment required to manage their own IT infrastructure. There are no limitations within the cloud that cause users to worry about their privacy or whether their personal information is protected when referring to cloud data. Users abandon cloud computing if they realise that the data is unprotected privacy data, suggesting that cloud computing places a premium on privacy protection.

Certain security concerns may occur as a result of the following: Insecurity caused by a high number of cloud users utilising hardware. The second argument is that physical limits have been introduced by virtual technologies. In other words, when a logic server hosts many virtual servers, the physical bounds of the logic server may be altered, but a virtual server can be associated with multiple logic servers. Customers of cloud services may suffer unfavourable consequences as a result of privacy and security concerns, impeding the growth of cloud-related services. The principal reasons of security and data integrity concerns are as follows:

1. The capacity of the attackers, such as internal and external attackers to attach the cloud.
2. The security risks of the cloud, mainly in places, where relevant considerations of attacks and Countermeasures are made.
3. Increasing and growing risks of cloud security.

Additionally, the cloud's security is impacted by the following issues: a lack of training and knowledge, unauthorized secondary usage, the complexities of regulatory compliance, legal uncertainty, a lack of user control, data security and breach disclosure, compelled disclosure to the government, data location, transfer, and retention, and data accessibility. The cloud server contains a large volume of data and cannot ensure its integrity or consistency.

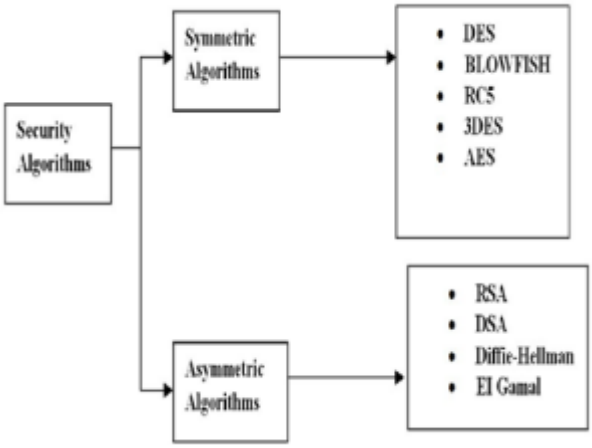


Figure 1. Security Algorithms

1.1 Security Methods for Cloud Computing:

The operational challenge in providing cloud services to customers is ensuring user authentication is secure and private. Users who supply sensitive information, such as bank details or medical records, expect privacy. Privacy is achieved by concealing the user's identity and enabling identification through a range of techniques, including cryptographic tools, anonymous authentication methods, zero-knowledge protocols, and group signatures.

1.1.1 Encryption-based Methods: A more straightforward and successful technique of maintaining the privacy of user data is based on the concept of data encryption prior to it being outsourced to the cloud, as Amazon's IS service does. While data encryption is a useful instrument for safeguarding data privacy, Standard encryption techniques either fail to encrypt the data or contain trapdoors that generate several copies of the cypher texts matching the data in the Cloud system, resulting in the data in the Cloud system being compromised. The number of Cloud users has a direct relationship with the number of copies that are generated. A lack of a sufficient balance between privacy and utility exists despite the fact that numerous methods of protecting one's private are available. When transmitting sensitive data to the cloud, one of the most effective methods of ensuring privacy is to encrypt it first, after which it may be recovered using a keyword-based search of the encoded data. While privacy protection systems based on encryption provide resistance to unauthorised access, they dramatically increase computing overhead. When data owners use mobile devices and large data files, the processing overhead is borne by them.

While data encryption in conjunction with fine-grained data access control is the ideal solution for cloud privacy protection, cryptographic data processing techniques such as homomorphic encryption and fine-grained cloud data access do not provide the same issues as large-scale operations. Significant overhead associated with data querying, publishing, and other related data operations is one of the downsides of huge data activities. For instance, homomorphic encryption looks to be prohibitively expensive when utilised to process massive amounts of data. The bulk of outsourcing plans include secret-sharing procedures, which result in considerable data flow between cloud shareholders during calculations involving enormous volumes of data, imposing the scaling challenge.

1.1.2 Decryption: When the user attributes and related access policy match, decryption is enabled. Along with the use of ABE in the design of secure access control, it is vital to protect user privacy when it comes to access control system. The aforementioned challenges is handled by anonymous ABE and its extensions. In anonymous ciphertext policy attribute-based encryption, decryption proceeds as follows:

- Putting the private attribute key on display for the user's perusal.
- Examine whether the attribute key satisfies the requirements of the access policy. If the attributes associated with the encryption keys satisfy the limitations of the ciphertext's connection policy, the message can be decrypted by the recipient. In other case, the user can only guess the access policy that was used by the data owner

II. LITERATURE REVIEW:

When it comes to cloud computing, it is a resource sharing platform that delivers high-quality cloud applications and services through the Internet. In terms of data storage and access,

cloud computing offers various advantages over traditional methods. Concerns about data privacy are becoming increasingly prevalent, which is limiting the growth of cloud computing. Although cloud computing's success is dependent on security and privacy, these factors also pose a plethora of complex issues. Numerous strategies are discussed for safeguarding data privacy in cloud computing.

Table 1. Compartive study of Cloud computing Security

Author's Name	Title/St	Method	Limitation	Advantages
Priyanka Ora (2018)	Blowfish and RSA Algorithms Secured Cryptosystem for Data in Public Cloud	RSA and Blowfish	Failure of AES	Data encryption is performed using Blowfish, and key encoding is performed using RSA.
Ronald S. Cordova (2017)	Effectiveness of Various Encryption Methods in Cloud Computing: A Comparative Analysis	RSA, AES and Blowfish	least processing time of Blowfish	RAM significantly aided in the acceleration and efficiency of the all algorithms examined.
Gaurav Jain (2017)	Using a variety of cryptographic techniques to improve security in cloud computing	RSA, AES and DES Encryption	Failure in MD5 and blowfish	High-level cloud security is achieved by the use of several approaches such as AES, RSA and DES.
Santosh Kumar Singh (2016)	Cloud Computing Data Security Using the RSA Algorithm	RSA	N/A	In Cloud Computing, the RSA algorithm is used to secure data.
Ammar Zahary (2016)	Blowfish, AES, and RSA: A Comparison of Cryptographic	Blowfish, AES	Need to improve the algorithms properties, encourage of	The symmetric Blowfish algorithm is faster than AES and RSA

	Algorithms		choosing the best algorithm especially for critical application, and perform another study that enhanced on methods that increase the security level of the application.	algorithms.
Mr.KATENDE Nicholas (2017)	Using the MD5 Cryptographic Hash functions and the Rsa Encryption Standard to Improve Cloud Computing Trust	RSA and MD5	No comparavtive analysis	When it concerns to cloud security challenges, a security testing of cloud providers is an important part of the process.
Shivlal Mewada (2016)	Performance Analysis of Encryption Algorithm in Cloud Computing	AES, DES, Blowfish and RSA	Taking of less techniques	Good buffer size of algorithms

1. PROPOSED ALGORITHM

3.1 BLOWFISH: This undertaking began in 1993. It is one of the most widely utilised open-source algorithms by Bruce Schneier. Blowfish is a 64-bit block cypher with a key length that is changeable. No known assault has been successful against this. The advantage of the Blowfish algorithm over rival methods in terms of information processing has been established in numerous experiments and research reviews. In terms of performance and power consumption, Blowfish surpasses other algorithms.

3.2 DES: This was created in 1998 as a replacement for DES. This standard's encryption technique is equivalent to that used in the previous DES, but this has been increased three times to increase encryption strength. 3DES, but at the other extreme, is notorious for being much quicker than other block data encryption. A key size of 192 bits is used in conjunction with a block size of 64 bits, which is an improvement over the previous version of DES. In terms of power consumption and throughput, 3DES performs worse than DES. 3DES

Because of its triple phase encryption properties, it always takes longer to decrypt than DES to decrypt.

3.3 AES: The National Institute of Standards and Technology has proposed the Advanced Encryption Standard (AES) as a substitute for DES. The brute-force assault, in which the hackers try every possible and using in an effort to decrypt the data, is the only known feasible attack against it. Both AES and DES are block cyphers. It can handle keys of 128, 192, or 256 bits in length, with 256 being the standard. Depending on the size of the key, it encrypted 128-bit blocks of data in ten, twelve, or fourteen rounds. AES encryption is rapid and flexible, and it's appropriate for a wide range of systems, but it's especially well-suited to small devices. Additionally, AES has been subjected to extensive testing across a range of security applications.

3.3 RSA: Leonard Adleman and Adi Shamir are the names of the three men that invented the RSA algorithm. Based on the property of positive integers, it can be used to solve many problems. It is modular exponentials that are used to create the RSA encryption and decryption techniques. When it concerns to encryption, there are a few things to keep in mind. For its functioning, RSA is a general populace technique, which indicates it utilises both a secret key. Everyone has access to the public key, which is then used to symmetric encryption and is visible to everyone. Only each private key can decode communications called the public key so because public key cannot decode communication protected with the private key.

3.4 RSA Algorithm:

a) p & q are two prime numbers chosen at random.

b) Solve n = p*q.

c) Solve $\Phi(n) = (p-1)*(q-1)$.

d) Choosing the encrypted message e at random, where $1<e<\Phi(n)$ and $gcd(e, \Phi(n)) = 1$.

e) Solve $d = e^{-1} \bmod \Phi(n)$, To find the decryption key.

f) Public encryption key: KU={e,n}.

g) Private decryption key: KR = {d,n}.

Encryption and Decryption:

a) Compute $C = M^e \bmod n$, where $0 < M < n$.

b) Compute $M = C^d \bmod n$, decryption.

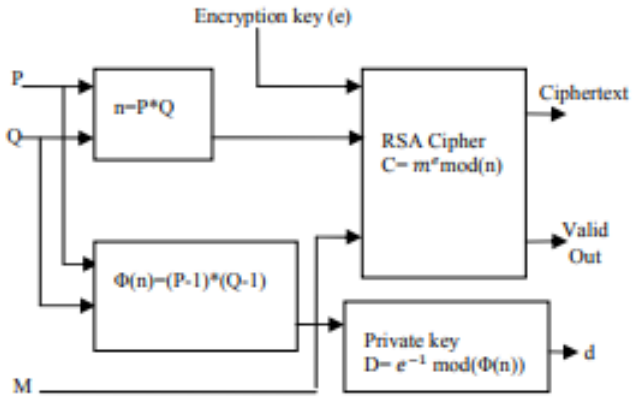


Figure 2 Block diagram of RSA algorithm

RSA uses 2 variables, e & d, with e indicating public information and d indicating private data. Proceed to encryption using M as the plaintext & C as the cypher text.

$C = M^e \bmod n$

And then there's the decryption side.

$M = C^d \bmod n$.

Where n is a huge number generated during the key creation process.

3.5 MD5 (Message Digest 5)

Ron Rivest was the one who came up with the MD5 message digest algorithm. MD5 is a quick algorithm for producing 128-bit message digests that is used in many applications. Following some preliminary processing, the incoming text is separated into 512-bit block. Four 32-bit blocks are generated, which are combined to make the 128-bit message digest by using this method. Padding and length extending, splitting the inputs into circuit diagram, instantiating chain based parameters, and processing blocks are only a few of the subcategories.

MD5 operations

- The parameters b, c, and d are first subjected to the process P. Each one of the 4 matches follows a different approach.
- The value of variable an is added to the procedure P output (i.e. to the register abcd)
- The memo sub-block M[i] is connected to the output of step2 to complete the message (i.e. to the register abcd).
- Step 3's output is multiplied by t[k], which is a constant (i.e. to the register abcd).
- The entries of register abcd (the result of step 4) are circular-left relocated by s bits, yielding the following result: (The level of significance is always changing.)
- b is a variable that appears in the step 5 output (i.e. to the register abcd).
- Step 6's output is the new abcd for the next step.

Figure 3 depicts the technique for performing a single MD5 operation, which includes all of the preceding phases. Because it comprises the processes P, the parameters a, b, c, and d, the communication sub-block M[i], and the constants t[k], it is essential for the MD5 algorithm to work.

3.6 Hash Algorithm:

The National Institute of Standards and Technology issued the Secure Hash Algorithms (SHA-1) as a federal information processing standard in 1993. FIPS 180-1, also known as SHA-1, was formed in 1995, and an improved version of the regulations was published as a result. There is a standard paper called the Secure Hash Standard, and it may be found on the Internet for free.. SHA is a hash algorithm that is based on the MD4 algorithm and has an architecture that is quite similar to the MD4 method. RFC 3174 also specifies SHA-1, which is a hash algorithm that essentially duplicates the data in FIPS 180-1 but provides a C implementation of the approach.

HA Algorithm Steps:

Step 1: Add the padding bits at the end:

The message has been padding to a length of 896 modulo 1024 [length 896(mod 1024)] in order to prevent it from becoming too long. Padding is always appended of the message, even if it is the correct length. As a result, the padding bit count ranges from one to ten thousand twenty-four. A single 1 bit is followed by the requisite amount of 0 bits to represent padding.

Step 2: Add the padding length at the end:

A 128-bit data block is linked with the message. This block includes the time of the original comment and is read as an undetermined 128-bit integer.

Step 3: Initialize the hash buffer:

The hash function's intermediate and final results are saved in a 512-bit internal buffer. Up to eight 64-bit values can be used to specify the buffer's size (a, b, c, d, e, f, g, h).

Step 4: Process blocks:

A module of 80 rounds is at the heart of the algorithm.

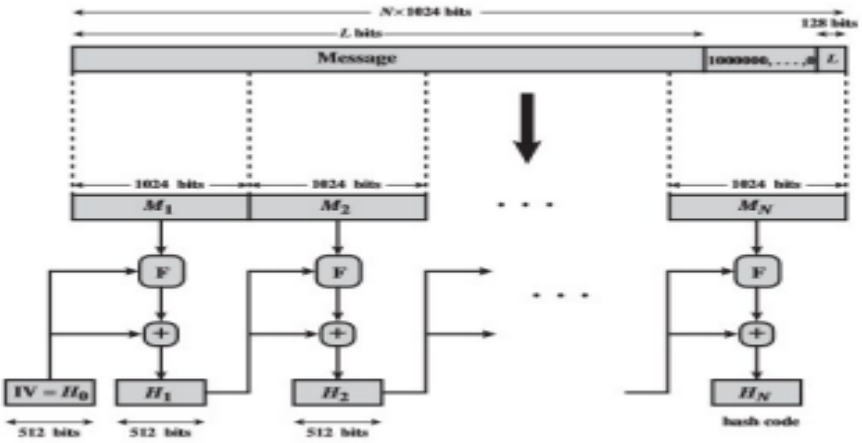


Figure 3. HA producing Message Digest

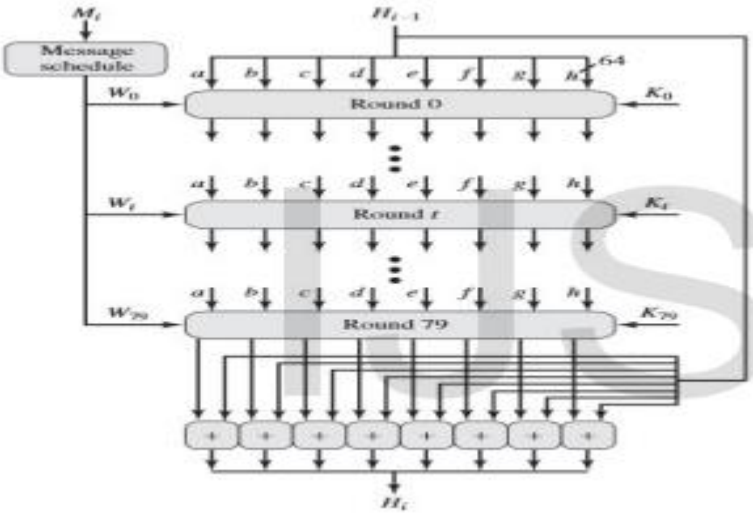


Figure 4. Single-Block Processing

Step 5: Output:

The 512-bits message digest is the result of the Nth step, even after N 1024-bits blocks have been processed.

3.6 Blowfish algorithm: This design has been around since 1993. Bruce Schneier uses it as a public algorithm on a regular basis. Blowfish is a 64-bit encryption algorithm with a 64-bit key length. There is no known successful attack against this. Numerous trials and research investigations established the Blowfish algorithm's processing speed advantage over rival algorithms. In terms of throughput and energy consumption, Blowfish surpasses other algorithms.

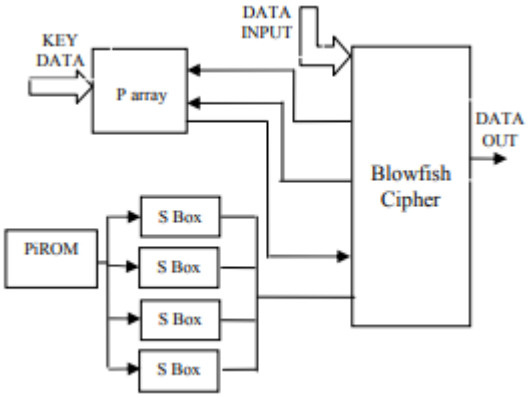


Figure 5: Blowfish Algorithm Block Diagram

Data Encryption

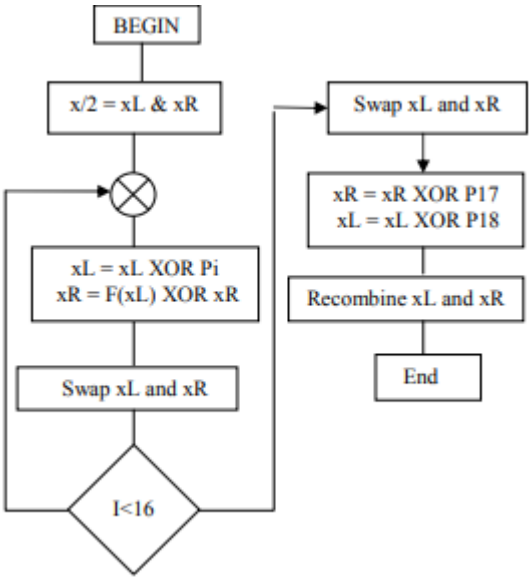


Figure 6. Flowchart of Blowfish Data Encryption

Table 2 Existing Algorithms

S.No	Algorithm	Drawbacks	Advantages
1	AES	It employs an overly simplistic algebraic structure. Each block is always encrypted	With a key sizes of 128, 192, and 256, this algorithm uses 128-bit blocks. AES is capable of providing significantly more security than

		identically. Software implementation is difficult. Because of the trade-off among performance and security, In software, AES in asymmetric cryptography is difficult to implement.	other algorithms. It is the most secure security technique accessible because it is incorporated including both software and hardware.
2	DES	If a message is encrypted with a certain key and is taken, the encryption of that message and key will be identical to that of the compliment message and key.	Encryption and decryption are done using the same algorithm, resulting in a single file. All it required is to invert the function and to hold the keys in the opposite manner. In term of software and hardware, this is a huge advantage.
3	BLOWFISH	Birthday Attacks, which are possible due to the small block size of Blowfish, can compromise the encryption technology.	It is not patented and is freely available for use. This means that anyone may take and use Blowfish for any purpose. Additionally, the Blowfish algorithm requires fewer operations to finish than other encryption techniques.
4	MD5	MD5 is relatively sluggish when compared to other algorithms such as the SHA algorithm. Using MD5, For two different inputs, a same hash function can be created. MD5 is less secure	Comparing and storing smaller hashes using MD5 Algorithms is much easier than storing a large variable-length text. Using MD5, a message digest can be readily constructed from the original message.

		than SHA because it is more susceptible to collision attacks.	
5	RSA	It may fail on occasion because complete encryption necessitates both symmetric and asymmetric encryption, whereas RSA only employs symmetric encryption. The data transfer rate is slow due to the large number of participants. On occasion, a third party may be necessary to validate the dependability of public keys.	The RSA algorithm is extremely safe and secure when it comes to transmitting secret data. Because of the complex mathematics involved, cracking the RSA technique is extremely difficult.. It's simple to distribute public keys to users.

4. HYBRID OF PROPOSED ALGORITHMS :

4.1 Blowfish and RSA Encryption Algorithm

The authors propose a hybrid Blowfish/RSA technique for cloud computing that makes use of FPGAs. Cloud computing on FPGAs is a viable choice due to its speed, compact size, low cost, and ease of implementation.

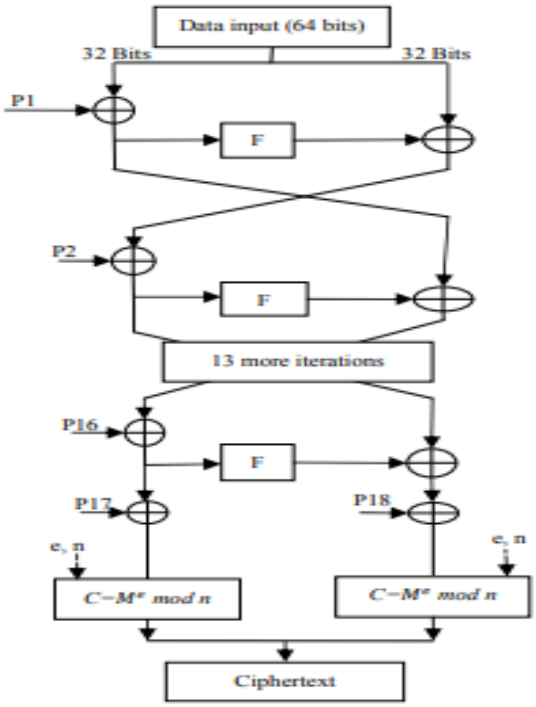


Figure 7. Network encryption based on RSA and Blowfish hybrids

The previously demonstrated hybrid technique incorporates the advantages of both symmetric and asymmetric procedures in a single operation. As a result, our recommended strategy maximises the benefits of both techniques to the greatest extent possible. Simplistic and easy to implement, the symmetric approach provides a solution that is fast, safe, memory efficient, and simple to apply. The terms "asymmetric cryptography" and "public key cryptography" are frequently used interchangeably when referring to encryption. It is mostly taken into consideration for authentication purposes. Asymmetric approaches encrypt data using a public key, but they can only be decoded by an authenticated user who also has access to the private key, which is used to encrypt the data. The most important factor is that the key size should be large enough to prevent it from being discovered by direct key substitution. As a result, the entire procedure is significantly slowed to a crawl. Since direct replacement is not allowed when Blowfish is employed, this hybrid technique permits asymmetrical techniques to be applied with a small key. Therefore, the overall process advances at a far faster rate than the individual stages. Blowfish also improves in security because decryption requires both RSA and blowfish keys, which increases the overall security of the system. Consequently, the number of blowfish rounds can be decreased to eight or four, resulting in an approach that is significantly faster than earlier strategies in the field.

4.2 Decryption Algorithm that Combines RSA and Blowfish

Except that the P-array has been employed in reverse order, the encryption process technique is identical to the encryption procedure. After the protected required information has been decrypted, RSA encryption is utilised. RSA requires the private key d, which also serves as an authentication key.

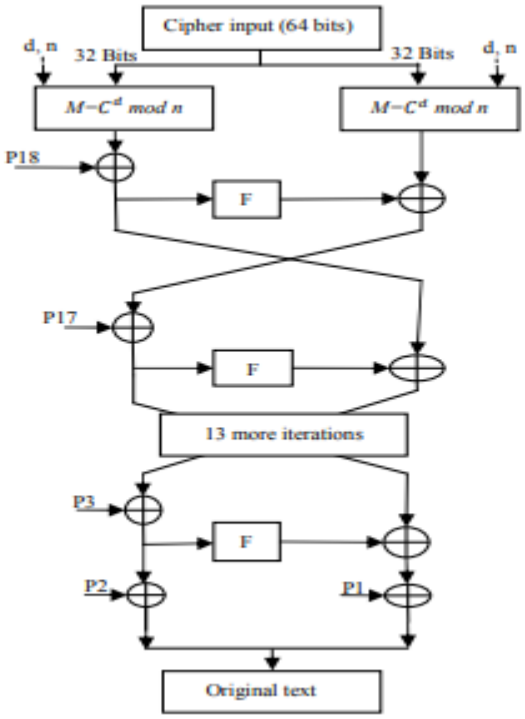
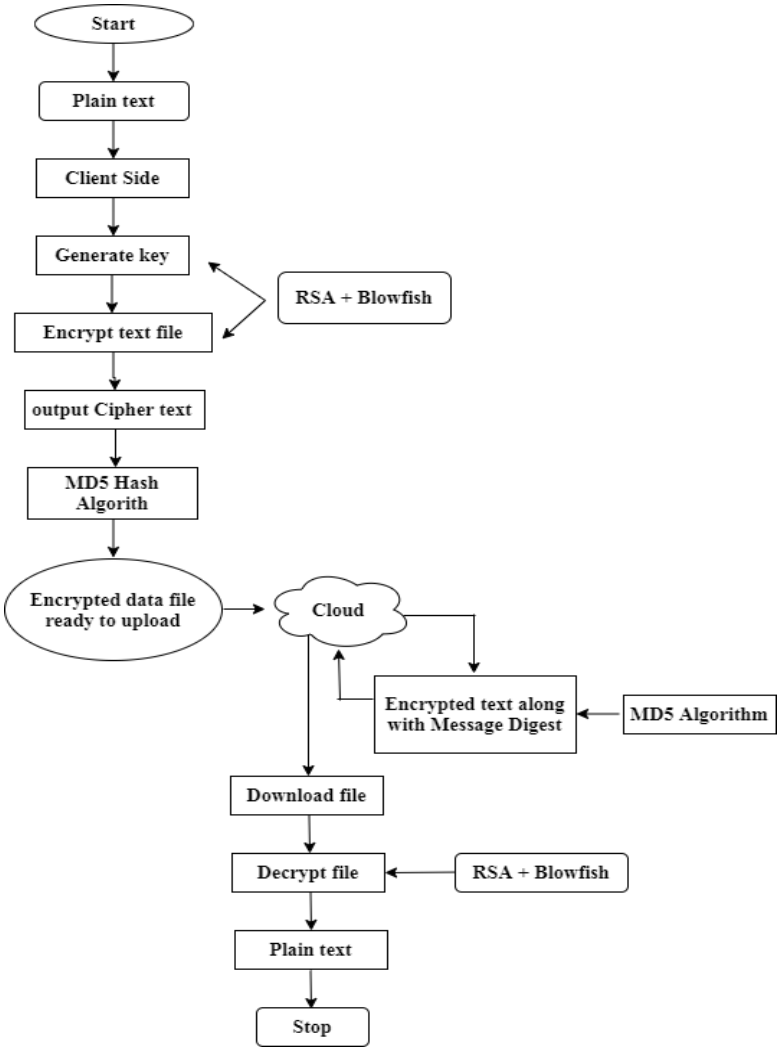


Figure 8. Decryption network based on RSA and Blowfish hybrids

Both decryption and encryption are carried out using the same Feistel network type. Furthermore, this method safeguards against brute force attacks. Due to the fact that this data is encrypted using two unique encryption techniques, it must be decoded using the correct combination of both keys, which is incredibly difficult to perform. Thus, the hybrid strategy proposed here exceeds earlier strategies in terms of security and features. Furthermore, both Blowfish and RSA are energy-efficient algorithms.

5. DESIGN OF ALGORITHM

As part of the Data Encryption Standard, which was published in the Federal Register as FIPS-46 in January 1977, the National Institute of Standards and Technology (NIST) developed a block cypher with a symmetric key. The DES method may convert a 64-bit plain into a 64-bit crypto text by using the same 56-bit encryption key at both the encryption and decryption locations. A 64-bit cypher text can be converted into another 64-bit plaintext using the DES algorithm, which uses the same 56-bit key. permutations (P-boxes) and Feistel rounds are used in total, with the first and last permutations being referred to as the beginning and final permutations. To ensure that each round has its own unique 48-bit round key, a specified mechanism is used to produce the cypher key for each round.



Flow 9 chart of cloud computing

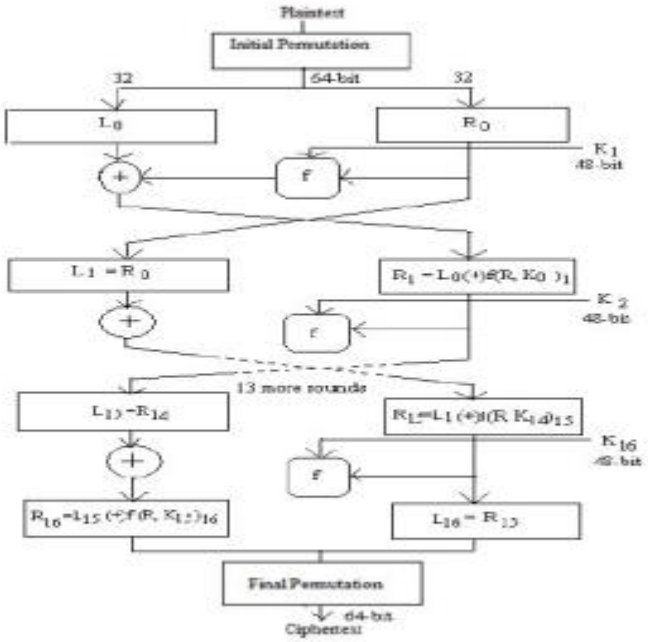


Figure 10 Encryption with DES

DES permutes the entire 64-bit data block at the start of the process. Feistel rounds are performed on the data after it has been partitioned into two 32-bit sub-blocks, L0 and R0, have been created. There are no differences between rounds, therefore increasing the number of rounds has the dual effect of increasing security while simultaneously decreasing the algorithm's temporal efficiency. The output values of the 32 bit L15 and R15 are switched after the sixteenth cycle, resulting in the formation of the so-called pre-output. This concatenation of [R15, L15] values is permuted using the inverse function of the permutation that was used to create it. This final permutation results in the creation of the 64-bit cypher text.

1. IMPLEMENTATION RESULT

The entire model is run on a public cloud. This cloud environment model makes use of the Openshift public cloud. Eclipse Kepler and JDK 1.6 are used for coding. The following are some critical snapshots:

Encryption: This form performs the model's first stage, which is the generation of private and public keys through file decryption and encryption. In this approach, the Data Owner just uploads their file and its public key. On the cloud server, the public key acts as the owner's identification. This form encrypt the files and returns the private key.

- **File Upload:** There are steps to this method. The method begins with the AES algorithm encrypting Clair text. Encrypt the AES key with the RSA-1024 technique in the second stage. The algorithm employs the following function:

Block (F)'s number: The number of blocks in the file F is returned.

ENC AES (B, K): It uses the AES method and the key K to encrypt block B.

Send to cloud (F'): It enables the encrypted file F to be sent to Cloud storage. It enables the encrypted file F to be sent to Cloud storage.

ENC RSA (k): The RSA Algorithm is used to encrypt k.

Save in server (K'): It allows you to save K' on the server.

Algorithm: File Upload

```
1.  Encrypt file (F) {
2.  /* a method for encrypting files and storing them in the cloud */
3.  /* to convert Clair text from file F to Cipher text from file F */
4.   /* Phase 1: Use the AES technique to encrypt Clair's text. */
5.  For B ← 1 to number of block (F) do
6.  {
7.  B=ENC AES (B, K)
8.  }
9.  Convey to cloud (F)
10. /* Phase 2: Encrypt AES Key with RSA algorithm */
11. For k ← 1 to size of (K) do
12. {
13. K= ENC RSA (K)
14. }
15. Save in server (K)
```

16. }

Decryption: This form uses the private key to decrypt the file. This form also requires a list of authenticated users' access permissions.

- **File Download:** Additionally, this approach is divided into two sections. The algorithm begins by using the RSA Algorithm to decrypt the AES key. It then translates the encrypted text using the AES key obtained in the second phase from the server. The following functions are used in the algorithm:

Block (F)'s number: The number of blocks in the file F is returned.
DEC RSA (k'): The RSA Algorithm is used to decrypt k'.
DEC AES (B', K): It uses the AES algorithm using key K to decrypt block B'.

Algorithm: File Download

1. Decrypt file (F) **{**
2. /* decryption algorithm for files downloaded via cloud storage */
3. /* to convert Cipher text contained in file F to Clair text contained in file F */
4. /* Phase 1; AES key decryption using the RSA technique */
5. for K ← 1 to size of (K) do
6. {
7. K= DEC RSA (k)
8.}
9. return (K)
10. /* Phase: 2 AES algorithm is used to decrypt cypher text */
11. for B ← 1 is the number of block (F) do
12. {
13. B= DEC AES (B, K)
14.}
15. return (F)
16. }

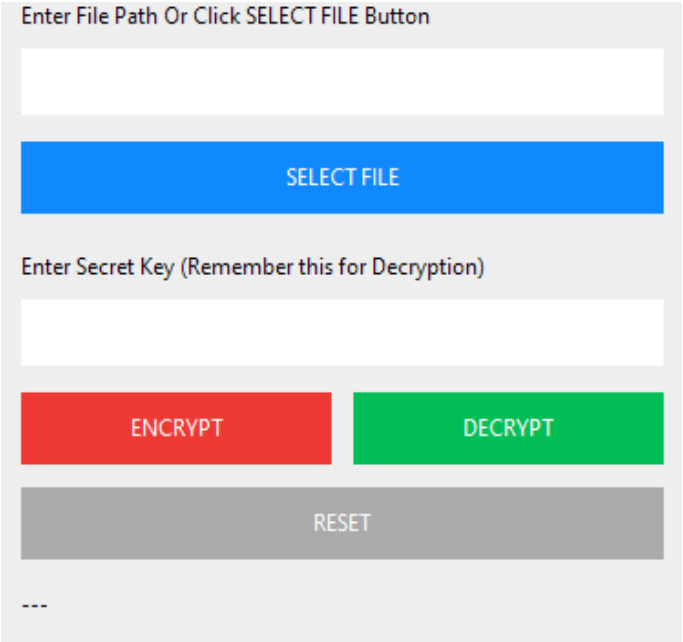


Figure 11. Encrypt and decrypt result

CONCLUSION:

It's worth noting that the majority of systems were designed with one or two types of encryption and hashing, which the cloud user used to determine the integrity of the data. This means that security audits are undertaken on either the cloud consumer's or cloud provider's side. This also indicates that neither cloud user nor cloud provider has committed to reciprocal auditability. And will be used to develop a model that will be capable of tracking the security of both the cloud consumer and the cloud provider through the use of MD5 hashing and the RSA encryption standard. This helps to ensure that the data's security and integrity are maintained at all times because you will be notified if the MD5 hash value changes as a result of updates. Additionally, to safeguard the security and integrity of cloud-based data. This approach employs the RSA partial homomorphic hashing algorithm with the MD5 hashing algorithm. Encryption and decryption are performed using the RSA partial method, while data backup is performed using the MD5 hashing approach. In the future, we will place a premium on adopting the recommended design alongside numerous comparisons to illustrate our method's efficiency. Cloud computing's strength is in its capacity to manage risks, particularly those related to security. We analysed encryption algorithms in this study and decided that when performance is a concern, BLOWFISH, AES, and DES are the best choices. If data security is a concern, AES is a viable option. Furthermore, the AES technique is quite efficient. While cloud storage has a number of advantages, there are a number of legitimate security concerns. If this security vulnerability can be addressed or overcome, cloud storage choices for large and small businesses will become the norm. Additionally, he provided a technique for open cloud data storage. Our algorithm protects your info. The data is accessible only to the authorised user. Even if an unauthorised user (intruder) gains access to the information mistakenly or maliciously, he would be unable to decrypt it because encryption required two separate keys held in two separate locations.

REFERENCES:

1. Fergus O’Sullivan, Top Ten Major Risks Associated with Cloud Storage, 2018.https://www.cloudwards.net/top-tenmajor-risksassociated-with-cloud-storage/.
2. Ch. Vijayalakshmi, L. Lavanya, and Ch. Navya, "A Hybrid Encryption Algorithm Based On AES and RSA", International Journal of Innovative Research in Computer and Communication Engineering, vol. 4, p. 1, 2016.
3. P. Priyadarshini, N. Prashant, D.G. Narayan, and S.M. Meena, "A Comprehensive Evaluation of Cryptographic Algorithms: DES, 3DES, AES, RSA and Blowfish", Procedia Comput. Sci., vol. 78, pp. 617-624, 2016.
4. Pawan Kumar Tiwari, Mukesh Kumar Yadav, R. K. G. A. . (2022). Design Simulation and Review of Solar PV Power Forecasting Using Computing Techniques. International Journal on Recent Technologies in Mechanical and Electrical Engineering, 9(5), 18–27. https://doi.org/10.17762/ijrmee.v9i5.370
5. Laser JS, Jain V. [2016] A Comparative Survey of various Cryptographic Techniques. International Research Journal of Engineering and Technology (IRJET), 3(03):11-17.
6. C. Gary, "An Overview of Cryptography", Embry-Riddle Aeronautical University - Daytona Beach, 2016.

7. Nouby M. Ghazaly, A. H. H. . (2022). A Review of Using Natural Gas in Internal Combustion Engines. International Journal on Recent Technologies in Mechanical and Electrical Engineering, 9(2), 07–12. https://doi.org/10.17762/ijrmee.v9i2.365
8. T. Gaur, "Divya sharma, "A Secure and Efficient Client-Side Encryption Scheme in Cloud Computing", I.J", Wireless and Microwave Technologies, vol. 1, pp. 23-33, 2016.
9. Xiaoqiang ZHANG, Ning WU, Gaizhen YAN, and Liling DONG, "Hardware Implementation of Compact AES S-box," IAENG International Journal of Computer Science, vol. 42, no.2, pp125-131, 2015.
10. K. Ughade and N. Chopde, "Survey on Security Threats and Security Algorithms in Cloud Computing", International Journal of Science and Research (IJSR), vol. 4, no. 4, 2015.
11. Bulla, P. . "Traffic Sign Detection and Recognition Based on Convolutional Neural Network". International Journal on Recent and Innovation Trends in Computing and Communication, vol. 10, no. 4, Apr. 2022, pp. 43-53, doi:10.17762/ijritcc.v10i4.5533.
12. D. Talukdar, "Study on symmetric key encryption: An Overview", International Journal of Applied Research, vol. 1, no. 10, pp. 543- 546, 2015.
13. Arora S. [2015] Enhancing Cryptographic Security using Novel Approach based on Enhanced-RSA and Elamal: Analysis and Comparison. International Journal of Computer Applications, 112(13):12-19.
14. Ananthakrishnan, B., V. . Padmaja, S. . Nayagi, and V. . M. "Deep Neural Network Based Anomaly Detection for Real Time Video Surveillance". International Journal on Recent and Innovation Trends in Computing and Communication, vol. 10, no. 4, Apr. 2022, pp. 54-64, doi:10.17762/ijritcc.v10i4.5534.
15. Manju RD. [2015] Sudesh Kumar. Analysis on Different Parameters of Encryption Algorithms for Information Security International Journal of Advanced Research in Computer Science and Software Engineering, 5(8):104- 108.
16. Dr. Tomislav Nad, "Advances and Trends in Cryptography", SIGS Technology Summit, 2015.
17. JoyMa, Top 10 Security Concerns for Cloud-Based Services, 2015.https://www.incapsula.com/blog/top10-cloud-securityconcerns.html
18. H. KAMAL IDRISSI, A. KARTIT, M. EL MARRAKI «FOREMOST SECURITY APPREHENSIONS IN CLOUD COMPUTING » Journal of Theoretical and Applied Information Technology 31 st January 2014. Vol. 59 No.3.
19. Dr. P. Dinadayalan, S. Jegadeeswari, Dr. D. Gnanambigai, "Data Security Issues in Cloud Environment and Solutions", World Congress on Computing and Communication Technologies 2014.
20. Dr. Mohammad V. Malakooti, Nilofar Mansourzadeh, "A Robust Information Security Model for Cloud Computing Based on the Scrambling Algorithm and Multi-Level Encryption", Proceedings of the International conference on Computing Technology and Information Management, Dubai, UAE, 2014, Islamic Azad University, UAE branch, Dubai, UAE.

A. Soofi, M. Khan and F. Amin, "Encryption Techniques for Cloud Data Confidentiality", International Journal of Grid and Distributed Computing, vol. 7, no. 4, pp. 11-20, 2014

21. K. Goodarzi and A. karimi, "Cloud Computing Security by Integrating Classical Encryption", Procedia Computer Science, vol. 42, pp. 320-326, 2014
22. NAGENDRA, M. et SEKHAR, M. Chandra. Performance Improvement of Advanced Encryption Algorithm using Parallel Imputation. International Journal of Software Engineering and Its Applications, 2014, vol. 8, no 2, p. 287-296.
23. L. Arockiam, S. Monikandan « Data Security and Privacy in Cloud Storage using Hybrid Symmetric Encryption Algorithm » International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 8, August 2013.
24. Gupta, D. J. . (2022). A Study on Various Cloud Computing Technologies, Implementation Process, Categories and Application Use in Organisation. International Journal on Future Revolution in Computer Science &Amp; Communication Engineering, 8(1), 09–12. https://doi.org/10.17762/ijfrcsce.v8i1.2064